UNIVERSIDADE D
COIMBRA

Fernando Jorge da Silva Antunes

METODOLOGIA PARA AVALIAÇÃO DA MATURIDADE DE CIBERSEGURANÇA

EM INFRAESTRUTURAS DE SERVIÇOS CRÍTICOS

Dissertação no âmbito do Mestrado em Segurança Informática, orientada pelo Professor Doutor Paulo Simões e pelo Professor Doutor Tiago Cruz e apresentada à Faculdade de Ciências e Tecnologia / Departamento de Engenharia Informática.

Setembro de 2023

Faculdade de Ciências e Tecnologia
Departamento de Engenharia Informática

Metodologia para Avaliação de Maturidade de CiberSegurança em Infraestruturas de Serviços Críticos

Fernando Jorge da Silva Antunes

Dissertação no âmbito do Mestrado em Segurança Informática, orientada pelo Professor Doutor Paulo Simões e pelo Professor Doutor Tiago Cruz e apresentada à Faculdade de Ciências e Tecnologia / Departamento de Engenharia Informática.

Setembro de 2023

UNIVERSIDADE D
COIMBRA

Esta página foi intencionalmente deixada em branco.

Agradecimentos

Em primeiro lugar, quero expressar os meus agradecimentos aos orientadores Professor Doutor Paulo Simões e Professor Tiago Cruz pelo apoio dado nesta etapa do trabalho e pela flexibilidade que sempre demonstraram em virtude dos contratempos pessoais que foram surgindo e perante os quais estiverem sempre disponíveis e com total disponibilidade para em conjunto conseguirmos uma solução. Agradeço ainda ao Professor Nuno Antunes que foi incansável no seu apoio. Agradeço ainda de forma geral a todo o corpo docente e não docente do DEI, que apesar de não ter contribuindo de forma direta nesta fase do trabalho, foram essenciais ao longo de todo o Mestrado em Segurança Informática nas cadeiras que lecionaram e podendo com isso retirar contributos para o trabalho.

Agradeço a todos os médicos, enfermeiros e auxiliares do Centro Hospital do Médio Tejo e do Centro Hospitalar e Universitário de Coimbra, com quem tive a felicidade de cruzarem a minha vida, e foram sempre um grande incentivo para não desistir apesar do mau do momento que atravessava, tendo eles acreditado mais em mim que eu próprio.

À minha esposa Célia e aos meus filhos Tomás e Sofia que estiveram comigo desde o primeiro dia e mais do que ninguém foram os principais prejudicados, pela falta de tempo em família que foi impactado em função da minha dedicação a este trabalho. O seu apoio foi sem dúvida importante e sem o qual não teria conseguido avançar.

Aos meus colegas de trabalho e empresas onde colaborei que sempre foram flexíveis e apoiaram de forma constante, tendo permitido que dedicasse tempo a este trabalho, disponibilizando materiais que vieram a ser relevantes na forma como fui abordando o tema do trabalho e progredido com o seu desenvolvimento.

Por último, mas não menos importante, agradeço de forma incondicional aos meus pais e sogros que foram eles que permitiram que este trabalho fosse uma realidade, através da forma como me educaram, criaram, preparam e continuam a apoiar-me para a vida. A minha vida, o que sou, é a Deus e a eles que devo e sou muito grato por serem o que são na minha vida.

Esta página foi intencionalmente deixada em branco.

Abstract

The dependence on computational and infrastructure resources allowing for a quick, effective, and permanent response to society's needs has been growing and diversifying over the past years. In fact, the criticality of an infrastructure increases with the number of services and consumers that rely on it, with the associated risks also increasing proportionally, requiring greater visibility and control. This concern has grown over the past two decades, especially when these infrastructures began to leverage the open protocols and the internet as a means to expand their reach and effectiveness, becoming accessible from small devices with internet connections.

The infrastructures that support essential services in various sectors of activity are thus required to be permanently available, moreover given their cross-domain utilization that often transcends national boundaries. This dependence necessarily translates into a concern that extends beyond the scope of the entities and organizations responsible for providing and maintaining these services. From this perspective, the involvement of bodies such as the European Commission has been notable, providing guidance to its member states to protect these infrastructures and creating specific legislation for this purpose, to be transposed for the local/national domains by each member state. In this way, each country is responsible for enforcing laws and monitor their applicability, thus ensuring that citizens are not deprived of these essential services, whose inhibition may impact a large number of people and interdependent services, potentially creating a ripple effect. With the rising tide of cyberattacks against critical infrastructures that the world has witnessed in recent years, as well as conflicts between countries that are themselves providers of essential services (but often have a strong history of involvement in cyberattacks against other nations), the need to enhance security and resilience in critical infrastructures is a mandatory and urgent requirement that must be safeguarded, considering the impact it would have if these infrastructures were compromised.

Throughout this work, we will propose the development of a methodology that can assess the maturity level of critical service infrastructures by validating the effectiveness of key controls associated with specific cybersecurity domains. To achieve this goal, we will consider the most relevant domains for this type of infrastructure, especially those with a lower maturity level and a higher exposure to the risk of compromise, which would have a more significant impact on the normal functioning of the entire infrastructure.

Keywords:

Infrastructures, Critical Services, Cybersecurity, Maturity Assessment

Resumo

A dependência computacional e de infraestruturas que permitam responder de forma rápida, efetiva e permanente às necessidades da sociedade, têm vindo a crescer e a diversificar-se ao longo dos últimos anos. Estas infraestruturas suportam serviços que são utilizados nos mais variados sectores de atividade, obrigando-os a uma disponibilidade permanente, face à sua utilização transversal que muitas vezes trespassam a fronteira de cada país. Esta dependência traduz-se numa preocupação que transpõe as entidades e organizações responsáveis por disponibilizarem e manterem estes serviços. Têm sido notório o envolvimento de organismos como a Comissão Europeia, que estando atenta e visando dar orientações aos seus estados-membros para proteger estas infraestruturas, criou legislação especifica para o efeito, obrigando a cada estado-membro transponha e aplique esta legislação mediante a sua realidade. Desta forma, cada país fica responsável por fazer aplicar as leis e supervisionar a sua aplicabilidade, garantido assim que os seus cidadãos não ficam privados destes serviços. A sua inibição impactará um elevado número de pessoas e serviços que dependem diretamente deles, podendo rapidamente criar um efeito de contágio. A criticidade de uma infraestrutura aumenta devido ao número de serviços e consumidores que deles dependem, aumentam os riscos que lhes estão associados na mesma proporção, requerendo uma maior visibilidade e controlo. Esta preocupação aumentou nas últimas duas décadas, em que o acesso à internet foi massificado, essencialmente quando estas infraestruturas começaram elas próprias a tirar partido da internet como meio de aumentar a sua abrangência e eficácia, ficando acessíveis a partir de um pequeno dispositivo com ligação à internet.

Com o cenário de ciberataques sobre infraestruturas críticas que o mundo tem assistido nos últimos anos, assim como o conflito em vários entre países que são eles próprios fornecedores de serviços essenciais, mas com forte historial de envolvimento em ciberataques a outros países, a necessidade de aumentar a segurança e resiliência nas infraestruturas críticas é um requisito obrigatório e urgente que deve ser salvaguardado, atendendo ao impacto que terá se essas infraestruturas foram comprometidas.

Ao longo deste trabalho vamos propor o desenvolvimento de uma metodologia que consiga aferir o estado de maturidade nas infraestruturas de serviços críticos, através da validação da efetividade de controlos-chave, associados a domínios específicos da cibersegurança. Para atingir este objetivo, serão tidos em conta os domínios mais relevantes a considerar para esta tipologia de infraestruturas, sobretudo aqueles que tendo um menor nível de maturidade, e tendo uma maior exposição ao risco de serem comprometidos, vão causar um maior impacto ao normal funcionamento de toda a infraestrutura.

Palavras-chave:

Infraestruturas e Serviços Críticos, Cibersegurança, Avaliação de Maturidade

Esta página foi intencionalmente deixada em branco.

Conteúdo

Esta página foi intencionalmente deixada em branco.

Lista de Acrónimos

ANC – Autoridade Nacional de Cibersegurança

AR – Assembleia da República

BIA – Business Impact Analysis

CCM – Cloud Computing Matrix

CE – Comissão Europeia

CERT – Computer Emergency Response Team

CIA – Confidentiality, Integrity and Availability

CIWIN - Critical Infrastructure Warning Information Network

CMMC - Cybersecurity Maturity Model Certification

CNCS – Centro Nacional de Cibersegurança

CSA - Cloud Security Alliance

CSIRT – Computer Security Incident Response Team

CSP – Cloud Services Provider

C2M2 – Cybersecurity Capability Maturity Model

DCS – Distributed Control Systems

DL – Decreto Lei

ENISA - European Union Agency for Cybersecurity

EPCIP - Programa Europeu para Protecção de Infraestruturas Críticas

EUA – Estado Unidos da América

GDPR - General Data Protection Regulation

GR – Gestão de Risco

ICS – Industrial Control System

IEC – International Electrotechnical Commission

IIOT - Industrial Internet of Things

ITU - International Telecommunication Union

IEEE - Institute of Electrical and Electronics Engineers

IOT – Internet of things

ISACA – Information Systems Audit and Control Association

ISC – Infraestruturas e serviços críticos

ISO – International Organization for Standardization

IDS – Intrusion Detection Systems

IDPS - Intrusion Detection Prevention Systems

IPS – Intrusion Prevention Systems

IT – Information Technology

KPI – Key Performance Indicator

MFA – Multi Factor Authentication

MSI – Mestrado em Segurança Informática

NAC – Network Access Control

NCAF – National Capabilities Assessment Framework

NCF – NIST Cybersecurity Framework

NSM – Network Security Monitoring

NIS - Network and Information Security

NIS2 - Network and Information Security2

NIST – National Institute of Standards and Technology

NOC – Network Operations Center

OT – Operational technology

PDCA - Plan Do Check Act

QNRCS – Quadro Nacional de Referência para a Cibersegurança

RACI – Responsible, Accountable, Consulted and Informed

RGPD – Regulamento Geral sobre a Protecção de Dados

RJSC – Regime Jurídico de Segurança do Ciberespaço

RPO – Recovery Point Objective

RTIC – Risco nas Tecnologias de Informação

RTO – Recovery Time Objective

SCADA – Supervisory Control and Data Acquisition

SSDLC – Secure Software Life Cycle

SGSI - Sistema de Gestão da Segurança da Informação

SI/TI – Sistemas de Informação / Tecnologias de Informação

SIEM – Security Information and Event Management

SOC – Security Operations Center

SSO – Single Sign On

STAR - Security Trust & Assurance Registry

TIC – Tecnologias de Informação e Comunicação

UE – União Europeia

UC – Universidade de Coimbra

VPN – Virtual Private Networks

XDR – Extended Detection and Response

2FA – Segundo Fator Autenticação

Esta página foi intencionalmente deixada em branco.

Lista de Figuras

Esta página foi intencionalmente deixada em branco.

Lista de Tabelas

Esta página foi intencionalmente deixada em branco.

Capítulo 1

A evolução tecnológica tem sido um motor impulsionador para o aumento do número de serviços e soluções eletrónicas que são essenciais às atividades quotidianas do mundo atual. Sobre estas tecnologias assentam infraestruturas que fornecem serviços vitais ao funcionamento da sociedade, causando um elevado impacto em cenários de falha. Estas infraestruturas são transversais a diversos sectores estruturantes, sendo classificadas como críticas pelo elevado número de pessoas e outros serviços que dependem de si. Alguns dos serviços que estas infraestruturas suportam situam-se no sector energético, de transportes ou mesmo de comunicações, conforme identificado pelo Decreto-Lei 46/2018 [8] que foi transposto da diretiva 2016/1148 [2] criada pela Comissão Europeia (CE), definida com o intuito de regular e obrigar a cada estado-membro a aplicar mecanismos de controlo sobre as infraestruturas críticas que estão nos seus territórios. A aplicabilidade de medidas de supervisão e controlo efetivo sobre as infraestruturas é obrigatória, atendendo ao impacto nefasto que resultará da inoperabilidade das mesmas. Se num passado não muito longínquo, o número de serviços críticos era menor, têm vindo a aumentar em função da natural evolução humana e tecnológica. Alguns destes serviços não têm medidas alternativas que possam ser implementadas para mitigar cenários de falha, ou existindo, essas alternativas nem sempre respondem da forma correta, muitas vezes porque é impossível prever e simular todos os cenários de indisponibilidade. As ameaças a que as infraestruturas que sustentam estes serviços críticos estão expostas aumentaram de uma forma natural a partir do momento que o acesso à internet foi massificado, sobretudo quando estas infraestruturas passaram elas próprias a estar ligadas de forma permanente à internet, porque o seu modo de operação assim o obriga. Este cenário requer que seja considerado um novo paradigma em torno da cibersegurança, que até há poucos anos não era relevante considerar (uma vez que estas infraestruturas estavam confinadas a um espaço físico bem definido, sendo necessário transpor diversas barreiras para chegar à infraestrutura).

Perante esta ameaça, o modelo de gestão de segurança das infraestruturas com serviços críticos tem de ser repensado de forma sistemática, aplicando novas medidas de prevenção, monitorização e resposta urgente. O cibercrime não tem rosto, não é previsível, e nenhuma organização se atreve a dizer que está imune a esta tipologia de ataque, obrigando-se a implementar os mecanismos necessários para aumentar a sua robustez contra ciberataques, sabendo que poderá num futuro próximo ser um alvo, ou pode inclusive ter sido ou estar a passar por isso, sem que tenha qualquer visibilidade. Estes ataques são por norma bem direcionados e com uma estratégia definida de forma a causar o maior impacto à organização e aos seus clientes em particular, e à sociedade geral. Os alvos são assim escolhidos de forma premeditada, explorando diversos vetores de ataque, sabendo que a infraestrutura está exposta para a internet, possibilitando explorar

mais probabilidades de o ataque ser bem-sucedido, caso não estejam implementados de forma eficiente e eficaz controlos que permitam resistir a esses ataques. Ter uma visão transversal da sua infraestrutura, assim como do nível de maturidade dos controlos de segurança que estão implementados, permitirá às organizações gerir de forma mais eficaz os seus activos críticos, possibilitando uma gestão de risco organizacional mais direcionada para ameaças externas, sobre áreas que são estratégicas ao funcionamento da organização e que podem estar mais suscetíveis de ser comprometidas.

Ao longo deste trabalho iremos definir uma metodologia que permitirá aferir o nível de maturidade em cibersegurança nas infraestruturas, começando por identificar quais os domínios de segurança relevantes. Para cada domínio utilizado, são identificados controlos chave, sendo o valor da maturidade obtida através da efetividade de cada controlo avaliado. A metodologia além de disponibilizar o nível de maturidade global da infraestrutura, dará uma visão individual por domínio, permitindo definir prioridades face ao risco que esses domínios estão expostos em virtude da sua baixa resiliência.

1.1 Contextualização

Este documento representa a dissertação final realizada no âmbito da disciplina de Dissertação e Estágio do Mestrado em Segurança Informática (MSI) da Universidade de Coimbra, sob a orientação dos Professores Paulo Simões e Tiago Cruz. A importância de aferir a maturidade de infraestruturas que fornecem e suportam serviços críticos à sociedade, entendemos ser um assunto relevante, e por isso escolhido enquanto tema para a dissertação face à realidade que o mundo atravessa, no que respeita a ataques informáticos, em particular aqueles que são direcionados a infraestruturas críticas com objetivo de causar o maior impacto possível com a sua indisponibilidade. Por outro lado, este tema relaciona-se diretamente com parte o conteúdo programático do MSI, permitindo assim aplicar conceitos e metodologias estudadas enquanto conteúdo pragmático do MSI.

1.2 Motivação

A potencialidade que a Internet trouxe ao nosso quotidiano permitiu num curto espaço de tempo a disponibilização e o acesso a serviços que há pouco anos eram imagináveis, sendo prova disso a pandemia inerente ao Covid19 [3] que recentemente afetou o mundo. Esta pandemia obrigou a uma restruturação recorde em muitas organizações para passarem a laborar de forma totalmente remota, abrindo uma porta para um modelo de trabalho que ainda hoje se mantêm, permitindo a que algo considerado excecional passasse a ser a regra, sem que isso tenha afetado a produtividade nessas organizações. Porém, existe um lado obscuro que o acesso massificado à internet trouxe: os ataques informáticos. Esta tipologia de ataques

tem vindo a aumentar, quer em quantidade quer em qualidade, ou seja, são cada vez mais os ataques bem-sucedidos e sendo o seu impacto cada vez maior. Esta preocupação aumenta naturalmente quando os alvos destes ataques são infraestruturas críticas, pelo impacto que pode resultar desses ataques. É necessário que as organizações responsáveis por estas infraestruturas tenham uma noção clara do paradigma cibernético que o mundo vive atualmente no contexto do cibercrime que criou todo um conjunto de novas ameaças às organizações que não devem ser deixadas para segundo plano, sendo por isso importante garantir novas medidas e controlos que tornem estas infraestruturas mais robustas e preparadas para essas ameaças que podem chegar de qualquer parte do mundo e a qualquer momento sem que haja um alerta prévio. É com base nesta premissa que pretendemos desenvolver uma metodologia que permita aferir o nível de maturidade para a cibersegurança de infraestruturas críticas

1.3 Definição do problema

O forte crescimento de ataques cibernéticos a infraestruturas que suportam serviços essenciais têm obrigado os estados a legislar e a definir requisitos de segurança, com vista a apoiar as organizações a melhorar a sua resiliência contra este tipo de ataques. Os mais recentes modelos e *frameworks* de gestão de risco organizacionais visam operacionalizar estas orientações tanto em organismos públicos como privados, contribuindo para o amadurecimento da sua estratégia de segurança. Com a aplicação destas *frameworks* é conseguida uma visão transversal da organização a diversos níveis e apurado um nível de maturidade de cibersegurança.

Os operadores de infraestruturas críticas são um dos grupos identificados no QNRCS [4] e entendemos que, pela sua criticidade para o funcionamento de serviços vitais à sociedade devem ter domínios e controlos bem identificados para os poderem aplicar nas suas infraestruturas, devendo fazer uma monitorização e avaliação regular de forma a garantir a sua eficiência, face às novas ameaças que surgem todos os dias.

Se analisarmos em detalhe o Quadro Nacional de Referência para a CiberSegurança (QNRCS) [4], disponibilizado pelo Centro Nacional de CiberSegurança (CNCS) e de aplicabilidade obrigatória no panorama nacional para as organizações alvo, verificamos que são dadas linhas orientadoras relevantes para protecção contra ameaças à segurança de activos, mas num contexto geral, não entrando em grande detalhe no que respeita a controlos específicos para infraestruturas críticas.

1.4 Objetivos

O principal objetivo deste trabalho de tese é apresentar uma metodologia que permita determinar o nível de maturidade para a cibersegurança em infraestruturas de serviços críticos.

Para cumprir com esse objetivo, a seguinte metodologia será aplicada:

- Estudo e análise:
  - Legislação disponível que regule as infraestruturas e os seus operadores;
  - Identificação e caracterização de infraestruturas críticas;
  - Levantamento do estado de arte sobre *frameworks* e metodologias existentes;
  - Identificação de trabalhos anteriormente desenvolvidos e que possam servir de base e ponto de partida para este trabalho.
- Apoiar na resposta ao decreto-lei 65/2021 aplicável a operadores de infraestruturas críticas e serviços essenciais, no que respeita à maturidade em cibersegurança, em linha com as orientações do CNCS;
- Identificar os domínios e controlos relevantes a considerar para realizar uma análise de maturidade a infraestruturas de serviços críticos;
- Desenvolver uma metodologia de cálculo de maturidade, enquadrada em níveis previamente definidos;
- Obter uma visão transversal e holística sobre a conformidade dos domínios da cibersegurança na infraestrutura;
- Dar contributos para a Gestão de Risco, através de uma visão realista dos riscos associados a infraestruturas que suportem serviços críticos
- Aplicar a metodologia desenvolvida através da realização de uma avaliação de maturidade exemplificada;
- Apresentação de resultados.

Com este contributo, pretendemos dar maior visibilidade sobre o estado de maturidade de uma infraestrutura critica no que à cibersegurança diz respeito, elencando as áreas que estão menos robustas, permitindo facilitar a tomada de decisão sobre as ações a implementar e a canalização de recursos com a devida prioritização, de forma a atingir o nível de maturidade pretendido. Entendemos ainda que esta avaliação dará contributos relevantes para a gestão de risco para os sistemas de informação.

1.5 Estrutura do documento

A estrutura restante documento está organizada da seguinte forma:

Capítulo 2 – Neste capítulo apresentamos um levantamento da informação relevante para o tema desenvolvido, materializado numa análise documental sobre os principais modelos e *standards* que serviram de suporte à realização do trabalho, em particular no desenvolvimento da metodologia.

os principais conteúdos legislativos e regulamentares, metodologias desenvolvidas e trabalhos elaborados, que sejam relevantes para o nosso trabalho.

Capítulo 3 – Neste capítulo é feito um levamento legal e regulamentar, com particular foco para legislação Portuguesa que obriga às organizações alvo destes regulamentos a procederem com ações concretas nas suas infraestruturas e serviços críticos de forma a assegurar a robustez das mesmas.

Capítulo 4 – Neste capítulo é apresentada a definição do problema e a abordagem seguida para a sua resolução. Será apresentada a metodologia definida em linha com a abordagem proposta, materializada num caso de uso realizado, com a apresentação de resultados.

Capítulo 5 - Neste capítulo serão apresentadas conclusões do trabalho elaborado, nomeadamente dos desafios encontrados durante a fase de elaboração e verificação da metodologia. Ainda neste capítulo é dada uma perspetiva sobre a forma como a metodologia poderá ser expandida de modo a torna-la mais abrangente, robusta e simplifica-la.

Capítulo 2

MODELOS E STANDARDS DE SEGURANÇA: UMA PERSPETIVA ABRANGENTE DO ESTADO DA ARTE

A recolha e análise de informação que caracterizou a parte inicial deste trabalho foi essencial para definir a estratégia e a abordagem ao problema, bem como a forma como pretendemos contribuir para o tema. Ao longo deste capítulo apresentaremos os principais conceitos, métodos e algumas *frameworks* desenvolvidas para avaliação de risco em sistemas de informação e que serviram de base ao nosso trabalho. Começaremos por analisar a preocupação das entidades governativas ao nível da CE, que muito têm focado a sua atenção em legislar e obrigar os seus estados-membros a implementar mecanismos de controlo e supervisão sobre as infraestruturas críticas, na tentativa de antecipar situações catastróficas, na eventualidade de ficaram indisponíveis, perante cenários de ataque informáticos.

Para além da análise documental realizada, foram ainda conduzidas entrevistas e reuniões com elementos da área, sobretudo de *Security Operations Center* (SOC) e *Network Operations Center (*NOC) que por meio dos seus contributos, permitiram ter uma visibilidade da sua função na monitorização de infraestruturas críticas, não somente numa perspetiva de segurança, mas também de disponibilidade. Estas duas perspetivas são complementares, atendendo que uma das características de tríada da segurança é a disponibilidade, além da integridade.

Entidades europeias e norte-americanas desenvolveram nos últimos anos *Frameworks* e metodologias para ajudar a enfrentar as organizações e preparem-se para a nova ameaça que começavam a pairar e para a qual havia muito desconhecimento sobre como a combater. A internet foi o grande veículo para o crescimento dos ciberataques, que foi crescendo à medida que o comércio eletrónico e outros serviços disponibilizados através da internet se multiplicavam diariamente. Existia nessa época pouca informação e sensibilidade para a segurança informática e os ciberataques eram desvalorizados, e vistos como um evento que só afetava outras organizações.

O aumento dos incidentes de segurança associados a ciberataques, obrigou o mundo empresarial a mudar a sua postura em relação à temática, e perceber que ninguém estaria totalmente protegido contra isso. O mercado empresarial mudou e começou a ter uma postura mais preventiva, através da contratação de profissionais da área e implementação de programas de formação para os seus quadros, por forma a difundir uma cultura orientada para a cibersegurança. Os governos foram lançando leis e regulamentos que obrigavam as organizações e implementarem políticas de segurança robustas para proteger os dados que

lhes eram confiados e as transações dos seus clientes. A segurança informática passou desta forma a ser um requisito obrigatório e transversal a toda a organização.

A CE desde cedo que percebeu o risco que era para os países-membros terem de enfrentar a ameaça da cibersegurança e, tal como vimos em capítulos anteriores não perdeu tempo a começar a legislar e fornecer ferramentas que permitissem de forma transversal e unida, começassem a ganhar conhecimento e maturidade para o tema.

2.1 *Framework* da CE para os estados-membros

A ENISA, com a sua missão de conseguir que toda a Europa consiga obter um nível elevado de conformidade na cibersegurança lançou em 2020 uma framework denominada *National Capabilities Assessment Framework* (NCAF) [29] por forma a ajudar os países membros da UE a enfrentar o aumento de ciberataques que têm vindo a ocorrer. A *Framework* assenta numa autoavaliação que cada país deve fazer, com intuito de perceber o seu estado de maturidade em determinadas áreas e desta definir a sua estratégia nesta matéria.

Esta *Framework* é constituída por dezassete objetivos estratégicos, inseridos em quatro grandes vertentes organizacionais que para a ENISA eram considerados fundamentais, para que a organização pudesse ter uma visão abrangente e assim avaliar quais os pontos mais fracos aos quais merecem atenção.

A figura 2.1 demonstra a *framework* criada pela ENISA para apoiar os estados-membros na aferição do seu nível de maturidade para implementação da estratégia interna para a cibersegurança.

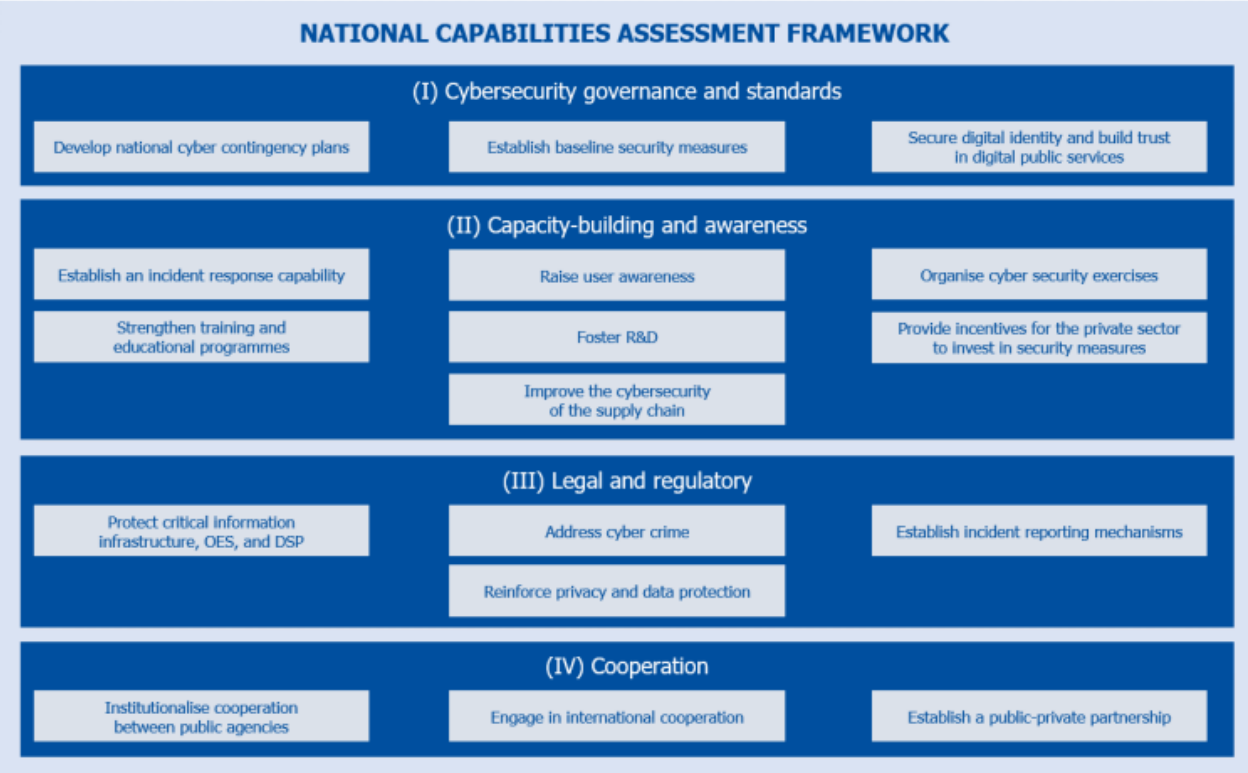

Figura 2. 1 Framework ENISA para avaliação de maturidade em cibersegurança, retirada de [29]

A *Framework* tem por base cinco níveis de maturidade no seu modelo de avaliação, conforme nos mostra a tabela 2.1.

ENISA - MATURITY LEVEL				
1	2	3	4	5
INITIAL / AD HOC	EARLY DEFINITION	ESTABLISHED	OPTIMISATION	ADAPTIVENESS

Tabela 2. 1 Níveis de maturidade definidos pela ENISA, retirada de [29]

A *Framework*, através das quatro vertentes pretende chegar às áreas relevantes e que devem ser avaliadas, por ditarem a maturidade global e capacidade de resistir a ciberataques:

- ***Cybersecurity governance and standards:*** Verifica a capacidade em estabelecer e implementar a governação, padronização e melhores práticas no domínio da cibersegurança;

- ***Capacity-building and awareness:*** Mede a capacidade em implementar uma cultura de sensibilização para a lidar com os riscos e ameaças inerentes à cibersegurança e para a importância de se investir em meios e recursos para enfrentar a cibersegurança;

- ***Legal and regulatory***: Visa medir a capacidade de implementar leis e regulamentos com vista a enfrentar, combater e travar o crescimento do crime cibernético e os incidentes que resultam desse crime de forma a proteger infraestruturas críticas;

- ***Cooperation***: A importância da cooperação e a troca de informação ao nível organizacional, sectorial, nacional e internacional é fundamental para combater o cibercrime, sendo por isso importante medir a capacidade de implementar esta cooperação.

Esta *Framework* visa desta forma medir a capacidade do estado-membro em lidar com a ameaça do cibercrime.

2.2 *Framework CNCS para Portugal*

Com objetivo de apoiar as organizações publicas e privadas em Portugal, transpondo as diretivas e regulamentos elaborados pela UE, o CNCS disponibiliza o QNRCS [4]. O QNRCS, pode ser interpretado como uma *Framework* onde são descritas várias medidas de segurança que, ao serem colocadas em prática, visam atingir objetivos específicos no capítulo da segurança informática. Para atingir estes objetivos a *Framework* disponibiliza linhas orientadoras e procedimentos concretos que suportam o processo de gestão de risco de cibersegurança.

O CNCS identifica cinco grandes objetivos da segurança conforme mostra a figura 2.2. Estes objetivos devem ser implementados de forma sequencial, não podendo nenhum ser suprimido ou desvalorizado sob pena de ser interrompido um processo critico da *Framework.*

Figura 2. 2 Figura 2. 3 Objetivos de segurança definidos pelo CNCS, retirada de [4]

Os objetivos de segurança assentam e podem ser compreendidos em três elementos-chave: Medidas de segurança, categorias e subcategorias.

As medidas de segurança surgem no topo e que são fundamentais no delinear do plano estratégico e tático para gerir o risco de cibersegurança. As medidas ajudam a balizar e a simplificar a forma como é organizada a informação, as tomadas de decisão e a forma como devem ser endereçadas as ameaças. Estas medidas de segurança devem estar em sintonia com o processo de gestão de incidentes, para canalizar o suporte financeiro para a cibersegurança.

Para cada objetivo são definidas as categorias relevantes com vista a cumpri-lo, podendo existir diversas subcategorias, para cada uma das categorias.

Na tabela 2.2 apresentamos com maior detalhe os cinco objetivos que o CNCS identifica como elementos sustentadores da *Framework*, assim como a descrição de cada um deles.

Objetivo	Descrição
Identificar	Compreensão do contexto da organização, dos ativos que suportam os processos críticos da atividade da organização e dos 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.
Proteger	Implementação de medidas destinadas a proteger os processos organizativos e os ativos da organização, independentemente da sua natureza tecnológica. Assim, nesta categoria, são definidas medidas orientadas à proteção da organização nas suas três dimensões: Pessoas, Processos e Tecnologia.
Detetar	Definição e implementação de medidas destinadas a identificar, de forma atempada, os incidentes. Ou seja, a deteção de eventos com um efeito adverso real na segurança das redes e dos sistemas de informação.
Responder	Definição e implementação de medidas de ação apropriadas, em caso de deteção de um incidente. As medidas propostas no âmbito deste objetivo pretendem mitigar o impacto do incidente, ou seja, reduzir os seus potenciais efeitos adversos.
Recuperar	Definição e implementação de atividades, que visam a gestão de planos e medidas de recuperação dos processos e serviços afetados por um incidente de cibersegurança. As medidas pertencentes a este objetivo pretendem assegurar a resiliência da organização nas suas dimensões: Pessoas, Processos e Tecnologia. E que, no caso de existência de um incidente, a organização consiga utilizar as medidas para suporte à recuperação em tempo útil da sua atividade.

Tabela 2. 2 Objetivos da segurança segundo o QRNCS do CNCS, retirado de [4]

A diversidade de serviços disponibilizados à sociedade tem permitido uma flexibilidade no nosso quotidiano, levando a uma transformação na forma como nos relacionamos com o mundo, onde a partir de um telemóvel com acesso à internet esperamos conseguir gerir toda a nossa vida, de forma rápida, cómoda e segura. Esta exigência obriga as organizações a estarem em constante novação e evolução nos serviços que disponibilizam, para manter os seus clientes fiéis, angariar novos, mas sobretudo para reduzirem os seus custos operacionais.

Esta transformação assenta sobretudo em serviços digitais, ou seja, são disponibilizados através da internet e desta forma chegam ao maior número de clientes. Para conseguir este objetivo as organizações foram expondo serviços para a internet, correndo os riscos que esta decisão acarreta. Com os seus serviços e infraestruturas acessíveis da internet, uma outra flexibilidade foi surgindo, possibilitando acessos remotos a colaboradores e prestadores de serviço.

A par da flexibilidade e comodidade que se criou, foram surgindo ameaças a estas infraestruturas, através de ciberataques que sendo bem-sucedidos comprometem o funcionamento das mesmas. Os países face à criticidade que as infraestruturas representam para sociedade, começaram a legislar com objetivo de obrigar as organizações a terem um maior controlo e implementarem mecanismos de segurança com vista a tornar essas infraestruturas mais resilientes a ciberataques, ficando o estado com a responsabilidade de supervisionar essas organizações, sendo elas públicas ou privadas.

2.3 Soluções baseadas em Cloud

A computação baseada em *Cloud* [30] trata-se de uma metodologia recente que veio alterar todo o paradigma tecnológico das organizações por lhes permitir uma maior flexibilização nos serviços que prestam aos seus clientes e simultaneamente reduzir a dependência de infraestruturas dedicadas, ficando essa responsabilidade delegada nos prestadores de serviços de *cloud.* Este tipo de computação oferece vantagens comparativamente aos modelos clássicos pela flexibilidade, eficiência, facilidade de gestão e administração, custos mais reduzidos, previsíveis e maiores padrões de segurança.

As soluções *cloud* são consideradas mais seguras pelo facto de ser o prestador de serviços a gerir e a responsabilizar-se pela segurança das suas infraestruturas que são alvo de auditorias e certificações a atestar o cumprimento das melhoras práticas de configuração e conformidade com os requisitos de *standards*. Esta gestão oferece por um lado garantias de que seguem as melhoras práticas e procedimentos de segurança e por outro não permitem aos seus clientes gerirem de forma menos correta ou negligente a segurança dos seus serviços. Se olharmos para *clouds* híbridas, o cenário altera-se atendendo que as organizações detentoras deste tipo de *clouds* tem um maior controlo sobre os recursos e no desenho das arquiteturas, podendo ser desvalorizada a segurança. Uma solução baseada em *cloud* tem ainda a vantagem de possuir um tempo de lançamento ou ativação reduzido, pelo facto da camada de infraestrutura que a suporta ser abstrata, ou seja, é independente e não exclusiva para ser utilizada por determinada aplicação. Perante cenários de catástrofe, esta tecnologia permite uma recuperação mais rápida, segura e controlada permitindo reduzir o impacto organizacional.

2.3.1 Tipologias de cloud

Atualmente existem quatro tipos de arquiteturas *cloud*, as públicas, privadas, híbridas e comunitárias. Cada uma tem as suas particularidades e funcionalidades, servindo propósitos distintos, mediante o modelo de negócio, operativo e estrutural de cada organização:

- **Cloud Pública –** Assenta numa arquitectura com recursos pertencentes a um fornecedor de serviços cloud (CSP) (p.e. *Google Cloud Platform, Microsoft Azure ou Amazon Web Services*) acessível através da internet, podendo os recursos ser partilhados por outras organizações ou clientes, apesar do CSP garantir a disponibilização e alocação dos recursos contratados. Estes recursos ou serviços podem ser previamente adquiridos independentemente de serem utilizados ou não, ou podem também ser adquiridos à medida das necessidades, sendo que esta última opção têm associado um maior custo devido à imprevisibilidade, embora apenas materializável se for utilizado contrariamente à primeira opção, onde existe sempre um custo associado, independentemente da utilização dada ao recurso. Alguns destes recursos não têm um custo associado à utilização, mas pode existir pelo armazenamento de dados que envolve, ou pelo número de visualizações realizadas, permitindo desta forma uma maior flexibilização para as organizações que adotem este modelo de cloud. Nesta modalidade não existe o conceito de *Datacenter* físico gerido pela organização, em virtude dos recursos, assim como os dados estarem sob a responsabilidade do CSP em localizações por estes geridas, podendo existir se assim for contratado a distribuição destes recursos por várias localizações distanciadas entre si, criando um cenário de redundância e alta disponibilidade.

  Na figura seguinte é apresentada uma arquitectura exemplificativa de uma *Cloud* pública Azure do prestador de serviços Microsoft.

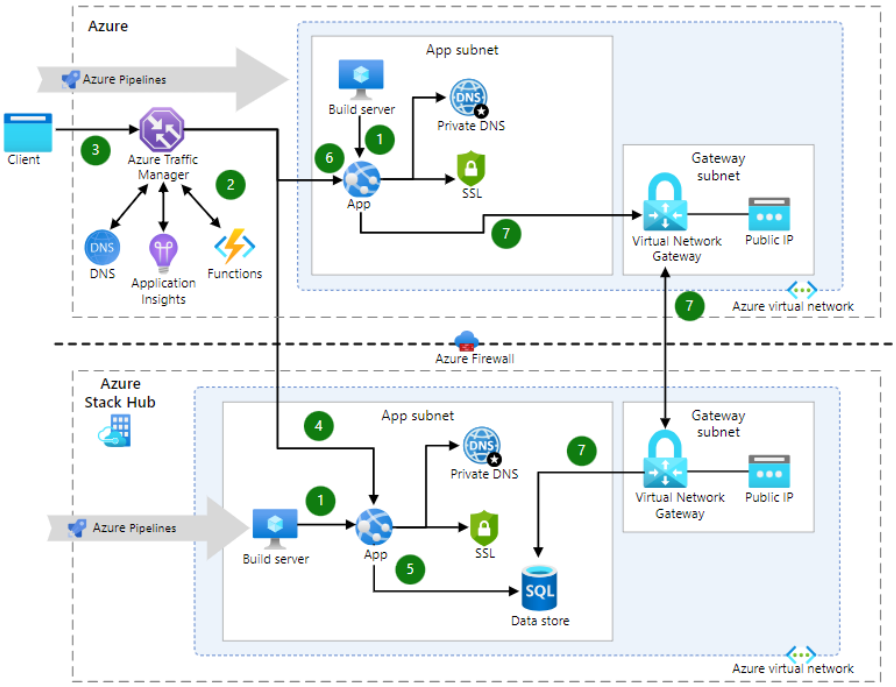

Figura 2. 4 Arquitectura Azure de uma Cloud pública, retirada de [41]

- **Cloud Privada –** Contrariamente ao modelo de *cloud* pública, a privada prevê ter uma infraestrutura de recursos dedicado à organização, num conceito de utilização mais personificado. No caso de organizações que possuam o seu próprio *Datacenter,* a *cloud* pode ser configurada diretamente nessa infraestrutura, ou não existindo, pode ser configurada num *Datacenter* de um fornecedor deste tipo de serviços ou disponibilizada por um prestador de serviços de *Cloud*, separando a infraestrutura que sustenta esta Cloud das restantes, de forma a ficar dedicada. A organização tem total controlo sobre os recursos existentes, sendo por norma a gestão, operação e manutenção da sua responsabilidade. Este modelo é o mais parecido com os modelos tradicionais onde as organizações possuem os seus próprios recursos num espaço controlado e gerido por si.

A figura seguinte exemplifica uma arquitectura simplificada de uma *Cloud* privada.

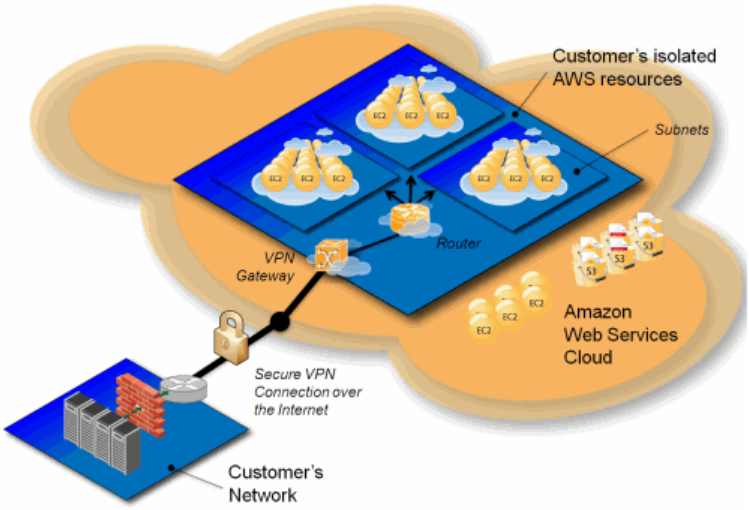

Figura 2. 5 Arquitetura AWS para uma Cloud privada, retirada de [40]

- **Cloud Híbrida –** Uma *Cloud* híbrida pode ser interpretada como a combinação entre a *Cloud* pública e a *Cloud* privada. Neste modelo os dados assim como as soluções aplicacionais existentes podem mover-se entre as duas arquiteturas, embora a organização possa manter os dados sempre sob o seu controlo e usufruindo apenas da vertente aplicacional e serviços partilhados que a *cloud* pública oferece. A adoção a uma *cloud* híbrida pode ser utilizada como um meio que as organizações seguem para transitar o seu *Datacenter* tradicional para uma componente de *cloud* temporária até ter uma arquitetura totalmente baseada em *cloud* pública.

Na imagem seguinte é apresentada uma arquitetura de serviços baseada em modelo de *Cloud* híbrida, com as delimitações bem definidas entre a componente privada e pública.

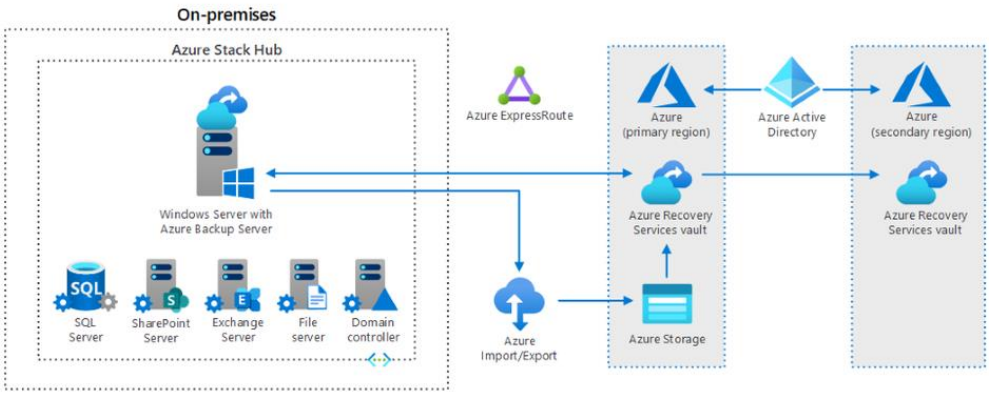

Figura 2. 6 Arquitetura Azure para uma *cloud* híbrida, retirada de [42]

- **Cloud Comunitária –** É um modelo de Cloud criada com o objetivo de permitir a partilha de recursos entre entidades, organizações ou grupos que possuem necessidades com requisitos equiparados. Não é um modelo muito utilizado em setores empresariais porque a partilha é encarada como algo pouco benéfico sobretudo em matérias de privacidade e disponibilidade de infraestrutura, assim como o baixo controlo que possa existir sobre os recursos, não havendo garantia que os mesmos estejam sempre disponíveis, pois dependerá da utilização que os restantes membros tenham em determinado período. Este modelo tende a ser economicamente atrativo pela partilha que lhe está inerente, onde o aumento de utilizadores baixa proporcionalmente o custo de utilização dos recursos existente. Além do custo, a flexibilidade, escalabilidade e disponibilidade são também vantagens que este modelo possui em semelhança com restantes.

  A figura seguinte representa uma configuração típica de uma Cloud em modelo de comunidade.

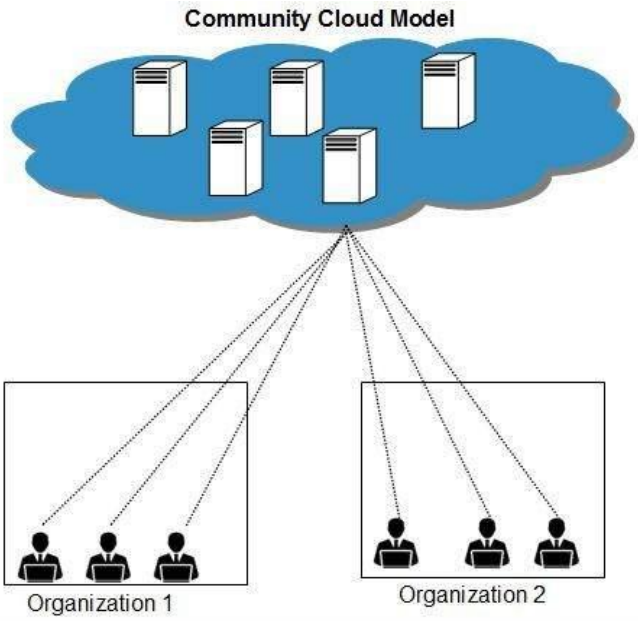

Figura 2. 7 Arquitetura *Cloud* em modelo de comunidade, retirada de [44]

2.3.1.1 Modelos de serviço para arquiteturas Cloud

Quando uma organização toma a decisão de implementar uma arquitectura cloud, seja para migrar a sua infraestrutura *on-premises* ou uma implementação nativa, deverá ter em conta que tipo de serviços que são os mais adequados à sua realidade. Algumas tipologias requerem uma maior dedicação, pelo facto da gestão ficar à responsabilidade da própria organização. Detalharemos de seguida as principais características de cada um dos serviços, salientando as vantagens e desvantagens entre eles.

- **Infrastructure as a Service (IaaS) –** Trata-se do modelo mais próximo das arquiteturas tradicionais, no qual a organização possuía um Datacenter com equipamentos, gerindo-os mediante as suas normas e procedimentos. Apesar do modelo IaaS envolver equipamentos como máquinas virtuais, rede ou de segurança, a organização não necessita de os adquirir, terá apenas de os contratar mediante a suas necessidades com base num modelo de pagamento previamente acordado. A organização não tem o ónus de assegurar o fornecimento de energia, controlo de acessos ou refrigeração, tudo isso é assegurado pelo CSP, sendo o custo variável em função da utilização, capacidade de processamento e armazenamento destes equipamentos, que são totalmente escaláveis mediante a necessidade de mais ou menos recursos. Este dinamismo permite uma flexibilidade e controlo sobre a infraestrutura, possibilitando que uma utilização dos recursos em

multiutilização de forma transparente. O modelo IaaS como verificámos permite um maior controlo da organização sobre os recursos, o que do ponto de vista de segurança poderá traduzir-se numa vantagem, possibilitando implementar configurações de segurança muito adaptadas aos requisitos organizacionais em linha com as políticas e processos internos.

Por norma este modelo de gestão é implementado por organizações de média ou grande dimensão, onde existem equipas dedicadas para gestão dos equipamentos e serviços. Também organização que preveem um rápido crescimento.

- **Software as a Service (SaaS) –** É um modelo de gestão também conhecido por serviços aplicacionais em *cloud*, tratando-se de um leque serviços aptos para serem utilizados. Tal como o nome sugere, trata-se apenas de software, ou seja, aplicações, sendo a componente de infraestrutura abstrata para a organização, uma vez que a sua gestão, operação e manutenção pertence ao CSP que garante a disponibilidade da solução mediante o contratado. Estes serviços podem ser contratados mediante o pagamento de um valor mensal ou anual. Este modelo minimiza o risco associado a más praticas de gestão de equipamentos, atualizações e aplicação de correções de segurança, tornando-a assim mais segura e disponível. No que respeita a escalabilidade, oferece ainda melhores índices quando comparada com o modelo IaaS, sendo o acesso a estes serviços tão simples como abrir um navegador de internet, um cliente aplicacional (p.e. cliente de base dados) necessitando apenas de uma ligação à internet. Existe ainda casos em que a organização dispõe de um período de oferta para conhecer e realizar uma prova de conceito ou valor sobre a utilização do serviço ou aplicação em causa.

- **Platform as a Service (PaaS) –** Trata-se de um modelo diferenciador de IaaS por não ser disponibilizada uma infraestrutura para gerir, também distinto do modelo de SaaS, porque não é disponibilizado um componente aplicacional, mas sim uma plataforma de recursos que permite uma elevada flexibilização. Este modelo deve ser adotado, quando se procura desenvolver, executar e gerir aplicações de forma customizada, ou seja, à medida das necessidades organizacionais. Apesar de se tratar de uma plataforma que permite desenvolvimentos, as componentes de segurança, comunicações, monitorização ou reporting estão asseguradas pelo CSP. O facto deste modelo permitir executar desenvolvimentos completamente customizados e executados num modelo ajustado à organização possibilita atingir resultados de forma rápida com baixo esforço e consequentemente custos reduzidos. A grande variedade de recursos e meios que PaaS

disponibiliza, abre a possibilidade de conseguir integrações com uma grande variedade de soluções e objetos de forma facilitada, com baixa necessidade de desenvolver conectores, facilitando a gestão.

Na figura seguinte é apresentada uma comparação entre os diversos modelos de serviços *cloud* e a vertente tradicional, denominada de *on-site*, no que respeita à responsabilidade e gestão.

Figura 2. 8 Comparação entre os diversos modelos de serviço *cloud*, retirada de [43]

2.3.1.2 Framework Cloud Security Alliance

A *Cloud Security Alliance* (CSA) [37] surgiu em 2008 enquanto organização mundial sem fins lucrativos totalmente dedicada à vertente *Cloud* com objetivo de definir procedimentos e práticas aplicacionais numa metodologia que começava a ter cada vez mais atratividade. A CSA é constituída por elementos provenientes das mais distintas áreas, setores e organizações, possibilitando uma vasta

abrangência em termos de conhecimento, experiência e contributo nesta aliança. Este leque de conhecimento é muito útil na contribuição para a definição de arquiteturas *cloud* mais seguras para quem fornece e consome este tipo de serviços. Ao longo da sua existência a CSA tem disponibilizado diversa documentação que serve de orientação para implementação, sobretudo para apoiar na gestão de risco associada a esta tipologia de soluções. O aumento de soluções baseadas em *cloud* requer a definição e implementação de mecanismos de segurança que respondam às ameaças a que estas soluções estão expostas, em linha com uma gestão de risco adequada. A framework da CSA denominada *Cloud Controls Matrix*(CCM) é composta por 197 controlos objetivos distribuídos por 17 domínios da segurança garantem uma cobertura em todas as vertentes desta tecnologia. Esta framework têm a capacidade de apoiar de uma forma prática a implementação de tecnologias *cloud* contribuindo com princípios orientadores. Através da CCM é possível realizar uma auditoria de conformidade, uma vez que pode ser utilizada como ferramenta de avaliação sistemática, elencando as vertentes ou controlos que devem ser revistos no sentido os tornar mais robustos. Apesar da CCM ser um questionário onde as respostas permitidas é apenas SIM e NÃO, não deixa de ser relevante e percetível se determinado controlo está ou não implementado, dando uma visão holística de quais os domínios que apresentam maior resiliência para enfrentar as constantes ameaças que lhe estão associados. Em cenários de *Cloud* privadas ou hibridas a exposição é menor e mais controlada, tendo por isso um risco inerente mais reduzido quando comparadas com as públicas.

A CSA dispõe de um programa de avaliação e certificação em tecnologias *Cloud* para prestadores desta tipologia de serviço denominado *Security Trust & Assurance Registry*(STAR) [38] funcionando a dois níveis distintos:

- **Nível 1 – Autoavaliação –** Neste primeiro nível a organização pode submeter um ou dois questionários de autoavaliação em segurança e privacidade. Para a vertente de segurança os questionários têm por base a CCM que de forma transversal avaliará e documentará todos os controlos de segurança. Para a vertente de privacidade ou protecção de dados, a avaliação é realizada com base no código de conduta do GDPR [39]. Este nível pode ser obtido por organizações que tenham um baixo ou nulo apetite ao risco, por aquelas que procuram oferecer uma maior transparência relativamente aos controlos de segurança que têm implementados e procuram balancear entre a confiança e a transparência nos serviços *Cloud* que disponibilizam.

- **Nível 2 – Certificação –** As organizações devem optar por este nível quando se propõem a obter uma certificação de *cloud* ou quando pretendem obter um outro nível de certificação para os seus serviços e tecnologias *cloud*, mas necessitam de ter em primeiro estágio esta certificação.

2.4 International Organization for Standardization (ISO)

Uma das principais *frameworks* quando trata de sistemas de informação é ISO pela confiança, versatilidade e adaptabilidade que durante os últimos anos tem demonstrado de forma transversal em organizações dos mais diversos setores. Se virmos o caso da certificação ISO 27001 é um exemplo desta diversidade que não distingue ou exclui organizações de poderem ter uma certificação que atesta ter implementado os processos e controlos que torna mais robusto o seu sistema de gestão de segurança da informação. A ISO é uma organização não governamental composta por órgãos padronizados em mais de 160 países, ou seja, por cada um destes países existe um representante. Este representante é uma organização de atuação nacional, no caso de Portugal, trata-se do Instituto Português da Qualidade que colabora diretamente na elaboração e promoção de diversos padrões para a indústria, tecnologia ou para a sociedade em geral. Sendo também a entidade que têm a responsabilidade pela venda dos diversos documentos que sustentam e detalhem estes padrões. O processo de definição, revisão e aprovação de um padrão ou norma para qualquer sector é complexo, e obriga à disponibilidade de recursos para o fazer, pelo grau de exigência requerido. Este processo envolve seis etapas que se inicia com a definição de uma proposta para desenvolver o padrão, em virtude da identificação de uma necessidade, passando pela análise e discussão entre os membros que terão de o aprovar e finalmente a publicação. Uma organização que pretenda obter uma certificação num destes padrões (standards) terá um longo caminho a fazer que envolverá tempo e recursos, mas sobretudo uma forte maturidade nos seus processos internos, mas com isso, atingirá um patamar que lhe permite garantir a excelência na produção de um determinado bem ou produto ou na prestação de um serviço com qualidade que o padrão exige.

A par da ISO, existe ainda a International Electrotechnical Comission (EIC) com funções e responsabilidades semelhantes embora mais vocacionada para a vertente das tecnologias eletrónicas, trabalhando em articulação outros órgãos standards da indústria como a *International Telecommunication Union (ITU), o Institute of Electrical and Electronics Engineers (IEEE)* e a ISO. Como resultado desta junção entre a ISO e a EIC surgiram diversos standards ou *frameworks* como é o caso da ISO/EIC 27000, 9000 ou a 31000.

2.4.1 Framework ISO 27001

A ISO 27001 pertence à família da ISO/EIC 27000 lançada com o propósito de emitir controlos, técnicas e procedimentos orientadores para a segurança em tecnologias de informação, ou seja, uma referência internacional para a certificação do Sistema de Gestão da Segurança da Informação (SGSI). Trata-se de uma norma bastante consolidada e uma das principais quando se aborda a temática da segurança

de informação. A ISO 27001 tem a sua origem num *standard* britânico, a BS7799 lançada em 1992, tendo posteriormente surgido diversas atualizações, em função de melhorias e alargamento de âmbito que aos poucos sido incluído. A primeira versão da ISO 27001, enquanto ISO surge em 2005, revista posteriormente em 2013 e mais recentemente em 2022, sendo esta última a que se encontra presentemente em vigor. Qualquer organização é livre de implementar esta norma no seu Sistema de Gestão de Segurança de Informação nas vertentes de operação, revisão e monitorização, obtendo uma visão holística no domínio da segurança de informação que é totalmente independente da tecnologia que a organização possui ou venha a adquirir mediante o crescimento e expansão ou evolução tecnológica. Não é obrigatório que uma organização tenho o seu SGSI certificado, nem o deve fazer enquanto não tiver um nível de maturidade e amadurecimento dos seus processos internos, sob pena de tornar o processo de certificação pesado e difícil de implementar, uma vez que existirão domínios mais robustos e em maior conformidade com a norma do que outros. O facto de uma entidade ter certificado o seu SGSI com a norma ISO 27001, de forma alguma significa que está imune a ciberataques ou que atingiu um patamar que não se tem de preocupar mais em evoluir e incrementar o seu nível de segurança, muito pelo contrário, significa que essa organização está mais bem preparada para enfrentar as ameaças. O nível de maturidade atingido quando se implementa este tipo de certificação, permite uma consciencialização e uma necessidade em fazer mais e melhor em prol do seu sistema de informação, abrindo os horizontes para outras necessidades como seja a implementação de novos processos e tecnologias em domínios com menor cobertura. Existem porem entidades que tem políticas normativas, processos e tecnologia implementada e não têm certificado o seu SGSI, por não ser um requisito de negócio, regulamentar ou legal, mas valorizam e investem tempo e recursos em segurança de forma equiparada, embora não o consigam demonstrar exteriormente por não possuírem a certificação.

A ISO define uma metodologia para implementação de certificação baseada em quatro etapas:

- **PLAN (P) –** Planear a implementação – Nesta fase é definido o contexto organizacional em termos de âmbito da gestão da informação, bem como a gestão de expectativas das partes envolvidas. São ainda identificados os responsáveis pela segurança da informação, a definição de política interna e o estabelecer de compromisso para com a iniciativa, garantido os recursos necessários. O planeamento de todas as atividades, definição de metas e objetivos são ainda definidos nesta etapa a par do modelo de comunicação e documentação processual, sem esquecer a vertente de formação e consciencialização dos colaboradores e parceiros.
- **DO (D) –** Executar e realizar – Segunda fase da metodologia onde ocorre a operacionalização através da execução das atividades de planeamento e controlo, aferição do nível de risco dos dados e implementação de medidas de mitigação dos riscos identificados. São ainda implementados mecanismos de monitorização e controlo sobre a execução do plano.

- **CHECK (C) –** Verificar, validar e medir – Esta fase visa verificar o nível de conformidade das atividades executadas face ao plano e requisitos iniciais aferindo a eficácia do plano. É crucial a definição de indicadores a diversos níveis, para suportar a avaliação de forma realista. As atividades que não cumpram os objetivos são corrigidas na próxima fase do processo
- **ACT (A) –** Agir – Última etapa do ciclo de implementação, visando a tomada de decisões com base nos resultados de cada uma das fases anteriores. É nesta etapa que é tomada a decisão para avançar ou não (GO/NoGo) podendo ser necessário aplicar medidas corretivas para os desvios identificados, caso seja possível fazê-lo e ter como objetivo primordial a melhora continua. Caso não seja possível corrigir os desvios, todas as fases anteriores devem ser percorridas novamente, tendo por base o historial do processo anterior.

Na figura seguinte é demonstrado as principais atividades inerentes à metodologia PDCA.

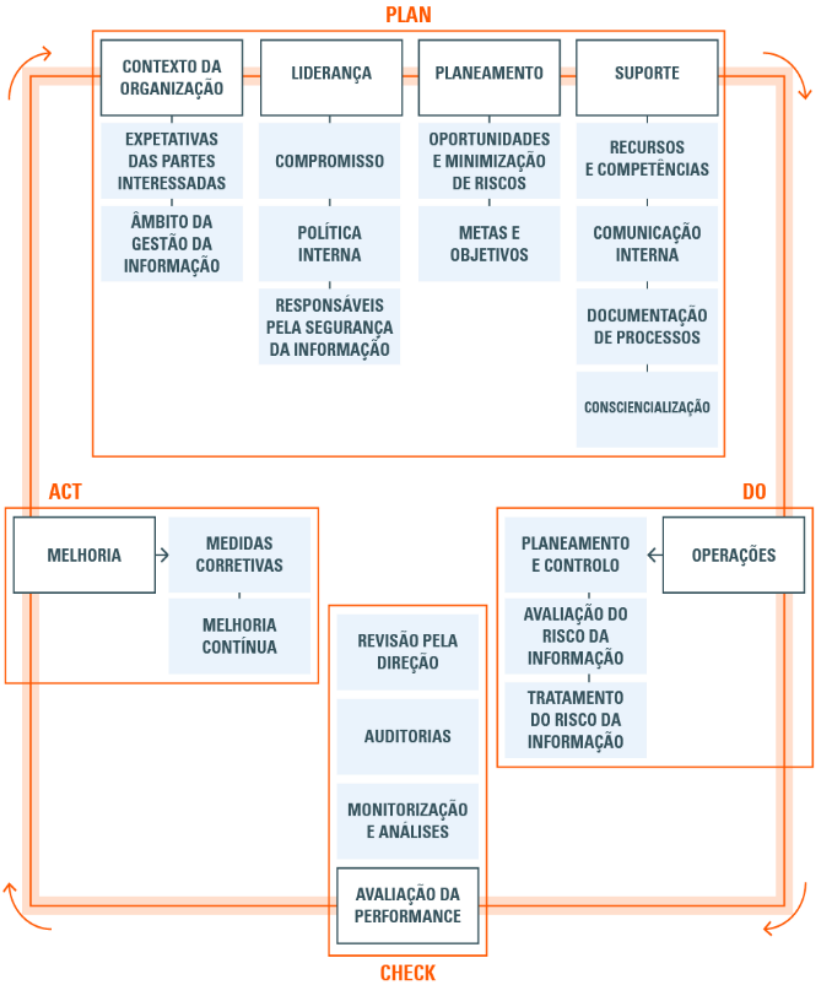

Figura 2. 9 Metodologia PDCA, retirada de [45]

Como verificámos anteriormente na metodologia PDCA, uma organização ao certificar o SGSI com base na ISO 27001, assume um compromisso da gestão de topo em manter e melhorar de forma continua o seu sistema de informação, através de uma gestão de risco mais eficiente e realista. A certificação requer ainda que os colaboradores obtenham um nível de formação adequada e regular que contemple o SGSI em toda a sua amplitude, traduzindo-se num fator motivacional por toda a organização, gerando confiança e colaboração. De forma natural, esta confiança é percecionada por clientes e prestadores de serviços diretos e indiretos aumentando a procura pelos serviços e produtos disponibilizados. De uma forma resumida, a certificação ISO 27001 pode ser interpretada como uma ferramenta eficaz para a gestão de risco, cyber resiliência e excelência operacional assegurando a tríade CIA subjacente à segurança da informação, a **C**onfidencialidade, **I**ntegridade e **D**isponibilidade

A certificação de um SGSI tem por base a ISO27001 enquanto standard internacional para gestão da segurança de informação. Contudo, os requisitos identificados por esta norma requer a utilização da norma ISO 27002 enquanto guia orientadora sobre a forma como estes controlos podem e devem ser implementados. Neste sentido, estas duas normas não devem ser desassociadas num processo de certificação de um SGSI.

A implementação da ISO 27001 deverá, tal como referido anteriormente, seguir a metodologia PDCA, onde se definem as etapas de implementação. A ISACA [46] identifica as seguintes etapas ou fases:

- *Business objectives and priorities;*
- *Existing IT maturity levels;*
- *User acceptability and awareness;*
- *Internal audit capability;*
- *Contractual obligations;*
- *Customer requirements;*
- *The enterprise's ability to adapt to change;*
- *Adherence to internal processes;*
- *Existing compliance efforts and legal requirements;*
- *Existing training programs.*

No que respeita a controlos de segurança, a ISO 27001 identificou e documentou 114 que constam num documento anexo à norma, aplicáveis a 14 domínios da segurança, intitulados de A-5 a A-18, conforme demonstra a figura 2.9

Figura 2. 10 Domínios da segurança de acordo com a ISO 27001, retirada de [47]

2.5 National Institute of Standards and Technology (NIST)

O National Institute of Standards and Technology (NIST) enquanto organização que se dedica à promoção da inovação e competitividade industrial materializada na definição de padrões, normas, orientações e tecnologia, teve a sua fundação em 1901 nos Estados Unidos. No que respeita a sectores de atividade, podemos verificar que a sua atuação é muito abrangente, não podendo deixar de incluir o sector da tecnologia e em particular da segurança. Uma das *frameworks* mais relevantes lançada pelo NIST para apoiar as organizações a implementarem mecanismos de controlo em diversos domínios organizacionais é a SP 800-53. Não se trata de uma framework recente, muito pelo contrário, atendendo que teve a sua primeira versão em 2005, sendo atualizada de forma regular para responder a novas tecnologias que imergem diariamente em função da evolução tecnológica sem nos inunda por vezes com pouca regulamentação. A sua abrangência, à semelhança da ISO27001, torna-a muito procurada pelas organizações e por outras *frameworks* que se baseiam nela, como sucede nas *frameworks* para a privacidade de informação ou para gestão de risco.

2.5.1 Framework for Improving Critical Infrastructure Cybersecurity (NIST)

O NIST elaborou uma *framework* com intuito de apoiar as organizações responsáveis por infraestruturas críticas [49] ao funcionamento da sociedade, a definir e implementar uma gestão de risco prudente e adequada à criticidade destas infraestruturas. É baseada na *framework* NIST Cybersecurity Framework (NCF) [50], tendo sido elaborada em 2013 e lançada durante o ano de 2014, revista e atualizada em 2018 com novas medidas e controlos para enfrentar as ameaças associadas a novas tecnologias que podem ser encontradas em IOT e IIOT [18] como forma de preparar estas organizações para a consciencialização e resposta aos ciberataques que podem ficar expostas em virtude da adoção de novas tecnologias, fruto das vulnerabilidades que as assolam. A *framework* assenta num modelo baseado em gestão de risco, acreditando o NIST que só tendo uma gestão de risco adequada é possível ter uma organização apta para adotar uma cultura orientada à prevenção contra as ameaças que a rodeiam. Na sua essência, a *framework* é composta por três componentes.

2.5.1.1 Framework Core

Nesta primeira componente são definidas as atividades, resultados esperados e referencias aplicáveis de forma equiparada em sectores de atividade semelhantes. Tudo o que são padrões de indústria, práticas, procedimentos e guias de orientação que permitam aplicar por toda a organização uma consciencialização para a cibersegurança com o apoio da gestão de topo para garantir o envolvimento de todos os colaboradores. O NIST identifica cinco funções core como contínuas e concorrentes. Estas funções destinam-se a organizar e priorizar atividades associadas à cibersegurança, visando numa perspetiva organizacional a gerir o risco cibernético, através de tomadas de decisão baseadas no resultado de uma análise de risco cuidadosa, permitindo à organização endereçar de uma forma mais realista as ameaças ao seu sistema de informação. Estas decisões podem resultar por exemplo no investimento em mais recursos humanos, formação dos atuais quadros ou investimento tecnológico.

Na imagem seguinte é apresentada a estrutura que compõe a componente core da NCF.

Figura 2. 11 Estrutura core da framework NIST para a Cibersegurança, retirada de [48]

Como podemos verificar na figura 2.14, a *framework* prevê quatro elementos, sendo elas as funções, categorias, subcategorias e referencias informativas. As **funções,** como mencionado em parágrafos anteriores, agrupam e organizam atividades relacionadas com cibersegurança ao nível da gestão de topo, definindo assim num plano mais estratégico como é feita a abordagem e metodologias para gestão de incidentes, as áreas onde deve ser feito um maior investimento financeiro e humano, entre outras, sempre com base numa gestão de risco.

As **categorias** são subdivisões feitas em cada uma das funções, através do agrupamento de atividades especificas que resultam de necessidade programáticas. Como exemplo, a gestão de fornecedores, gestão de acessos ou a gestão de activos.

No que respeita a **subcategorias**, podemos ver esta função como uma divisão mais detalhada ou mais baixa das categorias, ou seja, posicionam-se a nível dos controlos e ações concretas a implementar para mitigar riscos existentes nos activos. Se pensarmos na categoria de gestão de activos organizacionais, as subcategorias são os controlos implementados e práticas seguidas, como seja, a existência de normativo

para gestão de activos ou a utilização de uma ferramenta que faz a monitorização do ciclo de vida do activo, incluindo a sua monitorização.

As **Referências informativas** são normas, padrões e guias de orientação que abrangem todos os sectores de atividade que naturalmente têm infraestruturas críticas que servem de apoio e identificação aos controlos que são definidos em cada uma das subcategorias. O objetivo deste elemento é garantir a existência de uma cobertura exaustiva e abrangente todas as atividades, em linha com normas e padrões aplicáveis, independentemente do sector onde a organização esteja posicionada.

No que respeita às funções, o NIST considera cinco, enquanto atividades a seguir na gestão do ciberrisco, embora não exista uma hierarquia ou sequencia na execução destas funções, uma vez que poderão ser executadas de forma concorrencial ou alternada, dependendo da cultura e dimensão organizacional, ou ainda perante uma situação excecional que requeira uma avaliação de risco, como é o caso de um incidente de segurança, ou lançamento de uma nova aplicação ou serviço.

A figura seguinte representa as cinco funções pertencentes à componente core de *framework*.

Figura 2. 12 Funções core da framework NIST, retirada de [48]

1. **Identify –** Esta função procura endereçar quais os activos e processos que necessitam de ser protegidos, ou seja, fomentar uma cultura organizacional para gestão de risco de cibersegurança que englobe colaboradores, prestadores de serviço, processos, sistemas e normativo. Deve ser feito um levantamento exaustivo e detalhado dos processos críticos de negócio, assim como das soluções que os suportam, de forma a serem prioritizados em matéria de gestão de risco e investimento. No essencial esta função atua mais ao nível da estratégia organizacional para a cibersegurança suportada em gestão de risco, definindo o modelo de governo tático e técnico onde a organização deve posicionar-se.

2. **Protect** – Nesta função a *framework* procura definir, desenvolver e implementar as medidas de segurança necessárias para a entrega de serviços. A função visa também a criação de mecanismos para conter e minimizar o impacto causados por atividades maliciosas, como por exemplo, um incidente de segurança.

3. **Detect –** Identificar a ocorrência de incidentes de segurança é o principal objetivo desta função. Num sentido mais lato, é necessário implementar mecanismos para deteção atempada de eventos associados a incidentes de segurança. Este objetivo é atingidos através de inúmeras atividades, desde a monitorização, análise de comportamento de anómalos.

4. **Respond -** Quais as técnicas e táticas que devem ser implementadas para conter o impacto de incidentes? Esta função visa primordialmente responder a este dilema, que depende muito da tipologia, intensidade e duração do incidente.

5. **Recover -** Depois de um incidente de segurança ter sido contido, entra-se na fase de recuperação, ou seja, executar as atividades necessárias para recuperar as infraestruturas e os serviços impactados com o incidente, garantir que o plano de resiliência foi restaurado e implementadas melhorias por forma a evitar a repetição do incidente. Decorre ainda nesta função as comunicações necessárias atendendo que nesta fase dá por terminado o ciclo de atividades inerentes ao incidente de segurança.

2.5.1.2 Framework Implementation Tiers

A segunda componente da *framework* foca-se na vertente de gestão de risco numa perspetiva de camadas que contextualizam a forma como a organização perceciona e atua perante o ciberrisco, assim como tem definidos os processos que o suportam. Para isso, o NIST definiu uma escala que varia entre 1 e 4, sendo o valor 1 o mais reduzido e classificado como *Partial* e o mais elevado de *Adaptive*. Estes níveis permitem enquadrar a organização quanto a maturidade do seu processo de gestão de risco para a cibersegurança, apoiando a integração da gestão de risco cibernético enquanto função essencial e apoiada

pela gestão de topo. A organização deve considerar e integrar o risco cibernético no risco global, onde se avaliam outros riscos, como o risco operacional, de negócio, reputacional ou financeiro. Esta integração permite colocar o risco para a cibersegurança num patamar onde é valorizado, gerido formalmente e regido por normas, processos e práticas internas à semelhança dos restantes.

Uma outra vertente igualmente relevante são as obrigações legais e regulamentares que os prestadores de infraestruturas e serviços essências são obrigado a cumprir, e evidenciar que o fazem e como o fazem. Também esta avaliação permite avaliar a maturidade, ajudando a enquadrar a gestão de risco cibernética no nível mais adequado que a escala disponibiliza. Sabendo que a gestão de risco não funcionará de forma correta enquanto não tiver o apoio da gestão de topo, e a partir do momento que apoia, deverá fornecer os recursos necessários à sua execução. Recursos estes que podem ser humanos, materiais, tecnológicos ou processuais, mas suficientes para uma gestão de risco eficaz. Não é necessário a utilização de uma ferramenta tecnologicamente avançada para apoiar o processo de gestão de risco, se por outro lado não existir por exemplo, um registo actualizado dos activos, a sua criticidade e o responsável pelos mesmos.

A gestão de risco tem de ser uma prática constante e evolutivo, atendendo que nenhuma organização quando é constituída terá uma maturidade elevada nos seus processos, mas percebendo a importância que têm e praticando-a no seu dia a dia, a exigência vai sendo cada vez maior e com isso aumenta a maturidade e naturalmente a resiliência e preparação para enfrentar ciberataques. Nunca estará imune, mas certamente mais apta para responder.

Na figura seguinte estão representados os 4 níveis onde uma organização poderá ser enquadrada quando à maturidade do seu processo de gestão de risco e maturidade para a cibersegurança.

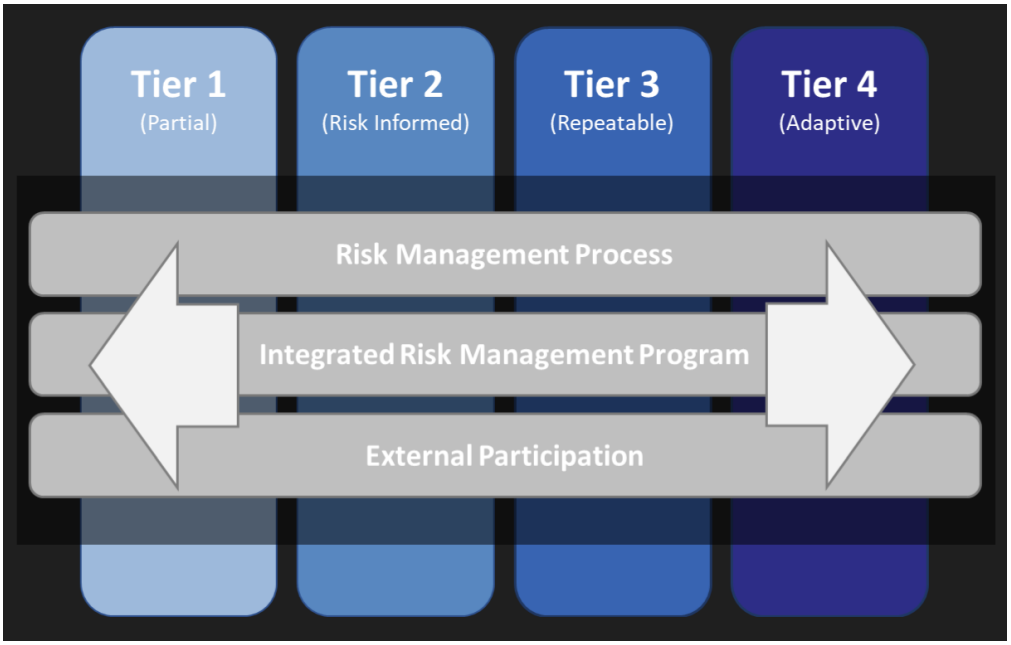

Figura 2. 13 Níveis para enquadramento de maturidade definidos pelo NIST, retirada de [49]

1. **Tier 1 (Parcial)** – Uma organização enquadrada neste nível, não tem ainda os seus processos de gestão de risco formalizados nem documentados, fazendo uma gestão ad-hoc e nem sempre em linha com os objetivos organizacionais. Não são definidas nem priorizadas atividades, atendendo que a gestão de risco não define guias orientadoras devido ao seu grau de imaturidade. A gestão de risco não é uma preocupação, nem vista como uma função importante, estando muito posicionada sobre si mesma, não interagindo com elementos externos, como sejam parceiros de negócio, clientes, fornecedores ou entidades reguladoras. Tendencialmente estas organizações estão mais suscetíveis a ciberataques e com maior dificuldade em lidar com eles, em virtude da sua inoperabilidade na preparação para este cenário.

2. **Tier 2 (Risk Informed) –** A gestão de topo já participa no processo de gestão de risco, apoiando a sua execução, embora não haja um formalismo para isso. A priorização das atividades referentes à cibersegurança e protecção do sistema de informação são delineadas pelos requisitos definidos pelo risco organizacional. Existe uma consciencialização para a cibersegurança e para o risco que isso acarreta, mas não está definido o processo para gerir estes riscos. Internamente a gestão de risco é abordada de uma forma informal e apesar de existir uma gestão de risco não processual, não é realizada de forma regular nem repetitiva. A organização perceciona a sua função no ecossistema

onde se insere, as suas obrigações e o seu relacionamento com outras entidades, mas não tira partido de informação relevante que lhe pode ser fornecida para fortalecer os seus processos internos, assim como a robustez dos seus activos.

3. **Tier 3 (Repetable) –** A organização dispõe de políticas e normas para gestão do risco cibernético, sendo o seu processo formalmente aprovado. É seguida uma metodologia baseada em melhoria continua e atualização das suas práticas de gestão de risco, para melhor responder aos ciberrisco. Este processo de gestão de risco é transversal a toda a organização e formalmente aceite, monitorizando-o de forma regular, bem como todas as componentes que o suportam, sejam activos, processos, procedimentos ou tecnologias. O Risco é comunicado de forma regular e formal à gestão pela área responsável, sendo o processo documentado em todas as etapas pela equipa mais operacional e revisto por equipas seniores. Estas equipas possuem formação especializada à execução das suas tarefas. Neste nível de risco existe uma vasta interação com elementos externos para partilha, envio e receção de informação com vista a apoiar e melhorar a gestão de risco.

4. **Tier 4 (Adaptive) –** No nível adaptável a organização implementa as suas atividades relativas à cibersegurança fundamentada em práticas e experiências anteriores e atuais, usufruindo de lições aprendidas e indicadores preventivos. A melhoria contínua faz parte integrante do processo de gestão de risco que é suportado em tecnologia e boas práticas, tendo a capacidade de adaptar-se de forma ágil à mudança, para melhor responder à imergentes e constantes ciberameaças. Organizacionalmente existe uma abordagem para gestão de riscos cibernéticos, suportada em políticas e processo bem definidos, que se materializam em procedimentos e tarefas orientados para resposta a incidentes de cibersegurança. A união entre a gestão de risco e a segurança dos sistemas de informação está em harmonia com os objetivos organizacionais definidos e suportam as tomadas de decisões. Os elementos mais seniores asseguram que o processo é seguido da forma correta e apoiam na conjugação do risco cibernético com outros riscos organizacionais. Neste nível a organização perceciona o seu papel, dependências e dependentes, contribuindo de forma ativa no ecossistema e comunidade onde está integrada. A troca de informações relevantes ocorre de forma regular e nos dois sentidos, antecipando incidentes de cibersegurança em virtude da proatividade e partilha de informações sobre vulnerabilidades e tipologias de ataques que normalmente são comuns entre organizações no mesmo setor de atividade.

   Os colaboradores fazem programas de formação e sensibilização de forma regular sobre cibersegurança, fazendo parte dos seus objetivos anuais de formação.

2.5.1.3 Framework Profile

A terceira e última componente funciona como elo entre as funções, categorias e subcategorias com os objetivos e requisitos organizacionais, o apetite e tolerância a riscos e activos. O perfil leva a organização a definir um rumo para reduzir o risco cibernético alinhado com os requisitos organizacionais, regulares, setoriais ou da indústria aplicando as melhores práticas na sua operacionalização. Cada organização é única pelo seu modelo de gestão, setor de atividade ou pelos serviços que disponibiliza, podendo optar por ter diversos perfis. Estes perfis podem ser utilizados de duas formas distintas, ou seja, para enquadrar a organização no estado onde de encontra mediante a avaliação realizada, mas também pode servir para definir o estado futuro onde pretende estar em determinada altura, definindo para isso os requisitos e objetivos necessários para atingir essa meta.

Os perfis funcionam como alicerces para os requisitos de negócio e na comunicação do risco internamente e entre organizações. Não existem perfis padronizados, porque isso seria difícil de implementar, atendendo às especificidades de cada organização, sendo totalmente flexíveis e adaptados à organização alvo.

2.5.2 Modelo para avaliação de maturidade NIST

No capítulo anterior foi analisada a NCF em termos de enquadramento organizacional no que respeita à sua maturidade para gestão do risco cibernético, enquanto parte integrante para melhorar a resiliência em matéria de cibersegurança nas infraestruturas críticas. O Departamento de Energia dos Estados Unidos com o apoio do NIST, lançou uma *framework* com o objetivo de suportar o processo de avaliação de maturidade que inclui uma vertente processual, e uma ferramenta que visa facilitar o cálculo, existindo um mapeamento bidirecional os controlos elencados nesta framework e aqueles que são identificados na NCF. Apelidada de Cybersecurity Capability Maturity Model (C2M2) [51] e lançada inicialmente em 2012, teve atualizações em 2014 e 2019, sendo desenvolvida em estreita colaboração o Governo americano, indústrias sob orientação do departamento energético e de segurança interno e como referido anteriormente, teve a colaboração do NIST. O objetivo inicial desta framework era apenas de apoiar organizações que operavam infraestruturas críticas, mas rapidamente foi estendido a todos os setores de atividade que operam sistemas de informação e tecnologias no geral. Enquanto a NCF previa quatro níveis ou camadas a C2M2 definia apenas três e no que respeita a domínios de segurança, processos, subcategorias e capacidades é igualmente inferior quando comparada com a NCF.

Uma outra framework lançada para avaliar o nível de maturidade de uma organização, foi a Cybersecurity Maturity Model Certification (CMMC) [52], criada pelo Departamento de Defesa dos Estados Unidos em 2019. Desde a sua criação foram surgindo diversas atualizações, encontrando-se em

vigor a versão 2.0 desde o final de 2021. Esta framework que tem associado uma certificação prevê três níveis de maturidade, sendo o nível 1 identificado como *Foundational*, o 2º de *Advanced* e 3º nível de *Expert*. O modelo inicial desta *framework* foi concebido com 5 níveis de maturidade. Na figura seguinte é apresentada uma comparação entre as duas versões desta *framework*.

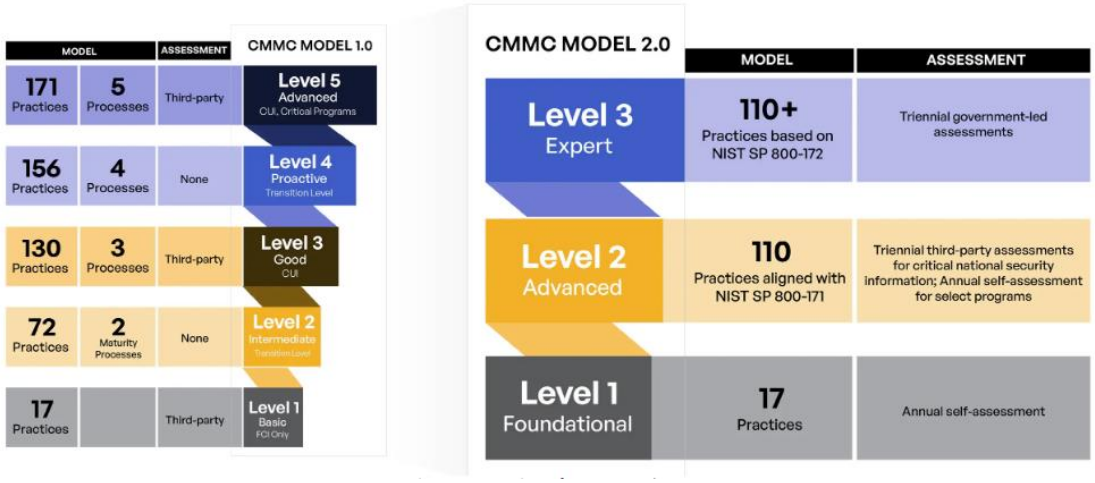

Figura 2. 14 Mapeamento entre os níveis de maturidade nas duas versões de CMMC, retirada de [53]

Como referido anteriormente, os níveis pretendem enquadrar a maturidade e o grau de preparação e prontidão para a cibersegurança, mas valida também os processos e a tecnologia existente que suportam atividades de monitorização, prevenção e reação a incidentes de segurança.

A figura seguinte demonstra graficamente as 5 Funções da NCF alinhadas com os 5 níveis de maturidade do CMM

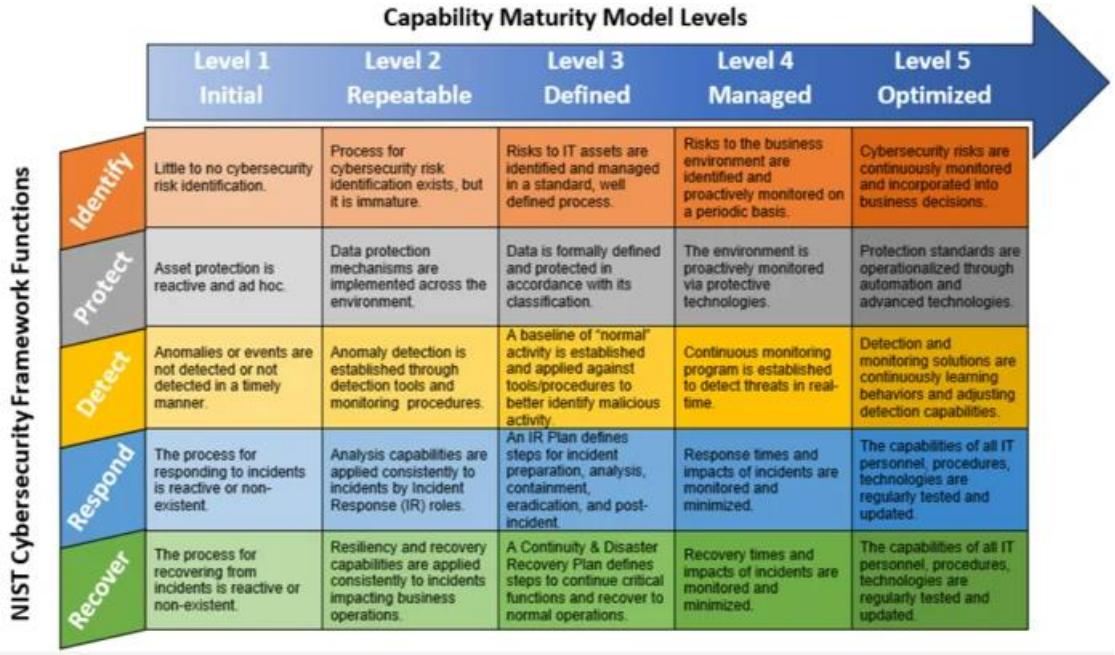

Figura 2. 15 Mapeamento das Funções da NCF com a CMM, retirada de [54]

1. **Level 1 (Initial) -** Organizações que apresentam pouco formalismo, as suas atividades são geridas de forma ad-hoc, sem processos definidos e atuando reactivamente em matéria de cibersegurança, classificam-se no nível 1 ou inicial na escala de maturidade. Existe uma baixa consciencialização e aptidão para a cibersegurança, com uma total ausência de formalismos em tomadas de decisão, não existindo documentação.

2. **Level 2 (Repeatable) –** Neste nível já é expectável que uma organização tenha definido alguns processos para gestão de risco, ainda que possa estar num estágio imaturo e apenas contemple uma parte da organização. Os mecanismos de protecção dos activos organizacionais estão identificados e parcialmente implementados e nem sempre com os requisitos bem definidos, como por exemplo a vertente de monitorização é realizada de forma pouco formalizada e em modo repetitivo. A consciencialização para a cibersegurança é percecionada com os colaboradores a terem capacidades em áreas especificas, embora não seja transversal a toda a organização.

3. **Level 3 (Defined) –** Organizações enquadradas com este nível de maturidade definem as funções e responsabilidades dos seus quadros, assignando-lhes formalmente essa responsabilidade e dando formação para tal. Os processos são definidos e padronizados em alinhamento com a estratégia

organizacional e com apoio da gestão de topo. A tecnologia para suportar atividades que envolvem a cibersegurança é implementada de forma adequada e aos requisitos definidos, embora esta prática possa ainda não ser comum a toda a organização.

4. **Level 4 (Managed) –** As atividades dos colaboradores são bem definida, avaliadas e geridas em função das suas atividades, tendo a formação adequada à execução dessas atividades. As políticas e processos internos são implementados de acordo com padrões, sendo avaliada a sua aplicabilidade em função do que está definido. Os processos tecnológicos são definidos em virtude dos requisitos e da estratégia para a cibersegurança, com medição e avaliação de forma regular.

5. **Level 5 (Optimized) –** As políticas, processos e procedimentos internos são revistos e atualizados em linha com as mudanças organizativas, requisitos legais e ajustes necessários para melhor responder a ameaças resultantes da adoção a novas tecnologias, ciberataques ou qualquer outra mudança com caracter de urgência. A proatividade é uma atitude que rege a organização permitindo-lhe encarar a mudança de forma positiva pelos seus colaboradores, que facilmente aderem a alterações estruturais, processuais e tecnológicas.

Os modelos e *standards* apresentados ao longo das seções deste capítulo, foram relevantes na definição da metodologia desenvolvida. A definição da escala para apuramento do nível de maturidade, os domínios utilizados e os controlos utilizados serão exemplo disso. Pelo fato de se tratarem modelos robustos, utilizados mundialmente e em diversos setores de atividade, dão confiança suficiente para erem reutilizados. Acreditamos que a utilização de modelos e *standards* permite que a avaliação de maturidade à infraestrutura seja realizada e forma objetiva e realista.

Capítulo 3

DO CONTEXTO NACIONAL À GESTÃO DE RISCO: UMA PERSPETIVA

A última década tem sido enriquecedora no que respeita a conteúdos produzidos com o objetivo de sensibilizar e consciencializar os cidadãos e as organizações para a temática da segurança informática, em resultado do aumento generalizado do cibercrime e das burlas informáticas. Algumas das organizações da especialidade têm disponibilizado metodologias e *frameworks* que ajudam as organizações na gestão de risco dos seus activos, com o intuito de as tornar mais resilientes a ciberataques, ajustando de forma progressiva estas *frameworks* em função de novas tipologias de ataques que vão surgindo e que obrigam estas organizações a atuar de forma rápida e eficaz [5]. Uma das primeiras etapas que algumas *frameworks* de gestão de risco endereçam é a identificação dos riscos, e para isso é essencial que haja um conhecimento claro de quais são os activos organizacionais, a sua criticidade, e os riscos inerentes aos mesmos. Sem esta informação, qualquer análise de risco não produzirá os resultados corretos e levará a organização a uma situação de desconhecimento sobre as suas fragilidades e riscos, e por isso, a um grau de exposição que a coloca perante cenários de ataques informáticos que não está preparada para enfrentar. Adicionalmente, uma má análise de risco levará a organização e por outro a fazer investimentos em áreas que podem não ser aquelas que apresentam uma maior fraqueza ou urgência de intervenção.

3.1 Contexto legal e de regulamentação nacional

3.1.1 Infraestruturas críticas

A CE define infraestruturas críticas como sendo activos ou sistemas essenciais à manutenção das funções vitais da sociedade, cujo qualquer dano causado sobre o funcionamento das mesmas, terá um impacto significativamente negativo para a segurança da União Europeia (UE) e sobre o bem-estar dos seus cidadãos [6]. Já o *National Institute of Standards and Technology* (NIST) [7], no contexto norte-americano, têm uma visão mais ampla, definindo estas infraestruturas como sendo activos físicos ou virtuais de importância vital para o Estados Unidos, cuja incapacitação ou destruição se traduz num impacto debilitante para o país, na segurança económica, na saúde publica interna ou em qualquer combinação destas áreas. Alguns países passaram a incluir na sua estratégia de defesa, as infraestruturas primordiais que permitem o funcionamento e a operacionalidade do país, de forma a poderem salvaguardar o seu funcionamento. O

Estado português, através da Lei 46/2018 [8] define uma infraestrutura crítica como sendo a componente, sistema ou parte deste, situado em território nacional, que é essencial para a manutenção de funções vitais para a sociedade, saúde, segurança e o bem-estar económico ou social, cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções.

3.1.2 Serviços Essenciais

De forma a se enquadrar os serviços essenciais [9] numa perspetiva de criticidade como vitais para a sociedade, a CE por meio de legislação criada para essa finalidade, identificou aqueles que seriam os setores fundamentais para o funcionamento da economia dentro do espaço comunitário, enumerando quais os serviços essenciais [10]. Sendo enquadrados os seguintes setores:

- Setor Energético;
- Setor dos transportes;
- Setor bancário;
- Setor infraestruturas de mercado financeiro;
- Setor da Saúde;
- Setor do fornecimento e distribuição de água potável;
- Setor das infraestruturas digitais.

O governo norte-americano [11], por sua vez além dos setores identificados pela CE, definiu nove adicionais, perfazendo um total de dezasseis setores como sendo vitais ao funcionamento da sua economia.

A identificação de todos estes serviços que foram classificados como essenciais é de extrema importância por permitir associá-los a operadores e organizações com responsabilidade sobre os mesmos, tendo estes operadores o dever de zelar pela segurança das infraestruturas que suportam o funcionamento de serviços essenciais.

3.1.3 Enquadramento regulamentar

A preocupação da CE em proteger e salvaguardar o funcionamento contínuo de infraestruturas críticas nos seus estados-membros não é recente, tendo já em 2004 sido lançado o Programa Europeu para Protecção de Infraestruturas Críticas (EPCIP) [12], levado a cabo pela *Critical Infrastructure Warning Information Network* (CIWIN). Este programa surgiu ainda no rescaldo dos atentados de onze de setembro de 2001 [13], ocorridos nos Estados Unidos da América (EUA), que despertaram o mundo para a ameaça terrorista sobre pessoas e bens, que deixara de ser só uma ameaça para ser uma realidade. Este

acontecimento consciencializou para a necessidade de proteger infraestruturas e serviços críticos para cenários de indisponibilidade que não, sendo devidamente acautelados podem impactar pessoas, organizações e, no limite, setores essências à sociedade. Os ataques terroristas ocorridos em 2004 em países europeus vieram reforçar a necessidade de um programa deste programa de protecção para infraestruturas críticas. Se na origem do programa esteve a ameaça terrorista sobre infraestruturas físicas públicas e privadas, as catástrofes naturais que assolaram algumas partes do mundo alguns anos mais tarde, por meio de furacões, tsunamis, sismos ou incêndios, demonstraram a importância que este programa de protecção assume perante diversos tipos de ameaças, sejam elas de origem intencional, não intencional, ou causada por fenómenos naturais.

Em 2008 a CE lançou a Diretiva 2008/114/EC, em complemento do normativo anterior, vindo reforçar o conceito de infraestruturas críticas no contexto da UE, definindo já a forma como estas infraestruturas devem ser avaliadas e protegidas para manter a sua operacionalidade, evitando disrupções para esse país e propagação ou contágio aos países vizinhos, trazendo naturalmente impacto à UE como um todo. Nesta diretiva são publicados critérios que permitam aos estados-membros definir, de norma equiparada aquelas que são as suas infraestruturas críticas e a estratégia a seguir na protecção das mesmas, envolvendo os operadores responsáveis por essas infraestruturas.

A diretiva europeia abordada anteriormente era muito orientada a apoiar os estados-membros a implementar uma estratégia de segurança em infraestruturas para cenários associados a atos de terrorismo, vandalismo e causas naturais. Porém, era necessário ir além destas ameaças e proteger também redes e a informação no contexto da UE, sendo criada em 2016 a diretiva 2016/1148 [2] para esse efeito. Esta diretiva reflete uma preocupação acrescida com serviços essenciais que sejam disponibilizados através de redes de comunicações e a necessidade de proteger as mesmas, sob pena de a sua inutilização ter efeito cascata para o estado-membro, com possibilidade de afetar estados vizinhos. Para que haja um maior controlo e cooperação entre os estados-membros da UE para responder às ameaças que também são comuns é definido que cada estado deverá ter uma entidade única que fornecerá linhas de orientação e apoio às entidades públicas e privadas a definirem a sua estratégia para a cibersegurança, funcionando também como ponto único de receção de incidentes de segurança, que as organizações identificadas nesta diretiva são obrigadas a reportar, onde se incluem incidentes com violação de dados pessoais (que pouco tempo depois teria um regulamento especifico, com entrada em vigor a 25 de Maio de 2018 o Regulamento Geral sobre a Protecção de dados (RGPD) [13]).

A diretiva da CE 2016/1148 [2], que têm obrigatoriedade de implementação em cada estado-membro sendo transposta para território nacional através da Lei 46/2018 [8], visando estabelecer o Regime Jurídico da Segurança do Ciberespaço (RJSC), com o intuito de uniformizar a implementação de medidas

de segurança das redes e sistemas de informação na UE. É ainda definida de forma explicita quem são as entidades às quais é aplicada a lei:

- A administração pública;
- Os operadores de infraestruturas críticas;
- Os operadores de serviços essenciais;
- Os Prestadores de serviços digitais;
- Outras entidades que sejam utilizadoras de redes e sistemas de informação.

De forma a identificar inequivocamente as organizações que se enquadram no âmbito da lei, foram criados capítulos específicos para cada uma das entidades alvo. Relativamente à **Administração Pública** são abrangidas pela lei as seguintes estruturas:

- O estado português;
- Regiões autónomas;
- Autarquias locais;
- Entidades administrativas que atuem de forma independente;
- Institutos públicos;
- Empresas públicas;
- Associações públicas.

Para uma correta interpretação sobre os **operadores de infraestruturas críticas**, é necessário entender o que são infraestruturas críticas, e sobre isso, a lei descreve-as como uma componente, um sistema ou parte deste, que estando situado em território nacional é fundamental para o funcionamento de funções vitais para a sociedade, segurança e o bem-estar económico ou social, e cuja perturbação ou destruição, terá um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções. No que respeita ao operador, trata-se de uma entidade pública ou privada que opera e têm responsabilidade sobre uma infraestrutura crítica. A CE consciente da necessidade em proteger infraestruturas críticas europeias, aprovou a 8 de dezembro de 2008 a diretiva 2008/114/CE [33] relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua protecção. Nesta diretiva a CE identifica os sectores da energia e dos transportes como aqueles que que requerem maior vigilância e protecção sob pena de causar elevados impactos quando são alvo de ataque, seja provocado por causas humanas ou naturais. De salientar que esta diretiva é publicada no rescaldo de diversos ataques terroristas ocorridos em países europeus, nomeadamente o 11 de setembro de 2001 ocorrido nos Estados Unidos que revolucionou o mundo no que à segurança diz respeito. A diretiva 2008/114 foi transposta para o território português através do decreto-lei 62/2011 [34], aprovado a 9 de maio de 2011. Como referido anteriormente

o foco do decreto-lei eram apenas os sectores da energia e transportes, incidindo sobre os seguintes subsectores:

- Sector energético
    - Eletricidade – Infraestruturas e instalações de produção e transporte de eletricidade, em termos de abastecimento;
    - Petróleo – Produção, refinação, tratamento, armazenagem e transporte de petróleo por oleodutos;
    - Gás – Produção, refinação, tratamento, armazenagem, transporte de gás por gasodutos e terminais para gás natural liquefeito;
- Sector dos transportes
    - Transportes rodoviários;
    - Transportes aéreos;
    - Transporte por vias navegáveis interiores;
    - Transporte marítimo, transporte marítimo de curta distância e portos

Contudo, cabe a cada membro da UE a obrigatoriedade de aplicar os critérios sectoriais para que numa primeira fase efetuem uma seleção das infraestruturas críticas em cada um dos sectores elencados pelo decreto-lei. Após terminada esta fase, cada membro seleciona aquelas que são as infraestruturas críticas tendo por base a sua definição e caracterização, avaliando em seguida o impacto que a mesma representa para cada estado-membro. Esta avaliação é realizada utilizando métodos definidos por cada membro, podendo ser complementada por critérios transversais, tendo em conta as alternativas existentes que possam assegurar o funcionamento destas infraestruturas de acordo com a duração da indisponibilidade. É igualmente responsabilidade de cada membro aplicar o elemento transfronteiriço definido para as infraestruturas críticas que tenham sido identificadas em âmbito da diretiva europeia para que assim se assegurar que são implementados os controlos necessários a protegê-las.

O aumento do cibercrime de forma generalizada e em particular na UE, levou ao surgimento do decreto-lei 46/2018 [8] onde é definido o Regime Jurídico da Segurança do Ciberespaço que mais tarde é regulamentado pelo decreto-lei 65/2021 [16] como forma de enfrentar esta ameaça e poder inverter esta tendência, obrigando as organizações a cumprir requisitos no que à segurança e á utilização do ciberespaço diz respeito. Perante esta realidade, foi necessário alargar os operadores de infraestruturas críticas nos setores identificados no decreto-lei 62/2011 [34] a outros que são igualmente críticos e cujo cibercrime tem procurado afetar.

Neste sentido, a 28 de janeiro de 2022 é aprovado o Decreto-Lei 20/2022 [32] que revoga o decreto-lei 62/2011, visando estabelecer os procedimentos para identificação, designação, protecção e

aumento da resiliência das infraestruturas críticas nacionais e europeias, requerendo a definição e implementação de mecanismos que capacitem estas infraestruturas de uma maior protecção e resiliência em cenários de disrupção, devendo assegurar níveis de disponibilidade que permitam continuar a operar mesmo em cenários excecionais. Este decreto-lei aplica-se a todas as estruturas europeias nos setores da energia e dos transportes assim como a todas as estruturas nacionais nos seguintes setores de atividade:

- Comunicações;
- Infraestruturas digitais e prestadores de serviços digitais;
- Abastecimento público de água e tratamento de resíduos;
- Alimentação;
- Saúde;
- Indústria;
- Serviços financeiros:
  - Setor bancário;
  - Mercados de instrumentos financeiros;
  - Setor regulador e dos fundos de pensões;
- Órgãos de Soberania e Governação;
- Segurança:
  - Infraestruturas da NATO;
  - Infraestruturas de defesa nacionais;

No que respeita a **Operadores de Serviços Essenciais**, segundo o decreto-lei 46/2018 [8] trata-se de uma entidade pública ou privada que presta um serviço essencial, enquadrada nos setores identificados nos capítulos anteriores, suportados em infraestruturas que dependem destas para funcionarem. Contudo, cabe ao CNCS atualizar anualmente a lista dos operadores de serviços essenciais.

Um **Prestador de Serviços Digitais** segundo o decreto-lei 46/2018 [8], é uma pessoa coletiva que presta um serviço digital, a saber, serviço de mercado em linha, serviço de motor de pesquisa em linha ou serviço de computação em nuvem.

3.1.4 Decreto Lei 65/2021

O decreto-Lei 65/2021 [16] aprovado a 30 de julho de 2021, surge como meio de regulamentar o Regime Jurídico da Segurança do Ciberespaço (RJSC), definindo as obrigações respeitantes à certificação da cibersegurança em execução do Regulamento 2019/881 [31] do Parlamento Europeu, aprovado a 17 de abril de 2019. O RJSC foi aprovado através da Lei 46/2018 [8] que transpôs para território nacional a

diretiva europeia 2016/1148 [2] de 6 de julho de 2016, visando obter uma base comum com elevados padrões de segurança para redes e sistemas de informação de forma transversal a toda a UE. Esta diretiva define regras claras em matéria de requisitos de segurança, e notificação de incidentes que as entidades e organizações abrangidas, teriam obrigatoriamente de cumprir.

Num mundo cada vez mais digital e baseado em tecnologias imergentes, as organizações não funcionam de forma isolada, necessitam de expor os seus serviços e produtos aos clientes de forma permanente, simplificada e segura. Estas qualidades podem ser uma vantagem competitiva, perante a vasta oferta de serviços que hoje os consumidores têm ao seu dispor. Esta exposição é inevitável e muito útil numa perspetiva de atratividade e fidelização de clientes, mas também pode ser utilizada e explorada de forma negativa por quem procura obter benefícios de forma ilegítima. Com base nesta realidade as organizações devem implementar mecanismos que protejam os seus serviços de uso abusivo e indevido, sabendo que esta ameaça é permanente e pode surgir de qualquer parte do globo, podendo apenas ser combativa ou pelos enfraquecida por meio da implementação de controlos eficazes e com abrangência transversal.

Atendendo a uma constante mutuação do ciberespaço, a sua regulação deverá ser sustentada por políticas transnacionais que visam uma cooperação internacional que somente através do fundamento e partilha de conhecimento é possível encarar e combater a ameaça global do cibercrime. A união de esforços e cooperação entre países, em oposição ao individualismo poderá fazer toda a diferente no confronto às ameaças surgidas diariamente, sem rosto nem identidade, mas determinadas a explorar novas técnicas, táticas e procedimentos. Não obstante outras obrigatoriedades que as entidades tenham de cumprir perante reguladores e organismos de supervisão, o DL 65/2021 [16] visando regular o RJSC define os seguintes princípios e regras gerais:

- Cumprimento dos requisitos identificados no decreto-lei, através da definição e aplicação de medidas técnicas e organizativas obedecendo ao princípio da adequação e proporcionalidade, tendo em conta por um lado as condições normais de funcionamento das redes e dos sistemas de informação, e por outro as situações que levem a cenários de exceções, associados a:
    - Incidentes de segurança que causem um efeito adverso e real na segurança das redes e sistemas de informação;
    - Incidentes de segurança de criticidade grave ou catástrofe que possam requerer a ativação de planos de emergência de protecção civil;
    - Declaração do estado de emergência, guerra ou de sítio;
    - Ativação de planos no âmbito do planeamento civil de emergência no setor da cibersegurança;

- Ocorrência de uma ameaça grave à segurança interna, incluindo as situações de ataques terroristas, nos termos previstos, nas disposições legais e regulamentares aplicáveis em matéria de segurança interna.

- Obrigatoriedade na notificação de incidentes em conformidade com as disposições respeitantes à segurança de matérias classificadas em âmbito nacional e em âmbito das organizações internacionais de que Portugal seja parte;
- O cumprimento dos requisitos de segurança e da obrigação na notificação de incidentes previstos no RJSC não se sobrepõem ou anulam obrigações de reporte a outras entidades de supervisão e reguladoras, como seja a Autoridade Nacional de Protecção de Civil (ANPC), Autoridade Nacional de Comunicações (ANACOM), a Comissão Nacional de Protecção de Dados (CNPD) ou outras autoridades setoriais, nos termos das disposições legais e regulamentares em vigor, bem como toda a legislação emitida pela União Europeia;
- No caso de prestadores de Serviços Digitais aplicam-se os requisitos impostos pelo Regulamento de Execução da União Europeia 2018/151 [35] em matéria de segurança e notificação de incidentes;
- As entidades abrangidas por este DL podem estabelecer formas de colaboração entre si com vista a melhor cumprirem com a implementação dos requisitos de segurança, assim como a notificação de incidentes prevista pelo RJSC e assim partilharem informação, conhecimento e experiência para assegurarem uma efetiva operacionalização por cada uma dessas entidades. Contudo, essa partilha não poderá desresponsabilizar a entidade perante um cenário de infração;
- O Centro Nacional de CiberSegurança (CNCS) poderá estabelecer condições especificas para o cumprimento dos requisitos de segurança e notificação de incidentes por parte das entidades da Administração Pública, numa lógica proporcional e adequados à sua dimensão e complexidade organizacional.

O DL 65/2021 estabelece princípios de obrigatoriedades que as entidades abrangidas devem seguir e responder com vista ao cumprimento dos requisitos de segurança estabelecidos RJSC, no que respeita à implementação de medidas, procedimentos e prazos.

- **Ponto de contacto permanente -** Uma das obrigatoriedades do DL é a disponibilização de um ponto de contacto permanente que seja mandatado e capaz de responder operacional e tecnicamente e assim garantir os fluxos com o CNCS. Perante um incidente com impacto relevante ou substancial é necessário obter informação especifica para reportar ao CNCS. Este contacto deverá estar acessível 24x7x365 e cumprir com os prazos definidos para

reporte de incidentes. Para facilitar e garantir que todas as entidades disponibilizam o mesmo conteúdo de informação, o CNCS disponibiliza um *template* para esse fim.

- **Responsável de segurança –** Cada entidade tem por si a obrigatoriedade de identificar e designar um responsável de segurança, que tem como função o garantir que são aplicadas medidas com vista a assegurar os requisitos de segurança e de notificação de incidentes. A comunicação ao CNCS do responsável de segurança além de obrigatório, existem prazos estabelecidos para que esta comunicação ocorra, bem como a tipologia de informação requisitada.
- **Inventário de ativos –** Manter uma lista atualizada de activos, além de uma boa prática na gestão de risco nos sistemas de informação de uma organização, também é obrigatória ao abrigo do DL 65/2021, bem como sua comunicação ao CNCS numa base anual
- **Plano de segurança –** Cada entidade abrangida tem obrigatoriedade de definir e manter actualizado o seu plano de segurança, onde conste declarada a sua política de informação, as medidas técnicas e organizativas, assim como a formação dos seus colaboradores. Deverão ainda constar as medidas aplicadas no que respeita a requisitos de segurança e notificação de incidentes. Neste plano deve também constar informação sobre o responsável organizacional pela segurança e um contacto permanente.
- **Relatório anual -** A elaboração e entrega anual de um relatório, com o DL65/2021 passa a ser mais uma obrigatoriedade, com datas estipuladas e assinado pelo responsável pela segurança da entidade. O CNCS tem disponível um documento com vista a orientar as entidades sobre o tipo de informação que deve ser compilada, bem como o seu detalhe, podendo o formato de entrega ser ajustado para acolher a informação que se pretende enviar.
- **Análise dos riscos e implementação dos requisitos de segurança –** A Administração Pública, os operadores de infraestruturas críticas e operadores de serviços essenciais têm a responsabilidade de realizar uma avaliação de risco aos seus activos de forma a garantir o funcionamento e continuidade das redes e dos sistemas de informação. No caso dos operadores de serviços essenciais deverão ainda ter em conta os activos que suportem serviços essenciais, tendo por base os seguintes critérios:
    - **Análise de âmbito global** - A realizar pelo menos uma vez por ano, mediante notificação do CNCS sobre um risco, ameaça ou vulnerabilidade com elevada probabilidade de ocorrência que sendo materializável causará um impacto relevante;

- **Análise de âmbito parcial -** A realizar sempre que ocorram alterações em ativos ou após a ocorrência de um incidente com impacto relevante ou outro evento relevante que tenha impacto nos ativos. À semelhança da análise de âmbito global, neste âmbito mais restrito, o CNCS poderá enviar uma notificação à entidade sobre um risco, ameaça ou vulnerabilidade com elevada probabilidade de ocorrência e sendo materializável causará um impacto relevante.

Embora não seja especificada ou obrigatória na utilização de uma metodologia especifica para avaliação de risco, o CNCS disponibiliza um guia para gestão de riscos em matéria de segurança nos sistemas de informação como forma de apoiar as entidades neste processo. A avaliação deve ser o mais completa possível, suportada e documentada nas fases de preparação, execução e a demonstração dos resultados obtidos.

- **Notificação de incidentes –** As entidades abrangidas pelo DL 65/2021 têm de notificar o CNCS perante a ocorrência de qualquer incidente cujo impacto seja relevante ou substancial em cumprimento com os artigos 15,17 e 19 do RJSC. Está ainda em âmbito de notificação os incidentes que sejam detetados pela própria entidade ou que lhe comunicada por clientes, utilizadores ou proveniente de outra fonte. É uma obrigação de cada entidade definir e implementar os meios e aos procedimentos necessários para detetar, avaliar o impacto e comunicar mediante os procedimentos estipulados. A comunicação de incidentes deverá ocorrer com base nas seguintes premissas:
  - **Notificação inicial** – A ser enviada logo após a entidade tenha concluído que existiu ou possa vir existir um impacto relevante ou substancial e até duas horas após essa avaliação terminar. Esta primeira notificação deve ser acompanhada de algum detalhe relativamente ao incidente que seja possível apurar, atendendo que a mesma é feita num estado muito inicial do incidente;
  - **Notificação de fim de impacto** – Deverá ser enviada no prazo máximo de duas horas após a perda de impacto relevante ou substancial. Esta notificação além de complementar a inicial, terá um maior detalhe sobre o impacto e as ações que foram implementadas para o reduzir ou anular, assim como a duração do incidente e o tempo estimado para recuperar todos os serviços afetados ao seu estado imediatamente anterior à ocorrência**;**
  - **Notificação final -** Enviada no máximo até trinta dias úteis após o incidente estar resolvido com todos os detalhes sobre o incidente, complementando as notificações anteriores. A esta notificação está subjacente um relatório abrangente podendo servir

também de base, caso seja necessário reportar a outras entidades, como seja a ANEPC, ANACOM, CNPD ou outras, mediante o setor onde a entidade esteja inserida.

- **Adoção de taxonomia de incidentes e de efeitos –** As entidades devem adotar uma taxonomia comum para o registo de incidentes e os seus efeitos, de forma a uniformizar e melhorar a comunicação de incidentes numa perspetiva nacional ou internacional. O CNCS disponibiliza uma taxonomia onde é possível enquadrar todas as tipologias de incidentes.
- **Sanções –** O regulamento do RJSC imposto pelo DL65/2021 prevê infrações pelo não cumprimento, de acordo com a tipologia de entidade, isto é, se for pessoa particular ou coletiva, de acordo com as seguintes frações:
  - Uso de marca de certificação da cibersegurança inválida, revogada ou expirada;
  - A utilização de expressão ou grafismo que expressa ou tacitamente sugira a certificação da cibersegurança de produto, serviço ou processo que não seja certificado;
  - Prestação de informação falsa ou omissão dolosa que seja relevante para o processo de certificação da cibersegurança em curso, mediante os requisitos para cada modelo de certificação.

3.1.5 Constituição de uma Entidade Nacional para a Cibersegurança

O Centro Nacional de CiberSegurança (CNCS) através do decreto-lei 46/2018 [8], passa a ser a entidade mandatada pelo estado português com a função de Autoridade Nacional de Cibersegurança [ANC], tendo a responsabilidade de zelar pelos interesses nacionais nesta matéria. Esta lei estabelece ainda a necessidade de ser criada uma equipa única de resposta a incidentes de segurança, tendo assim sido constituído o *Computer Emergency Response Team (*CERT.PT) [15] funcionando também como o ponto de contacto único internacional para reação a ciberincidentes. As entidades e organizações anteriormente referidas passam a ter a obrigatoriedade de implementar medidas de segurança nos seus activos, ficando obrigadas a reportar ao CNCS todos os incidentes de segurança com um impacto considerável, mediante uma escala previamente definida e num prazo estabelecido, mediante a criticidade de cada incidente que envolva as suas redes e sistemas de informação. A lei define também o Regime de fiscalização a ser adotado, assim como as sanções a aplicar caso as entidades não cumpram com a lei.

Na sua constituição o CNCS tem como missão contribuir para que cidadãos e empresas usem o ciberespaço de uma forma livre, confiável e segura, desenvolvendo para isso atividades que visem atingir a sua missão, através da sensibilização e treino para utilização responsável no uso da tecnologia e do

ciberespaço, bem como formação especializada em diversos domínios da cibersegurança. A produção e difusão de alertas, orientações e boas práticas na utilização de tecnologia, recomendações e elaboração de normativo é também uma vertente onde atua. Garante ainda a partilha de conhecimento sobre o estado da cibersegurança a nível nacional. Ao abrigo do DL 65/2021 o CNCS poderá apoiar a entidade notificante perante um cenário de incidente sobre informações relevantes que possam ajudar no tratamento eficaz do mesmo. No âmbito das suas competências, o CNCS pode ainda emitir orientações técnicas que complementem os requisitos de segurança e notificação de incidentes para cada entidade em função do setor de atividade onde se enquadram. Estas entidades têm especificidades mediante os serviços que disponibilizam, levando a que os ativos que suportam estes serviços tenham os seus próprios atributos e configurações, sendo necessário avaliar o grau de equivalência no que respeita às orientações para inventariar activos, relatório anual, requisitos de segurança e notificação de incidentes. O CNCS presta ainda apoio na análise de equivalência em articulação com as entidades de supervisão e reguladoras de cada setor.

3.1.6 A Diretiva NIS2

Em dezembro de 2022 o Parlamento Europeu em conjunto com o Conselho da União Europeia (UE)aprova a diretiva 2022/0255, a *Network and Information Security*2 (NIS2) [1] com a definição de medidas destinadas a garantir um elevado nível de comum de cibersegurança na União Europeia. A necessidade em criar esta diretiva demonstra novamente a preocupação da UE em reforçar a segurança dos estados-membros para melhor enfrentar a ameaça comum à segurança em torno dos sistemas, infraestruturas e redes de comunicações que sustentam o funcionamento de serviços críticos para o funcionamento da economia e da sociedade. A NIS2 entrou em vigor a 16 de janeiro de 2023, data a partir da qual os estados-membros dispõem de 21 meses para a transporem. Em Portugal existem já dois DL, o 46/2018 e 65/2021 que são a base de sustentação da NIS2, sendo por isso facilitada a transposição. A NIS2 surge como meio de enfrentar o aumento do cibercrime e colmatar as deficiências da NIS [36] que aquando da sua aprovação não tinha considerado setores importantes e críticos, concretamente a cadeia de abastecimento. Podemos considerar três principais objetivos elencados com a NIS2 [1]:

- Adoção de uma estratégia de segurança comum a toda a UE, onde prevaleça a cooperação, partilha de conhecimento e união para enfrentar a ameaça crescente do cibercrime. Não é a primeira diretiva europeia que pretende atingir um nível comum de cibersegurança para todos os estados-membros, mas pode ser entendida como um reforço a outras diretivas;

- Incrementar a resiliência e robustez cibernética em entidades e organizações que operam no espaço europeu em setores fundamentais, através da definição de um conjunto de medidas para entidades públicas e privadas implementarem no campo da cibersegurança.
- Alargamento a mais setores de atividade como seja telecomunicações, social media, produção de alimentos ou cadeia de abastecimento, independentemente da dimensão organizacional, passando a existir uma distinção entre entidades essenciais e entidades importantes, embora as diferenças entre ambas no que respeita a requisitos de segurança sejam mínimas;
- Criação de uma base de dados de para registo de vulnerabilidades a nível europeu, ficando a ENISA [20] com responsabilidade pela sua gestão. Esta medida preconizará uma melhor e mais rápida análise pelos estados-membros em resposta a novas vulnerabilidades;
- Maior responsabilização para entidades que apesar de não estarem sediadas na UE, operam no espaço europeu em setores de atividade abrangidos pela diretiva;
- Valorizar a cibersegurança através da responsabilização dos conselhos de administração das organizações, sempre que existam não-conformidades ou incidentes associados à inexistência ou inapropriados controlos para cumprir com os requisitos de segurança.

3.2 IOT e IIOT

O conceito de OT remete-nos de imediato para um contexto de Sistemas de Controlo Industrial (ICS) [17], fechados sobre si mesmos, onde hardware e software são utilizados para monitorizar, controlar dispositivos, processos e a infraestrutura em si. Muitas das infraestruturas de OT suportam serviços que são críticos nos mais diversos sectores, sendo essencial a sua monitorização e controlo para antecipar falhas. Em muitos casos trata-se de tecnologia antiga e já não suportada pelos seus fabricantes, mas o processo de substituição, além de ser dispendioso, é bastante complexo, moroso e requer um elevado esforço de implementação. O facto de se manterem tecnologias antigas em utilização é um risco que se corre do ponto de vista da segurança informática, tendo em conta que estas tecnologias foram desenvolvidas com objetivos de terem elevados níveis de disponibilidade e operacionalidade, em detrimento de segurança, que na altura do seu desenvolvimento, não era uma preocupação, sendo muitas vezes assentes em protocolos proprietários e fechados.

As componentes principais da OT são os ICS que podem incluir os mais diversificados componentes essências para gerir e controlar processos industriais. Alguns dos componentes mais conhecidos são os sistemas SCADA, PLCs RTUs e DCS. As OT têm assim um papel fundamental em

garantir o funcionamento de todos estes componentes, mantendo infraestruturas críticas em pleno funcionamento.

Com a evolução tecnológica, também estes sistemas aos poucos deixaram de ser fechados, começando a introduzir-se algumas componentes que já comunicavam com outros sistemas, através de protocolos de comunicação mais padronizados que começaram a fazer parte desta nova era tecnológica. Aos poucos, as OT começavam a ser interligadas à vertente IT das organizações, passando a haver comunicação bidirecional entre os "dois mundos". Esta transformação veio trazer inúmeras vantagens do ponto de vista operacional, mas também riscos à segurança de uma infraestrutura que antes estava devidamente segregada, sendo a interação muito física e presencial. Esta convergência entre o OT e o IT deve ser cuidadosamente preparada e munida dos mais eficientes controlos, assumindo sempre que as infraestruturas não foram preparadas para este cenário de exposição que a integração com o IT lhes atribui atualmente.

A partir do momento que começou a ser possível ligar uma grande variedade de equipamentos à internet, abriu-se a porta para a convergência entre as OT e o IT, com a disponibilização de equipamentos também para a indústria, ou seja, o Industrial Internet of Things (IIOT) [18]. Estas novas gerações de dispositivos com ligação à internet, representam uma preocupação acrescida porque não existe uma regulação efetiva sobre a sua produção, ficando de certo modo ao critério de cada fabricante as especificações dos seus equipamentos, não sendo obrigados a seguir padrões seguros. Muitas vezes, seguem exatamente uma cultura inversa, isto é, produzem equipamentos que suportam apenas protocolos antigos e pouco seguros para que assim sejam compatíveis com um maior número de infraestruturas onde vão ser utilizados. Perante este cenário, as organizações apenas têm duas opções a seguir, ou os adotam e para isso criam um risco de segurança, ou no caso de não o fazerem, mantém as suas infraestruturas estanques e mais isoladas, o que apesar de ser a forma mais segura, traduz-se também numa limitação que estão a impor à evolução das suas infraestruturas aumentando os custos da sua operação, perdem funcionalidades, deixando de ser competitivas perante os seus concorrentes de mercado.

Atendendo à baixa maturidade em cibersegurança associada em geral aos equipamentos IOT e IIOT [18], as organizações são obrigadas a definir novas arquiteturas que impliquem dotar as suas infraestruturas de uma maior segurança, porque precisam de acompanhar a evolução tecnológica sob pena de comprometer a sustentabilidade da sua organização. Esta nova arquitectura implicará utilizar modelos de segregação entre sectores e infraestruturas para isolar o mais possível a componente OT, ao mesmo tempo que terá de haver mecanismos de monitorização e controlo que permitam identificar comportamentos anómalos ou não justificados, atuando de forma célere.

3.3 Ciberataques e contexto de cibersegurança

O NIST define um ciberataque como sendo uma atividade maliciosa, que utiliza o ciberespaço para atingir um alvo com intuito de destruir, degradar, paralisar, recolher informação ou controlar com finalidades ilegítimas um sistema de informação [19]. As motivações por trás de um ciberataque podem ser financeiras, retaliativas, governamentais, espionagem, reconhecimento e autoafirmação ou de origem interna através da utilização incorreta seja propositada ou de forma neglicência.

Os ciberataques podem ser realizados por indivíduos ou organização criminosas utilizando diferentes técnicas. A Agência da União Europeia para a Cibersegurança (ENISA) [20], por meio de um relatório sobre cibersegurança, lançado em novembro de 2022 identifica as seguintes tipologias de ataques como sendo as mais exploradas em 2022 [21]:

- *Ransomware;*
- *Malware*;
- *Social Engineering;*
- *Threats against data;*
- *Threats against availability (denial of service);*
- *Threats against availability (internet threats);*
- *Disinformation – misinformation;*
- *Supply-chain attacks.*

A figura 3.1 mostra as diferentes tipologias de ataques mais explorada durante o ano 2022 no seio da UE.

Figura 3. 1 Tipologias de ciberataques

Desde os últimos anos é notória uma tendência crescente do cibercrime, abrangendo diversos sectores e áreas, incluindo prestadores de serviços essenciais ao quotidiano da sociedade. Portugal foi recentemente alvo de ciberataques bem-sucedidos nos sectores da energia, comunicações, transportes ou mesmo na comunicação social, embora não tenham resultado grandes impactos para os clientes de serviços, com exceção de ver os seus dados pessoais publicados na *dark web* [22], o que é considerado um incidente de segurança grave por parte de quem têm responsabilidade sobre o tratamento, manipulação e armazenamento seguro desses dados e assim não procedeu. Mediante a lei atual, este tipo de ataques, além de resultar em perdas financeiras para as entidades afetadas, estão ainda sujeitas a coimas e punições por parte da ANC por não ter implementado as medidas necessárias para resistir a ciberataques.

3.3.1 Ciberataques e contexto de cibersegurança

Os ataques a infraestruturas críticas visam na sua essência o controlo das mesmas para impedir que desempenhem as suas funções de forma normal. Este tipo de ataques nem sempre tem motivações financeiras, que visam obter proveitos através do roubo de informações ou cifragem de dados através de *ransomware*, mas retaliações ou uma forma de difundir o terrorismo, ou autopromoção de grupos associados ao cibercrime. Muitas infraestruturas ainda são baseadas em tecnologia antiga e por isso vulnerável, atendendo à época em que foram desenvolvidas, em que o número de ameaças e de ciberataques

era mais reduzido, além de que estas infraestruturas estavam confinadas a um espaço físico, não permitindo que fossem acedidas ou geridas de forma remota, á semelhança do que ocorre hoje em dia. À medida que estas infraestruturas foram sendo interligadas e expostas para a internet, nem sempre houve cuidado em avaliar se a mesma era detentora de mecanismos que impedissem ou no mínimo dificultassem o seu acesso de forma indevida. A existência de protocolos de comunicação obsoletos, assim como mecanismos de autenticação e autorização fracos ou falta de atualizações de segurança, permitiram que estas infraestruturas fossem comprometidas, sem que tenham sido necessário um acesso físico às mesmas.

A figura 3.2 mostra o número de incidentes de segurança associados a cibersegurança distribuídos pelos diferentes setores de atividade ocorridos na EU entre junho de 2021 e julho de 2022.

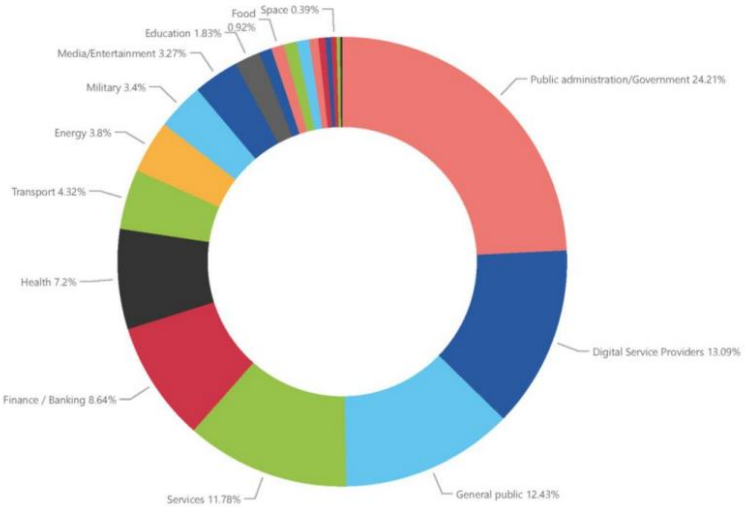

Figura 3. 2 Distribuição de incidentes associados a ciberataques na EU, retirada de [21]

Podemos verificar que uma percentagem considerável de incidentes a envolver a Administração e os serviços públicos, bem como os prestadores de serviços digitais. As infraestruturas que suportam serviços essenciais foram analisadas de forma individual, tendo sido alvo de um número considerável de incidentes, atendendo que são essenciais à sociedade.

Durante os últimos anos foram registados diversos ciberataques a infraestruturas críticas por todo o mundo [23], no sector da energia, água e comunicações, entre outros, tendo alguns deles causado um elevado impacto com a inibição dessas infraestruturas e/ou dos serviços prestados aos seus consumidores. Portugal não passou ao lado destes cibercrimes, tendo igualmente sido afetadas infraestruturas e serviços essenciais para os portugueses [24]:

- José de Mello- Hospitais CUF (Saúde) – agosto de 2018;
- EDP (produção, distribuição e comercialização de energia) – abril de 2020;
- Grupo SIC (Comunicação) – janeiro de 2022;
- Vodafone (operador de serviços digitais) – fevereiro de 2022;
- Grupo Sonae (Retalho e cadeia de distribuição) – março de 2022;
- TAP (Transportes) – setembro de 2022;
- Segurança Social (Administração pública) – novembro de 2022;
- INEM (Saúde) – dezembro de 2022.

O aumento generalizado do cibercrime durante o ano 2022 esteve muito associado ao conflito que opõe a Rússia à Ucrânia [25], iniciado em fevereiro de 2022. Este conflito tem sido travado em dois campos de batalha distintos, um deles da forma tradicional, no terreno e forma mais tradicional no qual as guerras por norma são travadas, e outro através de ciberataques [26]. Os ciberataques lançados pelos russos e outros seus aliados não visaram unicamente alvos ucranianos, mas também outros países que lhe prestam apoio enquanto países aliados.

Esta nova forma de combater merece uma grande reflexão, porque poderá vir futuramente a ser utilizada de forma mais transversal também como forma de retaliação entre países, uma vez que aniquilando determinadas infraestruturas que sejam fundamentais ao funcionamento de um país, é fácil conseguir a sua imobilização.

3.3.2 Consequências resultantes de um ciberataque

As consequências resultantes de um ciberataque são imprevisíveis, pois dependem de diversos fatores, como a intensidade, a duração, a informação obtida, o número e o nível de comprometimento em sistemas e infraestruturas, entre outros [27]. O aumento deste tipo de ataques faz antever que estão para durar e causar o maior dano possível. As organizações começam aos poucos a ganhar sensibilidade para esta temática e com isso a reservar verbas nos seus orçamentos para investir em meios materiais e humanos que possam ajudar a preparar as suas organizações para enfrentar esta terrível ameaça. Por outro lado, muitos sectores (essencialmente a administração pública e os operadores de serviços críticos, essenciais e digitais) têm a obrigatoriedade de implementar mecanismos de prevenção e defesa perante cenários de ciberataques. Estes sectores são ainda obrigados a ter implementados planos de resposta para incidentes de segurança, com vista a terem documentados os processos e procedimentos a seguir caso sejam alvo de um ciberataque.

Por norma, a dimensão de uma organização reflete-se no amadurecimento dos seus processos internos, onde se inclui a vertente da segurança informática, quer em termos de formação, procedimentos ou soluções. Este amadurecimento é muito impulsionado pela evolução tecnológica, mas essencialmente por questões regulamentares que a organização é obrigada a cumprir, evoluindo na implementação de por exemplo de protocolos de comunicação seguros, no acesso remoto de colaboradores e prestadores de serviço. Esta evolução têm um efeito de contágio positivo, obrigando os seus clientes e fornecedores a adotarem tecnologias mais seguras para continuarem a desempenhar os serviços, criando desta forma um efeito bola de neve, caminhando rumo à maturidade para a segurança informática. Esta envolvente é importante para a organização que passa a ter um maior controlo, não somente sobre as atividades dos colaboradores, mas sobre os seus parceiros de negócio que de forma direta interagem com a sua infraestrutura. Os efeitos que podem resultar de um ciberataque, são os seguintes:

- **Perdas financeiras** – Estes danos podem ser causados por inoperabilidade da organização, por exemplo devido a um ou mais serviços ter ficado indisponível. Ou porque o ataque tenha resultado no roubo de dinheiro por via de acesso a contas ou fundos;
- **Danos reputacionais** - A imagem da organização foi afetada pelo ataque, traduzindo-se em quebra de confiança no mercado;
- **Perda de clientes** – O evento resultou na perda de clientes, volume de negócio e dificuldade em angariar novos clientes e parceiros;
- **Exposição de dados sensíveis** – Foram divulgadas informações pessoais e sensíveis de colaboradores e parceiros;
- **Coimas** – Penalizações pelo facto de não ter sido acautelados os procedimentos corretos para proteger dados sensíveis que foram expostos devido ao incidente;
- **Suspensão temporária ou definitiva** – O ataque pode resultar numa suspensão temporária da atividade ou no limite o seu encerramento definitivo.

3.3.3 Planos de resposta a incidentes resultantes de ciberataques

As organizações que se preocupam ou têm obrigatoriedade legal de implementar medidas com vista a melhorar a sua capacidade de enfrentar um ciberataque, têm definido um plano que lhes permita responder a incidentes de segurança que daí possam resultar. A definição de um plano de resposta a incidentes requer um nível de maturidade considerável por parte da organização, visto poder envolver diversos departamentos ou serviços. O plano pode ser entendido com um guia ou uma lista de tarefas onde consta quem são as pessoas responsáveis pela sua execução. Com este plano, são eliminadas indecisões ou

dúvidas sobre se determinada tarefa deve ou não ser executada, quem a executa e a forma como deve ser executada. Com a elaboração de um plano de resposta a incidentes, a organização cumpre os seguintes objetivos perante um cenário de ciberataque:

- Identificar de forma inequívoca as falhas que possam existir na segurança da organização;
- Proteger informação da organização, colaboradores, e demais entidades que interagem e colaboram com a organização;
- Conter o incidente;
- Identificar e mitigar vulnerabilidades e os pontos de entrada;
- Recuperar do incidente;
- Reportar o incidente às entidades regulamentares;
- Fazer uma avaliação do incidente, tirando partido das lições aprendidas com o incidente.

Dependendo da dimensão da organização, poderá existir uma equipa dedicada a responder a incidentes de segurança (CSIRT) que é responsável por operacionalizar o plano definido pela organização. A CSIRT pode ser constituída por uma equipa interna, ou ser um serviço contratado a uma entidade com essa especialidade. Nas organizações de menor dimensão, a equipa de reposta pode ser a própria equipa de IT.

3.4 Gestão de Risco

A gestão da segurança aplicada no contexto organizacional é fundamental para enfrentar as ameaças à segurança, em particular à cibersegurança. Os meios tecnológicos são cada vez a base onde assentam os processos de negócio e por isso críticos para o funcionamento das organizações, que por meio da internet chegam de forma rápida aos seus clientes e parceiro de negócio, ao mesmo tempo que permite aos próprios colaboradores e fornecedores gerir de forma distante os sistemas internos. Os activos organizacionais, sejam eles equipamentos, processos, fluxos ou humanos, estão sujeitos a riscos que importa antes de mais conhecer e perceber quanto podem interferir ou impedir que esses activos desenvolvam as suas atividades da forma esperada. Para ajudar na gestão de risco, muitas organizações foram desenvolvendo *Frameworks* e metodologias que permitem às organizações perceber o estado dos seus activos, as medidas e controlos que devem ser implementados com vista a alcançar um determinado objetivo, minimizando ou reduzindo o risco nesses activo para valores que sejam aceites pela organização. A gestão de risco é um processo assente em etapas, tal como é demonstrado pela *Framework* da ISO através da ISO31000 para gestão de risco mais abrangente, e mais com mais orientação para a gestão de risco de

segurança nos sistemas de informação a ISO27005 [28], em alinhamento com os domínios e controlos especificados pelas ISO27001 e ISO27002.

A figura 3.3 mostra as etapas do processo de gestão risco, bem como a sequencia e interação entre essas etapas.

Figura 3. 3 Etapas do processo de gestão de risco definidas pela ISO27005, retirada de [4]

Etapa 1 – Definição do contexto: Primeira etapa do processo, onde são definidas as regras, metodologia, ferramentas e demais recursos necessários à sua implementação.

Etapa 2 – Identificação do risco: Através de um processo de levantamento de riscos, devem determinar-se as possíveis ocorrências que podem levar a organização a não atingir os seus objetivos pela materialização destes riscos. Nesta fase ocorrem atividades como a identificação de outros elementos relevantes para esta etapa, sendo eles:

- Os **activos** relevantes para o processo de gestão de risco. Pode a organização considerar que apenas quer os sistemas de informação, deixando de fora processos ou outros activos;
- Os **Controlos** que estejam atualmente implementados;
- As **Ameaças** que podem impactar negativamente o funcionamento dos activos;

- As **Vulnerabilidades** nos activos que possam ser exploradas pelas ameaças anteriormente identificadas;
- O **Impacto** que uma vulnerabilidade ao ser positivamente explorada, causa num activo, mediante a criticidade deste;
- A **Análise qualitativa do risco** tendo por base uma matriz ou escala de atributos que permite identificar os impactos em função da probabilidade de ocorrência;
- A **Análise quantitativa do risco** suportada numa escala numérica com vista a obter os valores inerentes ao impacto e a probabilidade de ocorrência.

Etapa 3 – Avaliação do risco: Depois dos riscos terem sido bem identificados na etapa anterior, nesta etapa são avaliados com base em critérios definidos na primeira etapa deste processo.

Etapa 4 – Tratamento do risco: A fase de tratamento é a mais materializável de todo o processo, após ter sido decidido a melhor estratégia de tratamento a aplicar.

A figura 3.4 identifica as estratégias para tratamento do risco que a metodologia prevê:

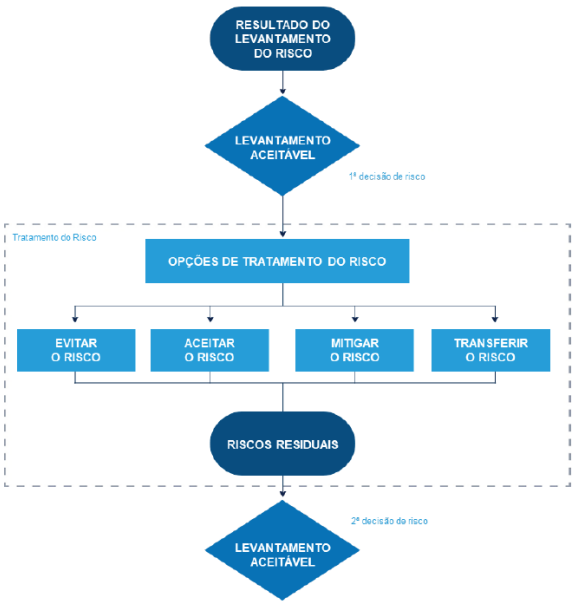

Figura 3. 4 Estratégias de tratamento para o risco, retirada de [4]

Podem ser adotadas uma ou mais estratégias para tratar o risco, seja na mesma interação ou em interação seguintes. O tratamento aplicado é sobre o risco inerente, ou seja, o risco que resulta do processo de avaliação antes de ser serem aplicadas quaisquer medidas de tratamento. O risco residual é obtido após o tratamento ser aplicado. Caso o valor obtido seja o pretendido, não será necessária nenhuma interação adicional, caso contrário, a plano de tratamento deve ser revisto e aplicado tantas vezes quantas aquelas que for necessário para atingir o nível pretendido.

Etapa 5 – Aceitação do risco: Aceitação formal do risco, após a etapa anterior, tenha permitido atingir um nível que seja aceite, mediante os critérios de aceitação previamente definidos e aprovados.
Etapa 6 – Comunicação e consulta do risco: O valor do risco deve ser comunicado às áreas e entidades que tenham sido identificadas como partes interessadas.
Etapa 7 – Monitorização e revisão do risco: O processo de gestão de risco não é estanque, devendo ser alvo de monitorização constante porque existem fatores que podem influenciar e obrigar a que todo o processo seja repetido, como por exemplo:

- Alterações organizativas e processuais;
- Alterações na arquitectura dos sistemas de informação;
- Alterações no processo de gestão de risco;
- Alterações na criticidade dos activos;
- Novas vulnerabilidades;
- Ocorrência de um incidente de segurança.

O processo de gestão de risco deve ainda conter uma Matriz RACI, onde especifica quem são os intervenientes no processo e a responsabilidade que assumem no mesmo.

Tolerância ao risco – Pode ser definido como o nível ou o valor de risco que uma organização está disposta a aceitar de forma a conseguir cumprir com os seus objetivos, tendo uma ideia muito clara dos impactos que possam resultar se essa tolerância for ultrapassada.

Apetite ao risco –Está associado à pré-disposição em assumir determinados riscos, independentemente da capacidade de suportar o impacto, caso o valor definido como sendo o limite para o apetite seja ultrapassado.

3.5 Gerir o risco de uma infraestrutura com base nas suas vulnerabilidades e ameaças

O nosso dia a dia é pautado por escolhas que muitas vezes tomamos de forma mais ou menos consciente, tendo por base o resultado que procuramos ou esperamos obter. Estas escolhas ou decisões não são mais do que gerir risco em virtude das opções que tomamos, sabendo que decisões diferentes podem levar a resultados diferentes, mediante a influência de fatores que não podemos controlar. Quanto mais informação temos e melhor é a sua qualidade, mais assertivas serão as decisões que tomamos.

A gestão de risco organizacional requer igualmente conhecimento de todos os cenários que enfrentam antes de poderem tomar qualquer decisão. Simplificando um pouco este processo, necessitam de perceber qual a probabilidade de uma ameaça explorar uma vulnerabilidade num dos seus ativos, tendo um determinado impacto, ou seja, estamos perante duas incógnitas, a probabilidade e o impacto. O impacto em si pode ser um valor conhecido, estando diretamente associado ao valor do ativo e aos impactos (financeiros, reputacionais, etc.), já a probabilidade é difícil.

A metodologia para avaliar a maturidade de uma infraestrutura que apresentamos nesta dissertação, acreditamos que irá apoiar no cálculo da probabilidade, por meio da obtenção de um valor para cada controlo avaliado. Quando menor for o valor do controlo menor será a sua resiliência e maior será a ameaça que representa para a infraestrutura no seu todo. Neste sentido acreditamos que a metodologia dará um forte contributo para a gestão de risco de ativos no que à cibersegurança diz respeito, dando uma visão realista sobre os domínios que carecem de uma maior atenção e consequente investimento, para que fiquem mais robustos às ciberameaças.

Capítulo 4

ABORDAGEM AO PROBLEMA

Neste capítulo são descritos os principais objetivos do trabalho, partindo da análise documental feita no capítulo anterior. Na Secção 4.1 são identificados os objetivos que nos propomos atingir com o trabalho. Na secção 4.2 encontram-se identificados os requisitos definidos para que o trabalho. Na seção 4.3 foram identificadas os principais modelos e standards que contribuíram para a realização da metodologia.

4.1 Identificação de objetivos, planeamento e riscos associados

O principal objetivo deste trabalho é percecionar o estado de maturidade em que se encontra uma infraestrutura que suporte serviços críticos, através da efetividade dos controlos pertencentes aos diversos domínios da cibersegurança que estão associados a essa infraestrutura. Para atingir esta meta, foi definida uma metodologia que se encontra descrita neste capítulo. Como boa prática que deveria ser seguida em todos os trabalhos, foi definido um planeamento das atividades realizadas e identificados os riscos que poderiam impactar o referido planeamento e causar desvios.

4.1.1 Objetivos

- Do ponto de vista regulamentar, as organizações abrangidas pelo decreto-lei 65/2021 têm o dever de prestar informação em matéria de cibersegurança ao CNCS sobre as infraestruturas e os serviços críticos que dispõem. O CNCS em si disponibiliza-se para apoiar as organizações a responder a esta obrigação, embora seja de total responsabilidade da organização fazê-lo de acordo com os moldes e calendário definido. Neste sentido, a metodologia como meio de responder ao requisito regulamentar;
- Identificar os domínios de segurança e controlos inerentes à cibersegurança para realizar uma análise de maturidade a infraestruturas de serviços críticos;
- Desenvolver uma metodologia de cálculo de maturidade, enquadrada numa escala que permita enquadrar por níveis a maturidade por controlo, domínio e global;

- Obter uma visão transversal e holística sobre a maturidade e conformidade dos domínios da cibersegurança na infraestrutura;
- Dar contributos para a Gestão de Risco, através de uma visão realista dos riscos associados a infraestruturas que suportem serviços críticos;
- Aplicar a metodologia desenvolvida através da realização de uma avaliação de maturidade exemplificada;
- Apresentação de resultados.

4.1.2 Planeamento das atividades

Entendemos que o trabalho é bastante desafiante, mas com alguma complexidade na sua realização devido às especificações que importam abordar, assim como o trabalho de pesquisa e análise que ainda será necessário realizar. De forma a assegurar que as tarefas vão sendo executadas dentro do tempo expectável e na ordem correta, apresentamos um plano que entendemos ser realista para conseguir concluir o trabalho na data acordada.

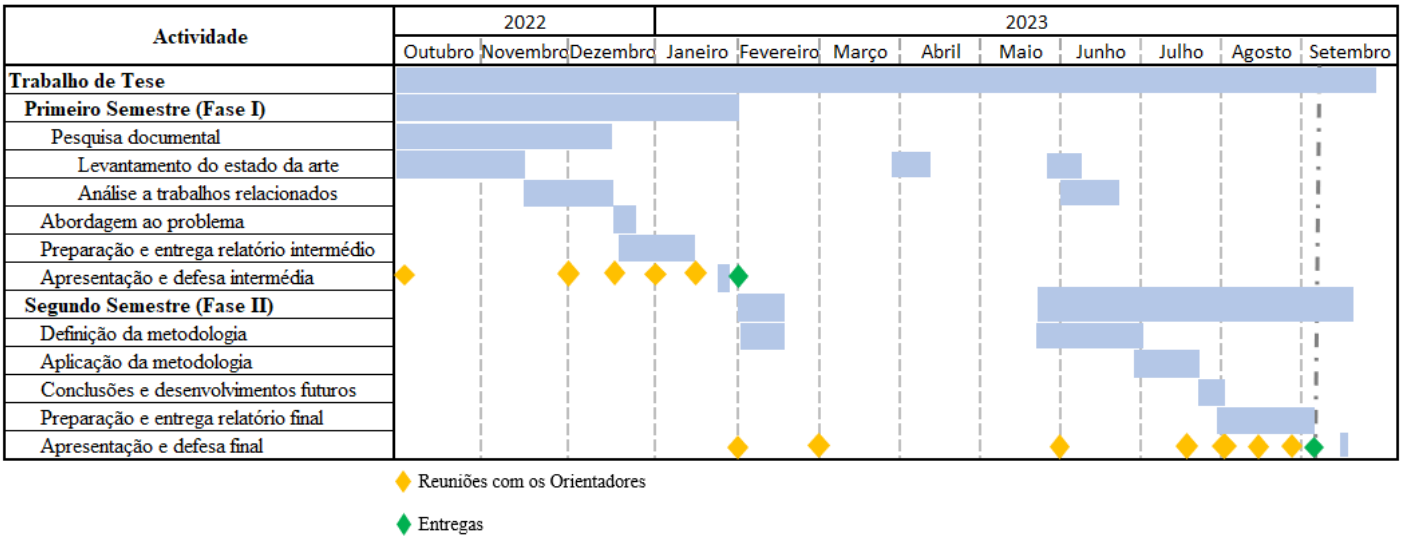

Figura 4. 1 Plano de trabalhos

O planeamento do trabalho foi definido com base na informação detida no momento, podendo, contudo, ser alterado em função de novas atividades que seja necessário contemplar ou por via de riscos não planeados, que podem influenciar de forma positiva ou negativa o plano.

4.1.3 Identificação de riscos

Nesta secção apresentamos os riscos identificados e que podem impactar o desenvolvimento do projecto, com base na probabilidade e no impacto de se materializarem. Apresentamos ainda um plano de tratamento para cada risco, por forma a mitigar e monitorizar a sua evolução, ajustamento sempre que for necessário o plano de tratamento, para que seja materializável.

ID#	Data Identificação	Descrição	Probabilidade (1 a 5)	Impacto (1 a 5)	Valor do Risco (P x I) (1 a 25)
R1	19/12/2022	Constrangimento ao nível da disponibilidade do aluno para cumprir o plano definido	3	5	15
R2	19/12/2022	Alterações ao âmbito do trabalho	2	4	8
R3	19/12/2022	Constrangimento ao nível dos professores orientadores	1	4	4

Tabela 4. 1 Principais riscos identificados para a execução do trabalho

Para cada um dos riscos identificados, é apresentado na tabela 4.2 um plano de tratamento.

ID#	Criticidade	Descrição	Data Limite	Responsável
R1	Alto	Realizar um controlo apertado das actividades definidas de forma a antecipar e minimizar alterações ao plano	durante o decorrer do trabalho	Aluno
R2	Médio	Reunir regularmente com os Professores orientadores de forma assegurar que as actividades previstas são realizadas dentro do contexto definido, por forma a não incluir alterações de âmbito que conduzem a atrasos na entrega	Reuniões de acompanhamento	Aluno
R3	Médio	Marcar com os Professores orientadores todas as reuniões de acompanhamento até ao final do trabalho	Início das actividades	Aluno

Tabela 4. 2 Planos de resposta aos riscos identificados

4.2 Requisitos

O principal objetivo deste trabalho é definir uma metodologia que permita aferir o nível de conformidade para a cibersegurança em infraestruturas que suportem serviços essenciais, não sendo assim desenvolvido qualquer sistema ou aplicação que apoie neste processo. Desta forma não se prevê a necessidade de definir requisitos funcionais e não funcionais, mas vamos definir requisitos que a metodologia deva cumprir com e desta forma balizá-la dentro dos objetivos traçados.

- **Requisito 1:** A metodologia deverá poder ser aplicada em qualquer infraestrutura, independentemente da sua dimensão, sector ou criticidade;
- **Requisito 2:** Antes da metodologia ser aplicada, deverá existir um conhecimento suficiente da infraestrutura para a poder avaliar. Para isso, poderá ser necessário consultar documentação sobre a infraestrutura e outros processos e normativos organizacionais, bem como entrevistas com todas as áreas relevantes;
- **Requisito 3:** A metodologia deve prever todos os domínios da segurança, com os respetivos controlos associados, e permitir que sejam removidos ou adicionados novos;
- **Requisito 4:** A metodologia deverá ter a capacidade de avaliar e calcular o estado de maturidade, mesmo quando existam domínios e controlos não aplicáveis à infraestrutura em análise;
- **Requisito 5:** A metodologia deverá ter um baixo índice de complexidade na sua utilização;
- **Requisito 6:** Os resultados obtidos deverão ser objetivos e realistas, traduzindo o resultado da análise realizada, devendo ser possível evidenciar esses resultados;
- **Requisito 7:** A metodologia será materializada através de uma folha de cálculo tipo Excel ou outra equiparada.

4.3 Resumo histórico

No Capítulo 2 foram identificados trabalhos e *frameworks* que serviram de ponto de partida e base geral para este trabalho, sendo identificadas na tabela 4.1 de forma resumida:

Data	Descrição	Entidade responsável
Junho/2019	Quadro Nacional de Referência para a Cibersegurança	CNCS
2013/2022	ISO27001	ISO/EIC
Fevereiro/2022	NIST Cybersecurity Framework	NIST
Dezembro/2021	Cloud Security Alliance	CSA
Setembro/2020	NIST 800-53	NIST

Tabela 4. 3 Tabela com historial de conteúdos associados ao trabalho

O QNRCS [4] do CNCS identifica de forma inequívoca os destinatários que devem colocar em prática a sua implementação. Contudo, esta framework foi desenhada com intuito de apoiar e traçar as principais linhas orientadoras a distintos destinatários, ficando deste modo genérica, cabendo a cada uma das organizações abrangidas, definir a sua própria metodologia, com base na framework. Neste sentido, este trabalho vai ao encontro desta necessidade, através da definição de uma metodologia para análise de maturidade de infraestruturas críticas para operadores de serviços essenciais, por se tratar de um dos destinatários que tem obrigação de cumprir com os requisitos do QNRCS.

4.4 Desenvolvimento da metodologia

Sendo o objetivo primordial deste trabalho, a avaliação de maturidade de cibersegurança nas infraestruturas críticas, uma das primeiras preocupações foi a forma como esta avaliação deveria ser realizada, para que não fosse subjetiva, ou seja, independentemente de quem a esteja a realizar, o resultado não deverá divergir. A forma como se tentou resolver este problema e assim obter uma solução que não seja teórica nem subjetiva, foi materializar a avaliação através de uma metodologia assente na identificação dos domínios de segurança, mais em concreto aqueles que diretamente se relacionam com a cibersegurança. A cada um destes domínios foram associadas áreas ou subdomínios e as estes foram assignados controlos. Tanto as áreas como os controlos podem repetir-se em diferentes domínios, mediante o que se pretende avaliar, podendo ter critérios diferentes de avaliação dependendo da perspetiva e do contexto onde o mesmo esteja inserido.

A avaliação de cada controlo assenta numa escala previamente definida, onde é dada uma descrição para cada um dos níveis de maturidade do controlo e assim facilitar a resposta. Cremos que através desta metodologia, o processo de avaliação é facilitado, assertivo e sobretudo objetivo

Ao longo do desenvolvimento da metodologia conclui-se que o valor do controlo não pode ser binário, ou seja, está implementado ou não está implementado, pois seria uma visão redutora sobre o seu estado. Concluiu-se assim que cada controlo pode estar em diferentes estados, incluindo-se o de não implementado e totalmente implementado. Durante a existência de um controlo é expetável que passe por diferentes estados, estando cada um desses estados associado a uma maturidade, ou seja, nem todos os controlos quando são implementados atingem no imediato a sua robustez máxima, pois dependerá da existência de recursos humanos e/ou tecnológicos e isso pode levar tempo a obter. Nestes cenários, ocorre que o controlo ficam parcialmente implementado, tendo por isso atingido o valor de maturidade máximo, podendo haver lugar à implementação de controlos compensatórios a título temporário para que no imediato fique mitigado e a ameaça mais difícil de explorar.

As diversas frameworks, assim como outra documentação referida no capítulo 2 deste trabalho identificam bastantes domínios de segurança, que são relevantes quando se pretende fazer uma avaliação profunda e transversal a toda a organização, por exemplo, para obtenção de uma certificação ISO27001 ou para operacionalizar uma gestão de risco que inclua todo o sistema de informação da organização. Para o nosso trabalho somente foram escolhidos domínios, porque terem sido considerados os mais relevantes e que melhor poderiam contribuir para o objetivo final, que é aferir a maturidade de infraestruturas críticas. Ao tomar esta opção, não se pretendeu desvalorizar os restantes domínios, mas focar naqueles que de forma direta entendemos estar mais relacionados com infraestruturas críticas. Por outro lado, a metodologia foi desenvolvida para permitir o seu crescimento e evolução através da adição de outros domínios, áreas e controlos, mas flexível o suficiente para avaliar uma infraestrutura crítica, como um serviço que funciona sem uma infraestrutura de igual criticidade. A metodologia permite ainda que nem todos os controlos tenham obrigatoriamente de ser aplicáveis a uma determinada infraestrutura, podendo simplesmente ser ignorado sem que isso prejudique a avaliação global.

O cibercrime têm aumentado, não tendo rosto ou origem e difundindo-se através de diferentes formas, meios e formatos, sendo a defesa e a prontidão a melhor resposta para enfrentar esta ameaça. Com base nesta premissa, foram escolhidos 11 domínios, 44 áreas e 186 controlos, sabendo que infraestruturas não funcionam de forma isolada, encontram-se expostas com aplicações e serviços sem si críticos para clientes em modelo 24x7x365, necessitando assim de valor de disponibilidade muito altos, não existindo muitas vezes janelas de indisponibilidade para operações de manutenção.

4.4.1 Domínios, áreas e controlos incluídos na metodologia de avaliação

Para elaboração da metodologia de avaliação foram tidas por base as diversas frameworks identificadas e descritas no capítulo 2 deste trabalho. Por uma questão de simplificação, e melhor estruturar o questionário de avaliação, foram criados subdomínios ou áreas, permitindo que o mesmo controlo seja utilizados diversas vezes em cada domínio. Esta configuração pretende ainda criar uma melhor experiência por parte de quem responde ao questionário e de forma clara tenha perceção de que é o mesmo controlo, mas aplicável a uma área diferente, ainda que seja no mesmo domínio. Finalmente, foram associados controlos às áreas, com um descritivo para cada nível de maturidade em que o mesmo possa estar em termos de materialização.

Ao longos dos próximos capítulos serão apresentados os domínios, áreas, controlos identificados, assim como a escala de maturidade utilizada, encontrando-se a metodologia operacionalizada no anexo 1 a este trabalho.

4.4.1.1 Domínio 1 - Governação organizacional

O primeiro domínio considerado na metodologia foi o da governação organizacional, enquanto responsável por toda a componente estratégica para a segurança da informação, no caso deste trabalho a vertente cibersegurança. Pode ser complexo uma organização crescer em maturidade de segurança sem que tenha definido toda a vertente de normativo que suportará definição e operacionalização de uma política de segurança de informação robusta, percecionada em toda a organização e nos parceiros em alinhamento com os objetivos de negócio e total comprometimento e apoio da gestão de topo. São ainda considerados os requisitos legais, de supervisão e setoriais, perante os quais a organização tem responsabilidade de acautelar e responder mediante a obrigatoriedade de cada. Tenho o suporte da gestão de topo, a organização em si perceciona a importância da cibersegurança, procurando disponibilizar os recursos necessários à sua execução. Algumas das áreas incluídas não estão diretamente ligadas a este domínio, mas por uma questão de simplificar e não ter de incluir todos os domínios, foram associadas.

A figura seguinte demonstra o mapeamento das áreas e controlos pertencentes ao domínio da governação organizacional.

1 - Governança Organizacional	Estratégia para a cibersegurança	Comprometimento da gestão de topo
		Disponibilização de recursos
		Envolvimento de terceiras partes
		Definição da estratégia
	Processo de Contratação	*Background check*
		Programa para retenção de talento e conhecimento
		Modelo de contratação de colaboradores
		Cláusulas de confidencialidade e retenção de informação
		Subcontratação em cadeia
		Código de ética e conduta profissional
		Normativo de segurança
	Gestão de Risco	Função Risco
		Normativo para gestão de risco
		Responsáveis pelo risco
		Conformidade
		Metodologia para gestão de risco
	Funções e responsabilidades	Formação em segurança da informação
		Definição de perfis e responsabilidades
	Formação	Gestão e evolução de carreiras
		Realização de exercícios e simulacros
		Gestão de budget para formação em cibersegurança
		Monitorização da eficácia do programa de formação em cibersegurança
		Formação adequada às funções
		Divulgação de normativos, processos e procedimentos organizacionais

Figura 4. 2 Áreas e controlos associados ao domínio governação organizacional

4.4.1.2 Domínio 2 – Gestão de ativos

Uma organização para funcionar necessita de ativos, podendo estes serem equipamentos, processos ou programas, devendo assim ter definidos processos, práticas e procedimentos seguros sobre a sua utilização. Contudo, uma das primeiras ações é a ter um inventário atualizado sobre todos os seus ativos, onde devem constar todas as características sobre eles, realçando a criticidade e detalhes sobre a segurança. Os ativos tem vulnerabilidades e face à sua utilização são expostos a ameaças, que sendo exploradas, representam um risco para a organização. Com base nesta premissa foi considerado o domínio de gestão de ativos como relevante para ser avaliado, assumindo que uma infraestrutura crítica em si também é um ativo, e para garantir o seu funcionamento, é necessário interagir com outros ativos, nomeadamente ativos que podem estar entregues a parceiros e fornecedores.

A figura seguinte demonstra o mapeamento das áreas e controlos pertencentes ao domínio da gestão de ativos.

2 - Gestão de ativos	Gestão de inventário	Inventariação
		Protecção contra adulteração de inventário de ativos
		Classificação de ativos
		Salvaguardas/Backups
		Ativos pertencentes a parceiros
		Ativos entregues a parceiros/fornecedores
		Devolução/recolha de equipamentos (colaboradores e parceiros
	Gestão de atualizações de segurança	Aplicação de atualizações de segurança
		Verificação de conformidade nos ativos
		Gestão de exceções
		CAB (change-advisory board)
		Baselines de segurança em ativos

Figura 4. 3 Áreas e controlos associados ao domínio de gestão de ativos

4.4.1.3 Domínio 3 - Segurança e conformidade do posto de trabalho

Apesar do posto de trabalho ser um ativo organizacional e poderia por assim ter sido incluído no domínio anterior, os resultados obtidos nos casos de uso realizados, levaram-nos a tomar esta decisão. O motivo era simplesmente porque estar-se-ia a nivelar por baixo os mecanismos de segurança no posto de trabalho comparativamente com os restantes ativos, como seja por exemplo, equipamentos de rede ou mesmos determinados servidores com níveis de exposição menores. Face a esta conclusão e pela criticidade que um posto de trabalho representa, teria um domínio dedicado. Sabemos que a preocupação com a segurança do posto deve ser grande, atendendo que são equipamentos muitas vezes móveis, que se ligam a ambientes e redes nem sempre seguros, mas também servem para navegar numa internet onde as ameaças e novas formas de explorar vulnerabilidades surgem todos os dias. É absolutamente crítico para a organização que além da segurança, a conformidade do posto seja garantir e quando isso não acontece, existam controlos que previnam o posto de executar tarefas que coloquem em causa o próprio posto, assim como a segurança da organização como um todo.

A figura seguinte demonstra o mapeamento das áreas e controlos pertencentes ao domínio da segurança e conformidade do posto de trabalho.

3 - Segurança e conformidade do posto de trabalho	Mecanismos de protecção	Antivírus
		Anti-Malware e Anti-Phishing
		Instalação de software padronizado
		Instalação de software não padronizado
		Elevação de privilégios
		Instalação de atualizações e correções de segurança
	Conformidade do posto de trabalho	Deteção de ativos em estado de inconformidade
		Protecção da informação
		Acesso a redes sem fios desconhecidas e inseguras
		Acesso controlado à internet
	Monitorização ativa sobre os postos de trabalho	Monitorização e resposta em modelo 24x7x365

Figura 4. 4 Áreas e controlos associados ao domínio de segurança e conformidade do posto de trabalho

4.4.1.4 Domínio 4 – Gestão de identidades e acessos

Gerir acessos é uma tarefa da maior importância, mas difícil pela complexidade que representa, atendendo que o nosso dia a dia gira em torno de acessos. É fundamental que as organizações definam e implementem políticas e controlos para gestão de acessos que sejam efetivas e de acordo com o nível de risco que representa cada acesso. O primeiro passo é identificar-se o tipo de acesso pretendido, de forma que este não tenha permissões a menos, mas sobretudo a mais do que é necessário. Esta componente diz respeito à autorização, já a vertente de autenticação, felizmente a evolução tecnológica trouxe-nos mecanismos adicionais que permitem confirmar que a pessoa é realmente quem diz ser, seja através de mecanismos como seja o MFA ou SSO, ainda que possam estar comprometidos. Uma boa prática é atribuição de permissões com base em Role-Based Access Control, podendo um utilizador ter diferentes níveis de permissões mediante a sua função em cada aplicação que utiliza, além de automatizar o processo de alterações de permissões se a sua função for alterada.

A figura seguinte demonstra o mapeamento das áreas e controlos pertencentes ao domínio da gestão de identidades e acessos.

4 - Gestão de Identidades e Acessos	Estratégia	Definição de uma estratégia e modelo de governo para gestão de acessos
		Monitorização, adequação e ajustes na estratégia para gestão de acessos
	Gestão de acessos	Processo de gestão de acessos
		Processo de atribuição de acessos aplicacionais e em infraestruturas (não privilegiados)
		Processo de atribuição de acessos aplicacionais e em infraestruturas (privilegiados)
		Utilização de uma plataforma/solução para acessos privilegiados
		Utilização de uma plataforma/solução para gestão de acessos via SSO
		Processo de alteração de acessos
		Mecanismos de bloqueio automatizado para acessos comprometidos
	Modelo de autenticação e autorização	Utilização de 2 fator de autenticação
		Utilização de diferentes modelos de autenticação
	Alterações, integrações e federações de identidades	Alterações em identidades
		Modelo de federação com entidades parceiras (colaboradores externos, fornecedores,…,etc.)
	Revisão e monitorização	Comprometimentos de acessos de parceiros
		Verificação e validação do nível de acesso
		Revisão de acesso a sistemas críticos (contém informação pessoal sensível de colaboradores, clientes ou parceiros)
		Revisão de acessos (Geral)

Figura 4. 5 Áreas e controlos associados ao domínio da gestão de identidades e acessos

4.4.1.5 Domínio 5 – Segurança de rede

Num contexto organizacional, a segurança da rede é um domínio relevante no que à cibersegurança diz respeito. Cada vez menos existem fronteiras que limitam e definem o que fisicamente está incluído ou não no seio da organização. As organizações não funcionam isoladas do mundo e por isso devem ter mecanismos de protecção robustos para os seus ativos, tanto aqueles que se encontram interiorizados, como seja os serviços impressão ou pastas de rede, ou aqueles que estão expostos, como é o caso de serviços de email, aplicações para clientes e colaboradores ou própria VPN. Apostar em serviços como Firewalls, WAF ou IDPS é uma necessidade e a forma mais segura de enfrentar as ameaças do cibercrime.

A massiva utilização da VPN, em muito forçada pelo COVID, mas continua com padrões de utilização elevados, requereu a implementação de mecanismos robustos e resilientes para permitir esta elevada utilização sem comprometer o normal funcionamento, atendendo à exposição que uma ligação VPN representa.

A figura seguinte demonstra o mapeamento das áreas e controlos pertencentes ao domínio da segurança de rede.

5 - Segurança de rede	Gestão de acessos	Acessos à rede interna (acesso físico)
		Acesso remotos para colaboradores
		Acesso remoto de parceiros
		Gestão de credenciais administrativas
		Disponibilização de acesso a redes sem fios para colaboradores e parceiros
	Monitorização e conformidade	Protecção de eventos de rede (logging)
		Supervisão, monitorização e restrições sobre comunicações com parceiros e entidades externas
		Gestão de alterações
		Deteção de ativos na rede (shadown IT)
	Gestão de incidentes na rede	Identificação, analise, tratamento e monitorização de incidentes envolvendo ativos de comunicação/rede
	Arquitectura de rede	Modelo de segregação de redes
	Politicas de rede	Documentação de rede
		Utilização aceitável e responsável da rede
	Gestão de vulnerabilidades na rede	Processo de deteção, análise e mitigação
		Instalação de atualizações de rede
		Deteção e tratamento de vulnerabilidades em ativos de rede

Figura 4. 6 Áreas e controlos associados ao domínio da segurança de rede

4.4.1.6 Domínio 6 – Gestão de parceiros/fornecedores

Não é novidade que muitas organizações tem os seus serviços externalizados, por uma questão de não terem essa capacidade internamente, e veem num parceiro uma melhor preparação e capacidade em fornecer esse serviço. Existem ainda casos em que a organização trabalha com parceiros específicos em determinadas matérias em modelo de reforço de capacidade, cujo objetivo será reforçar as equipas internas com consultores externos, mas é sempre a organização quem detém controlo sobre todos os seus serviços e aplicações. Um exemplo poder ser a gestão do Datacenter interno da organização, em que são contratadas pessoas com perfis de gestores e administradores de sistemas e redes para trabalharem conjuntamente com as pessoas internas, enquanto no primeiro cenário, a organização contrataria um serviço de Datacenter para alojar todos os seus serviços. Neste último cenário o parceiro teria toda a responsabilidade por assegurar a gestão dos equipamentos, acessos físicos ou mesmo a salvaguarda de informação.

Seja num cenário ou noutro, o parceiro irá ter acesso aos ativos organizacionais, onde se inclui informação privada e sensível, sendo assim de maior importância gerir de forma adequada o risco de cada parceiro. Neste contexto foi tido em conta a avaliação e gestão de parceiros enquanto domínio a considerar na avaliação de maturidade de cibersegurança sobre uma infraestrutura crítica.

A figura seguinte demonstra o mapeamento das áreas e controlos pertencentes ao domínio da gestão de parceiros e fornecedores

6 - Gestão de parceiros (fornecedores)	Políticas, Processos e procedimentos	Gestão de contratos
		Cumprimento do normativo interno
	Governação	Processo de contratação
		Avaliação prévia à contratação
		Gestão de não conformidade de parceiros
		Ponto de contato para gestão de pedidos
	Gestão de risco de parceiros	Avaliação de risco a parceiros
		Fontes para consulta de classificação de parceiros
		Disponibilização de acessos a informação sensível e classificada
		Renovação contratual
		Monitorização sobre a postura de segurança do parceiro
		Estratégia de saída

Figura 4. 7 Áreas e controlos associados ao domínio da gestão de parceiros

4.4.1.7 Domínio 7 – Monitorização de segurança

Para implementar uma monitorização de segurança deve ser previamente definida uma estratégia sobre o que se pretende monitorizar e a partir dessa fase definir processos de monitorização sobre equipamentos a supervisionados no que a alarmística diz respeito, como seja o caso de firewalls, WAF, servidores e postos de trabalho. A monitorização tem de ser interpretada como uma atividade corrente, e sempre em melhoria contínua, de forma a incluir os eventos de segurança relevantes das fontes ou ativos com maior risco. Se imaginarmos uma pequena organização, contendo apenas alguns ativos a monitorizar e cujo casos de uso de monitorização não sejam muitos, é possível, embora difícil analisá-los e fazer correlação entre eles de forma manual. Tal cenário é impossível quando o volume de eventos aumenta, sendo necessário como medida de resposta uma solução baseada em SIEM. Em paralelo deve ser definida

uma política para gestão de logs adequada, para evitar a produção, recolha, análise e armazenamento de eventos que pouco acrescentam à monitorização de segurança.

Outra ferramenta essencial à monitorização de segurança é a utilização de soluções baseadas em *Endpoint Detection and Response* (EDR) para postos de trabalho ou Network Security Monitoring (NSM) para a componente de rede. Em organizações com estado de maturidade mais avançado, serviços como os de Threat Intelligence e Threat Hunting também são implementados, pelo contributo que dão para a segurança organizacional.

A figura seguinte demonstra o mapeamento das áreas e controlos pertencentes ao domínio da monitorização de segurança

7 - Monitorização de segurança	Pessoas/Equipas	Equipa de monitorização
		Capacidade e prontidão
		Formação e sensibilização em cibersegurança
	Processos e procedimentos	Estratégia de monitorização
		Monitorização e supervisão da estratégia de monitorização
		Processos de monitorização
		Escalonamentos
		Gestão de exceções
		Modelo de reporte interno
		Modelo de reporte externo
		Processos para monitorização automatizada
		Processo de reporte de incidentes
		Gestão de incidentes
		Análise prévia a incidentes de segurança
		Critérios para definição de criticidades
		Tipificação de incidentes e eventos de segurança
		Gestão de eventos de cibersegurança
		Seleção de eventos de segurança
		Frequência definida para revisão de eventos de segurança
		Acesso e envio seguro aos eventos de segurança
		Informação sensíveis em eventos de segurança
		Prazos de retenção e conservação
		Threat Intelligence
		Threat Hunting
	Tecnologia	Ferramenta de Análise e correlação de eventos (SIEM)
		Alarmística
		Armazenamento de eventos de segurança
		Monitorização ativa de cibersegurança em postos de trabalho, servidores e ativos de rede
		Cobertura na monitorização de cibersegurança
		Segurança no correio eletrónico
		Gestão e monitorização de impressoras
		Análise a ficheiros na rede e pastas partilhadas

Figura 4. 8 Áreas e controlos associados ao domínio da monitorização de segurança

4.4.1.8 Domínio 8 – Gestão de vulnerabilidades

O domínio de gestão de vulnerabilidade foi incluído na metodologia pela importância que têm e pela ameaça que representa ter um ativo vulnerável, quando está exposto a ameaças que podem explorar essas vulnerabilidades. Os próprios colaboradores da organização são vulneráveis, levando a que técnicas baseadas em engenharia social possam obter resultados muito consideráveis para quem a pratica, sem que elevado esforço ou custo de implementação.

As vulnerabilidades tem o seu ciclo de vida, iniciando-se desde logo que vertente de identificação que pode ser conseguida de forma manual, automatizada ou apenas com base em conhecimento público, como seja uma determinada versão de hardware de uma firewall, ou o sistema operativo de um servidor. Estando a vulnerabilidade identificada, é necessário proceder à sua avaliação de forma a verificar a sua criticidade e impacto causado pela sua exploração. Por vezes, a vulnerabilidade pode em si ter uma classificação muito alta ou crítica, mas na realidade não é explorável face a controlos compensatórios que existe, mas é necessário aferir. Com base nesta premissa é decidido ou não tratar a vulnerabilidade e caso seja essa a opção seguida, é definido um plano de mitigação. Após implementação do plano, a vulnerabilidade deve ser retestada para aferir que ficou de fato fechada. Caso não tenha acontecido, deve ser definido um novo plano de mitigação. A últimas fases deste ciclo de vida, dizem respeito ao reporte e comunicação da vulnerabilidade, atualização do repositório. Caso tenha sido aceite o risco e por isso manter a vulnerabilidade por tratar, esta deve ser alvo de monitorização.

A figura seguinte demonstra o mapeamento das áreas e controlos pertencentes ao domínio da gestão de parceiros e fornecedores

8 - Gestão de vulnerabilidades	Normativo de suporte	Formalização de um processo para gestão de vulnerabilidades
		Operacionalização do processo
		Repositório centralizado de vulnerabilidades
	Identificação	Processo de identificação
		Tecnologias IOT
		Tecnologias *Cloud*
		Equipamentos de rede (routers, switches,
		Equipamentos móveis (telemóveis, smartphones, tablets,...,etc.)
		Equipamentos sem fios (WiFi)
		Novas vulnerabilidades (0-day)
		Equipas executantes
		Desenvolvimento interno
		Desenvolvimento externo
		Análise aplicacional periódica
		Tecnologia para deteção de vulnerabilidades
	Classificação	Escala de classificação
		Reclassificação de vulnerabilidades
	Mitigação e fecho	Identificação do plano de mitigação
		Processo de mitigação
		Responsabilidade pela mitigação
		Objetivos e métricas de mitigação
	Monitorização	Processo
		Revalidação automatizada de vulnerabilidades
		Exceções

Figura 4. 9 Áreas e controlos associados ao domínio da gestão de vulnerabilidades

4.4.1.9 Domínio 9 – Resposta a incidentes de segurança

Sendo notório o crescimento do número de incidentes em cibersegurança, assim como do seu impacto para o cidadão e particularmente para as organizações. Para enfrentar esta ameaça torna-se inevitável uma monitorização de segurança ativa e abrangente o suficiente, mas também uma resposta eficiente e eficaz. A globalização tecnológica aboliu fronteiras, podendo a ameaça surgir de todo o lado, não sendo opção o isolamento, pois isso seria fatal para qualquer organização. As organizações necessitam de ter políticas e processos fortes para responder a incidentes de segurança e com isso estar dotada das melhores pessoas e tecnologia para o fazer.

O processo de resposta a incidentes envolve diversas fases e por vezes cooperação entre diversas entidades, como sejam parceiros e clientes da organização. Ao abrigo do decreto-lei 65/2021 as organizações tem o dever de reportar determinadas tipologias de incidentes ao CNCS, assim como a outras entidades legais e de supervisão. Por assim se considerar um domínio relevante na metodologia de avaliação, este domínio também foi considerado.

A figura seguinte demonstra o mapeamento das áreas e controlos pertencentes ao domínio da resposta a incidentes de segurança.

9 - Resposta a incidentes de segurança	Governação	Política, norma e processo
	Equipa	Equipa dedicada para resposta a incidentes
		Análise forense
		Funções e responsabilidades
		Formação da equipa
		Simulacros e exercícios
	Operação e execução	Playbooks, workbooks e planos de resposta a incidentes
		Critérios para identificação de incidentes
		Classificação de incidentes
		Reclassificação de incidentes
		Interação com parceiros/fornecedores
	Tecnologia de suporte	Deteção e resposta automatizada
	Reporte	Reporte a reguladores e supervisores
		Recolha e envio de evidências

Figura 4. 10 Áreas e controlos associados ao domínio da resposta a incidentes de segurança

4.4.1.10 Domínio 10 – Arquitetura de segurança

O domínio arquitetura de segurança pode ser visto como transversal, uma vez que tem componentes que existem em outros domínios, como a gestão de vulnerabilidades, a segurança de rede ou a própria segurança aplicacional. Se pensarmos numa perspetiva mais aplicacional, devem existir arquiteturas de referência, mediante a tipologia de solução a desenvolver, onde nunca devem faltar os requisitos de cibersegurança. A arquitetura deve ser estar munida de políticas, processos e práticas seguras que a tornem mais robusta para enfrentar as diferentes ciberameaças. Uma revisão e atualização constante, assim como a partilha com parceiros e fornecedores é uma boa prática e uma baseline que estes devem seguir quando desenvolvem soluções para utilização da organização.

A figura seguinte demonstra o mapeamento das áreas e controlos pertencentes ao domínio da arquitetura de segurança.

10 - Arquitetura de segurança	Classificação de ativos relativamente à segurança	Definições de segurança
	Detalhes sobre os ativos	Responsável pelo ativo
		Renovação de ativos
		Isolamento de ativos obsoletos
		Soluções e ativos de terceiros
		Politicas, normas e procedimentos
	Arquiteturas de referência	Requisitos de segurança
		Arquiteturas diversificadas (cloud, onprem,...,etc.)
		Acompanhamento de segurança
		Ambientes produtivos e não produtivos
		Segregação entre ambientes
	Alta disponibilidade e resiliência	Redundância

Figura 4. 11 Áreas e controlos associados ao domínio da arquitetura de segurança

4.4.1.11 Domínio 11 – Segurança do software

O último domínio integrado na metodologia está associado à segurança do software por igualmente se considerar como importante a sua avaliação. O desenvolvimento aplicacional é necessário ser regulado e verificado antes de ser disponibilizado, sob pena de estar vulnerável e representar um risco financeiro e/ou reputacional para a organização. É crucial que sejam definidas e seguidas práticas seguras no desenvolvimento de código, acompanhadas de verificações e testes ao mesmo. Uma das melhores formas para garantir que o software é desenvolvido segundo os melhores controlos, é definir uma metodologia de Secure Software Developmente Life Cycle (SSDLC), uma vez que a segurança não deve apenas existir durante a fase de desenvolvimento, mas sobretudo depois da entrada em produção, quando de fato encontra-se exposta a ciberameaças.

A figura seguinte demonstra o mapeamento das áreas e controlos pertencentes ao domínio da segurança do software

11 - Segurança do software	Conformidade	Politicas, normas, processos e procedimentos
		Prevenção contra exfiltração de dados
		Aquisição de software de terceiros
		Repositório centralizado para código
		Metodologia de desenvolvimento
		Desenvolvimento interno e externo
		Segurança e privacidade por omissão e por desenho
	Gestão de alterações	Entradas e saídas de produção
	Testes de segurança Aplicacionais	Análise estática e dinâmica ao código
		Testes de penetração (pentesting)
		Testes a API
		Testes em modelo black box e white box

Figura 4. 12 Áreas e controlos associados ao domínio da segurança do software

No anexo 1 a este trabalho encontra-se a metodologia completa, onde foram detalhados os controlos para melhor serem enquadrados por níveis de maturidade.

4.4.2 Escala de maturidade

Com base nas diversas escalas de maturidade identificadas no capítulo dois deste trabalho, mas sobretudo pelo feedback obtido ao longo dos diversos casos de uso realizados, optou-se por uma escala de 4 (quatro) níveis, sendo eles:

- **Nível 1 –> Inicial** – Primeiro nível de maturidade que se caracteriza pela inexistência de processos, procedimentos e práticas definidas, sendo todas as atividades realizadas de forma ad-hoc. Este nível classificação por uma baixa consciencialização e aptidão para a cibersegurança.
- **Nível 2** – **Reativo –** Segundo nível considerado para a escala de maturidade, onde a organização a organização por norma funciona reactivamente. A organização não tem uma vasta formalização no que respeita a normativo e processos, mas existem procedimentos e guias de orientação que foram sendo definidos para responder às diversas situações que foram surgindo. Os recursos não são os mais experientes e preparados para responder a situações associadas a ciberataques e não existe muita tecnologia para suportar as atividades organizacionais associadas à cibersegurança.
- **Nível 3** – **Proactivo –** O terceiro nível classifica a organização que atua proactivamente, tendo para isso definido normativo, processos e procedimentos. A capacidade em antever e reagir às ameaças requer automatização de processos como seja os de monitorização e resposta a incidentes através da análise comportamental e conhecimento antecipado de vulnerabilidades. As organizações enquadradas neste nível estão menos suscetíveis a ciberataques pela robustez.
- **Nível 4** – **Antecipativo –** Quatro e último nível da escala de maturidade, onde são enquadradas as organizações que além de proativas, procuram a melhoria contínua para os seus recursos, processos e tecnologia que já se encontram totalmente automatizados, são neste nível otimizados.

Na tabela seguinte é apresentada a matriz de maturidade que foi elaborada e sustentará a metodologia de avaliação de maturidade

Níveis de maturidade			
Nível 1	**Nível 2**	**Nível 3**	**Nível 4**
Inicial (1-1,99)	**Reativo** (2-2,99)	**Proactivo** (3-3,99)	**Antecipativo** (4)

Tabela 4. 4 Matriz com os níveis de maturidade

4.4.3 Operacionalização da metodologia

Conforme descrito em capítulos anteriores, a metodologia desenvolvida tem como objetivo apoiar na avaliação de maturidade de uma infraestrutura que suporta serviços críticos, embora seja requisito a sua aplicação a qualquer ativo organizacional. Os domínios identificados, assim como os controlos compõem a essência da metodologia. De forma a facilitar o processo de avaliação e torná-lo o mais objetivo possível, foi criado uma matriz em Microsoft Excel com os domínios, áreas e controlos. Para cada controlo foram definidos quatro possíveis estados equivalendo em que o mesmo possa encontrar-se, sendo cada estado um nível de maturidade. Durante a avaliação, o estado de cada controlo é enquadrado num nível maturidade, estando previsto também o estado de não aplicável. O somatório de cada controlo permite aferir a maturidade média de cada domínio, tendo sido assumido que os controlos têm pesos semelhantes em termos de contributo para a média. Tendo os domínios todos aferidos é obtido de forma automática a maturidade global da infraestrutura.

4.5 Apresentação de testes e resultados

Ao longo deste capítulo será apresentado o caso de uso que sustentou a realização dos testes utilizando a metodologia, assim como os resultados obtidos. Foram realizados diversos casos de teste, tendo por base diferentes cenários em termos de infraestrutura e organizações alvo.

4.5.1 Descrição do caso de teste

A realização de diversos casos de testes, contemplando diferentes cenários permitiu identificar diversas falhas e incoerências na metodologia, que foram sendo corrigidas até obtermos uma versão que consideramos mais objetiva, assertiva, fácil de responder.

O caso de teste que passamos a descrever foi realizado por uma pequena organização com 8 anos de existência e cerca de 25 colaboradores. Trata-se de uma organização muito orientada para a prestação de serviços na vertente de tecnologias de informação e teve o seu maior crescimento quer em faturação quer em número de colaboradores após a chegada da pandemia (COVID-19). O *core* desta organização é a consultoria, apostando essencialmente em contratação de jovens licenciados nas áreas das TIC, em particular Cibersegurança. Apesar dos serviços Core onde apostam ser a consultoria, recentemente também se dedica a serviços criação e alojamento de sites e portais públicos para micro e pequenas que necessitam de expor os seus produtos, mas não querem ter qualquer administração e gestão sobre estes portais. Esta componente têm crescido de forma relevante em virtude de algumas parcerias e aquisições que tem vindo a ser realizadas.

Pela dimensão que tem, esta organização tem uma estrutura simplificada e pouco "pesada", onde o proprietário tem o papel de administrador e todas as decisões tem obrigatoriamente a sua aprovação. Existe ainda um departamento administrativo com 2 colaboradores que garantem toda a componente funcional e administrativa (RH, aquisições, contratações, pagamentos, cobranças, etc.). O departamento de IT têm um responsável sénior que é apoiado para outro colaborador menos experiente que asseguram o funcionamento de toda a componente interna de IT (servidores, impressoras, computadores, telemóveis, backups, etc.). Finalmente existem duas equipas de entrega, a equipa de consultores e uma equipa de menor dimensão que tem a responsabilidade de desenvolver sites e portais públicos.

4.5.2 Execução do caso de teste

O caso de teste foi executado de forma totalmente autónoma, após ter sido explicado a forma como a mesma foi concebida e como deveria interpretada. Foi solicitado às entidades que respondessem de forma honesta e o mais realista possível, para que os resultados pudessem espelhar a realidade da infraestrutura, e com isso percecionar o nível de maturidade que melhor a enquadra. O resultado do caso de uso pode ser consultado no anexo 2 a este trabalho.

O questionário de maturidade foi preenchido pelo administrador da organização com total apoio do responsável interno do IT. Durante a resposta ao questionário surgiram diversas dúvidas de interpretação que foram sendo clarificadas por meio de reuniões rápidas que foram sendo realizadas. Nas versões iniciais

do questionário havia uma tendência para que os resultados fossem inflacionados em virtude da má interpretação associadas à forma como os controlos eram descritos em cada nível. Verificou-se ainda que em todas as avaliações, os resultados eram também inflacionados por existia uma certa resistência em aceitar que poderiam ter valores baixos em determinados domínios. Os valores obtidos por norma eram ajustados para baixo nas reuniões ocorridas pós preenchimento do questionário.

Ainda foi equacionada e discutida a hipótese do questionário se respondido pelas organizações com o nosso apoio, mas não foi bem acolhida, porque era interpretada como algo mais formal, deixando de ser uma "autoavaliação" voluntária onde as organizações estão a colaborar e a contribuir para testar uma metodologia e simultaneamente perceberem a estado de maturidade das suas infraestruturas.

A realização do caso de uso permitiu incluir novos controlos que inicialmente não constavam e ajustar outros que não estavam claros.

Os gráficos seguintes demonstram o nível de maturidade por domínio, assim como a maturidade global da infraestrutura

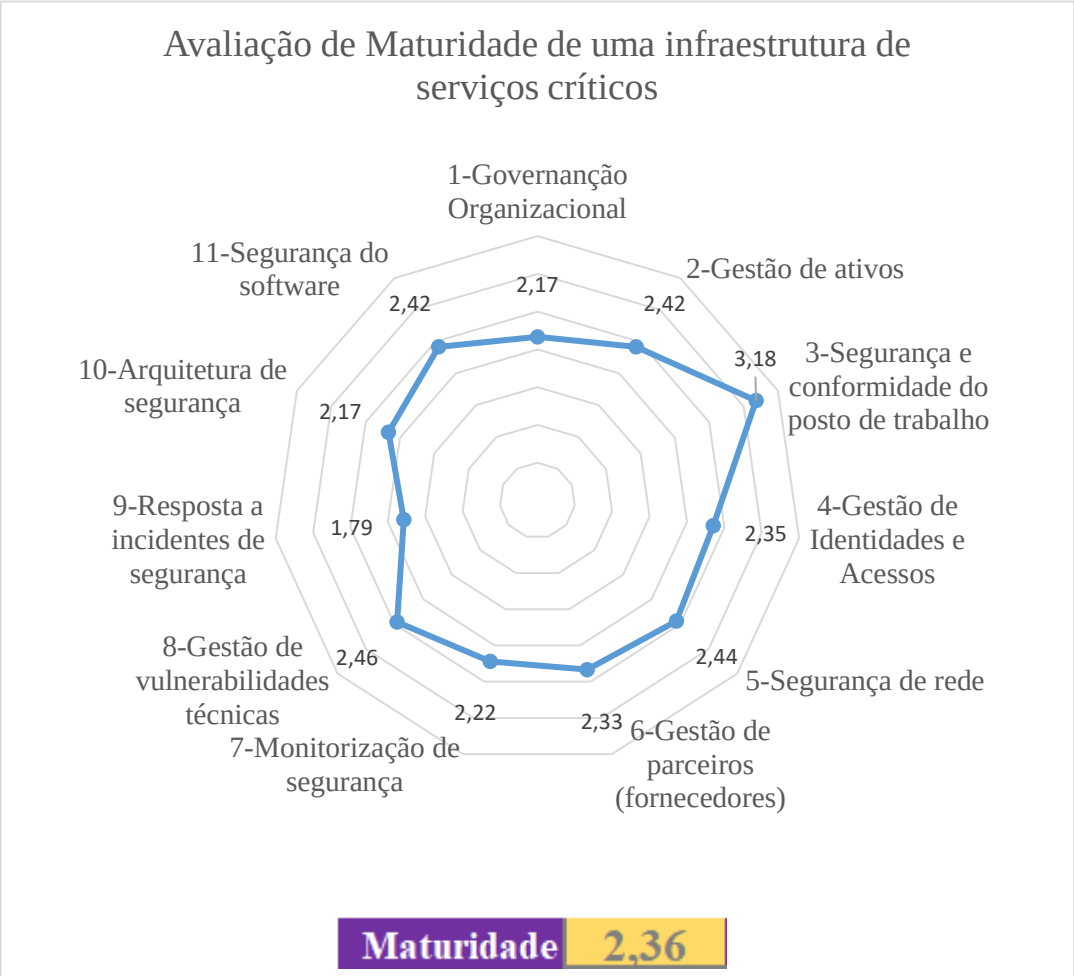

Figura 4. 13 Visão holística da maturidade por domínio

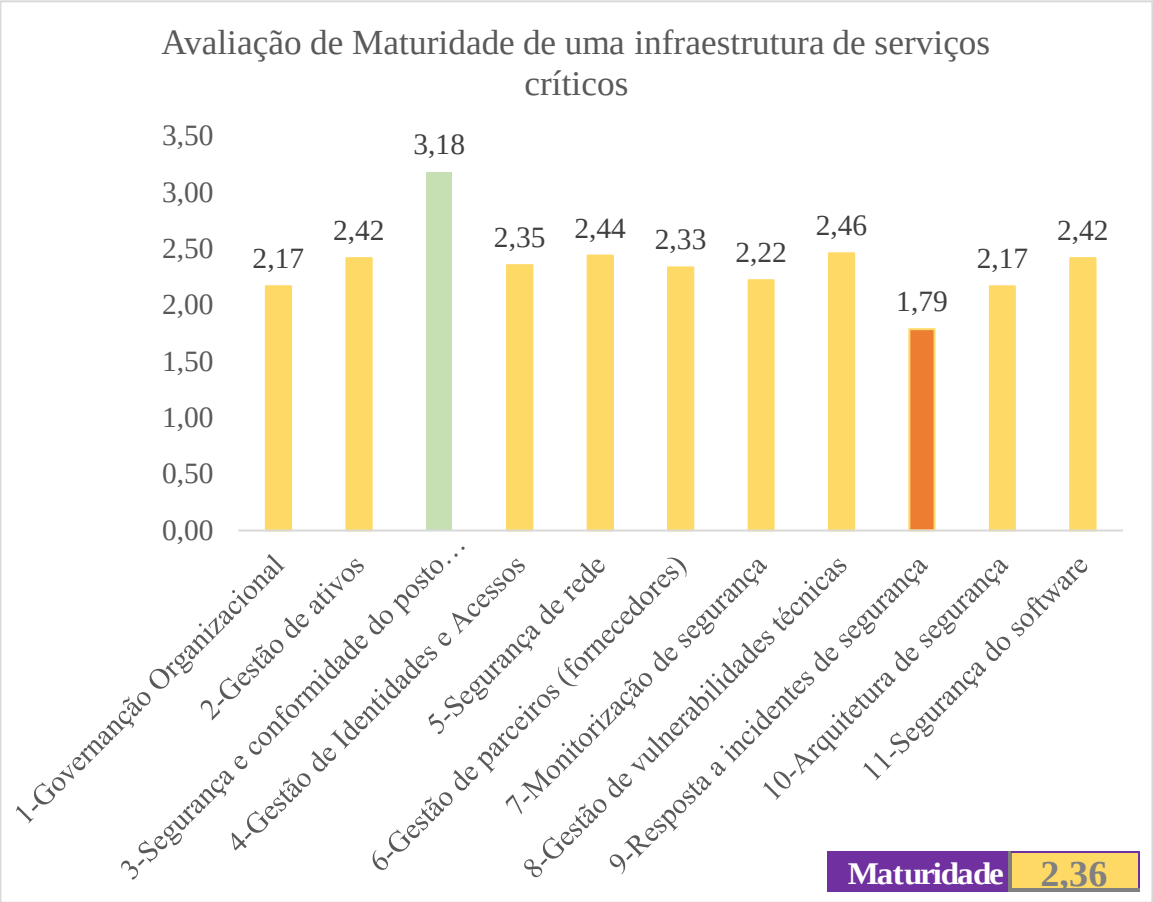

Figura 4. 15 Visão da maturidade em gráfico de barras

4.5.3 Interpretação de resultados

Numa escala definida com 4 níveis de maturidade, foi atingido um valor de 2,36, poderemos afirmar que no geral a organização tem uma postura reativa em matéria de cibersegurança na infraestrutura que foi avaliada. Fazendo uma análise mais detalhada e por domínio, verifica-se que ao nível da segurança e conformidade do posto de trabalho é obtido o nível 3, ou seja, proativo, pelo facto de existirem políticas e controlos implementados ao nível do posto em virtude dos requisitos que são solicitados pelos diversos clientes em virtude dos diferentes projetos de consultoria. Este é o único domínio classificado como proactivo. Em lado oposto, a organização classificou um domínio com nível 1 ou inicial, em virtude da pouca maturidade e consciencialização dá para a cibersegurança no que respeita a resposta a incidentes de segurança. Perante este resultado, podemos concluir que a capacidade de enfrentar um incidente de segurança e dar uma resposta assertiva e rápida é baixa.

Os restantes domínios enquadram-se no nível 2 da matriz, ou seja, nível reativo com baixa capacidade de enfrentar ciberameaças. Com a visibilidade dada pela avaliação, a organização está em melhor posição para traçar objetivos de crescimento, tomando as decisões mais assertivas que fazendo baixos investimentos, é possível obter resultados rápidos, aumentando a maturidade paralelamente em diversos domínios. Outra vertente que a metodologia permite é a vertente de gestão de risco, embora consideramos que seria necessário ter mais domínios avaliados.

Do ponto de vista prático a organização reconheceu a valor obtido na avaliação de maturidade da infraestrutura onde são disponibilizados serviços críticos para os seus clientes. Estes portais requerem uma disponibilidade de 24x7x365, traduzindo-se a sua indisponibilidade em quebras financeiras para os seus proprietários pelo facto de não poderem comercializar os seus produtos. Alguns destes portais tem disponibilizado um serviço de compras online (serviço disponibilizado por outras organizações). Neste sentido esta organização tem uma forte responsabilidade em manter disponível serviços aos seus clientes de forma permanente e segura.

Após realização da avaliação de maturidade foi definido um plano de ação a curto prazo onde foram identificadas medidas concretas de implementação rápida e com pouco esforço, mas que permitem colmatar deficiências e melhorias consideráveis (quick-wins). Ainda no curto prazo iria ser definido um plano com maior abrangência e um investimento considerável para implementar melhorias estruturais e profundas com vista a obter resiliência e maior segurança na componente de infraestrutura que se encontra exposta à internet.

Também a camada aplicacional alterações iriam ser realizadas ao nível do desenvolvimento e conceção aplicacional, mas sobretudo em testes e verificações de segurança a realizar antes da entrada em

produção de novos módulos e componentes, mas assegurar a realização de testes regulares que identifiquem vulnerabilidade do tipo (SQLi, XSS e outras).

Apesar da organização em causa não ter obrigação legal ou regulamentar ao abrigo do DL 65/2021 responder ao CNCS, indiretamente tem responsabilidades para com os seus clientes onde prestam serviços de consultoria em demonstrar avaliações de riscos e maturidade sobre os seus ativos. Neste sentido, a organização pode partilhar esta avaliação com estes clientes, caso assim o entenda fazer.

4.5.4 Contributos e lições aprendidas

Durante a realização do trabalho houve necessidade em rever diversas vezes a escala de maturidade a utilizar, por forma a melhorar a efetividade dos controlos que estavam a ser alvo de avaliação. Começou-se por utilizar a escala referida no capítulo 2 referente ao *Capability Maturity Model* (CMM). Contudo, mas após ter sido realizado o primeiro caso de uso, verificou-se que para determinados controlos era difícil distinguir as diferenças em termos de maturidade nos diferentes níveis da escala, devido aos 5 níveis utilizados.

Tomou-se nesta altura a decisão em alterar a escala para uma nova com apenas 3 níveis, sendo eles, o inicial, intermédio e avançado. Mediante esta alteração, a lista de controlos foi igualmente atualizada, mas rapidamente foi percetível que também não seria esta a solução, essencialmente pelo "gap" criado entre o nível intermédio e o nível avançado, levando a que alguns controlos sobre sobreavaliados porque o nível anterior era cumprindo minimamente e não na totalidade.

O passo seguinte foi recriar uma nova matriz de maturidades, desta vez com 4 níveis que após ter sido testada em diversos casos de uso verificou que seria a mais adequada e ajustada perante todos os cenários avaliados.

Os casos de uso permitiram ainda fazer diversos ajustes em termos de controlos, sobretudo na descrição dos mesmos e adequação aos diferentes níveis da matriz de maturidade, por forma a tornar mais claro a sua definição e aplicabilidades. Com esta decisão o número de controlos classificados como " Não Aplicável" baixou drasticamente.

Podemos concluir que a realização foram primordiais para testar o funcionamento da metodologia e dando confiança sobre os valores obtidos. Esta confiança foi obtida pelos ajustes realizados e pelo reconhecimento das organizações que se disponibilizaram e colaboraram na resposta ao questionário.

Capítulo 5

CONCLUSÕES E TRABALHOS FUTUROS

Neste capítulo é feita uma conclusão geral sobre o trabalho realizado, com particular foco na metodologia desenvolvida e apresentada no capítulo anterior. Ainda neste capítulo é feita uma reflexão sobre uma perspetiva de continuidade que pode ser dada à metodologia, de forma a torná-la mais abrangente e completa.

5.1 Conclusões

O aumento generalizado do cibercrime, requer que a sociedade adote uma atitude segura e proativa relativamente à cibersegurança. A ameaça é global e constante, podendo surgir de qualquer parte e a qualquer momento, obrigando a utilizador cibernauta estar atento e adotar uma postura também defensiva e desconfiar sobre o que lhes é oferecido.

Por outro lado, a evolução tecnológica e o crescimento de serviços digitalizados e online é uma inevitabilidade, sendo que uma parte da sociedade não está preparada para lidar com esta evolução, mas por outro lado também não pode ser motivo para não evoluir. A solução para este dilema é regular o crescimento, salvaguardando os interesses dos clientes e utilizadores destes serviços tecnológicos.

As organizações tem obrigação de salvaguardar os interesses e os dados dos seus clientes que lhes estão confiados. O estado através das diversas entidades reguladores e setoriais tem vindo a assumir cada vez mais um papel de supervisão e controlo sobre as actividades destas organizações, impondo-lhes medidas e ações que visem proteger os interesses dos clientes a quem estas organizações prestam serviços. Em diversos setores da atividade existem regulamentação de cumprimento obrigatório e felizmente no campo da cibersegurança e da utilização do ciberespaço não tem sido exceção, sendo prova disso o DL 65/2021. Este decreto-lei tem aplicabilidade a um contexto específico e a uma tipologia de organizações alvo, mas obrigam as organizações a definirem e implementarem mecanismos e controlos de segurança que robustos o suficiente para assegurar o funcionamento das suas infraestruturas e serviços essenciais.

Pelos mais diversos motivos algumas organizações não têm experiência, recursos, nem maturidade para implementar estes tipos de controlos que assegurem a robustez das suas infraestruturas por um lado e por outro poderem responder de forma assertiva os requisitos do DL 65/2021. Foi com base neste cenário

que surge esta dissertação e assim apoiar o processo de avaliação de maturidade de infraestruturas críticas. A definição da metodologia foi um processo moroso pela complexidade que lhe está inerente. Complexidade esta que inicialmente não foi contemplada, uma vez, que havia uma ideia generalizada que os modelos e standards pré-existentes ajudariam neste campo. Porém, logo na fase de definição foi percetível que estes modelos não tinham o detalhe necessário para qualificar os controlos em cada um dos níveis da escala. Esta situação levou a que fosse iniciada uma nova investigação por outros modelos que colmatassem esta deficiência. Modelos estes que ajudaram na definição e conceção da metodologia, mas na sua maioria verificou-se tratam os controlos de forma binário, ou seja, estão ou não estão implementados e aplicar este conceito, torna a avaliação mais subjetiva. Subjetiva porque obrigaria a trabalhar com pesos e ponderações para cada controlo e à definição de uma nova escala, em cada o nível de maturidade seria apurado mediante o número de controlos implementados. Se pensarmos num domínio de segurança com 100 controlos definidos e avaliados segundo uma escala com 4 níveis de maturidade, de forma rápida poderíamos afirmar que tendo 50 controlos implementados, teríamos um nível de maturidade de 50%. Este critério pareceu-me pouco viável pelos motivos já explicados e ainda pelo fato de não sabermos se todos os controlos que deveria ser definidos e avaliados para cada domínio.

Neste sentido, optou-se por uma escala com 4 níveis de maturidade, a utilização de controlos que já definidos e utilizados pelo principais modelos e standards seria a mais assertiva a enquadrar cada controlo num nível de maturidade mediante a completude e a efetividade que os caracterizam em cada nível. Esta completude e efetividade foi obtida tendo por base modelos da indústria da cibersegurança, boas práticas em e uma forte componente de experiência profissional na área de cibersegurança, assim como experiência em auditoria para certificação (ex. 27001, COBIT5,etc.). Entendemos que a metodologia desenvolvida que essencialmente assenta num questionário sobre a maturidade de controlos de cibersegurança está bem sustentada e apta para ser utilizada, havendo espaço para melhoria e inclusão de mais domínios, áreas e controlos, mas sobre esta componente, abordaremos no capítulo certo.

5.2 Trabalhos futuros

Os domínios utilizados na metodologia de avaliação não incluem todos os domínios atualmente existentes na segurança e cibersegurança, é possível alargar e completá-la com os restantes, ficando a mais completa e mais robusta. Por outro lado, os controlos utilizados também foram retirados das diversas frameworks explicadas no capítulo 2 deste trabalho, mas existem outros mais que podem ser também utilizados, mesmo nos 11 domínios que a metodologia utiliza atualmente. Talvez a parte mais difícil seja descrever cada controlo dentro dos 4 níveis de maturidade existente, mas esse trabalho faz-se com muita

pesquisa e análise, experiência, novas tipologias de ameaças e ciberataques que implica fazer oposição e novas tecnologias que aumenta a eficácia na resposta as estas ameaças.

A escala de maturidade conforme descrito anteriormente foi a que melhor se adaptou aos diversos casos de uso realizados. Contudo com a inclusão de novos domínios e controlos é crucial ser devidamente retestada para assegurar que assim se mantém. O alvo da metodologia foi uma infraestrutura crítica, mas poderá ser aplicada a um outro contexto, embora não tenha sido testada para isso, assim como os controlos utilizados foram selecionados para o cenário definido.

REFERÊNCIAS

[1] Network and Information Security 2 (2022*)*. Disponível no endereço: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555 (acedido a: 8 Junho de 2023).

[2] Diretiva da UE 2016/1148 - *Diretiva (UE) 2016/ 1148 do Parlamento Europeu e do Conselho*. Disponível no endereço: https://www.cncs.gov.pt/docs/diretiva-2016.pdf (Acedido em: 19 de dezembro de 2022).

[3] *Coronavirus* by *World Health Organization*. World Health Organization. Disponível no endereço: https://www.who.int/health-topics/coronavirus#tab=tab_1 (acedido a: 8 de dezembro de 2022).

[4] Quadro Nacional de Referência para a CiberSegurança - *Centro Nacional de Cibersegurança*. Disponível no endereço: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf (acedido a: 13 de dezembro de 2022).

[5] "O que é a gestão de risco e a sua importância" - *What is risk management? - IBM*. Disponível no endereço: https://www.ibm.com/topics/risk-management (acedido a: 18 de dezembro de 2022).

[6] "Definição de Infraestrutura critica, segundo a Comissão Europeia" - *Critical infrastructure - Migration and Home Affairs*. Disponível no endereço: https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en (acedido a: 6 de dezembro de 2022).

[7] "Definição de Infraestrutura critica, segundo o NIST" - *Critical Infrastructure Perspectives* (2021) *NIST*. Disponível no endereço: https://www.nist.gov/cyberframework/critical-infrastructure-perspectives (acedido a: 6 de dezembro de 2022).

[8] Lei 46/2018 – Estabelece o Regime Jurídico da Segurança do Ciberespaço – Publicada no *Dre.pt*. Disponível no endereço: https://dre.pt/dre/detalhe/decreto-lei/20-2022-178264070?_ts=1649635200044 (acedido a: 8 de dezembro de 2022).

[9] Serviços essenciais - *Employment, Social Affairs & Inclusion - Access to essential services - Employment, Social Affairs & Inclusion - European Commission*. Disponível no endereço: https://ec.europa.eu/social/main.jsp?catId=1592&langId=en (acedido a: 19 de dezembro de 2022).

[10] Sectores de atividade identificados como críticos pela UE - *Lex - L33259 - en - EUR-Lex*. Disponível no endereço: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33259 (acedido a: 19 de dezembro de 2022).

[11] Sectores de atividade identificados como críticos para economia norte-americana - *Critical Infrastructure Sectors - Cybersecurity and Infrastructure Security Agency CISA*. Disponível no endereço: https://www.cisa.gov/critical-infrastructure-sectors (acedido a: 19 de dezembro de 2022).

[12] Programa Europeu para Protecção de Infraestruturas Críticas - *Lex - l33260 - en - EUR-Lex EUR*. Disponível no endereço: https://eur-lex.europa.eu/EN/legal-content/summary/european-programme-for-critical-infrastructure-protection.html (acedido a: 19 de dezembro de 2022).

[13] O ataque terrorista ocorrido a 11 de setembro nos EUA - *Homepage | National September 11 Memorial & Museum*. Disponível no endereço: https://www.911memorial.org/ (acedido a: 19 de dezembro de 2022).

[14] Regulamento Geral sobre a Protecção de Dados - *Regulamento(ue) n.º 679/2016, DE 27 de abril*. Disponível no endereço: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&tabela=leis (acedido a: 19 de dezembro de 2022).

[15] CERT.PT (Equipa de resposta a incidentes de segurança) - SoftConcept, C.N.de C.S. (2019) *Cert.pt, CNCS*. Disponível, no endereço: https://www.cncs.gov.pt/pt/certpt/ (acedido a: 14 de janeiro de 2023).

[16] Decreto lei 65/2021 - (2021) *Dre.pt*. Disponível no endereço: https://dre.pt/dre/detalhe/decreto-lei/65-2021-168697988 (acedido a: 13 de dezembro de 2022).

[17] Sistemas de controlo industrial (ICS) - *Industrial Control System* (2022) *Wikipedia*. Wikimedia Foundation. Disponível no endereço: https://en.wikipedia.org/wiki/Industrial_control_system (acedido a: 14 de janeiro de 2023).

[18] O IIOT - Newark (2021) *The Industrial Internet of Things, IEEE Spectrum*. IEEE Spectrum. Disponível no endereço: https://spectrum.ieee.org/the-industrial-internet-of-things (acedido a: 23 de dezembro de 2022).

[19] “Definição de ciberataque segundo a NIST” - Editor, C.S.R.C.C. (no date) *Cyber attack - glossary: CSRC, CSRC Content Editor*. Disponível no endereço: https://csrc.nist.gov/glossary/term/cyber_attack (Acedido a: 23 de dezembro de 2022).

[20] ENISA (2022) *Sobre a ENISA - agência da união europeia para a Cibersegurança, ENISA*. Disponível no endereço: https://www.enisa.europa.eu/about-enisa/about/pt (acedido a: 14 de janeiro de 2023).

[21] Relatório ENISA sobre ciberataques em 2022 - *Enisa Threat Landscape 2022* (2022) *ENISA*. Disponível no endereço: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (Acedido a: 23 de dezembro de 2022).

[22] *Dark web - Dark web* (2022) *Wikipedia*. Wikimedia Foundation. Disponível no endereço: https://en.wikipedia.org/wiki/Dark_web (Acedido a: 23 de dezembro de 2022).

[23] Ciberataques contra infraestruturas críticas no mundo- Hemsley, K.E. and E. Fisher, D.R. (2018) *History of industrial control system cyber incidents*, *History of Industrial Control System Cyber Incidents (Technical Report) | OSTI.GOV*. Disponível no endereço: https://www.osti.gov/servlets/purl/1505628 (Acedido a: 23 de dezembro de 2022).

[24] Ciberataques em Portugal – Relatórios do CNCS - Caçador, F. (2022) *2022 foi um "ano terrível" para a Cibersegurança em Portugal e especialistas Avisam Que 2023 Pode Ser Pior, SAPO Tek*. Disponível no endereço: https://tek.sapo.pt/noticias/computadores/artigos/2022-foi-um-ano-terrivel-para-a-ciberseguranca-em-portugal-e-especialistas-avisam-que-2023-pode-ser-pior (acedido a: 02 de janeiro de 2023).

[25] O conflito Russo-Ucraniano - Team, T.V.J. (2022) *Ukraine conflict: Simple Visual Guide to the Russian invasion*, *BBC News*. BBC. Disponível no endereço: https://www.bbc.com/news/world-europe-60506298 (acedido a: 13 de dezembro de 2022).

[26] A guerra cibernética entre a Rússia e a Ucrânia - Bateman, J. (2022) *Russia's wartime cyber operations in Ukraine: Military impacts, influences, and implications*, *Carnegie Endowment for International Peace*. Disponível no endereço: https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657 (acedido a: 19 de dezembro de 2022).

[27] Consequências resultantes de um ciberataque - Deane, A.J. and Kraus, A. (2021) *CISSP Certified Information Systems Security professional: The official (ISC)2 CISSP CBK reference*. Hoboken, NJ: Sybex.

[28] *Framework* ISO27005 para gestão de risco nos sistemas de informação. Disponível no endereço: https://inen.isolutions.iso.org/obp/ui#!iso:std:iso-iec:27000:ed-5:v1:en. (acedido a: 23 de dezembro de 2022).

[29] *Framework NCAF* disponibilizada para comissão europeia - *National Capabilities Assessment Framework* (2021) *ENISA*. Disponível no endereço: https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework (acedido a: 15 de janeiro de 2023).

[30] O que é computação na nuvem? Google cloud (no date) Google. Google. Disponível no endereço: https://cloud.google.com/learn/what-is-cloud-computing?hl=pt-br (acedido a: 15 de fevereiro 2023).

[31] Regulamento EU 2019/881 – Lex – 32019R0881 – Eur-Lex EUR. Disponível no endereço: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=CELEX%3A32019R0881 (acedido a: 17 março de 2023).

[32] Decreto lei *20/2022* (2022) *Diariodarepublica.pt*. Disponível no endereço: https://diariodarepublica.pt/dr/detalhe/diario-republica/20-2022-178264068 (acedido a: 31 maio de 2023). [33] CE (2008) Directiva *2008/114/CE*, *EUR*. Disponível no endereço: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32008L0114 (acedido a: 01 junho de 2023).

[34] Decreto lei *62/2011* (2011) *Diariodarepublica.pt*. Disponível no endereço: https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2011-178360650-178364421 (acedido a: 01 junho de 2023).

[35] REGULAMENTO DE EXECUÇÃO (UE) 2018/151 Jornal Oficial da União Europeia (2018) *EUR*. Disponível no endereço: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679 (acedido a 07 junho de 2023).

[36] Network and Information Security (2016) *EUR*. Disponível no endereço: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679 (acedido a: 08 junho de 2023).

[37] Cloud Security Alliance. Disponível no endereço: https://cloudsecurityalliance.org/about/ (acedido a: 09 junho de 2023).

[38] CAS Security Trust & Assurance Registry. Disponível no endereço: https://cloudsecurityalliance.org/star (acedido a: 12 junho de 2023).

[39] *GDPR:* Code of conduct, Cloud Security Alliance. Disponível no endereço: https://cloudsecurityalliance.org/privacy/gdpr/code-of-conduct/ (acedido a: 12 junho de 2023).

[40] Russo, A.J. (2003) Cloud Privada, Amazon. Disponível no endereço: https://aws.amazon.com/pt/what-is/private-cloud/ (acedido a: 11 junho de 2023).

[41] Microsoft (2020) Build hybrid and multicloud architectures with Azure Hybrid Solution Architectures, Techcommunity.microsoft.com. Disponível no endereço: https://techcommunity.microsoft.com/t5/itops-talk-blog/build-hybrid-and-multicloud-architectures-with-azure-hybrid/ba-p/1984861 (acedido a: 11 junho de 2023).

[42] *Cross-cloud scaling - on-premises data - azure architecture center, Azure Architecture Center | Microsoft Learn*. Disponível no endereço: https://learn.microsoft.com/en-us/azure/architecture/example-scenario/hybrid/hybrid-cross-cloud-scale-on-premises-data (Acedido a: 12 junho de 2023).

[43] O que são serviços IaaS, PaaS e SaaS? Disponível no endereço: https://www.redhat.com/pt-br/topics/cloud-computing/iaas-vs-paas-vs-saas (acedido a: 12 junho de 2023).

[44] Cloud Community Model. Disponível no endereço: https://www.tutorialspoint.com/cloud_computing/cloud_computing_community_cloud_model.htm (acedido a: 15 junho de 2023).

[45] SGS, O CICLO PDCA E a ISO 27001. Disponível no endereço: https://www.sgs.pt/pt-pt/news/2022/10/o-ciclo-pdca-e-a-iso-27001 (acedido a: 15 junho de 2023).

[46] ISACA, A Global Business & Technology Community. Disponível no endereço: https://www.isaca.org/about-us (acedido a: 14 junho de 2023).

[47] Integrity, ISO 27001 Sistema de Gestão de Segurança da Informação. Disponível no endereço: https://www.27001.pt/iso27001_3.html (acedido a: 15 junho de 2023).

[48] Brumfield, C. and Haugli, B. (2022) *Cybersecurity Risk Management: Mastering the fundamentals using the NIST Cybersecurity Framework*. Hoboken: John Wiley & Sons.

49] NIST, Framework for improving critical infrastructure cybersecurity. Disponível no endereço: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (acedido a: 19 junho de 2023).

[50] NIST, *Cybersecurity framework*. Disponível no endereço: https://www.nist.gov/cyberframework (acedido a: 21 junho de 2023).

[51] US, Department of Energy, Cybersecurity Capability Maturity Model Framework. Disponível no endereço: https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf (acedido a: 17 junho de 2023).

[52] US, Department of Defense, Cybersecurity Maturity Model Certification. Disponível no endereço: https://dodcio.defense.gov/CMMC/ (acedido a: 17 junho de 2023).

[53] *CMMC 2.0*, compliance mapping for Sensitive Content Communications *(2023)*. Disponível no endereço: https://www.kiteworks.com/guide-cmmc-2-0-compliance-mapping-for-sensitive-content-communications/ (acedido a: 19 junho 2023).

[54] Guide to assessing security maturity - vmware. Disponível no endereço: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-a-guide-to-assessing-security-maturity.pdf (acedido a: 19 junho de 2023).

Capítulo 6

APÊNDICES

6.1 Metodologia desenvolvida

Domínio	Área	Controlo	Nível 1 - Inicial	Nível 2 - Reativo	Nível 3 - Proativo	Nível 4 - Antecipativo	Maturidade
Governança Organizacional	**Estratégia para a cibersegurança**	**Comprometimento da gestão de topo**	O envolvimento da Gestão de topo em matéria de segurança é informal e pouco dedicada	A gestão de topo têm uma baixa participação, muitas vezes ocorrendo na sequência de um incidente	A gestão de topo têm uma ampla participação e visibilidade sobre a temática da cibersegurança, percebendo a necessidade e apoiando a causa	Existe uma total participação da gestão de topo, que compreende a necessidade da cibersegurança para o funcionamento da organização, procurando estar envolvida e supervisionando as atividades	
		Disponibilização de recursos	São disponibilizados poucos recursos, por se interpretar a segurança como um custo e não um investimento	São disponibilizados alguns recursos, embora insuficientes face ao contexto organizacional	A organização percebe a importância da cibersegurança e esforça-se por disponibilizar os recursos necessários	A organização está comprometida em disponibilizar os recursos necessários (humanos, materiais e processuais)	
		Envolvimento de terceiras partes	A interação com parceiros é feita de forma pontual, ocorrendo muitas vezes em cenários de incidente. A organização não transmite os seus requisitos em matéria de cibersegurança, não podendo responsabilizá-los posteriormente	Existe alguma interação com os parceiros ainda que limitada e muitas vezes impulsionada por requisitos legais ou de regulatório	É estabelecido um contacto formal e permanente, obrigando o parceiro a cumprir com os requisitos organizacionais. Durante o processo de contratação é avaliado o risco e a resiliência de cada parceiro	É estabelecido um contacto formal e permanente obrigando o parceiro a cumprir com os requisitos organizacionais e monitorizando a atividade e resiliência do parceiro. A avaliação de risco de cada parceiro, assim como o seu rate é monitorizado diariamente, sendo despoletados alertas em caso de alterações no *rate* ou atividades associadas a ciberataques	

		Definição da estratégia	Em virtude da pouca sensibilização para a cibersegurança, a organização não formaliza uma estratégia para o governo da cibersegurança	É definida uma estratégia, embora não esteja difundida em todas as áreas da organização, sendo a revisão executada de forma pontual	Existe uma estratégia definida e difundida por toda a organização alinhada com as melhores práticas e suportada em frameworks robustas. A estratégia é revista anualmente e ajustada se necessário	Existe uma estratégia definida e alinhada com as melhores práticas e suportada em frameworks robustas, encontrando-se difundida por toda a organização. Cada departamento é solicitado para participar e contribuir ativamente na definição dessa estratégia. Existe um comité de segurança de informação que reúne trimestralmente, sendo responsável pela revisão periódica da estratégia		
	Processo deContratação	***Background check***	Não é realizada qualquer análise prévia à contratação sobre o background, sendo todo o processo tratado de forma informal	É realizado alguma verificação sobre o background, embora sem um processo definido	Existe um processo formalizado que é seguido durante o processo de contratação, seja para colaboradores ou parceiros	Existe um processo formalizado que é seguido durante o processo de contratação, seja para colaboradores ou prestadores de serviços. De forma regular é feito um background check em particular nos prestadores de serviços assim como os critérios incluídos na lista de verificações		
		Programa para retenção de talento e conhecimento	A organização não tem definido um programa para retenção de talento e conhecimento	A organização não tem definido um programa formal para retenção de talento e conhecimento, embora acontecem casos em que isso acontece, mas geridos pelos respetivos departamentos	A organização tem definido um programa para retenção de talento e conhecimento	A organização tem definido um programa para retenção de talento e conhecimento transversal a toda a organização, tendo cada departamento a responsabilidade de dar contributos sobre cada colaborador. A organização revê e atualiza regularmente o programa		

		Modelo de contratação de colaboradores	A organização não tem instituído um programa ou processo para contratação. A contratação é realizada à medida das necessidades	A organização não tem instituído um programa ou processo formal para contratação. A contratação é ad-hoc e numa primeira instância é assente em referenciação	A organização tem instituído um programa ou processo formal para contratação	A organização tem instituído um programa ou processo formal para contratação que assenta na referenciação e recomendação. Quando isso não é possível, recorre a empresas de *placement*		
		Cláusulas de confidencialidade e retenção de informação	Não existe qualquer cláusula no contrato de trabalho para colaboradores diretos ou no contrato de prestação de serviços sobre a confidencialidade e retenção de dados da organização	Existem cláusulas no contrato de trabalho para colaboradores diretos, bem como no contrato de prestação de serviços, sobre a confidencialidade e retenção de dados da organização	Existem cláusulas no contrato de trabalho para colaboradores diretos, bem como no contrato de prestação de serviços, sobre a confidencialidade e retenção de dados da organização, prevendo penalizações pelo seu incumprimento. A organização monitoriza o cumprimento destas cláusulas	Existem cláusulas no contrato de trabalho para colaboradores diretos, bem como no contrato de prestação de serviços, sobre a confidencialidade e retenção de dados da organização, prevendo penalizações pelo seu incumprimento. A organização monitoriza o cumprimento destas cláusulas e obriga a formação regular sobre a importância da confidencialidade		
		Subcontratação em cadeia	Não existe qualquer impedimento para a subcontratação em cadeia por partes dos parceiros	Todos os parceiros são obrigados a informar a organização caso pretendam realizar SUB subcontratações, mediante as cláusulas definidas no contrato de prestação de serviços	Todos os parceiros são obrigados a informar a organização caso pretendam realizar SUB subcontratações, mediante as cláusulas definidas no contrato de prestação de serviços com penalizações em caso de incumprimento. A organização dispõe de um prazo definido no contrato para se pronunciar sobre a SUB subcontratação. Findo esse prazo, caso o subcontratante não tenha recebido feedback poderá avançar	Os prestadores de serviço são obrigados a não implementar subcontratação em cadeia, mediante definido no contrato de prestação de serviços com penalizações em caso de incumprimento. A organização faz uma monitorização apertada e requer que todos os colaboradores externos cumpram com formação interna e adiram às políticas em vigor		

		Código de ética e conduta profissional	A organização não possui qualquer código de ética	A organização possui um código de ética, obrigando que todos os colaboradores internos ou externos adiram ao mesmo	A organização possui um código de ética obrigando que todos os colaboradores internos ou externos adiram ao mesmo, monitorizando a sua adequação e atualizando-o regularmente	A organização possui um código de ética obrigando que todos os colaboradores internos ou externos adiram ao mesmo, monitorizando a sua adequação e atualizando-o de forma regular, obrigando a que todos os colaboradores recebem formação atempada sobre a sua alteração. A organização possui ainda um departamento dedicado à ética e conduta profissional que é responsável por lidar com casos em que existe falha no cumprimento do mesmo		
		Normativo de segurança	A organização não definiu qualquer política ou norma relativamente à cibersegurança	Existe uma política de segurança de informação e um conjunto de normas que sustentam esta política	Existe uma política de segurança de informação e um vasto leque de política que sustentam esta política, procedendo-se à criação de novas políticas em virtude das necessidades	Existe uma política de segurança de informação e um vasto leque de política que sustentam esta política, sendo ágil o processo de elaboração de novas normas e a sua revisão feita anualmente para garantir a sua adequação. Num cenário de incidente de segurança ou outro evento relevante é avaliada a necessidade de rever alguma norma ou política		

	Gestão de Risco	**Função Risco**	A avaliação de risco é realizada de forma pontual e apenas em cenários de ocorrência de incidentes	Existe um processo de gestão de risco básico abrangendo apenas algumas áreas organizacionais, envolvendo revisões pontuais e pouco formalizadas	Existe um processo de gestão de risco formal, aprovado pela gestão de topo com cobertura total sobre os activos de informação, com revisões periódicas e monitorização apertada	Existe um processo de gestão de risco formal, aprovado pela gestão de topo com cobertura total sobre os activos e todos os parceiros. São realizadas revisões periódicas, sendo o risco monitorizado de forma apertada através de uma ferramenta de gestão de risco que despoleta alertas e reavaliações a activos que apresentam mais vulnerabilidades ou fraquezas, assim como a parceiros cujo seu *rate* de risco decresça		
		Normativo para gestão de risco	A organização não tem definida qualquer política ou norma para gestão de risco	A organização possui algum normativo para gestão de risco dos sistemas de informação, fazendo revisões pontuais, embora não seja seguido por todos os departamentos, nem a sua atualização é feita de forma regular	A organização possui normativo específico para gestão de risco dos sistemas de informação, fazendo a sua revisão de forma periódica ou sempre que existe um evento que assim o justifique, de forma a garantir a sua aplicabilidade ao contexto organizacional	A organização possui normativo específico para gestão de risco dos sistemas de informação, totalmente enquadrado no risco global, existindo revisões periódicas ou sempre que existe um evento que assim o justifique, de forma a garantir a sua aplicabilidade ao contexto organizacional. O risco é monitorizado e largamente suportado pela gestão de topo		
		Responsáveis pelo risco	Os responsáveis pelo tratamento do risco não são formalmente identificados	Os responsáveis pelo tratamento do risco são identificados e assignados aos riscos, embora não lhe seja imputada uma responsabilidade direta pelo tratamento dos mesmos	Os responsáveis pelo tratamento do risco são identificados e assignados formalmente aos riscos, sendo-lhes imputada a responsabilidade pelo tratamento dos riscos e definidos prazos para a sua implementação. Contudo, não existe uma rigidez na monitorização e cumprimento dos prazos	Os responsáveis pelo tratamento do risco são identificados e assignados formalmente aos riscos, sendo-lhes imputada a responsabilidade pelo tratamento dos riscos e definidos prazos para a sua implementação. Todos os riscos são monitorizados de forma apertada de acordo com o normativo em vigor e definida métricas para o seu cumprimento		

		Gestão da Conformidade	Não existe um processo formal para definição de requisitos de conformidade	São definidos requisitos de conformidade nos sistemas de informação, embora tratados ao nível departamental e sem um enquadramento transversal	São definidos e monitorizados requisitos de conformidade nos sistemas de informação ao nível da organização, havendo lugar a registo de não conformidades e atribuição das mesmas a um responsável	Existem processos e normativos que preveem a definição e monitorização de requisitos de conformidade nos sistemas de informação, com definição de métricas para o cumprimento das não conformidades, deficiências ou propostas de melhoria ao nível organizacional. Estes processos são suportados em ferramentas que permite um controlo mais apertado, melhoria continua e supervisão da gestão de topo e pelas áreas de auditoria interna e externa		
		Metodologia para gestão de risco	O processo de avaliação de risco é inexistente, ou quando existe é feito de forma ad-hoc sem qualquer regularidade ou formalismo	O processo de avaliação de risco está definido, embora não de forma transversal a toda a organização. É realizado sem uma periodicidade definida	O processo de avaliação de risco está definido de forma transversal a toda a organização. É realizado mediante normativo definido, com atribuição de responsabilidades para a sua execução e monitorização	A organização definiu o normativo necessário para suportar a função de risco em todas as áreas organizacionais e de forma regular, ou perante um cenário disruptivo. As responsabilidades estão bem definidas e a sua monitorização é executada. A operacionalização da avaliação de risco é suportada por uma ferramenta tecnológica que simplifica a sua realização, servindo também de evidência para auditorias e entidades reguladoras. O processo em si é alvo de revisão e atualização periódica		

	Funções e responsabilidades	**Formação em segurança da informação**	Não existe um programa formal e transversal para formação em cibersegurança	Apenas os recursos diretamente ligados à área de segurança de informação fazem formação em cibersegurança	É definido um programa transversal para todos os colaboradores sobre sensibilização para a segurança de informação mais em concreto cibersegurança. Este programa de formação faz parte do processo de admissão " induction". A organização monitoriza o seu cumprimento e atualiza de forma pontual estes conteúdos. Os recursos pertencentes à Área de segurança além destas formações, tem obrigatoriamente de realizar outras mais específicas	É definido um programa transversal para todos os colaboradores sobre sensibilização para a segurança de informação mais em concreto cibersegurança. Este programa de formação faz parte do processo de admissão " induction" e de forma regular a organização vai adaptando os conteúdos de forma a garantia que todos os recursos têm a formação e sensibilização necessária para a posição que ocupam. Os recursos pertencentes à Área de segurança além destas formações, tem obrigatoriamente de realizar outras mais específicas. Regularmente a organização executa programas que validam a formação e conhecimentos dos colaboradores		
		Definição de perfis e responsabilidades	Para a vertente da segurança de informação, não existe um formalismo na definição das funções e responsabilidades de cada colaborador	Existe formalismo na definição de responsabilidades de cada colaborador, embora nem sempre é seguido. Não existe segregação de funções em alguns casos	Existe formalismo na definição de funções e responsabilidades de cada colaborador, encontrando-se documentadas e revistas de forma regular	Existe formalismo na definição de funções e responsabilidades de cada colaborador, encontrando-se documentadas, monitorizadas e revistas de forma regular, em linha com os objetivos de cada colaborador e do departamento onde operam		

	Formação	**Gestão e evolução de carreiras**	Não está definido um processo para gestão e evolução da carreira profissional na vertente de segurança de informação	A organização dispõe de um programa formal de gestão e evolução de carreira, possibilitando a que cada colaborador possa evoluir e sendo de outras áreas internas, possa integrar a área de segurança	A organização dispõe de um programa formal de gestão e evolução de carreira, possibilitando a que cada colaborador possa evoluir e sendo de outras áreas internas, integrar a área de cibersegurança. Cada colaborador é livre de definir o seu programa de evolução, acompanhado de formação adequada	A organização dispõe de um programa formal de gestão e evolução de carreira, possibilitando a que cada colaborador possa evoluir, e sendo de outras áreas internas possa integrar a área de segurança. Cada colaborador é obrigado a definir o seu programa de evolução, em discussão com a sua chefia direta, traçando objetivos de evolução mediante a sua ambição e orientação interna. A organização monitoriza o programa de cada colaborador e apoia a sua execução		
		Realização de exercícios e simulacros	A organização não promove a realização de quaisquer exercícios ou simulacros para aferir a sensibilidade de cada colaborador para a cibersegurança	São realizados exercícios de phishing ou outros de forma pontual, onde são analisados os resultados, mas de forma informal e com pouco contributo para a definição de programas de formação específicos	São realizados exercícios de phishing e outros uma vez por ano, onde são analisados os resultados e recolhidos inputs para avaliação geral da sensibilidade dos colaboradores e apoiar na definição de programas de formação	São realizados diversos exercícios de engenharia social ao longo do ano, embora com programas iguais para todos os colaboradores em determinados domínios e outros mais específicos para a área de sistemas de informação. São analisados os resultados e recolhidos inputs para avaliação geral da sensibilidade dos colaboradores e apoiar na definição de programas de formação, e repetição dos exercícios após os colaboradores terem recebido formação		

		Gestão de budget para formação em cibersegurança	A organização não reserva ou prevê um valor anual dedicado à formação em cibersegurança	A organização prevê um valor anual para formação, embora gerido de forma ad-hoc e não requer a existência de um programa de formação previamente definido e validado	A organização prevê um valor anual para formação que é definido mediante o plano de atividades anual da Área de segurança. A organização tenta aprovar o pedido mediante justificação, sendo a sua execução monitorizada	A organização prevê um valor anual para formação que é definido mediante o plano de atividades anual da Área de segurança. A organização aprova o pedido após as devidas justificações, sendo a sua aplicabilidade monitorizada e revista de forma regular, podendo resultar em programas de formação específicos para toda a organização, como seja um programa global para todos os colaboradores, contendo conteúdos específicos em cibersegurança		
		Monitorização da eficácia do programa de formação em cibersegurança	Não existe uma aferição formal do programa de formação em segurança de informação	A eficácia do programa de formação é medido de forma informal e individualizada, não abrangendo a organização como um todo	A eficácia do programa de formação é medido de forma transversal numa base anual	A eficácia do programa de formação é medido de forma transversal através da recolha constante de inputs, que analisados de forma global e em perspetiva de melhoria continua, através da definição de métricas		
		Formação adequada às funções	A organização não promove formação alinhada a todas as funções no seio da organização	A organização define programas de formação genéricos para todos os colaboradores (ex. Segurança na utilização da internet ou no correio eletrónico), mas define também programas específicos para determinadas áreas (ex. desenvolvimento aplicacional seguro, formação em RGPD, etc.)	A organização define programas de formação genéricos para todos os colaboradores (ex. Segurança na utilização da internet ou no correio eletrónico), mas define também programas específicos para determinadas áreas (ex. Desenvolvimento aplicacional seguro, formação em RGPD, etc.). Esta formação especifica é regular e adequada às áreas alvo, havendo uma monitorização da sua completude a avaliação dos colaboradores sobre a sua interpretação	Existe um programa de formação formal e transversal a toda a organização com revisões periódicas e avaliação anual da sua adequação ao contexto organizacional, setorial, regulatório e legal		

		Divulgação de normativos, processos e procedimentos organizacionais	Não existe uma metodologia formal para divulgação de normativo e informação relevante aos colaboradores	Todos os normativos e documentos relevantes são disponibilizados num repositório central (ex. Intranet, pasta de rede, etc.) acessível a todos os colaboradores	Todos os normativos e documentos relevantes são disponibilizados em diversos repositórios com logging configurado. A organização recolhe a analisa o acesso para efeitos de métricas de consulta, divulgando por toda a organização sempre que é lançado um novo normativo ou actualizado um existente	A organização possui uma solução de divulgação e consulta de normativo e documentos relevantes à função de cada colaborador, guardando evidência que o mesmo foi acedido, sendo o colaborador obrigado a declarar que teve acesso ao seu conteúdo		
								Insira valor nos controlos
Gestão de ativos	**Gestão de inventário**	**Inventariação**	A organização dispõe de um inventário confiável de ativos, sendo a inventariação feita sem qualquer formalização	Existem diversos registos de ativos, com informação imprecisa e pouco consistente, pertencendo a departamentos distintos	A organização mantém um inventário único, existindo um departamento específico para o efeito, que executa revisões e atualização periódicas. Existe um processo para revisão de activos e uma ferramenta que suporta este processo	A organização mantém um inventário único, existindo um departamento específico para o efeito, que executa revisões e atualização periódicas. Existe um processo para revisão de activos e uma ferramenta que suporte este processo que procura de forma permanente ativos na rede, atualizando também o inventário de forma automatizada, gerando alertas sempre que são detetados ativos com determinadas características		
		Protecção contra adulteração de inventário de ativos	Não existem mecanismos de protecção contra adulteração do inventário de ativos	Estão implementados alguns mecanismos para protecção do inventário, embora básicos e não garantem o cumprimento da tríade CIA. Não existem alertas definidos para reportarem acessos indevidos	Estão implementados mecanismos para protecção do inventário e garantem o cumprimento da tríade CIA. Estão implementados também mecanismos de logging que registos eventos associados a acessos realizados ou tentativas de acesso	Estão implementados mecanismos para protecção do inventário e garantem o cumprimento da tríade CIA. Estão implementados também mecanismos de logging que registos eventos e monitorização ativa com capacidade para emitir alertas e notificações sobre o acesso indevido		

		Classificação de ativos	Não existe um processo para classificação de ativos	Os activos são classificados informalmente, mas o inventário não reflete essa classificação	Existe normativo específico para classificação de ativos	Existe normativo específico para classificação de ativos. A classificação de cada activo é revista anualmente ou sempre que exista um evento relevante sobre qualquer ativo. São definidas métricas para avaliar a conformidade e atualização da criticidade de cada ativo		
		Salvaguardas/Backups	Não estão definidos mecanismos de *backup* e *restore*	Encontram-se definidos mecanismos para *backup* e *restore*, embora não tenham sido definidos procedimentos que validem estes mecanismos	Encontram-se definidos mecanismos para *backup* e *restore da base de dados de ativos*, tendo sido definidos e executados de forma regular os procedimentos que validem estes mecanismos	Encontram-se definida uma política de salvaguarda de informação transversal a toda a organização, em linha com a criticidade de cada ativo ou processo, onde se inclui o *backup* ao inventário de ativos e respetivo restore. Esta política é difundida por toda a organização e revista regularmente		
		Ativos pertencentes a parceiros	A organização não dispõe informação acerca de ativos de parceiros que suportem serviços da própria organização	Apesar da organização não dispor de inventário formal sobre os ativos de parceiros, possui alguma informação sobre esses ativos	A organização dispõe de um inventário actualizado sobre os ativos de parceiros que suportam ou prestam serviço à organização	A organização dispõe de um inventário actualizado sobre os ativos de parceiros que suportam ou prestam serviço à organização. A inventariação destes ativos está formalizada na política organizacional para gestão de ativos com obrigatoriedade do parceiros comunicar sempre que existam alterações		

		Ativos entregues a parceiros/fornecedores	A organização não tem definido qualquer processo para gestão de ativos entregues a parceiros que colaboram com a organização	Existe um registo informal sobre o activo entregue a parceiros	A organização tem definido um processo para registo e monitorização de cada ativo entregue a parceiros	A organização tem definido um processo para registo e monitorização de cada ativo entregue a parceiros. Informação sobre o ativo é reportada à organização de forma automatizada por meio de um agente instalado. O processo define regras de utilização e cláusulas de responsabilização sobre a utilização dos respetivos ativos		
		Devolução/recolha de equipamentos (colaboradores e parceiros	A organização não tem definido um processo formal para recolha de equipamentos	A organização tem implementado um processo manual para controlo de equipamentos entregues a colaboradores. Os colaboradores em processo de saída são obrigados a devolver os equipamentos registados em seu nome	A organização definiu um processo para a recolha de equipamentos que valida regularmente o estado do ativo e do colaborador	Existe um processo automatizado através de uma gestão centralizada de ativos. Este processo é executado de forma regular, monitorizado e alvo de auditorias regulares		
	Gestão de atualizações de segurança	**Aplicação de atualizações de segurança**	A organização não tem definido um processo que vise gerir a instalação de atualizações. Estas ocorrem de forma pontual e manual	A organização dispõe de um processo para gestão de atualizações, embora seja automatizado, mas não abrange todos os ativos organizacionais	A organização dispõe de um processo para gestão de atualizações automatizado com calendário definido numa base mensal	A organização dispõe de um processo para gestão de atualizações de segurança automatizado com calendário definido para execução mensal, prevendo também instalações fora do ciclo, mediante a criticidade da atualização e o risco dos ativos a atualizar. A solução para gestão de atualizações de segurança permite aferir o nível de conformidade dos ativos, definir alertas regras para ativos que não cumpram requisitos mínimos de atualização		

		Verificação de conformidade nos ativos	A verificação de conformidade de ativos não existe ou quando existe é executada de forma manual e pouco eficiente	são definidos requisitos e métricas para verificar a conformidade de ativos relativamente a atualizações de segurança. Como se trata de um processo manual e que requer um esforço considerável, raramente são realizadas avaliações de conformidade	A organização tem definido um processo para avaliar o nível de conformidade do ativo face os requisitos definidos. A aferição do nível de conformidade é suportado numa solução que automatiza o processo e produz relatórios de conformidade que são analisados pela área de cibersegurança	A organização tem definido um processo para avaliar o nível de conformidade do ativo face os requisitos definidos. A aferição do nível de conformidade é suportado numa solução que automatiza o processo, monitorizando-o e produz relatórios de conformidade em linha com a criticidade e o risco de cada ativo		
		Gestão de exceções	Não existe um processo que prevê gerir exceções à instalação de atualizações de segurança	A exceções são identificadas de forma ad-hoc e quando aplicadas raramente são revisitadas	A gestão de atualizações de segurança prevê a ocorrência de exceções. Medidas compensatórias são definidas até que sejam revisitadas e corrigidas	A gestão de atualizações de segurança prevê a ocorrência de exceções que são identificadas através de mecanismos que testam o comportamento da atualização num ambiente controlado antes de serem aplicadas transversalmente. Contudo, também são consideradas informações provenientes de fontes seguras como seja em comunicados pelos fabricantes dos ativos ou em fóruns da especialidade. Medidas compensatórias são definidas para as exceções até que sejam corrigidas. Estas exceções são alvo de registo e monitorização em controlo interno e assignado a um responsável com data de resolução definida		

		CAB (change-advisory board)	A organização não tem definido um CAB formal, embora tenha um grupo informal responsável por avaliar a instalação de atualizações de segurança	A organização têm constituído um fórum que reúne pontualmente e define as regras para cada instalação de atualizações de segurança	Existe um CAB constituído pelas principais áreas organizacionais e pela gestão de topo que reúne mensalmente e analisa e decide as atualizações de segurança a aplicar em cada ciclo	Existe um CAB constituído pelas principais áreas organizacionais e pela gestão de topo que reúne semanalmente e sempre que se justifique. Em cada reunião é avaliada com atualização a aplicar no ciclo semanal com base em informação recolhida previamente pelo próprio CAB		
		Baselines de segurança em ativos	Não estão definidas baselines de segurança para ativos	A organização definiu uma baseline de segurança que aplica de forma ad-hoc em alguns ativos	A organização tem definidas diversas baselines de segurança mediante a criticidade de cada ativo/solução. A sua instalação é transversal, mas de forma manual	A organização tem definidas diversas baselines de segurança mediante a criticidade de cada ativo/solução e com mecanismos de atualização automatizados. A sua instalação é transversal e feita de forma automatizada. A organização monitoriza a conformidade dos ativos relativamente às baselines para garantir uma cobertura 100% da infraestrutura e a sua adequação face à criticidade de cada ativo		
								Insira valor nos controlos
Segurança e conformidade do posto de trabalho	**Mecanismos de protecção**	**Antivírus**	A organização tem uma gestão de antivírus pouco formalizada, podendo coexistir diversos fabricantes de soluções para antivírus, inclusive versões gratuitas, demonstrativas e não oficiais	A organização tem definida uma política para gestão de atualizações do antivírus. Cada posto de trabalho tem um agente de antivírus instalado e actualizado uma vez por dia, embora sem monitorização ou garantia que o faça	A organização tem definida uma política para gestão de atualizações do antivírus. Cada posto de trabalho tem um agente de antivírus instalado e actualizado pelo menos duas vezes por dia. A organização possui ainda uma infraestrutura centralizada de IDS e IPS que atuam como primeira linha de defesa para os postos de trabalho	A organização tem definida uma política para gestão de atualizações do antivírus. Cada posto de trabalho tem um agente de antivírus funcionando através análise comportamental e assinaturas que são atualizadas em tempo real. A organização possui também infraestrutura centralizada com IDS e IPS que atuam como primeira linha de defesa para os postos de trabalho		

		Anti-Malware e Anti-Phishing	A organização tem uma gestão de Anti-Malware e Anti-Phishing pouco formalizada, podendo coexistir diversos fabricantes de soluções , inclusive versões gratuitas, demonstrativas e não oficiais	A organização tem definida uma política para gestão de atualizações de Anti-Malware e Anti-Phishing. Cada posto de trabalho tem um agente de instalado e actualizado uma vez por dia, embora sem monitorização ou garantia que o faça	A organização tem definida uma política para gestão de atualizações de Anti-Malware e Anti-Phishing. Cada posto de trabalho tem um agente instalado (que poderá ser o mesmo do antivírus) que é atualizado pelo menos duas vezes por dia. A organização possui ainda infraestrutura centralizada de equipamentos que identificam, analisam e removem malware e phishing atuando como primeira linha de defesa	A organização tem definida uma política para gestão de atualizações de Anti-Malware e Anti-Phishing. Cada posto de trabalho tem um agente instalado (que poderá ser o mesmo do antivírus) e atualizado tempo real. A organização possui ainda infraestrutura centralizada de equipamentos que identificam, analisam e removem malware e phishing atuando como primeira linha de defesa. A componente de Anti-Malware e Anti-Phishing funcionam também com base comportamental, tendo a capacidade de isolar o ativo se assim tiver sido definido por políticas e mediante a criticidade da infeção	

		Instalação de software padronizado	A organização não tem definidos controlos para gerir a instalação de software nos seus postos de trabalho. Sempre que um colaborador necessita, procede à sua instalação independentemente do tipo ou da origem do software	A organização não tem definidos controlos para gerir a instalação de software nos seus postos de trabalho. Sempre que um colaborador necessita de um determinado software padronizado e catalogado pela empresa, consulta um repositório (pasta na rede), pesquisa e instala. Se não existir, fala com o departamento de informática e solicita-o	A organização dispõe de um catálogo online onde constam todas os softwares padronizados que estão aprovados pela organização e podem ser instalados diretamente pelo utilizador. No caso de ser necessário assegurar o custo de licenciamento, a chefia direta do colaborador recebe um fluxo para aprovar. Mediante a sua aprovação o software é instalado automaticamente no posto do colaborador	A organização dispõe de um catálogo online onde constam todas os softwares padronizados que estão aprovados pela organização e podem ser instalados diretamente pelo utilizador. No caso de ser necessário assegurar o custo de licenciamento, a chefia direta do colaborador recebe um fluxo para aprovar. Mediante a sua aprovação o software é instalado automaticamente no posto do colaborador. Este catálogo é revisto regularmente para assegurar a sua atualização e abrangência. Todos estes softwares são removidos automaticamente dos postos de trabalho se estiverem 90 dias sem utilização	

		Instalação de software não padronizado	A organização não tem definidos controlos para gerir a instalação de software nos seus postos de trabalho. Sempre que um colaborador necessita, procede à sua instalação independentemente do tipo ou da origem do software	A organização não tem definidos controlos para gerir a instalação de software nos seus postos de trabalho. Sempre que um colaborador necessita de um determinado software não padronizado, fala com a sua chefia direta para efeitos de aprovações financeiras e caso seja aprovado, solicita-o ao seu departamento de informática	Os softwares não padronizados são alvo de diversas validações antes de se proceder à sua aquisição, nomeadamente pela área de cibersegurança, arquitetura e gestão de ativos. O colaborador solicita o pedido de software, a chefia aprova, seguindo-se todo o processo de validação. Ultrapassada esta etapa, o software é adquirido e instalado no posto de trabalho	Os softwares não padronizados são alvo de diversas validações antes de se proceder à sua aquisição, nomeadamente pela área de cibersegurança, arquitetura e gestão de ativos. O colaborador solicita o pedido de software, a chefia aprova, seguindo-se todo o processo de validação. Ultrapassada esta etapa, o software é adquirido e instalado no posto de trabalho. A organização tenta evitar este processo por ser moroso e dispendioso, apostando em ter o seu catálogo mais amplo e a incluir uma maior variedade e disparidade de software. Todos estes softwares são removidos automaticamente dos postos de trabalho se estiverem 90 dias sem utilização	
		Elevação de privilégios	A organização não tem definido normativo para gerir acessos privilegiados nos postos de trabalho. Por defeitos todos os colaboradores são administradores locais	A organização não tem definido normativo para gerir acessos privilegiados nos postos de trabalho. Os colaboradores por defeito não são administradores locais, mas sempre que é necessário solicitam essa permissão de forma ad-hoc e nunca mais lhes é retirada. A organização não tem um controlo sobre estes casos	A organização tem definido normativo para gerir acessos privilegiados nos postos de trabalho. Os colaboradores por defeito não são administradores locais e quando necessitam de o ser, solicitam um pedido formal que tem diversas aprovações, ficando registado. Anualmente é feita uma revisão destes acessos pelas respetivas chefias	A organização tem definido normativo para gerir acessos privilegiados nos postos de trabalho. Os colaboradores por defeito não são administradores locais e quando necessitam de o ser, solicitam um pedido formal que tem diversas aprovações. Após aprovação, é instalado um agente no posto de trabalho que passa a gerir de forma automática e transparente todas as ações privilegiadas. Anualmente estes acessos são revistos pelos responsáveis de cada colaborador	

		Instalação de atualizações e correções de segurança	A organização não tem definida uma estratégia de atualização aplicável a postos de trabalho. As instalações ocorrem de forma ad-hoc e sem um calendário pré-definido	A organização não tem definida uma estratégia de atualização especifica para postos de trabalho. As instalações críticas e altas são instaladas, mas de forma ad-hoc	A organização tem definida uma estratégia e um processo de atualização específico para postos de trabalho. Existe um calendário pré-definido, embora atualizações críticas sejam instaladas de forma urgente	A organização tem definida uma estratégia e um processo de atualização específico para postos de trabalho. Existe um calendário pré-definido, embora atualizações críticas sejam instaladas de forma urgente. Antes de ser instalada qualquer atualização ou correção em produção, é testado em ambiente controlado para aferir o comportamento do posto mediante os testes realizados às aplicações utilizadas. Periodicamente o processo é revisto, atualizado e partilhado com todas as partes interessadas	
	Conformidade do posto de trabalho	**Deteção de ativos em estado de inconformidade**	A organização não dispõe requisitos definidos que validam o estado de conformidade do posto de trabalho e mediante isso conceder acesso aos diversos recursos corporativos	A organização tem mecanismos que apenas permitem postos de trabalho corporativos tenham acesso aos recursos internos, mas não avaliam o seu estado de conformidade	A organização tem definidas políticas e mecanismos que validam o estado de conformidade do posto de trabalho e com base nesse estado permitem o seu acesso aos recursos organizacionais. Os postos em estado de inconformidade são colocados em quarentena	A organização tem definidas políticas e mecanismos que validam o estado de conformidade do posto de trabalho e com base nesse estado permitem o seu acesso aos recursos organizacionais. Tanto o colaborador com área de gestão de activos são alertados para o estado de inconformidade que o posto irá entrar, se não forem tomadas determinadas ações. Todos os postos em estado de inconformidade, acedem de forma limitada aos recursos organizacionais, numa área restrita (denominada de quarentena) para recuperarem o seu estado de conformidade	

		Protecção da informação	A organização não tem definidas políticas para protecção de informação contida nos postos de trabalho	A organização não definiu qualquer política para protecção de informação nos postos de trabalho, mas dispõe de uma solução que permita a encriptação dos discos internos, mas não força a sua utilização	Existem políticas e processos definidos para protecção de informação nos postos de trabalho e uma solução que encriptação para discos internos e amovíveis ligados ao posto para transferir informação. A organização força a utilização, embora não monitorize a sua conformidade	Existem políticas e processos definidos para protecção de informação nos postos de trabalho e uma solução que encriptação para discos internos e amovíveis ligados ao posto para transferir informação. A organização força a utilização e monitoriza a sua conformidade. Os utilizadores mesmo sendo administradores do posto não tem permissões para desativar ou suspender a sua utilização. Se por algum motivo o posto ficar com o seu disco sem cifra, são despoletados alertas para a equipa de gestão de ativos e ações tomadas de imediato. Exceções estão previstas e são monitorizadas até a sua resolução	
		Acesso a redes sem fios desconhecidas e inseguras	A organização não tem definidas políticas para gerir ligações a redes sem fios. O colaborador tem liberdade para estabelecer ligação com qualquer rede	A organização não tem definidas políticas para gerir ligações a redes sem fios. Na eventualidade de ser realizada uma ligação a este tipo de rede, o colaborador recebe um alerta sobre as consequências de avançar	A organização tem definidas políticas para gerir ligações a redes sem fios, em particular aqueles com níveis de segurança mais reduzidos	A organização tem definidas políticas para gerir ligações a redes sem fios. No caso de redes pouco seguras, a ligação é estabelecida, mas o proxy não permite saída para a internet por não ter classificado a mesma com segura	

		Acesso controlado à internet	O acesso à internet não é gerido através de uma solução baseada em proxy ou noutra tecnologia	O acesso à internet é gerido através de uma solução baseada em proxy, embora sirva apenas para gerir o acesso à internet quando o posto está localizado nas instalações	O acesso à internet é baseado numa solução avançada de proxy (ex.: Zscaler, Akamai,,etc....) onde qualquer ligação à internet realizada pelo posto é filtrada por esta solução	O acesso à internet é baseado numa solução avançada de proxy (ex.: Zscaler, Akamai,,etc....) onde qualquer ligação à internet realizada pelo posto é filtrada por esta solução. Todas as soluções internas que necessitam de acesso à internet estão configuradas para serem permitidas. A organização atualiza de forma regular as lista para permitir e negar acessos através URL específicos ou por assunto (ex.: vídeo streaming, redes sociais, apostas online,,etc.)		
	Monitorização ativa sobre os postos de trabalho	**Monitorização e resposta em modelo 24x7x365**	A organização não possui mecanismos para monitorizar, nem equipa de resposta a incidentes que envolvam postos de trabalho em modelo 24x7x365	A organização possui mecanismos que monitorizam o estado dos postos de trabalho em modelo 9x5, mas não tem equipas de resposta a incidentes envolvendo postos que cubram este horário	A organização possui mecanismos que monitorizam o estado dos postos de trabalho em modelo 24x7x365, embora a equipa de resposta a incidentes em 24x7x365 não seja exclusiva para postos e para assuntos relacionados com cibersegurança, executando apenas ações pré-definidas e básicas	A organização possui mecanismos que monitorizam o estado dos postos de trabalho em modelo 24x7x365. Existe ainda uma equipa dedicada a incidentes que envolvam postos de trabalho		
								Insira valor nos controlos
Gestão de Identidades e Acessos	**Estratégia**	**Definição de uma estratégia e modelo de governo para gestão de acessos**	A organização não tem definida uma estratégia formal para gestão de acessos.	A organização tem definidas algumas regras para gestão de acessos, embora pouco formalizada e operacionalizadas	A organização têm definida uma estratégia para gestão de acessos, documentada e formalizada transversalmente. Encontra-se implementada na grande maioria das áreas organizacionais	A organização têm definida uma estratégia para gestão de acessos, documentada e formalizada transversalmente. A sua implementação é ampla em toda a organização		

		Monitorização, adequação e ajustes na estratégia para gestão de acessos	Por não existir uma estratégia definida para a gestão de acessos, não existem atividades inerentes à sua monitorização, adequação ou governação	A organização não tem uma estratégia formal definida, contudo foi definido um grupo de trabalho que tem como missão alavancar e ter um maior controlo e visão sobre a gestão de ativos	A organização definiu um modelo de governo para gestão de acessos. A área responsável tem a missão de supervisionar e definir ações de melhoria abrangendo todos os acessos internos ou externos.	A organização definiu um modelo de governo para gestão de acessos. A área responsável pela gestão de acesso tem a missão de supervisionar e definir ações de melhoria abrangendo todos os acessos internos e externos. Anualmente é feita uma revisão para garantir a conformidade da estratégia em virtude do número de exceções existentes, incidentes de segurança envolvendo acessos e novos requisitos legais e regulamentares		
	Gestão de acessos	**Processo de gestão de acessos**	Não é seguido qualquer processo para gerir acessos. Estes são tratados caso a caso, de forma não centralizada e não monitorizada	Existe um processo mas não envolve todos os acessos. Este processo não é monitorizado ou documentado	A gestão de acessos encontra-se formalizada através de um processo transversal a toda a organização. Este processo é alvo de monitorização e avaliação anual	A gestão de acessos encontra-se formalizada através de um processo transversal a toda a organização. Este processo é alvo de monitorização e avaliação anual, existindo controlos que identificam a atividades que envolvem acessos em incumprimento com o processo definido e aprovado. Os acessos são geridos com base em análise de risco, podendo por exemplo necessitar de mais que uma aprovação, ou serem atribuídos apenas de forma temporal		

		Processo de atribuição de acessos aplicacionais e em infraestruturas (não privilegiados)	Não estão definidas quaisquer políticas e processos para atribuição de acessos aplicacionais e para infraestruturas. Os acessos são atribuídos de forma ad-hoc sem qualquer registo ou controlo	Não estão definidas quaisquer políticas e processos para atribuição de acessos aplicacionais e para infraestruturas. Os acessos são atribuídos de forma ad-hoc, embora exista um registo para cada acesso atribuído	A organização tem definidas políticas e processos para atribuição de acessos que estão documentadas e são de uso obrigatório em toda a organização. Os acessos são atribuídos de forma automatizada por meio de uma solução para gestão de acessos	A organização tem definidas políticas e processos para atribuição de acessos de forma centralizada, sendo os acessos atribuídos de forma automatizada através de uma solução para gestão de acessos configurada de acordo com as políticas definidas e baseado em funções e responsabilidades dos utilizadores e perfis definidos para cada aplicação. É utilizada uma solução para gerir passwords (ex. Key vault)		
		Processo de atribuição de acessos aplicacionais e em infraestruturas (privilegiados)	A organização não faz distinção na forma como gere acessos privilegiados e não privilegiados	A organização não tem definidas quaisquer políticas e processos para gestão de acessos privilegiados, a sua gestão é feita ad-hoc. Contudo faz uma avaliação da real necessidade e avalia o risco da sua atribuição, procedendo à configuração de uma conta dedicada "privilegiada" diferente da conta "normal"	As políticas organizacionais definem regras e procedimentos específicos para atribuição de acessos privilegiados estão documentadas e são aderidas por toda a organização. Estes acessos são geridos de forma automatizada por uma solução aplicacional que assegura a sua atividade e monitorização	A organização tem definidas políticas e processos para atribuição de acessos de forma centralizada, sendo os acessos atribuídos de forma automatizada através de uma solução para gestão de acessos configurada de acordo com as políticas definidas e baseado em funções e responsabilidades dos utilizadores e perfis definidos para cada aplicação. Os acessos privilegiados requerem sempre uma aprovação da gestão de topo. É ainda utilizada uma solução para gerir passwords (ex. Key vault) Todo este processo é alvo de monitorização regular e auditado anualmente, sendo ainda definidos e avaliados KPIs mensais		

		Utilização de uma plataforma/solução para acessos privilegiados	A organização não dispõe de uma solução para gerir acessos privilegiados	A organização não adquiriu nenhuma solução que permita gerir acessos privilegiados, contudo determinou que somente algumas podem ser utilizadas, prevenindo que cada utilizador escolha a que mais gosta de usar (ex. RDP para sistemas Windows e SSH para sistemas Linux apenas)	A organização possui apenas uma solução para gerir acessos privilegiados nos postos de trabalho	Existe uma solução para gestão de acessos privilegiados em todos os ativos, procedendo ao registo de logging e gravando a sessão do utilizador. Esta solução permite ainda identificar acessos privilegiados que sejam realizados à margem desta solução		
		Utilização de uma plataforma/solução para gestão de acessos via SSO	A organização não dispõe de uma solução para gerir acessos aplicacionais via SSO	A organização apenas têm configuradas algumas soluções aplicacionais que permitem aos utilizadores acederem via SSO, apenas se os colaboradores estiverem a aceder a partir da rede interna	As soluções aplicacionais mais utilizadas pelos colaboradores têm configurado acesso apenas via SSO, a partir da rede interna ou VPN	Todas as soluções aplicacionais, sejam internas e externas, com maior ou menor utilização apenas permitem acessos via SSO a partir da rede interna ou VPN		
		Processo de alteração de acessos	A organização não tem definido qualquer processo para alteração de acessos. Quando existe necessidade de alterar, é executado de forma ad-hoc e pouco formalizado	A organização não tem definido qualquer processo para alteração de acessos. Contudo, sempre que um colaborador sai da organização os acessos concedidos via SSO são removidos automaticamente. Contudo, quando o colaborador altera as suas funções, não são removidos os acessos anteriormente concedidos	A organização tem definidas políticas e processos para alteração de acessos que se encontram documentadas e de adesão obrigatória por toda a organização. Sempre que um colaborador é alvo de uma alteração relevante (ex. saída da organização, alteração de funções, ausência prolongada,,etc.....) o processo de alteração de acessos é despoletado de forma manual, mediante informação fornecida pelos Recursos Humanos à área de gestão de acessos	A organização tem definidas políticas e processos para alteração de acessos que se encontram documentadas e de adesão obrigatória por toda a organização. Sempre que um colaborador é alvo de uma alteração relevante (ex. saída da organização, alteração de funções, ausência prolongada,,etc.....) o processo de remoção de alteração é despoletado automaticamente. Todo este processo é alvo de monitorização regular e auditado anualmente, sendo ainda definidos e avaliadas métricas mensais		

		Mecanismos de bloqueio automatizado para acessos comprometidos	A organização não possui uma forma automatizada para bloqueio de acessos comprometidos. O seu bloqueio é sempre manual e pouco eficiente	A organização não possui uma forma automatizada para bloqueio de acessos comprometidos. O bloqueio é manual, mas executado de forma célere dentro do horário 9x5	A organização não dispõe de uma forma automatizada para bloqueio de acessos comprometidos. Contudo, a organização dispõe de equipa em modelo 24x7x365 que prontamente desativam o acesso	A organização dispõe de uma solução que automatiza o bloqueio de acessos comprometidos. Esta solução faz uma análise de risco, e mediante o resultado bloqueia todos os acessos associados a uma entidade/conta		
	Modelo de autenticação e autorização	**Utilização de 2 fator de autenticação**	A utilização de acessos organizacionais com multifactor de autenticação não está definida	A utilização de acessos com multifactor de autenticação está definida e a sua adesão ocorre de forma ad-hoc em determinados cenários (acesso a aplicações com maior criticidade, acessos privilegiados,,etc.)	A utilização de acessos com multifactor de autenticação é sempre utilizada para acessos remotos, acessos privilegiados, aplicações que tenham requisitos de autenticação forte	A utilização de acessos com multifactor de autenticação é obrigatória em todos os cenários, exceto em aplicação que tenham configurado SSO ou outras quando acedidas na rede interna		
		Utilização de diferentes modelos de autenticação	A organização não definiu um processo ou regras específicas para diferenciar o modelo de autenticação. Esta gestão é feita ad-hoc	A organização definiu um processo e regras específicas para implementar diferenciados modelos de autenticação. Contudo, este processo não está difundido por toda a organização e por isso não é seguido na íntegra	A organização definiu um processo ou regras específicas para implementar diferentes modelos de autenticação, mediante se o acesso é de um colaborador ou de um parceiro. O processo é gerido de forma centralizada sendo a sua implementação executado de forma manual	A organização definiu um processo ou regras específicas para implementar modelos distintos de autenticação, de acordo com a criticidade e risco que cada acesso tem associado. O processo é gerido de forma centralizada e a sua implementação é suportada por uma solução que automatiza todo o processo		
	Alterações, integrações e federações de identidades	**Alterações em identidades**	Não é seguido qualquer processo para alteração de entidades na gestão de acessos. Esta alteração é executada de forma informal e manual	As alterações são realizadas de forma manual, informal e pouco regular. Informação proveniente dos RH e da gestão de fornecedores "alimentam" as alterações, mas nem sempre ocorrem dentro de prazos coerentes com as alterações realizadas	As alterações ocorrem de forma manual de acordo com o fluxos de dados automatizados provenientes das diversas fontes onde existem identidades (RH, Gestão de fornecedores, Gestão de serviço,,etc.)	As alterações ocorrem de forma totalmente automatizada de acordo com o fluxos de dados também automatizados provenientes das diversas fontes onde existem identidades (RH, Gestão de fornecedores, Gestão de serviço,,etc.)		

		Modelo de federação com entidades parceiras (colaboradores externos, fornecedores,,etc.)	Não está definido um processo para federação com entidades parceiras. São utilizados meios inseguros para troca de informação sobre acessos necessários por parte das entidades parceiras	Não existe um processo ou modelo formal para federação com entidades parceiras. Contudo a organização tem regras definidas de acordo com o perfil de risco do acesso, mediante a criticidade da solução/infraestrutura a ser acedida	A organização tem definido um processo que avalia o modelo de federação a configurar para cada parceiro tendo em conta vários critérios. Este processo está amplamente difundido por toda a organização . Cada área organizacional que envolva a participação e interação com parceiros é parte interessada no processo e contribui ativamente para ele	A organização tem definido um processo que serve de apoio à implementação do modelo de federação para parceiros. este modelo prevê a utilização somente de um modelo de federação por cada perfil de risco obtido quando se cruza o perfil do fornecedor vs. o perfil da solução/infraestrutura a que terá acesso. Este processo está amplamente difundido por toda a organização e auditado regularmente. Cada área organizacional que envolva a participação e interação com parceiros é parte interessada no processo e contribui ativamente para ele		
	Revisão e monitorização	**Comprometimentos de acessos de parceiros**	A organização não tem definidos processos nem implementadas soluções que alertem e bloqueiem sempre que os acessos de parceiros estejam comprometidos	A organização tem definidos alguns mecanismos de monitorização e bloqueio sobre acessos de parceiros que possam estar comprometidos, mas não cobrem todos os cenários ou abrangem todos os tipos de autenticadores utilizados	A organização tem definidos processos e uma solução de monitorização e bloqueio sobre acessos de parceiros que possam estar comprometidos, que alertam em tempo real, embora não tenham uma cobertura total sobre todos os acessos de todos os parceiros	A organização tem definidos processos e uma solução de monitorização sobre acessos de parceiros que possam estar comprometidos, que alertam em tempo real e com uma cobertura total sobre todos os acessos de todos os parceiros		
		Verificação e validação do nível de acesso	Não estão definidos processos para validar o nível de acessos solicitados	A organização não tem definidos processos formais para revisão e monitorização de acessos, mas estão instituídos mecanismos manuais executados de forma pontual que validam a adequação do nível de acesso	A organização tem definidas políticas e processos para validação de acessos, mas não são executados de forma regular. A validação do nível de acesso nem sempre está alinhado com o nível de risco dos ativos ou das entidades	A organização tem definidas políticas e processos para validação de acessos que se encontram operacionalizados e executados regularmente para assegurar a sua adequação e adoção por todos as áreas. A validação do nível de acesso está totalmente alinhado com o nível de risco dos ativos ou das entidades		

		Revisão de acesso a sistemas críticos (contém informação pessoal sensível de colaboradores, clientes ou parceiros)	Não estão definidos processos específicos para revisão de acessos a sistemas que contenham informação sensível	Não estão definidos processos específicos para rever acessos a sistemas que contenham informação sensível, apenas existem orientações e boas práticas resultantes de áreas ou colaboradores com maior sensibilidade para o assunto e assim implementam controlos de acessos específicos	Os acessos a sistemas críticos estão identificados e são revistos anualmente, mediante obrigatoriedade imposta por políticas internas	Os acessos a sistemas críticos estão identificados e são revistos semestralmente mediante obrigatoriedade imposta por políticas internas. Devido à criticidade destes acessos, estão implementados controlos adicionais em termos de monitorização e registo de eventos (logging)		
		Revisão de acessos (Geral)	A organização não dispõe de um processo para revisão de acessos, fazendo-o pontualmente e de forma ad-hoc	A organização não dispõe de um processo definido para revisão de acessos, fazendo-o de forma ad-hoc	A organização tem definido um processo para revisão de acessos privilegiados e as soluções que apresentem um maior risco. Esta revisão ocorre anualmente, sendo realizado pela área de gestão de acessos	A organização tem definido um processo que prevê a revisão anual de acessos com maior risco, incluindo acessos de parceiros. Este processo é auditado regularmente. São definidas e avaliadas métricas para o cumprimento destes processos		
								Insira valor nos controlos
Segurança de rede	**Gestão de acessos**	**Acessos à rede interna (acesso físico)**	A organização permite o acesso à rede de qualquer ativo, seja interno ou externo	A organização não permite que sejam ligados ativos externos à organização. A sua proibição é baseada em barreiras físicas	A organização não permite que ativos externos sejam ligados às suas redes, tendo para isso implementado mecanismos que valida o endereço *Mac*, necessitando que este tenha sido previamente aprovisionado	A organização não permite que ativos externos sejam ligados às suas redes, tendo para isso implementado mecanismos que verificam a autenticidade do ativo através de determinados fatores contra a base dados de ativos organizacionais atualizada em tempo real		

		Acesso remotos para colaboradores	A organização permite a configuração de acessos remotos para colaboradores. A instalação é feita ad-hoc e sem regulação. O acesso é baseado em método de autenticação com fator simples (utilizador e palavra-passe)	A organização permite a configuração de acessos remotos para colaboradores. Contudo, só é permitido o acesso remoto a determinadas soluções/infraestruturas e configurados segundo regras e critérios previamente aprovados. Este acesso é baseado num método de autenticação de múltiplo fator (2FA)	A organização permite a configuração de acessos remotos para colaboradores através de um agente instalado no posto de trabalho e totalmente gerido, Contudo, só é permitido o acesso remoto a um número limitado de soluções/infraestruturas, nomeadamente aquelas que apresentam um risco menor. O acesso é amplamente gerido e monitorizado e requer utilização de múltiplo fator (2FA).	A organização permite a configuração de acessos remotos para colaboradores baseado no perfil e função de cada colaborador. Contudo, só é permitido o acesso remoto a determinadas soluções/infraestruturas e atribuídos segundo regras e critérios previamente aprovados, permitindo apenas determinadas operações e sempre com recurso a 2FA. Sempre que o colaborador inicia uma sessão remota, é executada uma avaliação automatizada e dinâmica que afere o cumprimento de controlos específicos como seja o IP, dispositivo ou a existência de um incidente que foi previamente referenciado e associado ao colaborador		

		Acesso remoto de parceiros	A organização tem implementado o mesmo modelo de acessos remotos para colaboradores e parceiros	A organização tem definido um modelo de acesso remoto para parceiro segregado do acesso remoto para colaboradores. O acesso é configurado via VPN com recurso à utilização de múltiplo fator (2FA), mas nem sempre estes acessos permitem que os parceiros acedem apenas a aplicações/infraestruturas e serviços por eles geridos	O acesso remoto de parceiro é baseado em postos de trabalho virtualizados disponibilizados pela organização, que após autenticação com 2FA permitem aceder a determinados recursos internos, mediante as permissões configuradas no posto virtualizado. Cada parceiro tem dedicado a si diversos postos virtualizados. O acesso é monitorizado e auditado. Os postos de trabalho dos parceiros nunca são ligados à rede da organização	O acesso remoto é configurado através de VPN que após autenticação com 2FA permite aceder a uma poll de recursos que estão acessíveis ao parceiro, podendo inclusive segregar-se acessos e permissões entre colaboradores do mesmo parceiro, em virtude da segurança e flexibilidade que esta publicação permite. O acesso é monitorizado e auditado. Os postos de trabalho dos parceiros nunca são ligados à rede da organização		
		Gestão de credenciais administrativas	A organização não tem definido qualquer requisito para gerar e armazenar credenciais usadas na gestão equipamentos	As credenciais usadas para gerir ativos administrativos são definidas pelos gestores dos ativos e guardadas num documento que está partilhado entre todos eles	As credenciais são definidas de acordo com o normativo definido e guardadas de forma segura numa solução implementada para o efeito (Keepass, Key vault,,etc.)	A organização utilização uma solução centralizada para gestão de acessos, que é responsável por gerar palavras-passe, guardar e forçar a sua rotatividade para cumprir com o normativo definido		
		Disponibilização de acesso a redes sem fios para colaboradores e parceiros	A organização disponibiliza o acesso a redes sem fios sem restrições e de forma aberta a todos os colaboradores e parceiros	A organização disponibiliza o acesso a redes sem fios com protocolos de encriptação pouco robustos a todos os colaboradores e parceiros, embora existe um processo de registo e solicitação de acesso	A organização disponibiliza o acesso a redes sem fios com protocolos de encriptação robustos a todos os colaboradores e parceiros, mas com SSIDs e chaves diferentes. Estes redes sem fios não estão em segmentos de rede distintos	A organização disponibiliza o acesso a redes sem fios com protocolos de encriptação robustos a todos os colaboradores e parceiros, mas com SSIDs e chaves diferentes. Estes redes sem fios estão em segmentos de rede distintos, em que o segmento disponibilizado para parceiros permite unicamente um acesso à internet, monitorizado e auditado		

	Monitorização e conformidade	**Protecção de eventos de rede (logging)**	Não estão implementados requisitos específicos para proteger os eventos	Os administradores têm acesso total aos eventos, embora o seu acesso fique também auditado	O acesso de escrita/alteração dos eventos está protegida. Apenas é possível realizar operações de leitura	O acesso de escrita/alteração dos eventos está protegida. Apenas é possível realizar operações de leitura. Os eventos estão protegidos contra adulteração ou manipulação		
		Supervisão, monitorização e restrições sobre comunicações com parceiros e entidades externas	As comunicações internas de e para parceiros não estão definidas e são tratadas de forma informal	As comunicações internas de e para parceiros são documentadas na altura em que são implementadas, mas não é feito um "tracking" deste registo	As comunicações internas de e para parceiros estão documentadas face ao modelo de análise e aprovação em vigor que obriga a seguir um fluxo com determinadas atividades e controlos	As comunicações internas de e para parceiros estão documentadas e atualizadas. Cada comunicação obriga à avaliação de risco e após aprovada a sua implementação são criadas regras de firewall, registadas e implementadas através numa plataforma centralizada. regularmente são recolhidas métricas sobre as regras implementadas, permitindo por exemplo fechar regras que deixaram de ser utilizadas		
		Gestão de alterações	As alterações preconizadas na rede são realizadas de forma informal pela equipa responsável, não existindo qualquer processo de revisão, autorização e acompanhamento	As alterações preconizadas na rede são realizadas de forma informal pela equipa responsável. Não existe um processo para gestão de alterações e por isso não requerem aprovação. O horário de implementação é definido pela equipa implementadora com base na sua sensibilidade e experiência no que respeita ao potencial impacto que poderá causar	A organização tem definido um processo para gestão de alterações, onde se incluem as alterações nos serviços de rede. Todas as aprovações seguem o seu fluxo de aprovação, existindo um período definido para a sua implementação, tendo em conta o impacto esperado nos utilizadores e serviços. Contudo, a janela de intervenção poderá ser ajustada mediante o parecer da equipa implementadora	A organização tem definido um processo para gestão de alterações, onde se incluem as alterações nos serviços de rede. Todas as alterações são analisadas e aprovadas em reunião de CAB que ocorre semanalmente. Ainda na reunião de CAB é avaliado o impacto e decidida a janela de intervenção mediante o impacto esperado e a criticidade da solução/infraestrutura a ser intervencionada. Para intervenções urgentes é seguido um processo "Agile" aprovado pelos responsáveis aplicacionais/infraestrutura e gestão de serviço		

		Deteção de ativos na rede (shadown IT)	A organização não dispõe de processos e tecnologia para detetar e identificar postos de trabalho ou outros ativos desconhecidos ou não geridos na rede	A organização de forma pontual avalia a existência de postos de trabalho e outros ativos não geridos na rede. Esta análise é manual	A organização tem definido um processo que é suportado por uma solução tecnológica baseada em varrimentos em tempo real nas diversas redes (cablada e/ou sem fios). Adicionalmente a organização dispõe ainda de uma solução baseada em NAC que autentica o posto através do seu endereço mac	A organização tem definido um processo que é suportado por uma solução tecnológica faz varrimentos em tempo real nas diversas redes (cablada e/ou sem fios). Este processo é revisto anualmente e todos os ativos identificados são alvo de análise. As exceções são registadas em matéria de risco e acompanhadas até à sua mitigação. Adicionalmente a organização dispõe ainda de uma solução para autenticação e autorização de ativos na rede, baseada em RBAC através do registo do ativo na AD, impedindo que qualquer ativo não registado possa conectar-se às redes da organização, inclusive por VPN		
	Gestão de incidentes na rede	**Identificação, analise, tratamento e monitorização de incidentes envolvendo ativos de comunicação/rede**	Não existe monitorização regular sobre os eventos. O acesso é feito pontualmente e em cenários de incidente	Existe alarmística sobre os eventos gerados através do envio de notificações (ex. por email, SMS,,etc.). Os administradores consultam os eventos mediante os alertas recebidos	A organização possui uma solução de agregação de eventos de ativos, que alem de guardar, também permite correlacionar e notificar. Os administradores acedem aos eventos e iniciam investigação mediante os alertas recebidos	A organização possui um NOC, com equipa dedicada que gere o ciclo de vida do incidente. Esta equipa faz uma primeira análise sobre os alertas e respetivos eventos, apoiando-se na capacidade de inteligência e correlação que a solução disponibiliza . Caso se justifique, o incidente é escalado à equipa de administração dos ativos para tratamento		

	Arquitectura de rede	**Modelo de segregação de redes**	Os limites das redes não estão definidos, não existindo uma verdadeira segmentação	Existe uma segregação física e lógica entre a rede interna e a rede exposta para o exterior (DMZ)	Existem diversos níveis de segregação na rede (ex. dmz, rede produtiva e rede não produtiva), sendo esta segregação lógica	Encontra-se implementada uma arquitetura de rede transparente onde a rede interna está segregada por zonas, mediante a criticidade dos ativos em cada zona. O modelo de acesso varia por zona, obrigando a mais requisitos de segurança mediante a criticidade da zona		
	Políticas de rede	**Documentação de rede**	A organização não dispõe de documentação detalhada sobre as suas redes. A informação apenas reside "na cabeça" dos administradores de rede	A organização dispõe de documentação sobre as suas redes e segmentos. Contudo, não existe um processo de atualização e revisão sobre esta documentação	A organização dispõe de documentação detalhada sobre as suas redes e respetivos segmentos. A informação é guardada num repositório central à semelhança da restante informação sobre aplicações e infraestruturas	A organização dispõe de documentação detalhada sobre as suas redes e respetivos segmentos. A informação é guardada num repositório central à semelhança da restante informação sobre aplicações e infraestruturas. Anualmente as equipas de administrações de redes recebem tarefas de revisão sobre a documentação. Sempre que são realizados projecto ou atividade de maior impacto, um fluxo é gerado automaticamente pela solução ITSM e enviado ao executante das alterações para que proceda também à atualização da documentação		
		Utilização aceitável e responsável da rede	A organização não tem definidas políticas ou práticas que definem uma correta utilização dos recursos de rede	Estão documentadas as melhores práticas na utilização da rede, embora seja apenas um documento informal servindo de guia de orientação	A organização tem definida e publicada uma política para uso aceitável dos recursos de rede	A organização tem definida e publicada uma política para uso aceitável dos recursos de rede. A cada colaborador é dado conhecimento da política na fase de contratação. Anualmente a política é revista e cada colaborador recebe um fluxo, onde é obrigado a dar conhecimento e aceitação sobre a sua adesão à referida política		

	Gestão de vulnerabilidades na rede	**Processo de deteção, análise e mitigação**	A organização não possui um processo para deteção de vulnerabilidade na rede. Tem conhecimento apenas quando recebe informação se fontes públicas	A organização não possui um processo para deteção de vulnerabilidade na rede. Contudo, pontualmente executa atividades de scans de vulnerabilidades, sobretudo quando surgem notícias públicas sobre determinados ciberataques que envolvem equipamentos semelhantes aos que a organização utiliza	A organização possui um processo para deteção de vulnerabilidade na rede que assenta na realização de scans de vulnerabilidade anuais a todos os ativos de rede	A organização possui um processo para deteção de vulnerabilidades na rede que assenta na realização de scans de vulnerabilidade mensais a todos os ativos de rede. Estes scans são realizados por equipas internas e externas. São ainda recebidas informações sobre vulnerabilidades diretamente dos fabricantes dos ativos, assim como de outras fontes de *Treath Intel* por forma a serem tratadas o mais urgentemente possível para evitar serem exploradas publicamente		
		Instalação de atualizações de rede	A organização não tem definido um processo que vise gerir a instalação de atualizações em ativos de rede	O processo de instalação de atualizações não abrange ativos de rede. A aplicação de atualizações é pontual e por norma para corrigir vulnerabilidades	O processo de instalação de atualizações abrange ativos de rede. Contudo, a sua aplicabilidade não é regular em virtude do potencial impacto	O processo de instalação de atualizações abrange também ativos de rede, cuja sua aplicação decorrer de forma regular e contempla todos os ativos de rede de todos os ambientes existentes		
		Deteção e tratamento de vulnerabilidades em ativos de rede	A organização não tem definido um processo para identificar e acompanhar o tratamento de vulnerabilidades	A organização tem definido um processo para identificar vulnerabilidade, mas o mesmo não tem um acompanhamento até final do ciclo de vida da vulnerabilidade	A organização tem definido um processo para identificar vulnerabilidade e acompanhar o seu tratamento. A vulnerabilidade é registada na base dados de vulnerabilidades e criado um pedido na ferramenta de ITSM para mitigação. Quando a mitigação for confirmada a base dados é manualmente atualizada	A organização tem definido um processo para identificar vulnerabilidade e acompanhar o tratamento de vulnerabilidades. O ciclo de vida da vulnerabilidade é automatizado totalmente materializado através da solução que a identificou		
								Insira valor nos controlos

Gestão de parceiros (fornecedores)	**Políticas, Processos e procedimentos**	**Gestão de contratos**	Os contratos assinados com parceiros são pouco detalhados e clausulados, limitando-se apenas ao que é comum num contrato entre duas partes	Os contratos assinados com parceiros são pouco detalhados, em particular sobre deveres e responsabilidades envolvendo a temática da cibersegurança	Os contratos assinados endereçam cláusulas de deveres, responsabilidade e obrigatoriedade em cumprir todos os requisitos de cibersegurança e privacidade. O contrato prevê ainda que a organização supervisione e audite todas as atividades realizadas	Os contratos assinados endereçam cláusulas de deveres, responsabilidade e obrigatoriedade em cumprir com todos requisitos de cibersegurança, privacidade, práticas de segurança na utilização e configuração de equipamentos e devolução de equipamentos. O contrato é revisto regularmente para garantir a sua atualização e inclusão de novos requisitos e práticas de segurança, que contemplam penalizações por incumprimento. A organização ao abrigo do contrato tem legitimidade para supervisionar, auditar		
		Cumprimento do normativo interno	A organização não partilha normativo com parceiros/fornecedores, ou partilha, mas não força o seu cumprimento	A organização partilha o seu normativo, incluindo normativo específico para parceiro com o parceiro apenas na fase de contratação de serviços	A organização partilha o seu normativo com o fornecedor na fase de contratação e sempre que existem alterações relevantes	A organização partilha o seu normativo com o fornecedor na fase de contratação e sempre que existem alterações relevantes. A organização monitoriza o cumprimento do normativo por parte dos parceiros e em reuniões de serviço que ocorrem mensalmente, sendo este um ponto na agenda da reunião		

	Governação	**Processo de contratação**	O processo de contratação de parceiros/fornecedores ocorrem sem formalismos, ocorrendo à medida que é necessário	O processo de contratação não é realizado por departamento de forma informal. Existem algumas orientações para a realização da contratação, mas nem sempre ou nem todos os departamentos seguem essas práticas	A organização dispõe de uma área central de compras, existindo um processo estabelecido que define as regras de contratação	A organização tem definido um processo de contratação com regras e requisitos definidos. Quando é identificada uma necessidade de contratar serviços externos, é seguido um fluxo passando pelas diversas áreas que formalmente estão definidas como sendo parte do processo e outras que variam em função do tipo e natureza dos serviços a contratar, embora a área de segurança participe em todas as contratações que envolvem TIC		
		Avaliação prévia à contratação	A organização geralmente não executa uma avaliação prévia à contratação (incluindo parceiro e função contratada)	A contratação ocorre ao nível departamental, sendo realizada uma avaliação de prévia, embora por formalizada e não difundida por toda a organização	A análise prévia à contratação do parceiro é uma preocupação e um requisito obrigatório. Os riscos identificados em particular os de maior criticidade são analisados e supervisionados pela organização, tendo sido definidos prazos para a sua mitigação	A avaliação prévia à contratação do parceiro é uma preocupação e um requisito transversal para qualquer contratação, independentemente do valor co contrato. O resultado da avaliação é um fator crítico a ter em conta para fechar a contratação. No caso da contratação ser estabelecida, os riscos identificados são alvo de uma supervisão apertada pela organização, definindo prazos para a sua mitigação e implementados controlos compensatórios. Regularmente são realizadas ações de avaliação de risco pela organização através do seu processo de risco, recorrendo também a avaliação através de ferramentas que avaliam diariamente os riscos e o "rate" de cada parceiro		

		Gestão de não conformidade de parceiros	A organização não tem definidos processos e procedimentos para monitorizar a conformidade dos seus parceiros. Sempre que uma não conformidade é identificada, a organização trata-a de forma informal	A organização não tem definidos processos formais para gestão de não conformidades envolvendo fornecedores. Apesar de existirem orientações para tratar não conformidades, estas centram-se e tratam-se ao nível departamental	A organização tem definidos processos para gestão de não conformidade de parceiros, sendo tratados e monitorizados ao nível da organização	A organização tem definidos processos para gestão de não conformidade de parceiros, sendo tratados e monitorizados ao nível da organização. O processo é monitorizado e atualizado de forma regular para ter uma maior cobertura para os diversos cenários e diferentes parceiros		
		Ponto de contato para gestão de pedidos	A organização não tem definido um canal e um contacto formal para interagir com parceiros para as mais diversas situações. As interações ocorrem de forma informal e através de diferentes pessoas	A organização não tem definido um canal e um contacto formal para interagir com parceiros para as mais diversas situações. Contudo, todas as interações ocorrem a nível do departamento ou área responsável pelo serviço prestado pelo parceiro	A organização tem definido um canal e um ponto de contato formal para interação com parceiros	A organização tem definido um canal e um ponto de contato formal para interação com parceiros, tratando da área de gestão de serviço		
	Gestão de risco de parceiros	**Avaliação de risco a parceiros**	A organização não avalia riscos dos seus parceiros	A organização realiza avaliação de risco de alguns parceiros, sobretudo aqueles que estão envolvidos em soluções com arquitectura mais críticas	A organização tem definidos processos para avaliação de riscos associados a parceiros. A organização monitoriza de forma regular o risco e respetiva classificação dos seus parceiros	A organização tem definidos processos para avaliação de riscos associados a parceiros. A organização monitoriza de forma regular o risco e respetiva classificação de cada parceiro. Estão definidas métricas relativamente ao rate de parceiros, que são monitorizadas e analisadas mensalmente em reuniões de Steering. A organização incentiva ao incremento no rate dos seus parceiros. Em caso de descida de rate, a organização analisa e toma as devidas diligências		

		Fontes para consulta de classificação de parceiros	A organização não tem definido processos para obter e gerir classificação dos seus parceiros	A organização não tem definido processos para obter e gerir classificação dos seus parceiros. Contudo, obtém classificações através de fontes públicas e contatos próximos	A organização tem definidos processos e soluções (ex.: bitsight, SecurityScoreCard, ,etc.) que fornecem informação sobre classificação de parceiros	A organização tem definidos processos, soluções (ex.: bitsight, SecurityScoreCard,,etc.) que fornecem informação sobre classificação de parceiros. Estas soluções disponibilizam informação coerente, realista e atualizada regularmente. A organização valida os dados obtidos de forma regular e define medidas de melhoria sobre a coerência e audibilidade aos sistemas fonte		
		Disponibilização de acessos a informação sensível e classificada	A organização não tem implementados controlos específicos para gerir o acesso a informação sensível por parte dos seus parceiros	A organização tem definidos alguns controlos e mecanismos para restringir o acesso a informação sensível pelos parceiros. Estes controlos são implementados de forma ad-hoc e não garantem uma abrangência global	A organização tem implementados controlos centralizados que impedem o acesso a informação sensível. Estes controlos são transversais a toda a organização e também auditam e monitorizam todos os conteúdos acedidos	A organização tem implementados controlos centralizados que impedem o acesso a informação sensível. Estes controlos são transversais a toda a organização e também auditam e monitorizam todos os conteúdos acedidos. A organização tem ainda implementadas políticas e uma solução de classificação de informação, que igualmente impedem o acesso a informações classificadas através da utilização de etiquetas classificativas		

		Renovação contratual	A renovação de contrato com parceiros é informal, sem qualquer reavaliação	A renovação de contrato é executada tendo por base um questionário interno sobre o qual é obtido pareceres das áreas relevantes, como seja cibersegurança, privacidade ou gestão de serviço	A organização tem um processo formal para renovação contratual, onde são lançados questionários internos sobre a apreciação global do serviço prestado. São ainda lançados alguns questionários base e outros específicos de acordo com o resultado obtido nos questionários base	A organização tem um processo formal para renovação contratual, envolvendo as principais áreas internas, incluindo a área de segurança, que tem obrigatoriamente de emitir um parecer sobre a renovação. São lançados questionários internos sobre a apreciação global do serviço prestado. A classificação do parceiro no que respeita a risco é considerada neste processo		
		Monitorização sobre a postura de segurança do parceiro	Não são realizadas atividades no decorrer do contrato que visem avaliar a postura, sensibilidade e capacidade do parceiro em matéria de cibersegurança	São realizadas atividades pontuais decorrer do contrato que visam avaliar a postura, sensibilidade e capacidade do parceiro em matéria de cibersegurança. Estas avaliações centram-se em questionários lançados e recolha de pareceres junto dos colaboradores internos	A organização monitoriza de forma regular as atividades do parceiro, retirando daí indicadores. Os parceiros são convidados a participar em formação, exercícios e campanhas de sensibilização para a cibersegurança	A organização monitoriza de forma regular as atividades do parceiro, tendo definidos KPIs. Os parceiros são obrigados a participar em formação, exercícios e campanhas de sensibilização para a cibersegurança. Cada parceiro tem ainda obrigatoriedade de formar os seus quadros para a temática da cibersegurança e dar evidências sobre essas formações		

		Estratégia de saída	Quando o contrato é assinado com parceiros, não é definida uma estratégia de saída	Os contratos assinados com parceiros, incluem informação sobre a estratégia de saída, embora muito alto nível	Todos os contratos com parceiros definem uma estratégia de saída, onde se inclui informação sobre a gestão do processo de saída no que respeita a passagem de conhecimento, tempo necessário para apoiar a integração de um novo parceiro, formato e moldes em que a passagem de conhecimento deve ocorrer	Todos os contratos com parceiros definem uma estratégia de saída, onde se inclui informação sobre o processo de saída no que respeita a passagem de conhecimento, tempo necessário para apoiar a integração de um novo parceiro, formato e moldes em que a passagem de conhecimento deve ocorre. A organização define uma equipa interna de apoio à saída do parceiro para assegurar que o conhecimento fica também retido no seio da organização e assegurar uma passagem para o novo parceiro sem incidentes, atendendo ao momento sensível que é a substituição de um parceiro		
								Insira valor nos controlos
Monitorização de segurança	**Pessoas/Equipas**	**Equipa de monitorização**	A organização não tem uma equipa dedicada à de monitorização de cibersegurança	A organização não tem uma equipa dedicada para monitorizar e tratar temas de cibersegurança. Sempre que necessário é constituída um grupo de trabalho informal para acompanhar e proceder com as diligências necessárias	A organização tem uma equipa dedicada para monitorizar e tratar temas de cibersegurança	A organização tem uma equipa dedicada para monitorizar e tratar temas de cibersegurança. A equipa é autónoma a tratar todas as situações que envolvem cibersegurança, interagindo com parceiros, grupos de especialidade e entidades legais, regulamentares, supervisoras e setoriais		

		Capacidade e prontidão	O facto da organização não ter uma equipa dedicada à monitorização e resposta a temas de cibersegurança, a capacidade e qualidade de resposta a qualquer assunto desta natureza não será eficaz	A organização não tem uma equipa dedicada à monitorização e resposta sobre temas de cibersegurança. Contudo, existem informalmente determinadas funções e perfis que respondem a situações que o exigem, embora a resposta seja dada com base no melhor esforço	A equipa de monitorização e resposta a temas de cibersegurança encontra-se definida e com aptidão para responder	A equipa de monitorização e resposta a temas de cibersegurança encontra-se definida e com aptidão para responder. As funções são revistas regularmente de forma a garantir uma total cobertura para temas de cibersegurança, tendo por base análise e tendências sobre novas tipologias de ameaças e ataques cibernéticos		
		Formação e sensibilização em cibersegurança	As equipas tem uma formação mínima em cibersegurança	As equipas tem alguma formação e sensibilização para lidar com temas de cibersegurança, embora o conhecimento seja muito individualizado	A organização possui equipas dedicadas a temas que envolvem cibersegurança, estando para isso capacitadas com formação que lhes é administrada no início das suas funções e atualizada regularmente	A organização possui equipas dedicadas a temas que envolvem cibersegurança, estando para isso capacitadas com formação que lhes é administrada no início das suas funções e atualizada regularmente de acordo com os seus planos de formação. A organização monitorização a atividades destas equipas e define métricas para avaliar a sua atividade e a partir desses indicadores são definidas formações específicas em determinados domínios consoante as necessidades e a capacidade em conseguir responder correta e eficazmente as todos os temas relacionados com cibersegurança		

	Processos e procedimentos	**Estratégia de monitorização**	A organização não tem definida uma estratégia para monitorização de cibersegurança	A organização não tem formalizada uma estratégia para monitorização de cibersegurança. Contudo, existe uma equipa que faz monitorização global sobre os ativos e não dedicada a temas de cibersegurança que informa perante a existência de comportamentos anómalos ou alertas associados a cibersegurança	A organização tem definida uma estratégia para monitorização de segurança. Esta monitorização é essencialmente realizada de forma manual e não abrange todos os ativos organizacionais, somente aqueles que tem associado um maior risco devido à sua utilização e exposição	A organização tem definida uma estratégia para monitorização de segurança assente numa total automatização na análise de eventos e resposta a alertas e incidentes. Todos os ativos são alvo de monitorização mediante o nível de risco de cada um. A estratégia de monitorização é avaliada regularmente para aferir a sua eficácia e capacidade de responder às novas ameaças e ataques.		
		Monitorização e supervisão da estratégia de monitorização	A gestão de topo tem uma reduzida participação e envolvimento no acompanhamento da estratégia de monitorização	A gestão de topo é envolvida e participa no programa de monitorização, embora em alto nível, focando-se apenas nos valores mensais sobre a atividade da área	A gestão de topo é envolvida e participa no programa de monitorização, existindo um comité de segurança que reúne trimestralmente. Este Comité é composto por elementos da gestão de topo e áreas relevantes e que contribuem ativamente para ampliar e melhorar a monitorização de cibersegurança	A gestão de topo é envolvida e participa no programa de monitorização, existindo um comité de segurança que reúne trimestralmente. Este Comité é composto por elementos da gestão de topo e áreas relevantes e que contribuem ativamente para a causa. Este comité serve ainda para analisar modelos, processos e tecnologias imergentes que visem incrementar a segurança da organização, em particular a cibersegurança		
		Processos de monitorização	A organização não tem definidos nem implementados processos para monitorização de segurança	A organização não tem formalmente definidos processos de monitorização, contudo são executados procedimentos e de forma ad-hoc e manuais	Os processos de monitorização estão formalmente definidos e documentados, embora não sejam totalmente seguidos. A organização tenta manter os processos atualizados e adaptados às novas ameaças	A organização tem os processos formalmente definidos e bastante amadurecidos em virtude da senioridade das equipas de monitorização. Todos os processos são revisto regularmente atualizados em linha com os principais "standards" da indústria		

		Escalonamentos	A organização não tem definidos nem implementados fluxos de escalonamentos aliados ao processo de monitorização	A organização não tem definidos nem implementados formalmente os fluxos de escalonamentos aliados ao processo de monitorização. Contudo, existe uma lista de contatos informais da área de segurança para onde podem ser escalados temas	A organização tem formalmente definidos e implementados fluxos de escalonamentos aliados ao processo de monitorização, existindo para isso um canal estabelecido para escalonamentos	A organização tem formalmente definidos e implementados fluxos de escalonamentos aliados ao processo de monitorização em modelo 24*7*365. O processo de escalonamentos define as funções e responsabilidades de cada equipa e o procedimento a seguir, bem como os responsáveis de cada equipa		
		Gestão de exceções	Todas as exceções são tratadas de forma informal à medida que vão surgindo	As exceções são discutidas com a área de segurança e comunicadas informalmente a toda a organização	As exceções são discutidas com a área de segurança, propostas a aprovação, aprovadas e formalmente comunicadas a toda a organização	As exceções são discutidas com a área de segurança, propostas a aprovação, aprovadas e formalmente comunicadas a toda a organização. Regularmente todas as exceções são analisadas entre a área de segurança e as áreas preponderantes para avaliar a sua continuidade		
		Modelo de reporte interno	Não está definido um modelo de reporte interno	Não está definido um modelo de reporte. Contudo, a equipa de segurança está preparada e responde de forma informal	A organização tem definido um modelo de reporte no que respeita a conteúdos e métricas. Mensalmente são produzidos e partilhados os relatórios	A organização tem definido um modelo de reporte totalmente automatizado. Mensalmente são produzidos e partilhados os relatórios definidos. A gestão de topo recebe os relatórios. Os templates são revistos e atualizados regularmente de forma a contemplarem informação relevante para a gestão de topo		

		Modelo de reporte externo	Não está definido um modelo de reporte interno	Não está definido formalmente um modelo de reporte externo. A equipa de segurança reporta a entidades externas (supervisores, entidades policiais, regulamentares,,etc.....)	A organização tem definido um modelo de reporte externo. Este modelo define o canal e a área responsável por comunicar com entidades externas (supervisores, entidades policiais, regulamentares,,etc.....)	A organização tem definido um modelo de reporte externo automatizado e "estandardizado" de forma a responder uniforme e atempadamente às obrigações impostas. Este modelo define todos os detalhes que o reporte deve respeitar, desde a sua conceção, ao envio e reposta a pedidos de provenientes de todas as entidades perante as quais a organização tem essa obrigatoriedade (supervisores, entidades policiais, regulamentares,,etc.....)		
		Processos para monitorização automatizada	A organização não tem definido qualquer processo automatizado para monitorização de segurança	A organização não tem definido qualquer processo automatizado, embora tenha equipas que apoiam na monitorização, mas numa base manual	A organização tem implementado um serviço de monitorização assente em SOC (interno ou externo) que automatiza parcialmente o processo de monitorização de segurança	A organização tem implementado um serviço de monitorização assente em SOC (interno ou externo) que automatiza na íntegra o processo de monitorização de segurança		
		Processo de reporte de incidentes	A organização não tem definido um processo para reporte de incidentes de segurança. Geralmente são comunicados de forma informal	A organização não tem formalmente definido um processo para reporte de incidentes de segurança, embora estejam informalmente implementados alguns canais, métodos e modelos de comunicação de incidentes	A organização tem definido um processo para reporte de incidentes de segurança. Neste processo estão definidos canais, métodos e modelos de comunicação de incidentes, embora possam ser utilizados outros canais paralelos (email, telefone, chat,,etc.)	A organização tem definido um processo para reporte de incidentes de segurança. Neste processo estão definidos canais, métodos e modelos de comunicação de incidentes. A organização monitoriza regularmente a forma como os incidentes são reportado. De forma regular os colaboradores realizam formação em cibersegurança e simultaneamente são treinados sobre a forma como devem reportar quaisquer incidentes de cibersegurança interna ou externamente		

		Gestão de incidentes	A gestão de incidentes é executada caso a caso, sem que siga um processo ou fluxo	A gestão de incidentes não está formalmente definida, embora sejam seguidas regras em linha com as características de cada incidente	A organização tem definido e implementado um processo para gestão de incidentes	A organização tem definido e implementado um processo para gestão do ciclo de vida do incidente alinhado com os principais "standards" da indústria		
		Análise prévia a incidentes de segurança	Não é realizada uma análise prévia a incidentes de cibersegurança de forma a descartar falsos positivos	Formalmente não existe o conceito de análise prévia a incidentes de cibersegurança de forma a descartar falsos positivos. Muitas vezes esta pré-análise é feita com base na experiência da pessoa que recebe o incidente	Em virtude de existirem alguns processos automatizados para análise de incidentes de segurança, a análise prévia é realizada permitindo excluir casos associados a falsos positivos	A organização tem o seu sistema de monitorização de segurança totalmente automatizado, permitindo uma maior e melhor análise a todos os eventos, assim como uma correlação entre eles. Este processo permite uma análise prévia mais eficiente, reduzindo substancialmente o número de falsos positivos que são alvo de análise		
		Critérios para definição de criticidades	A organização não tem definidos quaisquer critérios para atribuição de criticidade a incidentes de cibersegurança A atribuição é feita caso a caso e sem uma base orientadora	Não estão definidos critérios para atribuição de criticidades a incidentes de cibersegurança, embora sejam seguidas algumas práticas nessa classificação, alinhadas com a criticidade associada ao ativo alvo do incidente	A organização têm definidos critérios para atribuição de criticidade aos incidentes de cibersegurança. Este critério está alinhado com a criticidade do ativo e com o impacto financeiro e reputacional	A organização têm definidos critérios para atribuição de criticidade aos incidentes de segurança. Este critério está alinhado com a criticidade do ativo e com o impacto financeiro e reputacional. O processo de atribuição de criticidade calcula automaticamente a criticidade em função dos casos de uso pré-definidos. Regularmente a organização revê a criticidade de cada ativo, em função dos inputs proveniente da avaliação de risco executada		

		Tipificação de incidentes e eventos de segurança	Não é seguido qualquer processo ou prática para tipificar incidentes de cibersegurança	Apesar de não existir um processo ou critério para tipificar incidentes, a organização segue um conjunto de práticas que tem por base *standards* ainda que pouco formalizados e nem sempre atualizados	A organização tem definido critérios para tipificação de incidentes de segurança. Esta prática é seguida formal e obrigatoriamente em linha com *standards*	A organização tem definido critérios para tipificação de incidentes de segurança. Esta prática é seguida formal e obrigatoriamente em linha com *standards*. A organização participa regularmente em fóruns da especialidade (ex. CNCS) de forma a garantir que segue as melhores práticas e procedimentos na tipificação de incidentes de segurança		
		Gestão de eventos de cibersegurança	A organização não tem definido um processo para gestão do ciclo de vida de eventos de cibersegurança	A organização não tem definido um processo para gestão do ciclo de vida de eventos de cibersegurança. Contudo, são recolhidos, analisados e tratados determinados eventos, mas apenas quando sucedem alertas ou incidentes de segurança	A organização tem definido um processo para gestão do ciclo de vida de eventos de cibersegurança. A operacionalização deste processo é realizada pela equipa de cibersegurança	A organização tem definido um processo para gestão do ciclo de vida de eventos de cibersegurança. A operacionalização deste processo é realizada pela equipa de cibersegurança. Este processo é alvo de revisão regular de forma a garantir a sua atualização, adequação e abrangência às ameaças que surgem no dia a dia		
		Seleção de eventos de segurança	A organização não tem instituída uma norma ou guia que defina quais os eventos de segurança que devem ser produzidos e recolhidos	A organização não tem formalmente instituída uma norma ou guia que defina quais os eventos de segurança que devem ser produzidos e recolhidos como objeto de "alimentar" a monitorização de cibersegurança, embora algumas fontes estejam configuradas para produzir eventos de segurança por defeito, mas não existe um *standard*	A organização tem formalmente instituído normativo define quais os eventos de segurança que devem ser produzidos e recolhidos como objeto de monitorização de segurança	A organização tem formalmente instituído uma norma que define quais os eventos de segurança que devem ser produzidos e recolhidos como objeto de monitorização de cibersegurança. Esta norma "mapeia" os casos de uso implementados na monitorização, sendo assim alvo de atualizações constantes por forma a refletir todos os casos de uso que vão sendo implementados		

		Frequência definida para revisão de eventos de segurança	Não existe uma frequência ou regularidade definida para revisão de eventos de segurança	Não está definida uma frequência ou regularidade formal para rever eventos de segurança. Esta revisão ocorre de forma ad-hoc em resultado de alertas ou incidentes de cibersegurança ocorridos	A organização tem implementado um processo de revisão dos eventos de segurança produzidos e recebidos com objetivo de cumprirem com os casos de uso existentes	A organização tem implementado um processo de revisão dos eventos de segurança produzidos e recebidos de forma regular para assegurar que cada de uso definido na monitorização tem os eventos necessária para uma avaliação completa e assertiva		
		Acesso e envio seguro aos eventos de segurança	A organização não recolhe eventos de segurança de ativos O acesso a estes eventos é feito através dos gestores de infraestrutura	A organização não recolhe eventos de segurança dos ativos. Contudo, sempre que necessário essa recolha, a mesma é processada de forma segura. O acesso a estes eventos é feito através dos gestores de infraestrutura, ficando auditado todas as operações realizadas	A organização tem definido um processo para recolha e envio de eventos de segurança de forma segura, seja para análise interna (ex. equipa de segurança, SOC,,etc.....), seja para entidades externas (ex. Reguladores, entidades judiciárias,...,etc.). Os ativos (fontes) que produzem eventos, registam qualquer ação ocorrida sobre eles	A organização tem definido um processo para recolha e envio de eventos de segurança de forma segura e por meio de um canal previamente definido, seja para análise interna (ex. equipa de segurança, SOC,,etc.....), seja para entidades externas (ex. Reguladores, entidades judiciárias,...,etc.). Os ativos (fontes) que produzem eventos, registam qualquer ação ocorrida sobre estes		
		Informação sensíveis em eventos de segurança	A organização não tem definida qualquer norma ou guia que indique a informação deve ou não constar nos eventos de segurança	A organização não tem definida qualquer norma ou guia para definição da informação que deve ou não constar nos eventos de segurança. Contudo, existe sensibilização por parte das equipas em não guardar dados pessoais ou sensíveis nos eventos de segurança	A organização tem definidas normas ou guias que indicam que tipologia de informação deve ou não constar nos eventos de segurança, mediante os requisitos que constam em regulamentos como seja o RGPD, instruções da CNPD ou outros *standards*	A organização tem definidas normas que indicam que tipologia de informação deve ou não constar nos eventos de segurança dos ativos fonte, mediante os requisitos que constam em regulamentos como seja o RGPD, instruções da CNPD ou outros *standards*. Os eventos gerados são alvo de auditorias regulares para assegurar que cumprem com as normas e orientações definidas		

		Prazos de retenção e conservação	A organização não define nem aplica prazos de retenção nos eventos de segurança	A organização não define nem aplica prazos de retenção nos eventos de segurança. Cada ativo é configurado de forma ad-hoc e de acordo com a pessoa que o configurou	A organização tem formalmente definidos prazos para retenção e conservação de eventos de segurança, quer ao nível dos ativos fonte quer ao nível do armazenamento central	A organização tem formalmente definidos prazos para retenção e conservação de eventos de segurança, quer ao nível dos ativos fonte quer ao nível do armazenamento central. Estes prazos estão alinhados com os requisitos de negócio e legais/regulamentares. Anualmente ou sempre que surjam alterações formais, estes prazos são revistos e o normativo atualizado		
		Threat Intelligence	A organização não tem quaisquer fontes de TI internas ou externas. Apenas obtém informações públicas	A organização não tem quaisquer fontes formais de TI internas ou externas. De forma ad-hoc a equipa de segurança tem conhecimento de algumas fontes	A organização tem definido um processo de TI baseado em informações públicas do setor onde está inserida, dos diversos reguladores e de um serviço contratado	A organização tem definido um processo de TI baseado em informações públicas do setor onde está inserida, dos diversos reguladores e de um serviço contratado. Regularmente a organização revê o processo de forma a aferir a consistência do serviço contratado, procurando de forma ativa melhorá-lo e aumentar o seu âmbito		
		Threat Hunting	A organização não tem implementado qualquer serviço de TH	A organização não tem implementado qualquer serviço de TH. Contudo, a equipa de segurança faz pequenas investigações com base em informação pública ou que recebe de forma informal	A organização tem implementado serviços de TH, contratados externamente	A organização tem implementado serviços de TH formado por equipas internas e um serviço contratado externamente, funcionando em plena articulação		

	Tecnologia	**Ferramenta de Análise e correlação de eventos (SIEM)**	A organização não tem implementada qualquer solução baseada em SIEM	A organização não tem formalmente implementada qualquer solução baseada em SIEM. Contudo, são utilizadas de forma pontual e informal mecanismos que permitem fazer análises automatizadas e correlação de eventos de segurança	A organização tem implementada uma solução de SIEM (interna ou externalizada) que operacionaliza a automatização da monitorização de cibersegurança	A organização tem implementada uma solução de SIEM (interna ou externalizada) que operacionaliza a automatização da monitorização de cibersegurança. Regularmente são realizadas auditorias à solução e ao processo que a sustenta de forma a assegurar a sua correta operação e melhoria contínua		
		Alarmística	A organização não tem implementada qualquer solução que permite enviar alertas/notificações ou outros meios de informar acerca de incidentes de segurança	A organização tem implementados mecanismos para o envio de alertas/notificações sobre incidentes de segurança, embora predomine um elevado valor de falsos positivos atendendo que não é realizada qualquer triagem	A organização tem implementados mecanismos para o envio de alertas/notificações sobre incidentes de cibersegurança.	A organização tem implementados mecanismos para o envio de alertas/notificações sobre incidentes de cibersegurança. Estes alertas de criticidade mais reduzida são automatizados, sendo os restantes procedidos de um contato pela equipa de monitorização. A organização revê regularmente os casos de uso que despoletam os alertas/notificações de forma a torná-los mais assertivos e evitar que as equipas percam o foco perante casos realmente importantes e críticos		

		Armazenamento de eventos de segurança	A organização não recolhe quaisquer eventos dos ativos que os produzem	A organização não recolhe formalmente eventos de segurança dos ativos. Num cenário de incidente os eventos são recolhidos de forma ad-hoc e armazenados em localizações temporárias e depois removidos	Os eventos de segurança são recolhidos dos ativos e encaminhados para um repositório centralizado, onde é possível fazer pesquizas rápidas	Os eventos de segurança recolhidos dos ativos e encaminhados para um repositório centralizado, onde é possível fazer pesquizas rápidas sobre qualquer evento de qualquer fonte, caso ainda não tenha sido ultrapassado o prazo de retenção. A solução de armazenamento de eventos é monitorizada em modelo 24x7x365 para assegurar a sua permanente disponibilidade assim como o espaço disponível/ocupado		
		Monitorização ativa de cibersegurança em postos de trabalho, servidores e ativos de rede	A organização não possui qualquer solução para deteção de comportamento anómalo nos seus ativos	A organização não possui qualquer solução para deteção de comportamento anómalo nos seus ativos. Em cenários de alerta ou incidentes de cibersegurança são executadas algumas aplicações (muitas vezes baseadas em *freeware* ou *shareware) para análise dos ativos*	A organização possui parte do seu parque tecnológico dotado de uma solução que permite a monitorização e reposta em tempo real para comportamentos anómalos de colaboradores e respetivos equipamentos (XDR)	A organização possui o seu parque tecnológico dotado de uma solução que permite a monitorização e reposta em tempo real para comportamentos anómalos dos colaboradores e respetivos equipamentos (XDR) no caso de postos de trabalho e servidores. Para equipamentos de rede são utilizados IDS, WAF e firewall		
		Cobertura na monitorização de cibersegurança	A organização não tem uma cobertura formal de todos os seus ativos no que respeita à monitorização de cibersegurança	A organização não tem uma cobertura formal de todos os seus ativos no que respeita à monitorização de segurança, embora existam ativos é dado um maior foco e importância pela criticidade que representam	A organização tem uma monitorização total dos seus ativos, embora não tenha uma equipa a suportar essa monitorização em 24x7x365	A organização tem uma monitorização total dos seus ativos com uma equipa dedicada a suportar essa monitorização em 24x7x365		

		Segurança no correio eletrónico	A organização não tem implementado qualquer controlo de segurança sobre os emails recebidos pelos seus colaboradores	A organização tem implementado alguns controlos de segurança para melhorar a segurança sobre os emails recebidos pelos seus colaboradores	A organização tem definidas e implementadas políticas e mecanismos para bloqueio/reter emails que representam uma ameaça para a organização	A organização tem definidas e implementadas políticas e mecanismos para bloqueio/retenção de emails que representem uma ameaça para a organização, impedindo que estes chegam aos colaboradores. Estes mecanismos são atualizados automaticamente com informação proveniente de fontes de Threat Intelligence e Threat Hunting		
		Gestão e monitorização de impressoras	A organização não tem implementado controlos com objetivo de gerir e monitorizar o parque de impressão	A organização não tem implementado controlos com objetivo de gerir e monitorizar o parque de impressão. Contudo, os administradores de sistemas implementam de forma ad-hoc determinados controlos, mas não de forma formal nem abrangem todos os servidores de impressão	A organização tem implementado controlos com objetivo de gerir e monitorizar o parque de impressão. As impressoras são geridas centralmente e atualizadas assim que surjam atualizações pelos fabricantes. Os servidores de impressão são alvo de monitorização e atualizados de acordo com o ciclo pré-definido	A organização tem implementado controlos com objetivo de gerir e monitorizar o parque de impressão. As impressoras são geridas centralmente e atualizadas assim que surjam atualizações pelos fabricantes. Os servidores de impressão são alvo de monitorização e atualizados de acordo com o ciclo pré-definido. A utilização de impressoras locais não está autorizada por defeito		
		Análise aos ficheiros na rede e pastas partilhadas	A organização não tem implementado qualquer controlo de segurança para identificar e analisar ameaças na rede e em pastas partilhadas	A organização não tem implementado qualquer controlo de segurança para identificar e analisar ameaças na rede e pastas partilhadas. Perante um cenário de ameaça, são utilizadas soluções ad-hoc	A organização tem definidas e implementadas políticas e mecanismos que permitem monitorizar em tempo real atividade maliciosas na rede em concreto nas pastas partilhadas	A organização tem definidas e implementadas políticas e mecanismos que permitem monitorizar em tempo real atividades maliciosas na rede em concreto nas pastas partilhadas. Estes mecanismos são atualizados automaticamente com informação proveniente de fontes de Threat Intelligence e Threat Hunting		
								Insira valor nos controlos

Gestão de vulnerabilidades técnicas	**Normativo de suporte**	**Formalização de um processo para gestão de vulnerabilidades**	A organização não tem formalizado um processo para gestão de vulnerabilidades	A organização não tem formalizado um processo para gestão de vulnerabilidades. Contudo, existe documentação e procedimentos que servem de guia orientador e suportam as atividades associadas à gestão de vulnerabilidades	A organização tem formalizado um processo para gestão de vulnerabilidades documentado em políticas, normas, processos e procedimentos	A organização tem formalizado um processo para gestão de vulnerabilidades documentado em políticas, normas, processos e procedimentos. Este processo é alvo de monitorização regular para garantir a sua abrangência e adequação aos requisitos de segurança organizacionais		
		Operacionalização do processo	A organização não segue um processo formal para operacionalizar a gestão de vulnerabilidades. As vulnerabilidades são geridas caso a caso sem qualquer formalismo	A organização não segue um processo formal para operacionalizar a gestão de vulnerabilidades. Contudo, são seguidas orientações e procedimentos informais para operacionalizar a identificação, analisar/classificação, tratamento, revalidação, monitorização de vulnerabilidades	A organização têm formalizado e instituído um processo para operacionalizar a identificação, análise/classificação, tratamento revalidação, monitorização de vulnerabilidades	A organização têm formalizado e instituído um processo para operacionalizar a identificação, análise/classificação, tratamento revalidação, monitorização de vulnerabilidades. Este processo é alvo de monitorização regular para garantir a sua adequação e abrangência transversal a toda a organização, incluindo novos ativos que vão sendo desenvolvidos e integrados no seio da organização		
		Repositório centralizado de vulnerabilidades	A organização não possui um repositório centralizado para gestão de vulnerabilidades	A organização não possui um repositório centralizado para gestão de vulnerabilidades. Existem diversos repositórios não formais que armazenam diversos tipos de vulnerabilidades	A organização possui um repositório centralizado para gestão de vulnerabilidades, embora possam existir outros repositórios para vulnerabilidades específicas	A organização possui um repositório único e centralizado para gestão de vulnerabilidades		
	Identificação	**Processo de identificação**	A organização não tem formalizado um processo específico para identificação de vulnerabilidades	A organização não tem formalizado um processo específico para identificação de vulnerabilidades. Contudo, existem procedimentos que servem de guia orientador e suportam as atividades associadas à identificação de vulnerabilidades	A organização tem formalizado um processo específico para identificação de vulnerabilidades	A organização tem formalizado um processo específico para identificação de vulnerabilidades. Este processo é alvo de monitorização e avaliação regular para garantir a sua abrangência e adequação aos requisitos de segurança organizacionais		

		Tecnologias IOT	A organização não executa testes específicos para identificar vulnerabilidades em tecnologias IOT	A organização não executa formalmente testes para identificar vulnerabilidades em tecnologias IOT. Contudo, participa e consulta fóruns da especialidade e dos respetivos fabricantes para obter informação sobre vulnerabilidades. Com base na informação recolhida, são realizados testes ad-hoc para identificar vulnerabilidades	A organização executa de forma regular testes para identificar vulnerabilidades em tecnologias IOT	A organização executa de forma regular testes para identificar vulnerabilidades em tecnologias IOT. Regularmente a organização avalia a forma como as tarefas são executadas para assegurar a sua adequação e abrangência		
		Tecnologias *Cloud*	A organização não executa testes específicos para identificar vulnerabilidades em tecnologias cloud	A organização não executa formalmente testes específicos para identificar vulnerabilidades em tecnologias *cloud*. Contudo, são executados testes ad-hoc para identificação de vulnerabilidades semelhantes às que são realizadas nas restantes tecnologias	A organização tem definidos critérios e tarefas especificas para identificar vulnerabilidades em tecnologias *cloud*	A organização tem definidos critérios e tarefas especificas para identificar vulnerabilidades em tecnologias *cloud*. Anualmente são realizadas reuniões com os fornecedores dos serviços de *cloud* para avaliar a adequação nos processos implementados para identificar vulnerabilidades nestas tecnologias		
		Equipamentos de rede (routers, switches,	A organização não executa testes específicos sejam externos ou internos para identificar vulnerabilidades em tecnologias e ativos de rede	A organização não executa formalmente testes específicos, externos ou internos para identificar vulnerabilidades em tecnologias e ativos de rede. Contudo, são executados testes ad-hoc, embora sem uma regularidade ou âmbito definido	A organização executa de forma regular testes internos e externos para identificar vulnerabilidades em tecnologias e ativos de rede	A organização executa de forma regular testes internos e externos para identificar vulnerabilidades em tecnologias e ativos de rede. Regularmente a organização avalia a forma como os testes são executados para assegurar a sua adequação e abrangência		

		Equipamentos móveis (telemóveis, smartphones, tablets,,etc.)	A organização não executa testes específicos para identificar vulnerabilidades em tecnologias móveis	A organização não executa formalmente testes específicos para identificar vulnerabilidades em tecnologias e ativos móveis. Contudo, são executados testes ad-hoc para identificação, embora de carácter mais geral como seja em cenário de incidente de segurança, ou mediante conhecimento de uma(s) vulnerabilidade(s) crítica	A organização executa de forma regular testes para identificar vulnerabilidades em tecnologias e equipamentos móveis	A organização executa de forma regular testes para identificar vulnerabilidades em tecnologias e ativos móveis. Regularmente a organização avalia a forma como os testes são executados para assegurar a sua adequação e abrangência		
		Equipamentos sem fios (WiFi)	A organização não executa testes específicos para identificar vulnerabilidades em tecnologias sem fios	A organização não executa formalmente testes específicos para identificar vulnerabilidades em tecnologias e ativos sem fios. Contudo, são executados testes ad-hoc para identificação, embora de carácter mais geral como seja em cenário de incidente de segurança, ou mediante conhecimento de vulnerabilidade(s) crítica	A organização executa de forma regular testes para identificar vulnerabilidades em tecnologias e ativos sem fios	A organização executa de forma regular testes para identificar vulnerabilidades em tecnologias e ativos sem fios. Regularmente a organização avalia a forma como os testes são executados para assegurar a sua adequação e abrangência		
		Novas vulnerabilidades (0-day)	A organização não executa testes para identificar novas vulnerabilidades em qualquer dos seus ativos	A organização não executa formalmente e com uma regularidade definida testes para identificar novas vulnerabilidades em qualquer dos seus ativos. Pontualmente são executados testes com vista a identificar vulnerabilidades novas em ativos com maior criticidade e exposição	A organização tem implementado um processo contempla a realização de testes regulares com objetivo de identificar novas vulnerabilidades nos seus ativos	A organização tem implementado um processo que contempla a realização de testes regulares com objetivo de identificar novas vulnerabilidades nos seus ativos. Este processo é alvo de revisão periódica para avaliar a sua adequação e abrangência em função da criticidade de cada ativo		

		Equipas executantes	A organização não tem uma equipa interna ou externa para realização de testes com vista a identificar vulnerabilidades nos ativos	A organização não tem uma equipa interna ou externa para realização de testes com vista a identificar vulnerabilidades nos ativos. Pontualmente são solicitados testes de vulnerabilidades a parceiros	A organização dispõe de uma equipa para realizar testes para deteção de vulnerabilidades nos ativos	A organização possui uma equipa interna dedicada a realizar testes para identificar vulnerabilidades nos ativos. Existe ainda uma equipa externa contratada para realizar testes de específicos em determinados domínios e em ativos que requerem uma maior especificidade/complexidade. As equipas internas e externas interagem entre si para melhor articulação das tarefas		
		Desenvolvimento interno	A organização não tem definido um processo formal para realização de testes sobre vulnerabilidades nas aplicações desenvolvidas internamente	A organização não tem definido um processo formal para realização de testes sobre vulnerabilidades nas aplicações desenvolvidas internamente. Contudo, as soluções mais críticas são alvo de testes antes de serem colocadas em produção	A organização tem definido um processo formal para realização de testes a vulnerabilidades nas aplicações desenvolvidas internamente antes que sejam colocadas em produção	A organização tem definido um processo formal para realização de testes sobre vulnerabilidades nas aplicações desenvolvidas internamente antes que sejam colocadas em produção. O processo é revisto regularmente de forma a assegurar a sua adequação, abrangência e inclusão de novos métodos		

		Desenvolvimento externo	A organização não tem definido um processo formal para realização de testes a vulnerabilidades nas aplicações desenvolvidas por terceiros para uso na organização	A organização não tem definido um processo formal e regular para realização de testes a vulnerabilidades nas aplicações desenvolvidas por terceiros para uso na organização. Contudo, pontualmente são realizados testes embora só aos ativos de maior criticidade	A organização tem definido um processo formal para realização de testes sobre vulnerabilidades nas aplicações desenvolvidas por terceiros para uso na organização. Contudo, o âmbito dos testes está bem definido, previamente acordado e aceite pelo parceiro. A realização destes testes ocorrem obrigatoriamente antes da entrada em produção	A organização tem definido um processo formal para realização de testes sobre vulnerabilidades nas aplicações desenvolvidas por terceiros para uso na organização. Contudo, o âmbito dos testes está bem definido, previamente acordado e aceite pelo parceiro. A organização revê periodicamente este processo de forma a estar alinhado com a criticidade dos ativos e requisitos de segurança, sendo também definidas métricas para avaliar o processo. A realização destes testes ocorrem obrigatoriamente antes da entrada em produção		
		Análise aplicacional periódica	A organização não tem definido um processo formal para regularmente executar de testes sobre vulnerabilidades aplicacionais	A organização não tem definido um processo formal para regularmente executar de testes sobre vulnerabilidades aplicacionais. Os testes são realizados de forma ad-hoc e apenas em ativos classificados com maior criticidade	A organização tem definido um processo formal para regularmente executar de testes sobre vulnerabilidades aplicacionais em linha com o normativo existente para o efeito. Os testes realizados incluem análise estática e dinâmica de código	A organização tem definido um processo formal para regularmente executar de testes sobre vulnerabilidades aplicacionais em linha com o normativo existente para o efeito. Periodicamente a organização revê o processo de forma a assegurar a sua adequação, abrangência e eficácia, sendo também definidas métricas que para avaliar o processo. Os testes realizados incluem análise estática e dinâmica de código		

		Tecnologia para deteção de vulnerabilidades	A organização não utiliza soluções especificas para identificar vulnerabilidades	A organização não tem formalmente definidas soluções para identificar vulnerabilidades. Contudo, utiliza de forma ad-hoc soluções gratuitas (shareware, freeware) para deteção e análise	A organização tem formalmente definidas e implementadas soluções para identificar vulnerabilidades	A organização tem formalmente definidas e implementadas soluções para identificar vulnerabilidades. regularmente são avaliadas todas as soluções utilizadas para identificar soluções para garantir que cumprem com os requisitos de segurança, abrangentes e adequadas face aos ativos organizacionais		
	Classificação	**Escala de classificação**	A organização não tem adotada uma *framework* para classificação de vulnerabilidades	A organização não tem adotada uma *framework* para classificação de vulnerabilidades. Para as vulnerabilidades identificadas internamente é atribuída uma classificação com base na criticidade do ativo	A organização utiliza uma *framework* para classificação de vulnerabilidades	A organização utiliza uma *framework* para classificação de vulnerabilidades. Periodicamente é feita uma revisão assim como uma comparação com outras *frameworks* de forma a assegurar que são utilizados os mais corretos critérios. Sempre que uma framework é atualizada a organização reflete isso nos seus processos internos		
		Reclassificação de vulnerabilidades	A organização não tem formalizado um processo para rever e reclassificar vulnerabilidades	A organização não tem formalizado um processo para rever e reclassificar vulnerabilidades . Contudo, informalmente é feita uma análise às vulnerabilidades de maior criticidade que pode resultar numa reclassificação	A organização tem formalizado um processo para rever e reclassificar vulnerabilidades mediante a não materialização e/ou aplicabilidade ao contexto organizacional	A organização tem formalizado um processo para rever e reclassificar vulnerabilidades mediante a não materialização e/ou aplicabilidade ao contexto organizacional podendo envolver áreas internas e externas à organização mediante o ativo em causa. O processo é avaliado regularmente sendo analisados os critérios de reclassificação		

	Mitigação e fecho	**Identificação do plano de mitigação**	A organização tem instituído um processo para apoiar na definição do plano de mitigação adequado a cada vulnerabilidade	A organização não tem instituído um processo para apoiar na definição do plano de mitigação adequado a cada vulnerabilidade. Contudo, para as vulnerabilidades de maior criticidade é definida de forma ad-hoc uma solução de mitigação	A organização tem instituído um processo para apoiar na definição do plano de mitigação adequado a cada vulnerabilidade. A solução é discutida com a área de segurança em linha com o normativo interno no que respeita ao prazo definido para cada criticidade	A organização tem instituído um processo a seguir para apoiar na definição do plano de mitigação adequado a cada vulnerabilidade. A solução é discutida com a área de segurança em linha com o normativo interno no que respeita ao prazo definido para cada criticidade. Este processo é alvo de monitorização e avaliação regular para garantir a sua adequação, abrangência e cumprimento com o normativo em vigor e requisitos de segurança instituídos		
		Processo de mitigação	A organização não tem formalizado um processo específico para mitigação de vulnerabilidades	A organização não tem formalizado um processo específico para mitigação de vulnerabilidades. Contudo, existem procedimentos que servem de guia orientador e suportam as atividades associadas à mitigação de vulnerabilidades	A organização tem formalizado um processo específico para mitigação de vulnerabilidades. Somente após a confirmação da resolução, é executado o fecho da vulnerabilidade	A organização tem formalizado um processo específico para mitigação de vulnerabilidades. Este processo é alvo de monitorização e avaliação regular para garantir a sua abrangência e adequação aos requisitos de segurança organizacionais. Somente após se confirmar a resolução, a vulnerabilidade é fechada		
		Responsabilidade pela mitigação	A organização não tem definido um processo que apoie na identificação e atribuição de um responsável pelo tratamento de cada vulnerabilidade identificada	A organização não tem formalmente definido um processo que suporte a identificação e atribuição de um responsável pelo tratamento de cada vulnerabilidade identificada. Contudo, é feita uma atribuição ad-hoc em função da área onde o ativo se localiza	A organização tem definido um processo para apoiar na identificação e atribuição de um responsável pelo tratamento de cada vulnerabilidade identificada	A organização tem definido um processo para identificação e atribuir de um responsável (interno ou externo) pelo tratamento de cada vulnerabilidade identificada. Periodicamente o processo é revisto e atualizado		

		Objetivos e métricas de mitigação	A organização não tem definidos objetivos nem métricas para mitigação de vulnerabilidades	A organização não tem formalmente definidos objetivos nem métricas para mitigação de vulnerabilidades. Contudo, para as de maior criticidade é dado um maior foco e urgência na sua mitigação	A organização tem definidos objetivos e métricas mensais para mitigação de vulnerabilidades	A organização tem definidos objetivos e métricas mensais para mitigação de vulnerabilidades. Estas métricas são formalizadas transversalmente por cada área que tem envolvimento na mitigação de vulnerabilidades. Os contratos com parceiros preveem SLAs para assegurar que os prazos de tratamento mapeiam as métricas organizacionais. Sempre que existe atualização nos tempos de mitigação, estes são partilhados e discutidos com os diversos parceiros de forma a existir concordância com o seu cumprimento		
	Monitorização	**Processo**	A organização não tem definido um processo ou procedimento para reavaliação de vulnerabilidades após a sua mitigação e assim garantir que podem ser fechadas	A organização não tem definido um processo ou procedimento para reavaliação de vulnerabilidades após a sua mitigação e assim garantir que podem ser fechadas. A revalidação é executada de forma ad-hoc e sem seguir um processo formal	A organização tem definido um processo ou procedimento para reavaliação de vulnerabilidades após a sua mitigação e assim garantir que podem ser fechadas. Neste processo são estipulados as forma de revalidação a utilizar, bem como os prazos para ocorrerem	A organização tem definido um processo ou procedimento para reavaliação de vulnerabilidades após a sua mitigação e assim garantir que podem ser fechadas. Estão definidos testes específicos a realizar, tais como testes de regressão. Caso o tratamento não tenha sido o mais eficaz, o mesmo é avaliado num fórum específico (CAB). Regularmente o processo é analisado, sendo também definidas métricas que permitem aferir a eficácia dos planos de tratamento		

		Revalidação automatizada de vulnerabilidades	A organização não utiliza uma solução que automatiza a revalidação de vulnerabilidades	A organização não utiliza uma solução que automatiza a revalidação de vulnerabilidades. Contudo, pontualmente são realizadas revalidações com recurso a ferramentas gratuitas apenas para as vulnerabilidades de maior criticidade	A organização tem operacionalizada uma solução que automatizam a revalidação de vulnerabilidade. Somente após a confirmação, é executado o fecho da vulnerabilidade	A organização tem operacionalizadas diversas soluções que automatizam a revalidação de vulnerabilidades, mediante a tipologia do ativo onde a mesma foi identificada. O processo é totalmente automatizado, através de fluxo que são criados automaticamente quando a vulnerabilidade é registada. Somente após a confirmação, é executado o fecho da vulnerabilidade		
		Exceções	A organização não tem instituído um processo formal para monitorização de vulnerabilidades que não foram alvo de mitigação	A organização não tem instituído um processo formal para monitorização de vulnerabilidades que não foram alvo de mitigação, apenas as vulnerabilidades de maior criticidade são alvo de monitorização	A organização tem instituído um processo formal para monitorização de vulnerabilidades que não foram alvo de mitigação por assim se ter decidido	A organização tem instituído um processo formal para monitorização de vulnerabilidades que não foram alvo de mitigação por assim se ter decidido. Este processo é revisto periodicamente e avaliada a sua adequação e abrangência em linha com a gestão de risco nos sistemas de informação		
								Insira valor nos controlos
Resposta a incidentes de segurança	**Governação**	**Política, norma e processo**	A organização não tem definida uma política, norma ou processo para resposta a incidentes de segurança	A organização não tem definida uma política, norma ou processo para resposta a incidentes de segurança. Informalmente são seguidos procedimentos e guias para apoiar na resposta a incidentes de segurança	A organização tem definida uma política, norma e processo para formalizar a resposta a incidentes de segurança	A organização tem definida uma política, norma e processo para formalizar a resposta a incidentes de segurança. Periodicamente é feita uma revisão ao normativo de forma a manter a sua adequação ao contexto organizacional e às novas tipologias de incidentes		

	Equipa	**Equipa dedicada para resposta a incidentes**	A organização não tem constituída uma equipa para responder a incidentes de segurança	A organização não tem constituída uma equipa para responder a incidentes de segurança. A resposta é dada de forma individual e ad-hoc	A organização dispõe de uma equipa dedicada (CSIRT) para dar resposta a incidentes de segurança	A organização dispõe uma equipa dedicada (CSIRT) para dar resposta a incidentes de segurança elementos com competências variadas e capazes de responder às mais diversas tipologias de incidentes de segurança.		
		Análise forense	A organização não tem constituída uma equipa com capacidade de realizar uma análise forense	A organização não tem constituída uma equipa com capacidade de realizar uma análise forense. Na eventualidade de ser necessário, é contratado um serviço externo específico para a situação em causa	A organização não tem constituída uma equipa com capacidade de realizar uma análise forense. Contudo, está contratado um serviço externo que é invocado quando necessário	A organização tem constituída uma equipa com capacidade de realizar uma análise forense		
		Funções e responsabilidades	A organização não tem formalizada nem materializada a definição de funções e responsabilidades para responder a incidentes de segurança	A organização não tem formalizada nem materializada a definição de funções e responsabilidades para responder a incidentes de segurança. A equipa é de pequena dimensão, informal e sem segregação de funções entre os elementos da equipa	A organização tem formalizada e materializada a definição de funções e responsabilidades para responder a incidentes de segurança	A organização tem formalizada e materializada a definição de funções e responsabilidades para responder a incidentes de segurança. A equipa está estruturada de forma redundante para assegurar a disponibilidade permanente de elementos nas diferentes tipologias de incidentes		
		Formação da equipa	O conhecimento da equipa é limitado para responder a incidentes de segurança	A equipa detém os conhecimentos mínimos para responder a incidentes de segurança	A equipa de resposta a incidentes possui conhecimentos e formação para execução das suas atividades especificas, possuindo um conhecimento generalizado em todos os domínios de segurança	A equipa de resposta a incidentes possui conhecimentos e formação para execução das suas atividades especificas, possuindo conhecimento generalizado em todos os domínios de segurança. Cada elemento da equipa é obrigado a definir um plano de formação anual para atualizar e reciclar os seus conhecimentos		

		Simulacros e exercícios	Não são realizados simulacros ou outros exercícios que permitam à equipa adquirir e testar conhecimentos e práticas a seguir na resposta a incidentes de cibersegurança	Pontualmente são realizados simulacros ou outros exercícios que permitam à equipa adquirir e consolidar conhecimentos e práticas na resposta a incidentes de cibersegurança	Anualmente a organização realiza um simulacro anualmente envolvendo toda a equipa de resposta a incidentes de cibersegurança	Anualmente a organização realiza um simulacro e diversos exercícios(table top cybersecurity exercises) envolvendo toda a equipa de resposta a incidentes de cibersegurança. Estes exercícios envolvem também equipas externas que tenham sido contratadas para apoiar a organização na sua missão de responder eficientemente. Os exercícios e simulacros são revisto de forma a contemplar os diversos e mais recentemente tipologias de ciberataques		
	Operação e execução	**Playbooks, workbooks e planos de resposta a incidentes**	A organização não tem definidos procedimentos e outros documentos que apoiam na resposta a incidentes de cibersegurança	A organização não tem definidos procedimentos e outros documentos que apoiam na resposta a incidentes de cibersegurança, embora de forma informal sejam seguidos procedimentos definidos e atualizados com base na experiência da equipa	A organização tem definidos procedimentos e outros documentos como sejam *playbooks, workbooks,,etc...,* que apoiam na resposta a incidentes de cibersegurança	A organização tem definidos procedimentos e outros documentos como sejam *playbooks, workbooks,,etc...,* que apoiam na resposta a incidentes de cibersegurança. Regularmente estes procedimentos são revistos e atualizados para abranger todos os tipos de incidentes		
		Critérios para identificação de incidentes	A organização não tem instituído um processo com critérios definidos que permitam identificar o que são incidentes de cibersegurança. A identificação é feita ad-hoc com base com conhecimento individual	A organização não tem instituído um processo com critérios definidos que permitam identificar o que são incidentes de cibersegurança. A equipa de segurança faz a identificação com base na partilha de experiências em situações semelhantes	A organização tem instituído um processo com critérios definidos que permitam identificar o que são incidentes de cibersegurança, permitindo fácil e rapidamente distinguir de outra tipologia de incidentes	A organização tem instituído um processo com critérios definidos que permitam identificar o que são incidentes de segurança, permitindo fácil e rapidamente distinguir de outra tipologia de incidentes. Os critérios são revistos regularmente e atualizados para abranger novas tipologias de incidentes que surgem de forma constante		

		Classificação de incidentes	A organização não tem definido critérios para atribuição de criticidade a incidentes de cibersegurança. A atribuição é feita caso a caso e baseado na experiência individual	A organização não tem definido um critério para atribuição do nível de criticidade a incidentes de cibersegurança, embora sejam seguidas algumas boas práticas nessa classificação com base na partilha de conhecimento da equipa e no historial de incidentes de características semelhantes. Por norma a criticidade do incidente está mapeada com a criticidade e exposição do ativo ou dos ativos associados ao incidente	A organização têm definidos critérios para atribuição de criticidade aos incidentes de cibersegurança. Este critério está alinhado com a criticidade do ativo e com o impacto financeiro e reputacional que o mesmo poderá ter para a organização	A organização têm definidos critério claros para atribuição de criticidade aos incidentes de cibersegurança. Este critério está alinhado com a criticidade do ativo e com o impacto financeiro e reputacional. O processo de atribuição de criticidade calcula automaticamente a criticidade em função dos casos de uso pré-definidos. Regularmente a organização revê a criticidade de cada ativo, em função dos inputs provenientes da avaliação de risco executada para cada ativo, atualizando com base nesta informação os critério	
		Reclassificação de incidentes	A organização não tem definido critérios para reclassificar a criticidade de um incidente de cibersegurança. A classificação atribuída inicialmente é mantida até que o incidente seja fechado	A organização não tem definido critérios para reclassificar a criticidade de um incidente de cibersegurança, embora existam procedimentos informais que a equipa de resposta segue para o fazer, mas esta reclassificação ocorre pontualmente e de forma ad-hoc	A organização tem definido critérios para reclassificar a criticidade de um incidente de cibersegurança. Na fase de análise ao incidente, está prevista a sua reclassificação caso seja aplicável	A organização tem definido critérios para reclassificar a criticidade de um incidente de cibersegurança. Na fase de análise ao incidente, está prevista a sua reclassificação caso seja aplicável. Regularmente os critérios são revistos para que estejam alinhados com a criticidade dos ativos e o impacto para a organização (financeiro, reputacional,,etc.)	

		Interação com parceiros/fornecedores	A organização não tem definido um procedimento para interagir com os seus parceiros relativamente a incidentes de cibersegurança	A organização não tem definido um procedimento para interagir com os seus parceiros relativamente a incidentes de cibersegurança. Contudo, perante um cenário de incidente é estabelecido um canal informar para comunicação entre as duas partes	A organização tem definido um procedimento para interagir com todos os seus parceiros para reporte de incidentes de cibersegurança. Este procedimento define o canal de comunicação, quem reporta o incidente e em que circunstâncias deve ser reportado	A organização tem definido um procedimento para interagir com todos os seus parceiros para reporte de incidentes de cibersegurança. Este procedimento define o canal de comunicação, quem reporta o incidente e em que circunstâncias deve ser reportado. Este procedimento é visitado e revisto regularmente e comunicado a todos os parceiros		
	Tecnologia de suporte	**Deteção e resposta automatizada**	A organização não dispõe de tecnologia para automatizar a resposta a incidentes de cibersegurança. O processo é totalmente manual e reativo	A organização tem implementada alguma tecnologia que operacionaliza uma resposta automatizada em algumas tipologias de incidentes de cibersegurança, embora em formato 9x5	A organização tem implementada tecnologia (SOAR) que automatiza as fases do processo de resposta a incidentes de cibersegurança, embora existam ainda alguns procedimentos que não estejam totalmente integrados num formato 24x7x365	A organização tem implementada tecnologia (SOAR) que automatiza todas as fases do processo de resposta a incidentes de cibersegurança com cobertura 24x7x365		
	Reporte	**Reporte a reguladores e supervisores**	A organização não tem definido um procedimento para reporte de incidentes de cibersegurança a entidades legais, supervisores ou setoriais. Todas as solicitações são tratadas de forma ad-hoc e sem um critério definido	A organização não tem definido um procedimento para reporte de incidentes de cibersegurança a entidades legais, supervisores ou setoriais. A comunicação é feita de forma ad-hoc, mas segue um padrão pré-definido que vem sendo atualizado ao longo do tempo	A organização tem definido critérios e procedimentos para reportar incidentes de cibersegurança a entidades legais, supervisão ou setoriais. A comunicação é feita por meio de um canal pré-definido através do responsável da segurança	A organização tem definido critérios e procedimentos para reportar incidentes de cibersegurança a entidades legais, supervisão ou setoriais. A comunicação é feita por meio de um canal pré-definido através do responsável da segurança. Os critérios assim como os procedimentos são revistos, atualizados e comunicados regularmente		

		Recolha e envio de evidências	A organização não tem especificado um procedimento para recolha, análise e envio de evidências associadas a um pedido de entidades legais, supervisão ou setoriais. Quando existem pedidos de evidências, a organização responde de forma ad-hoc de acordo com as instruções da entidade requisitante	A organização não tem especificado um procedimento para recolha, análise e envio de evidências associadas a um pedido de entidades legais, supervisão ou setoriais. Cada pedido é processado de forma ad-hoc e enviado pelo colaborador que procedeu ao seu tratamento	A organização tem especificado um procedimento para recolha, análise e envio de evidências associadas a um pedido de entidades legais, supervisão ou setoriais. O pedido é processado de acordo com o procedimento definido, sendo avaliado e validado pelo responsável pela segurança que trata do seu envio pelo canal e da forma definida	A organização tem especificado um procedimento para recolha, análise e envio de evidências associadas a um pedido de entidades legais, supervisão ou setoriais. O pedido é processado de acordo com o procedimento definido e por uma equipa especifica a responder a esta tipologia de pedidos, sendo avaliado e validado pelo responsável pela segurança, que trata do seu envio pelo canal e da forma definida. Este procedimento é revisto e atualizado regularmente e partilhado internamente		
								Insira valor nos controlos
Arquitetura de segurança	**Classificação de ativos relativamente à segurança**	**Definições de segurança**	A organização não tem um processo para classificação de ativos onde se inclua a vertente de cibersegurança nas suas características	A organização não tem um processo para classificação de ativos onde se inclua a vertente de cibersegurança nas suas características, apenas classifica-os quanto à criticidade e nível de exposição ao risco	Todos os ativos organizacionais são classificados tendo em conta a vertente de cibersegurança e risco	Todos os ativos organizacionais são classificados tendo em conta a vertente de cibersegurança, risco e operação. Regularmente a classificação é revista e atualizada para refletir o valor do risco que é aferido anualmente em cada ativo, a probabilidade e o impacto resultante de um potencial incidente de segurança		

	Detalhes sobre os ativos	**Responsável pelo ativo**	A organização não atribui um responsável aplicacional a todos os ativos	A organização não atribui formalmente um responsável aplicacional aos seus ativos, apenas aqueles que apresentam maior criticidade, fazendo-o de forma ad-hoc e sem um critério de regularidade	Todos os ativos organizacionais tem associado um responsável aplicacional que em primeira instância é quem deve assegurar que o mesmo cumpre com os requisitos de cibersegurança definidos	Todos os ativos organizacionais tem associado um responsável aplicacional que em primeira instância é quem deve assegurar que o mesmo cumpre com os requisitos de cibersegurança definidos. Regularmente a organização faz uma revisão de forma a assegurar que exista um mapeamento correto entre o responsável e o ativo		
		Renovação de ativos	A organização não tem instituídas políticas para renovação de ativos	A organização não tem instituídas políticas para renovação de ativos, embora existam preocupações e controlos compensatórios sobre os ativos que se encontram obsoletos	A organização tem definidas políticas para renovação de ativos	A organização tem definidas políticas para renovação de ativos. Os critérios são revistos com regularidade para assegurar que qualquer ativo é renovado atempadamente, tendo por base a dificuldade, tempo necessário e impacto causado direta e indiretamente em outros ativos		

		Isolamento de ativos obsoletos	A organização não tem instituídos processos para definir e implementar uma arquitetura que permita isolar ou implementar controlos compensatórios para ativos que se encontrem obsoletos ou vulneráveis	A organização não tem instituídos processos para definir e implementar uma arquitetura que permita isolar ou implementar controlos compensatórios para ativos que se encontrem obsoletos ou vulneráveis. Contudo, é feita uma análise de risco aos ativos nesta situação e implementados mecanismos ad-hoc que visem aumentar a segurança e robustez dos mesmos	A organização não tem instituídos processos para definir e implementar uma arquitetura que permita isolar ou implementar controlos compensatórios para ativos que se encontrem obsoletos ou vulneráveis, cuja substituição ou mitigação não seja possível sem a sua total substituição. É definida uma arquitectura especifica e temporária para estes ativos	A organização não tem instituídos processos para definir e implementar uma arquitetura que permita isolar ou implementar controlos compensatórios para ativos que se encontrem obsoletos ou vulneráveis, cuja substituição ou mitigação não seja possível sem a sua substituição. É definida uma arquitectura especifica e temporária para estes ativos. Periodicamente a organização revê e atualiza as arquiteturas definidas para estes casos e força a substituição dos mesmos e assim terminar com estas soluções temporárias	
		Soluções e ativos de terceiros	A organização não define, verifica ou valida arquiteturas de segurança sobre soluções e ativos de parceiros	A organização não define, verifica ou valida arquiteturas de segurança sobre soluções e ativos de parceiros. Contudo, guarda informação sobre estas arquiteturas. Este controlo não se aplica a soluções em modelo SaaS ou PaaS	Antes de ser contratada uma solução externa, a arquitetura é analisada pela organização de forma a cumprir com os requisitos definidos. Este controlo não se aplica a soluções em modelo SaaS ou PaaS	Antes de ser contratada uma solução externa, a arquitetura é analisada pela organização de forma a cumprir com os requisitos definidos. Periodicamente a organização solicita aos parceiros informação atualizada sobre estas arquiteturas. Este controlo não se aplica a soluções em modelo SaaS ou PaaS	

		Políticas, normas e procedimentos	A organização não tem instituído um quadro normativo orientado a suportar a definição e implementação de arquiteturas de referência em diversas vertentes, incluindo a de cibersegurança	A organização não tem definido um quadro normativo orientado a suportar a definição e implementação de arquiteturas de referência em diversas vertentes, incluindo a de cibersegurança. Contudo, durante a fase de implementação de umas novas arquiteturas são incluídos alguns controlos	A organização tem definido um quadro normativo orientado a suportar a definição e implementação de arquiteturas de referência em diversas vertentes, incluindo a de cibersegurança	A organização tem definido um quadro normativo orientado para suportar a definição e implementação de arquiteturas de referência em diversas vertentes, incluindo a de cibersegurança. O quadro normativo é revisto e atualizado regularmente e publicado para toda a organização e parceiros		
	Arquiteturas de referência	**Requisitos de segurança**	A organização não tem definida uma arquitetura de referência que contemple requisitos de cibersegurança	A organização não tem definida uma arquitetura de referência que contemple requisitos de cibersegurança, embora sejam definidos de forma ad-hoc determinados requisitos sobretudo quando envolve ativos de maior criticidade	A organização tem definida uma arquitetura de referência que contempla requisitos de cibersegurança	A organização tem definida uma arquitetura de referência que contempla requisitos de cibersegurança. periodicamente a organização revê e atualiza a arquitetura de referência para contemplar os mais recentes requisitos de segurança face a novos ciberataques e ameaças		
		Arquiteturas diversificadas (cloud, onprem,,etc.)	A organização não tem definidas diferentes arquiteturas, tendo em conta o ambiente, contexto e localização das mesmas	A organização não tem definidas diferentes arquiteturas, tendo em conta o ambiente, contexto e localização das mesmas. Contudo, no que respeita a requisitos de cibersegurança são definidos alguns de forma informal	A organização tem definidas arquiteturas de referência diversificadas, mediante o contexto onde são aplicadas	A organização tem definidas arquiteturas de referência diversificadas, mediante o contexto onde são aplicadas. Regularmente são revistas, atualizadas e difundidas por todos os parceiros da organização de forma a garantir a conformidade com o requisito		

		Acompanhamento de segurança	A organização não tem definido requisitos que obrigue ao acompanhamento e supervisão de um arquiteto de cibersegurança durante o ciclo de implementação de uma arquitetura aplicacional	A organização não tem definido requisitos que obrigue ao acompanhamento e supervisão de um arquiteto de cibersegurança durante todo o ciclo de implementação de uma arquitetura aplicacional, embora participe pontualmente e mediante solicitação da equipa aplicacional	A organização tem definido requisitos que obrigue ao acompanhamento de um arquiteto de cibersegurança durante o ciclo de implementação de uma arquitetura aplicacional. A equipa de cibersegurança tem definida uma lista de requisitos e verificações para as diferentes arquiteturas	A organização tem definido requisitos que obrigue ao acompanhamento e supervisão de um arquiteto de cibersegurança durante o ciclo de implementação de uma arquitetura aplicacional. A equipa de cibersegurança tem definida uma lista de requisitos e verificações de segurança, seguida pelos arquitetos de segurança e atualizada regularmente para contemplar novas ameaças e arquiteturas		
		Ambientes produtivos e não produtivos	A organização tem definido um único ambiente, sobre o qual estão localizados todos os ativos e aplicações	A organização tem definido um ambiente produtivo e um ambiente não produtivo onde são desenvolvidas e testadas algumas aplicações antes de entrarem em produção	A organização tem definido e implementado quatro ambientes (desenvolvimento, pré-Produção, produção e d*isaster recover),* embora nem todas as aplicações estejam configuradas em todos eles	A organização tem definido e implementado quatro a ambientes (desenvolvimento, pré-Produção, produção e d*isaster recover).* Todas as soluções aplicacionais tem obrigatoriamente um ambiente de desenvolvimento, pré-produção e produção, sendo o ambiente de d*isaster recover* configurado apenas para as soluções com RTO e RPO mais críticos. As exceções são registadas e revistas regularmente		
		Segregação entre ambientes	Não existe segregação lógica e física entre ambientes	Não existe segregação lógica e física entre ambientes em termos de arquitetura, embora determinados componentes estejam segregados entre o que é produtivo e não produtivo	A arquitetura define requisitos de segregação entre cada um dos ambientes, embora possam existir componentes comuns, sobretudo ao nível físico	A arquitetura define requisitos de segregação entre cada um dos ambientes. Exceções estão previstas e são devidamente avaliadas. Periodicamente é feita de revisão para assegurar uma revalidação do risco e necessidade em manter as exceções		

	Alta disponibilidade e resiliência	**Redundância**	A organização não têm definidos requisitos ou critérios para avaliar a necessidade de implementar redundância aplicacional	A organização não têm definidos requisitos ou critérios para avaliar a necessidade de implementar redundância aplicacional. Contudo, existe consciencialização sobre a criticidade de algumas aplicações, levando à implementação de controlos compensatórios para assegurar redundância dessas aplicações	A organização têm definidos requisitos ou critérios para avaliar a necessidade de implementar redundância aplicacional com base no resultado dos BIA (Business Impact Analysis) realizados às aplicações	A organização têm definidos requisitos ou critérios para avaliar a necessidade de implementar redundância aplicacional com base no resultado dos BIA (Business Impact Analysis) realizados às aplicações. Regularmente a organização procede à atualização dos BIA de forma a assegurar que refletem a verdadeira criticidade da solução no decorrer do seu ciclo de vida	

							Insira valor nos controlos
Segurança do software	**Conformidade**	**Políticas, normas, processos e procedimentos**	Não existe normativo associado à segurança do software, em particular sobre aquele que é desenvolvimento internamente	Não existe normativo associado à segurança do software, em particular sobre aquele que é desenvolvimento internamente. Contudo, são seguidas boas práticas, como seja a não utilização de protocolos inseguros, cifras fracas ou bibliotecas obsoletas	Existe normativo associado à segurança do software, seja desenvolvido internamente ou adquirido	Existe normativo associado à segurança do software, seja desenvolvido internamente ou adquirido. Este normativo é revisto e atualizado regularmente e partilhado com todos os parceiros e fornecedores de forma a cumprirem com os requisitos definidos	
		Prevenção contra exfiltração de dados	Não está definido um processo com controlos para prevenir a exfiltração de dados	Não está definido um processo com controlos para prevenir a exfiltração de dados. O controlo é feito sob uma perspetiva teórica e com alguns controlos implementados ad-hoc	Encontra-se definido um processo com controlos para prevenir a exfiltração de dados	Encontra-se definido um processo com controlos para prevenir a exfiltração de dados, incluindo o acesso a portais que permitam identificar e corrigir bugs no código desenvolvido	

		Aquisição de software de terceiros	Não é seguido nenhum processo para análise e avaliação prévia à aquisição de software a terceiros	Não existe um processo formal para avaliação a softwares de terceiros. Esta avaliação é feita ad-hoc e essencialmente teórica e baseada em informação pública sobre o software em causa	Existe um processo formal para avaliação a softwares de terceiro assim como o próprio fornecedor. Esta avaliação é feita através de diversos questionários que avaliam em diferentes vertentes a aplicação com particular foco na cibersegurança. Estes questionários são atualizados de forma regular para refletirem novos requisitos em matéria de cibersegurança.	Existe um processo formal para avaliação a softwares de terceiro assim como o próprio fornecedor. Esta avaliação é feita através de diversos questionários que avaliam em diferentes vertentes a aplicação com particular foco na cibersegurança. Estes questionários são atualizados de forma regular para refletirem novos requisitos em matéria de cibersegurança. Em certos casos podem ser realizados testes de segurança à aplicação em causa mediante um acordo formal entre as partes. Geralmente é realizado um piloto (prova de conceito) interna que permite testar as funcionalidades da aplicação antes de se avançar com a aquisição	
		Repositório centralizado para código	Não existe um repositório centralizado onde é armazenado todo o código aplicacional desenvolvido internamente	Não existe um repositório centralizado onde é armazenado todo o código aplicacional desenvolvido internamente. Contudo, estão implementados controlos compensatórios que visam assegurar que o código desenvolvido não sai da organização	Existe um repositório centralizado onde é armazenado todo o código aplicacional desenvolvido internamente. Este repositório é abrangido pela política de gestão de acessos, ficando o registo de cada acesso realizado	Existe um repositório centralizado onde é armazenado todo o código aplicacional desenvolvido internamente e sobre o qual ocorrem testes regulares. Este repositório é abrangido pela política de gestão de acessos, ficando o registo de cada acesso realizado. Adicionalmente, todos os desenvolvimentos são realizados nos ativos internos de forma a evitar qualquer exfiltração	

		Metodologia de desenvolvimento	Não é seguida uma metodologia de desenvolvimento de software	Não é seguida uma metodologia formal para desenvolvimento de software. Contudo, são seguidos critérios e práticas que cobrem todo o ciclo de vida de um software	É seguida uma metodologia para desenvolvimento que contempla todas as fases do SDLC	É seguida uma metodologia para desenvolvimento que contempla todas as fases do SDLC. A metodologia é revista regularmente para assegurar que a área de cibersegurança tem participação ativa neste processo através da definição de requisitos e realização de testes de segurança		
		Desenvolvimento interno e externo	O desenvolvimento aplicacional pode ser realizado por equipas internas ou externas à organização sem que haja um processo definido que regula esse desenvolvimento	O desenvolvimento aplicacional pode ser realizado por equipas internas ou externas à organização sem que haja um processo formal definido que regula esse desenvolvimento, embora estejam definidos alguns procedimentos e regras sobre a forma como a equipas externas devem realizar o seu trabalho	O desenvolvimento aplicacional pode ser realizado por equipas internas ou externas à organização com base num processo definido que estipula regras e procedimentos	O desenvolvimento aplicacional pode ser realizado por equipas internas ou externas à organização com base num processo definido que estipula regras e procedimentos. Este processo é revisto e atualizado regularmente e partilhado com todas as partes interessadas		
		Segurança e privacidade por omissão e por desenho	Não existem cláusulas ou requisitos que obriguem à implementação de mecanismos de segurança e privacidade por omissão e desenho	Não existem cláusulas ou requisitos que obriguem à implementação de mecanismos de segurança e privacidade por omissão e desenho, embora sejam adotados de forma ad-hoc procedimentos que contemplam segurança e privacidade por omissão e defeito nas soluções de maior criticidade	Existem cláusulas ou requisitos que obrigam à implementação de mecanismos de segurança e privacidade por omissão e desenho	Existem cláusulas ou requisitos que obrigam à implementação de mecanismos de segurança e privacidade por omissão e desenho. As cláusulas e requisitos são revistos e atualizados regularmente para assegurar a sua adequação e abrangência, sendo partilhados com todas as partes interessadas		

	Gestão de alterações	**Entradas e saídas de produção**	Não está definido um processo para gerir as alterações preconizadas nas aplicações	Não está definido um processo para gerir as alterações preconizadas nas aplicações. Contudo, para as alterações em ambiente de produção é seguido um fluxo de aprovações que avaliam o risco da alteração em causa	Está definido um processo para gestão de alterações, suportado por um pedido formal em ITSM	Está definido um processo um processo para gestão de alterações, tendo obrigatoriamente de passar por um pedido formal em ITSM que é levado a um CAB semanal com todas as áreas relevantes para rever e aprovar a sua implementação	
	Testes de segurança Aplicacionais	**Análise estática e dinâmica ao código**	Não é formalmente realizada análise estática e/ou dinâmica ao código tanto em fase de desenvolvimento como produção	Não é formalmente realizada análise estática e/ou dinâmica ao código quer em fase de desenvolvimento nem em produção. Apenas são realizadas análises e verificações de forma ad-hoc	Na metodologia SDLC seguida estão definidos requisitos para realizar análise estática e/ou dinâmica ao código tanto em fase de desenvolvimento como produção, embora nem todas as aplicações sejam alvo desta análise	Na metodologia SDLC seguida estão definidos requisitos para realizar análise estática e/ou dinâmica ao código tanto em fase de desenvolvimento como produção a todas as soluções aplicacionais desenvolvidas internamente. Exceções estão previstas mediante justificação e tendo o risco sido aceite	
		Testes de penetração (pentesting)	Não são realizados testes de penetração às aplicações durante a fase de desenvolvimento ou pós entrados em produção	Não são formalmente realizados testes de penetração às aplicações durante a fase de desenvolvimento. Contudo, os ativos e soluções de maior criticidade sejam alvo de testes depois da entrada em produção e de forma regular	Na metodologia SDLC seguida estão definidos requisitos para a realização de testes de penetração quer em fase de desenvolvimento quer depois da entrada produção, embora nem todas as aplicações sejam alvo de testes, somente as aplicações com maior criticidade e exposição. Exceções estão previstas mediante justificação e tendo o risco sido aceite	Na metodologia SDLC seguida estão definidos requisitos para a realização de testes de penetração quer em fase de desenvolvimento quer depois da entrada em produção a todas as soluções aplicacionais. Exceções estão previstas mediante justificação e tendo o risco sido aceite	

		Testes a API	Não são realizados testes às API invocadas pelas aplicações durante a fase de desenvolvimento ou depois da entrada em produção	Não são realizados testes às API invocadas pelas aplicações durante a fase de desenvolvimento ou depois da entrada em produção , embora sejam realizadas avaliações ad-hoc a algumas API	Na metodologia SDLC seguida estão definidos requisitos para a realização de testes às API quer em fase de desenvolvimento quer depois da entrada em produção, embora nem todas as API sejam alvo de testes, somente as aquelas que apresentem uma maior criticidade e exposição	Na metodologia SDLC seguida estão definidos requisitos para a realização de testes a todas as API desenvolvidas ou alteradas para utilização nas aplicações quer em fase de desenvolvimento quer depois da entrada em produção a todas as soluções aplicacionais. Exceções estão previstas mediante justificação e tendo o risco sido aceite		
		Testes em modelo black box e white box	Não são realizados testes em modo black e white box às aplicações desenvolvidas pela internamente	Não são realizados testes em modo black e white box às aplicações desenvolvidas internamente. Contudo, para as soluções de maior risco e exposição são realizados testes pontuais	Estão definidos requisitos para a realização de testes em modo black e white box às soluções desenvolvidas internamente embora nem todas as soluções sejam alvo desta tipologia de testes, somente aquelas que apresentem uma maior criticidade e exposição. Estão testes em aplicações de parceiros sempre que a organização o pretenda fazer, embora requeira obrigatoriamente uma autorização prévia e formal	Na metodologia SDLC seguida estão definidos requisitos para a realização de testes em modo black e white box a todas as aplicações desenvolvidas ou que tenham sido alvo de alterações, embora nem todas as aplicações sejam alvo desta tipologia de testes. Estão testes em aplicações de parceiros sempre que a organização o pretenda fazer, embora requeira obrigatoriamente uma autorização prévia e formal. Exceções estão previstas mediante justificação e tendo o risco sido aceite		
								Insira valor nos controlos

Maturidade por Domínio	
Domínios	**Maturidade**
0	**Insira valor nos controlos**
0	**Insira valor nos controlos**
0	**Insira valor nos controlos**
0	**Insira valor nos controlos**
0	**Insira valor nos controlos**
0	**Insira valor nos controlos**

0	Insira valor nos controlos
0	Insira valor nos controlos
0	Insira valor nos controlos
0	Insira valor nos controlos
0	Insira valor nos controlos
Maturidade Global	**0,00**

6.2 Caso de uso

Domínio	Área	Controlo	Nível 1 - Inicial	Nível 2 - Reativo	Nível 3 - Proativo	Nível 4 - Antecipativo	Maturidade
Governança Organizacional	Estratégia para a cibersegurança	Comprometimento da gestão de topo	O envolvimento da Gestão de topo em matéria de segurança é informal e pouco dedicada	A gestão de topo têm uma baixa participação, muitas vezes ocorrendo na sequência de um incidente	A gestão de topo têm uma ampla participação e visibilidade sobre a temática da cibersegurança, percebendo a necessidade e apoiando a causa	Existe uma total participação da gestão de topo, que compreende a necessidade da cibersegurança para o funcionamento da organização, procurando estar envolvida e supervisionando as atividades	2
		Disponibilização de recursos	São disponibilizados poucos recursos, por se interpretar a segurança como um custo e não um investimento	São disponibilizados alguns recursos, embora insuficientes face ao contexto organizacional	A organização percebe a importância da cibersegurança e esforça-se por disponibilizar os recursos necessários	A organização está comprometida em disponibilizar os recursos necessários (humanos, materiais e processuais)	3

		Envolvimento de terceiras partes	A interação com parceiros é feita de forma pontual, ocorrendo muitas vezes em cenários de incidente. A organização não transmite os seus requisitos em matéria de cibersegurança, não podendo responsabilizá-los posteriormente	Existe alguma interação com os parceiros ainda que limitada e muitas vezes impulsionada por requisitos legais ou de regulatório	É estabelecido um contacto formal e permanente, obrigando o parceiro a cumprir com os requisitos organizacionais. Durante o processo de contratação é avaliado o risco e a resiliência de cada parceiro	É estabelecido um contacto formal e permanente obrigando o parceiro a cumprir com os requisitos organizacionais e monitorizando a atividade e resiliência do parceiro. A avaliação de risco de cada parceiro, assim como o seu rate é monitorizado diariamente, sendo despoletados alertas em caso de alterações no *rate* ou atividades associadas a ciberataques		2
		Definição da estratégia	Em virtude da pouca sensibilização para a cibersegurança, a organização não formaliza uma estratégia para o governo da cibersegurança	É definida uma estratégia, embora não esteja difundida em todas as áreas da organização, sendo a revisão executada de forma pontual	Existe uma estratégia definida e difundida por toda a organização alinhada com as melhores práticas e suportada em frameworks robustas. A estratégia é revista anualmente e ajustada se necessário	Existe uma estratégia definida e alinhada com as melhores práticas e suportada em frameworks robustas, encontrando-se difundida por toda a organização. Cada departamento é solicitado para participar e contribuir ativamente na definição dessa estratégia. Existe um comité de segurança de informação que reúne trimestralmente, sendo responsável pela revisão periódica da estratégia		2
	Processo deContratação	***Background check***	Não é realizada qualquer análise prévia à contratação sobre o background, sendo todo o processo tratado de forma informal	É realizado alguma verificação sobre o background, embora sem um processo definido	Existe um processo formalizado que é seguido durante o processo de contratação, seja para colaboradores ou parceiros	Existe um processo formalizado que é seguido durante o processo de contratação, seja para colaboradores ou prestadores de serviços. De forma regular é feito um background check em particular nos prestadores de serviços assim como os critérios incluídos na lista de verificações		2
		Programa para retenção de talento e conhecimento	A organização não tem definido um programa para retenção de talento e conhecimento	A organização não tem definido um programa formal para retenção de talento e conhecimento, embora acontecem casos em que isso acontece, mas geridos pelos respetivos departamento	A organização tem definido um programa para retenção de talento e conhecimento	A organização tem definido um programa para retenção de talento e conhecimento transversal a toda a organização, tendo cada departamento a responsabilidade de dar contributos sobre cada colaborador. A organização revê e atualiza regularmente o programa		1

		Modelo de contratação de colaboradores	A organização não tem instituído um programa ou processo para contratação. A contratação é realizada à medida das necessidades	A organização não tem instituído um programa ou processo formal para contratação. A contratação é ad-hoc e numa primeira instância é assente em referenciação	A organização tem instituído um programa ou processo formal para contratação	A organização tem instituído um programa ou processo formal para contratação que assenta na referenciação e recomendação. Quando isso não é possível, recorre a empresas de *placement*		2
		Cláusulas de confidencialidade e retenção de informação	Não existe qualquer cláusula no contrato de trabalho para colaboradores diretos ou no contrato de prestação de serviços sobre a confidencialidade e retenção de dados da organização	Existem cláusulas no contrato de trabalho para colaboradores diretos, bem como no contrato de prestação de serviços, sobre a confidencialidade e retenção de dados da organização	Existem cláusulas no contrato de trabalho para colaboradores diretos, bem como no contrato de prestação de serviços, sobre a confidencialidade e retenção de dados da organização, prevendo penalizações pelo seu incumprimento. A organização monitoriza o cumprimento destas cláusulas	Existem cláusulas no contrato de trabalho para colaboradores diretos, bem como no contrato de prestação de serviços, sobre a confidencialidade e retenção de dados da organização, prevendo penalizações pelo seu incumprimento. A organização monitoriza o cumprimento destas cláusulas e obriga a formação regular sobre a importância da confidencialidade		3
		Subcontratação em cadeia	Não existe qualquer impedimento para a subcontratação em cadeia por partes dos parceiros	Todos os parceiros são obrigados a informar a organização caso pretendam realizar SUB subcontratações, mediante as cláusulas definidas no contrato de prestação de serviços	Todos os parceiros são obrigados a informar a organização caso pretendam realizar SUB subcontratações, mediante as cláusulas definidas no contrato de prestação de serviços com penalizações em caso de incumprimento. A organização dispõe de um prazo definido no contrato para se pronunciar sobre a SUB subcontratação. Findo esse prazo, caso o subcontratante não tenha recebido feedback poderá avançar	Os prestadores de serviço são obrigados a não implementar subcontratação em cadeia, mediante definido no contrato de prestação de serviços com penalizações em caso de incumprimento. A organização faz uma monitorização apertada e requer que todos os colaboradores externos cumpram com formação interna e adiram às políticas em vigor		2

		Código de ética e conduta profissional	A organização não possui qualquer código de ética	A organização possui um código de ética, obrigando que todos os colaboradores internos ou externos adiram ao mesmo	A organização possui um código de ética obrigando que todos os colaboradores internos ou externos adiram ao mesmo, monitorizando a sua adequação e atualizando-o regularmente	A organização possui um código de ética obrigando que todos os colaboradores internos ou externos adiram ao mesmo, monitorizando a sua adequação e atualizando-o de forma regular, obrigando a que todos os colaboradores recebem formação atempada sobre a sua alteração. A organização possui ainda um departamento dedicado à ética e conduta profissional que é responsável por lidar com casos em que existe falha no cumprimento do mesmo		3
		Normativo de segurança	A organização não definiu qualquer política ou norma relativamente à cibersegurança	Existe uma política de segurança de informação e um conjunto de normas que sustentam esta política	Existe uma política de segurança de informação e um vasto leque de política que sustentam esta política, procedendo-se à criação de novas políticas em virtude das necessidades	Existe uma política de segurança de informação e um vasto leque de política que sustentam esta política, sendo ágil o processo de elaboração de novas normas e a sua revisão feita anualmente para garantir a sua adequação. Num cenário de incidente de segurança ou outro evento relevante é avaliada a necessidade de rever alguma norma ou política		3
	Gestão de Risco	**Função Risco**	A avaliação de risco é realizada de forma pontual e apenas em cenários de ocorrência de incidentes	Existe um processo de gestão de risco básico abrangendo apenas algumas áreas organizacionais, envolvendo revisões pontuais e pouco formalizadas	Existe um processo de gestão de risco formal, aprovado pela gestão de topo com cobertura total sobre os activos de informação, com revisões periódicas e monitorização apertada	Existe um processo de gestão de risco formal, aprovado pela gestão de topo com cobertura total sobre os activos e todos os parceiros. São realizadas revisões periódicas, sendo o risco monitorizado de forma apertada através de uma ferramenta de gestão de risco que despoleta alertas e reavaliações a activos que apresentam mais vulnerabilidades ou fraquezas, assim como a parceiros cujo seu *rate* de risco decresça		2

		Normativo para gestão de risco	A organização não tem definida qualquer política ou norma para gestão de risco	A organização possui algum normativo para gestão de risco dos sistemas de informação, fazendo revisões pontuais, embora não seja seguido por todos os departamentos, nem a sua atualização é feita de forma regular	A organização possui normativo específico para gestão de risco dos sistemas de informação, fazendo a sua revisão de forma periódica ou sempre que existe um evento que assim o justifique, de forma a garantir a sua aplicabilidade ao contexto organizacional	A organização possui normativo específico para gestão de risco dos sistemas de informação, totalmente enquadrado no risco global, existindo revisões periódicas ou sempre que existe um evento que assim o justifique, de forma a garantir a sua aplicabilidade ao contexto organizacional. O risco é monitorizado e largamente suportado pela gestão de topo		3
		Responsáveis pelo risco	Os responsáveis pelo tratamento do risco não são formalmente identificados	Os responsáveis pelo tratamento do risco são identificados e assignados aos riscos, embora não lhe seja imputada uma responsabilidade direta pelo tratamento dos mesmos	Os responsáveis pelo tratamento do risco são identificados e assignados formalmente aos riscos, sendo-lhes imputada a responsabilidade pelo tratamento dos riscos e definidos prazos para a sua implementação. Contudo, não existe uma rigidez na monitorização e cumprimento dos prazos	Os responsáveis pelo tratamento do risco são identificados e assignados formalmente aos riscos, sendo-lhes imputada a responsabilidade pelo tratamento dos riscos e definidos prazos para a sua implementação. Todos os riscos são monitorizados de forma apertada de acordo com o normativo em vigor e definida métricas para o seu cumprimento		2
		Gestão da Conformidade	Não existe um processo formal para definição de requisitos de conformidade	São definidos requisitos de conformidade nos sistemas de informação, embora tratados ao nível departamental e sem um enquadramento transversal	São definidos e monitorizados requisitos de conformidade nos sistemas de informação ao nível da organização, havendo lugar a registo de não conformidades e atribuição das mesmas a um responsável	Existem processos e normativos que preveem a definição e monitorização de requisitos de conformidade nos sistemas de informação, com definição de métricas para o cumprimento das não conformidades, deficiências ou propostas de melhoria ao nível organizacional. Estes processos são suportados em ferramentas que permite um controlo mais apertado, melhoria continua e supervisão da gestão de topo e pelas áreas de auditoria interna e externa		2

		Metodologia para gestão de risco	O processo de avaliação de risco é inexistente, ou quando existe é feito de forma ad-hoc sem qualquer regularidade ou formalismo	O processo de avaliação de risco está definido, embora não de forma transversal a toda a organização. É realizado sem uma periodicidade definida	O processo de avaliação de risco está definido de forma transversal a toda a organização. É realizado mediante normativo definido, com atribuição de responsabilidades para a sua execução e monitorização	A organização definiu o normativo necessário para suportar a função de risco em todas as áreas organizacionais e de forma regular, ou perante um cenário disruptivo. As responsabilidades estão bem definidas e a sua monitorização é executada. A operacionalização da avaliação de risco é suportada por uma ferramenta tecnológica que simplifica a sua realização, servindo também de evidência para auditorias e entidades reguladoras. O processo em si é alvo de revisão e atualização periódica		3
	Funções e responsabilidades	**Formação em segurança da informação**	Não existe um programa formal e transversal para formação em cibersegurança	Apenas os recursos diretamente ligados à área de segurança de informação fazem formação em cibersegurança	É definido um programa transversal para todos os colaboradores sobre sensibilização para a segurança de informação mais em concreto cibersegurança. Este programa de formação faz parte do processo de admissão " induction". A organização monitoriza o seu cumprimento e atualiza de forma pontual estes conteúdos. Os recursos pertencentes à Área de segurança além destas formações, tem obrigatoriamente de realizar outras mais específicas	É definido um programa transversal para todos os colaboradores sobre sensibilização para a segurança de informação mais em concreto cibersegurança. Este programa de formação faz parte do processo de admissão " induction" e de forma regular a organização vai adaptando os conteúdos de forma a garantia que todos os recursos têm a formação e sensibilização necessária para a posição que ocupam. Os recursos pertencentes à Área de segurança além destas formações, tem obrigatoriamente de realizar outras mais específicas. Regularmente a organização executa programas que validam a formação e conhecimentos dos colaboradores		2

		Definição de perfis e responsabilidades	Para a vertente da segurança de informação, não existe um formalismo na definição das funções e responsabilidades de cada colaborador	Existe formalismo na definição de responsabilidades de cada colaborador, embora nem sempre é seguido. Não existe segregação de funções em alguns casos	Existe formalismo na definição de funções e responsabilidades de cada colaborador, encontrando-se documentadas e revistas de forma regular	Existe formalismo na definição de funções e responsabilidades de cada colaborador, encontrando-se documentadas, monitorizadas e revistas de forma regular, em linha com os objetivos de cada colaborador e do departamento onde operam		3
	Formação	**Gestão e evolução de carreiras**	Não está definido um processo para gestão e evolução da carreira profissional na vertente de segurança de informação	A organização dispõe de um programa formal de gestão e evolução de carreira, possibilitando a que cada colaborador possa evoluir e sendo de outras áreas internas, possa integrar a área de segurança	A organização dispõe de um programa formal de gestão e evolução de carreira, possibilitando a que cada colaborador possa evoluir e sendo de outras áreas internas, integrar a área de cibersegurança. Cada colaborador é livre de definir o seu programa de evolução, acompanhado de formação adequada	A organização dispõe de um programa formal de gestão e evolução de carreira, possibilitando a que cada colaborador possa evoluir, e sendo de outras áreas internas possa integrar a área de segurança. Cada colaborador é obrigado a definir o seu programa de evolução, em discussão com a sua chefia direta, traçando objetivos de evolução mediante a sua ambição e orientação interna. A organização monitoriza o programa de cada colaborador e apoia a sua execução		2
		Realização de exercícios e simulacros	A organização não promove a realização de quaisquer exercícios ou simulacros para aferir a sensibilidade de cada colaborador para a cibersegurança	São realizados exercícios de phishing ou outros de forma pontual, onde são analisados os resultados, mas de forma informal e com pouco contributo para a definição de programas de formação específicos	São realizados exercícios de phishing e outros uma vez por ano, onde são analisados os resultados e recolhidos inputs para avaliação geral da sensibilidade dos colaboradores e apoiar na definição de programas de formação	São realizados diversos exercícios de engenharia social ao longo do ano, embora com programas iguais para todos os colaboradores em determinados domínios e outros mais específicos para a área de sistemas de informação. São analisados os resultados e recolhidos inputs para avaliação geral da sensibilidade dos colaboradores e apoiar na definição de programas de formação, e repetição dos exercícios após os colaboradores terem recebido formação		1

		Gestão de budget para formação em cibersegurança	A organização não reserva ou prevê um valor anual dedicado à formação em cibersegurança	A organização prevê um valor anual para formação, embora gerido de forma ad-hoc e não requer a existência de um programa de formação previamente definido e validado	A organização prevê um valor anual para formação que é definido mediante o plano de atividades anual da Área de segurança. A organização tenta aprovar o pedido mediante justificação, sendo a sua execução monitorizada	A organização prevê um valor anual para formação que é definido mediante o plano de atividades anual da Área de segurança. A organização aprova o pedido após as devidas justificações, sendo a sua aplicabilidade monitorizada e revista de forma regular, podendo resultar em programas de formação específicos para toda a organização, como seja um programa global para todos os colaboradores, contendo conteúdos específicos em cibersegurança		2
		Monitorização da eficácia do programa de formação em cibersegurança	Não existe uma aferição formal do programa de formação em segurança de informação	A eficácia do programa de formação é medido de forma informal e individualizada, não abrangendo a organização como um todo	A eficácia do programa de formação é medido de forma transversal numa base anual	A eficácia do programa de formação é medido de forma transversal através da recolha constante de inputs, que analisados de forma global e em perspetiva de melhoria continua, através da definição de métricas		2
		Formação adequada às funções	A organização não promove formação alinhada a todas as funções no seio da organização	A organização define programas de formação genéricos para todos os colaboradores (ex. Segurança na utilização da internet ou no correio eletrónico), mas define também programas específicos para determinadas áreas (ex. desenvolvimento aplicacional seguro, formação em RGPD, etc.)	A organização define programas de formação genéricos para todos os colaboradores (ex. Segurança na utilização da internet ou no correio eletrónico), mas define também programas específicos para determinadas áreas (ex. Desenvolvimento aplicacional seguro, formação em RGPD, etc.). Esta formação especifica é regular e adequada às áreas alvo, havendo uma monitorização da sua completude a avaliação dos colaboradores sobre a sua interpretação	Existe um programa de formação formal e transversal a toda a organização com revisões periódicas e avaliação anual da sua adequação ao contexto organizacional, setorial, regulatório e legal		1

		Divulgação de normativos, processos e procedimentos organizacionais	Não existe uma metodologia formal para divulgação de normativo e informação relevante aos colaboradores	Todos os normativos e documentos relevantes são disponibilizados num repositório central (ex. Intranet, pasta de rede, etc.) acessível a todos os colaboradores	Todos os normativos e documentos relevantes são disponibilizados em diversos repositórios com logging configurado. A organização recolhe a analisa o acesso para efeitos de métricas de consulta, divulgando por toda a organização sempre que é lançado um novo normativo ou actualizado um existente	A organização possui uma solução de divulgação e consulta de normativo e documentos relevantes à função de cada colaborador, guardando evidência que o mesmo foi acedido, sendo o colaborador obrigado a declarar que teve acesso ao seu conteúdo		2
								2,17
Gestão de ativos	**Gestão de inventário**	**Inventariação**	A organização dispõe de um inventário confiável de ativos, sendo a inventariação feita sem qualquer formalização	Existem diversos registos de ativos, com informação imprecisa e pouco consistente, pertencendo a departamentos distintos	A organização mantém um inventário único, existindo um departamento específico para o efeito, que executa revisões e atualização periódicas. Existe um processo para revisão de activos e uma ferramenta que suporta este processo	A organização mantém um inventário único, existindo um departamento específico para o efeito, que executa revisões e atualização periódicas. Existe um processo para revisão de activos e uma ferramenta que suporte este processo que procura de forma permanente ativos na rede, atualizando também o inventário de forma automatizada, gerando alertas sempre que são detetados ativos com determinadas características		3
		Protecção contra adulteração de inventário de ativos	Não existem mecanismos de protecção contra adulteração do inventário de ativos	Estão implementados alguns mecanismos para protecção do inventário, embora básicos e não garantem o cumprimento da tríade CIA. Não existem alertas definidos para reportarem acessos indevidos	Estão implementados mecanismos para protecção do inventário e garantem o cumprimento da tríade CIA. Estão implementados também mecanismos de logging que registos eventos associados a acessos realizados ou tentativas de acesso	Estão implementados mecanismos para protecção do inventário e garantem o cumprimento da tríade CIA. Estão implementados também mecanismos de logging que registos eventos e monitorização ativa com capacidade para emitir alertas e notificações sobre o acesso indevido		3
		Classificação de ativos	Não existe um processo para classificação de ativos	Os activos são classificados informalmente, mas o inventário não reflete essa classificação	Existe normativo específico para classificação de ativos	Existe normativo específico para classificação de ativos. A classificação de cada activo é revista anualmente ou sempre que exista um evento relevante sobre qualquer ativo. São definidas métricas para avaliar a conformidade e atualização da criticidade de cada ativo		2

		Salvaguardas/Backups	Não estão definidos mecanismos de *backup* e *restore*	Encontram-se definidos mecanismos para *backup* e *restore,* embora não tenham sido definidos procedimentos que validem estes mecanismos	Encontram-se definidos mecanismos para *backup* e *restore da base de dados de ativos*, tendo sido definidos e executados de forma regular os procedimentos que validem estes mecanismos	Encontram-se definida uma política de salvaguarda de informação transversal a toda a organização, em linha com a criticidade de cada ativo ou processo, onde se inclui o *backup* ao inventário de ativos e respetivo restore. Esta política é difundida por toda a organização e revista regularmente		2
		Ativos pertencentes a parceiros	A organização não dispõe informação acerca de ativos de parceiros que suportem serviços da própria organização	Apesar da organização não dispor de inventário formal sobre os ativos de parceiros, possui alguma informação sobre esses ativos	A organização dispõe de um inventário actualizado sobre os ativos de parceiros que suportam ou prestam serviço à organização	A organização dispõe de um inventário actualizado sobre os ativos de parceiros que suportam ou prestam serviço à organização. A inventariação destes ativos está formalizada na política organizacional para gestão de ativos com obrigatoriedade do parceiros comunicar sempre que existam alterações		2
		Ativos entregues a parceiros/fornecedores	A organização não tem definido qualquer processo para gestão de ativos entregues a parceiros que colaboram com a organização	Existe um registo informal sobre o activo entregue a parceiros	A organização tem definido um processo para registo e monitorização de cada ativo entregue a parceiros	A organização tem definido um processo para registo e monitorização de cada ativo entregue a parceiros. Informação sobre o ativo é reportada à organização de forma automatizada por meio de um agente instalado. O processo define regras de utilização e cláusulas de responsabilização sobre a utilização dos respetivos ativos		3
		Devolução/recolha de equipamentos (colaboradores e parceiros	A organização não tem definido um processo formal para recolha de equipamentos	A organização tem implementado um processo manual para controlo de equipamentos entregues a colaboradores. Os colaboradores em processo de saída são obrigados a devolver os equipamentos registados em seu nome	A organização definiu um processo para a recolha de equipamentos que valida regularmente o estado do ativo e do colaborador	Existe um processo automatizado através de uma gestão centralizada de ativos. Este processo é executado de forma regular, monitorizado e alvo de auditorias regulares		2

	Gestão de atualizações de segurança	**Aplicação de atualizações de segurança**	A organização não tem definido um processo que vise gerir a instalação de atualizações. Estas ocorrem de forma pontual e manual	A organização dispõe de um processo para gestão de atualizações, embora seja automatizado, mas não abrange todos os ativos organizacionais	A organização dispõe de um processo para gestão de atualizações automatizado com calendário definido numa base mensal	A organização dispõe de um processo para gestão de atualizações de segurança automatizado com calendário definido para execução mensal, prevendo também instalações fora do ciclo, mediante a criticidade da atualização e o risco dos ativos a atualizar. A solução para gestão de atualizações de segurança permite aferir o nível de conformidade dos ativos, definir alertas regras para ativos que não cumpram requisitos mínimos de atualização		3
		Verificação de conformidade nos ativos	A verificação de conformidade de ativos não existe ou quando existe é executada de forma manual e pouco eficiente	são definidos requisitos e métricas para verificar a conformidade de ativos relativamente a atualizações de segurança. Como se trata de um processo manual e que requer um esforço considerável, raramente são realizadas avaliações de conformidade	A organização tem definido um processo para avaliar o nível de conformidade do ativo face os requisitos definidos. A aferição do nível de conformidade é suportado numa solução que automatiza o processo e produz relatórios de conformidade que são analisados pela área de cibersegurança	A organização tem definido um processo para avaliar o nível de conformidade do ativo face os requisitos definidos. A aferição do nível de conformidade é suportado numa solução que automatiza o processo, monitorizando-o e produz relatórios de conformidade em linha com a criticidade e o risco de cada ativo		2

		Gestão de exceções	Não existe um processo que prevê gerir exceções à instalação de atualizações de segurança	A exceções são identificadas de forma ad-hoc e quando aplicadas raramente são revisitadas	A gestão de atualizações de segurança prevê a ocorrência de exceções. Medidas compensatórias são definidas até que sejam revisitadas e corrigidas	A gestão de atualizações de segurança prevê a ocorrência de exceções que são identificadas através de mecanismos que testam o comportamento da atualização num ambiente controlado antes de serem aplicadas transversalmente. Contudo, também são consideradas informações provenientes de fontes seguras como seja em comunicados pelos fabricantes dos ativos ou em fóruns da especialidade. Medidas compensatórias são definidas para as exceções até que sejam corrigidas. Estas exceções são alvo de registo e monitorização em controlo interno e assignado a um responsável com data de resolução definida		2
		CAB (change-advisory board)	A organização não tem definido um CAB formal, embora tenha um grupo informal responsável por avaliar a instalação de atualizações de segurança	A organização têm constituído um fórum que reúne pontualmente e define as regras para cada instalação de atualizações de segurança	Existe um CAB constituído pelas principais áreas organizacionais e pela gestão de topo que reúne mensalmente e analisa e decide as atualizações de segurança a aplicar em cada ciclo	Existe um CAB constituído pelas principais áreas organizacionais e pela gestão de topo que reúne semanalmente e sempre que se justifique. Em cada reunião é avaliada com atualização a aplicar no ciclo semanal com base em informação recolhida previamente pelo próprio CAB		2

		Baselines de segurança em ativos	Não estão definidas baselines de segurança para ativos	A organização definiu uma baseline de segurança que aplica de forma ad-hoc em alguns ativos	A organização tem definidas diversas baselines de segurança mediante a criticidade de cada ativo/solução. A sua instalação é transversal, mas de forma manual	A organização tem definidas diversas baselines de segurança mediante a criticidade de cada ativo/solução e com mecanismos de atualização automatizados. A sua instalação é transversal e feita de forma automatizada. A organização monitoriza a conformidade dos ativos relativamente às baselines para garantir uma cobertura 100% da infraestrutura e a sua adequação face à criticidade de cada ativo	3
							2,42
Segurança e conformidade do posto de trabalho	**Mecanismos de protecção**	**Antivírus**	A organização tem uma gestão de antivírus pouco formalizada, podendo coexistir diversos fabricantes de soluções para antivírus, inclusive versões gratuitas, demonstrativas e não oficiais	A organização tem definida uma política para gestão de atualizações do antivírus. Cada posto de trabalho tem um agente de antivírus instalado e actualizado uma vez por dia, embora sem monitorização ou garantia que o faça	A organização tem definida uma política para gestão de atualizações do antivírus. Cada posto de trabalho tem um agente de antivírus instalado e actualizado pelo menos duas vezes por dia. A organização possui ainda uma infraestrutura centralizada de IDS e IPS que atuam como primeira linha de defesa para os postos de trabalho	A organização tem definida uma política para gestão de atualizações do antivírus. Cada posto de trabalho tem um agente de antivírus funcionando através análise comportamental e assinaturas que são atualizadas em tempo real. A organização possui também infraestrutura centralizada com IDS e IPS que atuam como primeira linha de defesa para os postos de trabalho	4
		Anti-Malware e Anti-Phishing	A organização tem uma gestão de Anti-Malware e Anti-Phishing pouco formalizada, podendo coexistir diversos fabricantes de soluções , inclusive versões gratuitas, demonstrativas e não oficiais	A organização tem definida uma política para gestão de atualizações de Anti-Malware e Anti-Phishing. Cada posto de trabalho tem um agente instalado e actualizado uma vez por dia, embora sem monitorização ou garantia que o faça	A organização tem definida uma política para gestão de atualizações de Anti-Malware e Anti-Phishing. Cada posto de trabalho tem um agente instalado (que poderá ser o mesmo do antivírus) que é atualizado pelo menos duas vezes por dia. A organização possui ainda infraestrutura centralizada de equipamentos que identificam, analisam e removem malware e phishing atuando como primeira linha de defesa	A organização tem definida uma política para gestão de atualizações de Anti-Malware e Anti-Phishing. Cada posto de trabalho tem um agente instalado (que poderá ser o mesmo do antivírus) e atualizado tempo real. A organização possui ainda infraestrutura centralizada de equipamentos que identificam, analisam e removem malware e phishing atuando como primeira linha de defesa. A componente de Anti-Malware e Anti-Phishing funcionam também com base comportamental, tendo a capacidade de isolar o ativo se assim tiver sido definido por políticas e mediante a criticidade da infeção	3

		Instalação de software padronizado	A organização não tem definidos controlos para gerir a instalação de software nos seus postos de trabalho. Sempre que um colaborador necessita, procede à sua instalação independentemente do tipo ou da origem do software	A organização não tem definidos controlos para gerir a instalação de software nos seus postos de trabalho. Sempre que um colaborador necessita de um determinado software padronizado e catalogado pela empresa, consulta um repositório (pasta na rede), pesquisa e instala. Se não existir, fala com o departamento de informática e solicita-o	A organização dispõe de um catálogo online onde constam todas os softwares padronizados que estão aprovados pela organização e podem ser instalados diretamente pelo utilizador. No caso de ser necessário assegurar o custo de licenciamento, a chefia direta do colaborador recebe um fluxo para aprovar. Mediante a sua aprovação o software é instalado automaticamente no posto do colaborador	A organização dispõe de um catálogo online onde constam todas os softwares padronizados que estão aprovados pela organização e podem ser instalados diretamente pelo utilizador. No caso de ser necessário assegurar o custo de licenciamento, a chefia direta do colaborador recebe um fluxo para aprovar. Mediante a sua aprovação o software é instalado automaticamente no posto do colaborador. Este catálogo é revisto regularmente para assegurar a sua atualização e abrangência. Todos estes softwares são removidos automaticamente dos postos de trabalho se estiverem 90 dias sem utilização		3
		Instalação de software não padronizado	A organização não tem definidos controlos para gerir a instalação de software nos seus postos de trabalho. Sempre que um colaborador necessita, procede à sua instalação independentemente do tipo ou da origem do software	A organização não tem definidos controlos para gerir a instalação de software nos seus postos de trabalho. Sempre que um colaborador necessita de um determinado software não padronizado, fala com a sua chefia direta para efeitos de aprovações financeiras e caso seja aprovado, solicita-o ao seu departamento de informática	Os softwares não padronizados são alvo de diversas validações antes de se proceder à sua aquisição, nomeadamente pela área de cibersegurança, arquitetura e gestão de ativos. O colaborador solicita o pedido de software, a chefia aprova, seguindo-se todo o processo de validação. Ultrapassada esta etapa, o software é adquirido e instalado no posto de trabalho	Os softwares não padronizados são alvo de diversas validações antes de se proceder à sua aquisição, nomeadamente pela área de cibersegurança, arquitetura e gestão de ativos. O colaborador solicita o pedido de software, a chefia aprova, seguindo-se todo o processo de validação. Ultrapassada esta etapa, o software é adquirido e instalado no posto de trabalho. A organização tenta evitar este processo por ser moroso e dispendioso, apostando em ter o seu catálogo mais amplo e a incluir uma maior variedade e disparidade de software. Todos estes softwares são removidos automaticamente dos postos de trabalho se estiverem 90 dias sem utilização		3
		Elevação de privilégios	A organização não tem definido normativo para gerir acessos privilegiados nos postos de trabalho. Por defeitos todos os colaboradores são administradores locais	A organização não tem definido normativo para gerir acessos privilegiados nos postos de trabalho. Os colaboradores por defeito não são administradores locais, mas sempre que é necessário solicitam essa permissão de forma ad-hoc e nunca mais lhes é retirada. A organização não tem um controlo sobre estes casos	A organização tem definido normativo para gerir acessos privilegiados nos postos de trabalho. Os colaboradores por defeito não são administradores locais e quando necessitam de o ser, solicitam um pedido formal que tem diversas aprovações, ficando registado. Anualmente é feita uma revisão destes acessos pelas respetivas chefias	A organização tem definido normativo para gerir acessos privilegiados nos postos de trabalho. Os colaboradores por defeito não são administradores locais e quando necessitam de o ser, solicitam um pedido formal que tem diversas aprovações. Após aprovação, é instalado um agente no posto de trabalho que passa a gerir de forma automática e transparente todas as ações privilegiadas.		3

						Anualmente estes acessos são revistos pelos responsáveis de cada colaborador	
		Instalação de atualizações e correções de segurança	A organização não tem definida uma estratégia de atualização aplicável a postos de trabalho. As instalações ocorrem de forma ad-hoc e sem um calendário pré-definido	A organização não tem definida uma estratégia de atualização especifica para postos de trabalho. As instalações críticas e altas são instaladas mas de forma ad-hoc	A organização tem definida uma estratégia e um processo de atualização específico para postos de trabalho. Existe um calendário pré-definido, embora atualizações críticas sejam instaladas de forma urgente	A organização tem definida uma estratégia e um processo de atualização específico para postos de trabalho. Existe um calendário pré-definido, embora atualizações críticas sejam instaladas de forma urgente. Antes de ser instalada qualquer atualização ou correção em produção, é testado em ambiente controlado para aferir o comportamento do posto mediante os testes realizados às aplicações utilizadas. Periodicamente o processo é revisto, atualizado e partilhado com todas as partes interessadas	3

	Conformidade do posto de trabalho	**Deteção de ativos em estado de inconformidade**	A organização não dispõe requisitos definidos que validam o estado de conformidade do posto de trabalho e mediante isso conceder acesso aos diversos recursos corporativos	A organização tem mecanismos que apenas permitem postos de trabalho corporativos tenham acesso aos recursos internos, mas não avaliam o seu estado de conformidade	A organização tem definidas políticas e mecanismos que validam o estado de conformidade do posto de trabalho e com base nesse estado permitem o seu acesso aos recursos organizacionais. Os postos em estado de inconformidade são colocados em quarentena	A organização tem definidas políticas e mecanismos que validam o estado de conformidade do posto de trabalho e com base nesse estado permitem o seu acesso aos recursos organizacionais. Tanto o colaborador com área de gestão de activos são alertados para o estado de inconformidade que o posto irá entrar, se não forem tomadas determinadas ações. Todos os postos em estado de inconformidade, acedem de forma limitada aos recursos organizacionais, numa área restrita (denominada de quarentena) para recuperarem o seu estado de conformidade	3
		Protecção da informação	A organização não tem definidas políticas para protecção de informação contida nos postos de trabalho	A organização não definiu qualquer política para protecção de informação nos postos de trabalho, mas dispõe de uma solução que permita a encriptação dos discos internos, mas não força a sua utilização	Existem políticas e processos definidos para protecção de informação nos postos de trabalho e uma solução que encriptação para discos internos e amovíveis ligados ao posto para transferir informação. A organização força a utilização, embora não monitorize a sua conformidade	Existem políticas e processos definidos para protecção de informação nos postos de trabalho e uma solução que encriptação para discos internos e amovíveis ligados ao posto para transferir informação. A organização força a utilização e monitoriza a sua conformidade. Os utilizadores mesmo sendo administradores do posto não tem permissões para desativar ou suspender a sua utilização. Se por algum motivo o posto ficar com o seu disco sem cifra, são despoletados alertas para a equipa de gestão de ativos e ações tomadas de imediato. Exceções estão previstas e são monitorizadas até a sua resolução	3

		Acesso a redes sem fios desconhecidas e inseguras	A organização não tem definidas políticas para gerir ligações a redes sem fios. O colaborador tem liberdade para estabelecer ligação com qualquer rede	A organização não tem definidas políticas para gerir ligações a redes sem fios. Na eventualidade de ser realizada uma ligação a este tipo de rede, o colaborador recebe um alerta sobre as consequências de avançar	A organização tem definidas políticas para gerir ligações a redes sem fios, em particular aqueles com níveis de segurança mais reduzidos	A organização tem definidas políticas para gerir ligações a redes sem fios. No caso de redes pouco seguras, a ligação é estabelecida, mas o proxy não permite saída para a internet por não ter classificado a mesma com segura		3
		Acesso controlado à internet	O acesso à internet não é gerido através de uma solução baseada em proxy ou noutra tecnologia	O acesso à internet é gerido através de uma solução baseada em proxy, embora sirva apenas para gerir o acesso à internet quando o posto está localizado nas instalações	O acesso à internet é baseado numa solução avançada de proxy (ex.: Zscaler, Akamai,,etc...) onde qualquer ligação à internet realizada pelo posto é filtrada por esta solução	O acesso à internet é baseado numa solução avançada de proxy (ex.: Zscaler, Akamai,,etc...) onde qualquer ligação à internet realizada pelo posto é filtrada por esta solução. Todas as soluções internas que necessitam de acesso à internet estão configuradas para serem permitidas. A organização atualiza de forma regular as lista para permitir e negar acessos através URL específicos ou por assunto (ex.: vídeo streaming, redes sociais, apostas online,,etc.)		4
	Monitorização ativa sobre os postos de trabalho	**Monitorização e resposta em modelo 24x7x365**	A organização não possui mecanismos para monitorizar, nem equipa de resposta a incidentes que envolvam postos de trabalho em modelo 24x7x365	A organização possui mecanismos que monitorizam o estado dos postos de trabalho em modelo 9x5, mas não tem equipas de resposta a incidentes envolvendo postos que cubram este horário	A organização possui mecanismos que monitorizam o estado dos postos de trabalho em modelo 24x7x365, embora a equipa de resposta a incidentes em 24x7x365 não seja exclusiva para postos e para assuntos relacionados com cibersegurança, executando apenas ações pré-definidas e básicas	A organização possui mecanismos que monitorizam o estado dos postos de trabalho em modelo 24x7x365. Existe ainda uma equipa dedicada a incidentes que envolvam postos de trabalho		3
								3,18
Gestão de Identidades e Acessos	**Estratégia**	**Definição de uma estratégia e modelo de governo para gestão de acessos**	A organização não tem definida uma estratégia formal para gestão de acessos.	A organização tem definidas algumas regras para gestão de acessos, embora pouco formalizada e operacionalizadas	A organização têm definida uma estratégia para gestão de acessos, documentada e formalizada transversalmente. Encontra-se implementada na grande maioria das áreas organizacionais	A organização têm definida uma estratégia para gestão de acessos, documentada e formalizada transversalmente. A sua implementação é ampla em toda a organização		3

		Monitorização, adequação e ajustes na estratégia para gestão de acessos	Por não existir uma estratégia definida para a gestão de acessos, não existem atividades inerentes à sua monitorização, adequação ou governação	A organização não tem uma estratégia formal definida, contudo foi definido um grupo de trabalho que tem como missão alavancar e ter um maior controlo e visão sobre a gestão de ativos	A organização definiu um modelo de governo para gestão de acessos. A área responsável tem a missão de supervisionar e definir ações de melhoria abrangendo todos os acessos internos ou externos.	A organização definiu um modelo de governo para gestão de acessos. A área responsável pela gestão de acesso tem a missão de supervisionar e definir ações de melhoria abrangendo todos os acessos internos e externos. Anualmente é feita uma revisão para garantir a conformidade da estratégia em virtude do número de exceções existentes, incidentes de segurança envolvendo acessos e novos requisitos legais e regulamentares		3
	Gestão de acessos	**Processo de gestão de acessos**	Não é seguido qualquer processo para gerir acessos. Estes são tratados caso a caso, de forma não centralizada e não monitorizada	Existe um processos, mas não envolve todos os acessos. Este processo não é monitorizado ou documentado	A gestão de acessos encontra-se formalizada através de um processo transversal a toda a organização. Este processo é alvo de monitorização e avaliação anual	A gestão de acessos encontra-se formalizada através de um processo transversal a toda a organização. Este processo é alvo de monitorização e avaliação anual, existindo controlos que identificam a atividades que envolvem acessos em incumprimento com o processo definido e aprovado. Os acessos são geridos com base em análise de risco, podendo por exemplo necessitar de mais que uma aprovação, ou serem atribuídos apenas de forma temporal		2

		Processo de atribuição de acessos aplicacionais e em infraestruturas (não privilegiados)	Não estão definidas quaisquer políticas e processos para atribuição de acessos aplicacionais e para infraestruturas. Os acessos são atribuídos de forma ad-hoc sem qualquer registo ou controlo	Não estão definidas quaisquer políticas e processos para atribuição de acessos aplicacionais e para infraestruturas. Os acessos são atribuídos de forma ad-hoc, embora exista um registo para cada acesso atribuído	A organização tem definidas políticas e processos para atribuição de acessos que estão documentadas e são de uso obrigatório em toda a organização. Os acessos são atribuídos de forma automatizada por meio de uma solução para gestão de acessos	A organização tem definidas políticas e processos para atribuição de acessos de forma centralizada, sendo os acessos atribuídos de forma automatizada através de uma solução para gestão de acessos configurada de acordo com as políticas definidas e baseado em funções e responsabilidades dos utilizadores e perfis definidos para cada aplicação. É utilizada uma solução para gerir passwords (ex. Key vault)		2
		Processo de atribuição de acessos aplicacionais e em infraestruturas (privilegiados)	A organização não faz distinção na forma como gere acessos privilegiados e não privilegiados	A organização não tem definidas quaisquer políticas e processos para gestão de acessos privilegiados, a sua gestão é feita ad-hoc. Contudo faz uma avaliação da real necessidade e avalia o risco da sua atribuição, procedendo à configuração de uma conta dedicada "privilegiada" diferente da conta "normal"	As políticas organizacionais definem regras e procedimentos específicos para atribuição de acessos privilegiados estão documentadas e são aderidas por toda a organização. Estes acessos são geridos de forma automatizada por uma solução aplicacional que assegura a sua atividade e monitorização	A organização tem definidas políticas e processos para atribuição de acessos de forma centralizada, sendo os acessos atribuídos de forma automatizada através de uma solução para gestão de acessos configurada de acordo com as políticas definidas e baseado em funções e responsabilidades dos utilizadores e perfis definidos para cada aplicação. Os acessos privilegiados requerem sempre uma aprovação da gestão de topo. É ainda utilizada uma solução para gerir passwords (ex. Key vault)Todo este processo é alvo de monitorização regular e auditado anualmente, sendo ainda definidos e avaliados KPIs mensais		2

		Utilização de uma plataforma/solução para acessos privilegiados	A organização não dispõe de uma solução para gerir acessos privilegiados	A organização não adquiriu nenhuma solução que permita gerir acessos privilegiados, contudo determinou que somente algumas podem ser utilizadas, prevenindo que cada utilizador escolha a que mais gosta de usar (ex. RDP para sistemas Windows e SSH para sistemas Linux apenas)	A organização possui apenas uma solução para gerir acessos privilegiados nos postos de trabalho	Existe uma solução para gestão de acessos privilegiados em todos os ativos, procedendo ao registo de logging e gravando a sessão do utilizador. Esta solução permite ainda identificar acessos privilegiados que sejam realizados à margem desta solução		2
		Utilização de uma plataforma/solução para gestão de acessos via SSO	A organização não dispõe de uma solução para gerir acessos aplicacionais via SSO	A organização apenas têm configuradas algumas soluções aplicacionais que permitem aos utilizadores acederem via SSO, apenas se os colaboradores estiverem a aceder a partir da rede interna	As soluções aplicacionais mais utilizadas pelos colaboradores têm configurado acesso apenas via SSO, a partir da rede interna ou VPN	Todas as soluções aplicacionais, sejam internas e externas, com maior ou menor utilização apenas permitem acessos via SSO a partir da rede interna ou VPN		2
		Processo de alteração de acessos	A organização não tem definido qualquer processo para alteração de acessos. Quando existe necessidade de alterar, é executado de forma ad-hoc e pouco formalizado	A organização não tem definido qualquer processo para alteração de acessos. Contudo, sempre que um colaborador sai da organização os acessos concedidos via SSO são removidos automaticamente. Contudo, quando o colaborador altera as suas funções, não são removidos os acessos anteriormente concedidos	A organização tem definidas políticas e processos para alteração de acessos que se encontram documentadas e de adesão obrigatória por toda a organização. Sempre que um colaborador é alvo de uma alteração relevante (ex. saída da organização, alteração de funções, ausência prolongada,,etc.....) o processo de alteração de acessos é despoletado de forma manual, mediante informação fornecida pelos Recursos Humanos à área de gestão de acessos	A organização tem definidas políticas e processos para alteração de acessos que se encontram documentadas e de adesão obrigatória por toda a organização. Sempre que um colaborador é alvo de uma alteração relevante (ex. saída da organização, alteração de funções, ausência prolongada,,etc.....) o processo de remoção de alteração é despoletado automaticamente. Todo este processo é alvo de monitorização regular e auditado anualmente, sendo ainda definidos e avaliadas métricas mensais		2

		Mecanismos de bloqueio automatizado para acessos comprometidos	A organização não possui uma forma automatizada para bloqueio de acessos comprometidos. O seu bloqueio é sempre manual e pouco eficiente	A organização não possui uma forma automatizada para bloqueio de acessos comprometidos. O bloqueio é manual, mas executado de forma célere dentro do horário 9x5	A organização não dispõe de uma forma automatizada para bloqueio de acessos comprometidos. Contudo, a organização dispõe de equipa em modelo 24x7x365 que prontamente desativam o acesso	A organização dispõe de uma solução que automatiza o bloqueio de acessos comprometidos. Esta solução faz uma análise de risco, e mediante o resultado bloqueia todos os acessos associados a uma entidade/conta		2
	Modelo de autenticação e autorização	**Utilização de 2 fator de autenticação**	A utilização de acessos organizacionais com multifactor de autenticação não está definida	A utilização de acessos com multifactor de autenticação está definida e a sua adesão ocorre de forma ad-hoc em determinados cenários (acesso a aplicações com maior criticidade, acessos privilegiados,,etc.)	A utilização de acessos com multifactor de autenticação é sempre utilizada para acessos remotos, acessos privilegiados, aplicações que tenham requisitos de autenticação forte	A utilização de acessos com multifactor de autenticação é obrigatória em todos os cenários, exceto em aplicação que tenham configurado SSO ou outras quando acedidas na rede interna		3
		Utilização de diferentes modelos de autenticação	A organização não definiu um processo ou regras específicas para diferenciar o modelo de autenticação. Esta gestão é feita ad-hoc	A organização definiu um processo e regras específicas para implementar diferenciados modelos de autenticação. Contudo, este processo não está difundido por toda a organização e por isso não é seguido na íntegra	A organização definiu um processo ou regras específicas para implementar diferentes modelos de autenticação, mediante se o acesso é de um colaborador ou de um parceiro. O processo é gerido de forma centralizada sendo a sua implementação executado de forma manual	A organização definiu um processo ou regras específicas para implementar modelos distintos de autenticação, de acordo com a criticidade e risco que cada acesso tem associado. O processo é gerido de forma centralizada e a sua implementação é suportada por uma solução que automatiza todo o processo		2
	Alterações, integrações e federações de identidades	**Alterações em identidades**	Não é seguido qualquer processo para alteração de entidades na gestão de acessos. Esta alteração é executada de forma informal e manual	As alterações são realizadas de forma manual, informal e pouco regular. Informação proveniente dos RH e da gestão de fornecedores "alimentam" as alterações, mas nem sempre ocorrem dentro de prazos coerentes com as alterações realizadas	As alterações ocorrem de forma manual de acordo com o fluxos de dados automatizados provenientes das diversas fontes onde existem identidades (RH, Gestão de fornecedores, Gestão de serviço,,etc.)	As alterações ocorrem de forma totalmente automatizada de acordo com o fluxos de dados também automatizados provenientes das diversas fontes onde existem identidades (RH, Gestão de fornecedores, Gestão de serviço,,etc.)		3

		Modelo de federação com entidades parceiras (colaboradores externos, fornecedores,,etc.)	Não está definido um processo para federação com entidades parceiras. São utilizados meios inseguros para troca de informação sobre acessos necessários por parte das entidades parceiras	Não existe um processo ou modelo formal para federação com entidades parceiras. Contudo a organização tem regras definidas de acordo com o perfil de risco do acesso, mediante a criticidade da solução/infraestrutura a ser acedida	A organização tem definido um processo que avalia o modelo de federação a configurar para cada parceiro tendo em conta vários critérios. Este processo está amplamente difundido por toda a organização . Cada área organizacional que envolva a participação e interação com parceiros é parte interessada no processo e contribui ativamente para ele	A organização tem definido um processo que serve de apoio à implementação do modelo de federação para parceiros. este modelo prevê a utilização somente de um modelo de federação por cada perfil de risco obtido quando se cruza o perfil do fornecedor vs. o perfil da solução/infraestrutura a que terá acesso. Este processo está amplamente difundido por toda a organização e auditado regularmente. Cada área organizacional que envolva a participação e interação com parceiros é parte interessada no processo e contribui ativamente para ele		2
	Revisão e monitorização	**Comprometimentos de acessos de parceiros**	A organização não tem definidos processos nem implementadas soluções que alertem e bloqueiem sempre que os acessos de parceiros estejam comprometidos	A organização tem definidos alguns mecanismos de monitorização e bloqueio sobre acessos de parceiros que possam estar comprometidos, mas não cobrem todos os cenários ou abrangem todos os tipos de autenticadores utilizados	A organização tem definidos processos e uma solução de monitorização e bloqueio sobre acessos de parceiros que possam estar comprometidos, que alertam em tempo real, embora não tenham uma cobertura total sobre todos os acessos de todos os parceiros	A organização tem definidos processos e uma solução de monitorização sobre acessos de parceiros que possam estar comprometidos, que alertam em tempo real e com uma cobertura total sobre todos os acessos de todos os parceiros		2

		Verificação e validação do nível de acesso	Não estão definidos processos para validar o nível de acessos solicitados	A organização não tem definidos processos formais para revisão e monitorização de acessos, mas estão instituídos mecanismos manuais executados de forma pontual que validam a adequação do nível de acesso	A organização tem definidas políticas e processos para validação de acessos, mas não são executados de forma regular. A validação do nível de acesso nem sempre está alinhado com o nível de risco dos ativos ou das entidades	A organização tem definidas políticas e processos para validação de acessos que se encontram operacionalizados e executados regularmente para assegurar a sua adequação e adoção por todos as áreas. A validação do nível de acesso está totalmente alinhado com o nível de risco dos ativos ou das entidades		3
		Revisão de acesso a sistemas críticos (contém informação pessoal sensível de colaboradores, clientes ou parceiros)	Não estão definidos processos específicos para revisão de acessos a sistemas que contenham informação sensível	Não estão definidos processos específicos para rever acessos a sistemas que contenham informação sensível, apenas existem orientações e boas práticas resultantes de áreas ou colaboradores com maior sensibilidade para o assunto e assim implementam controlos de acessos específicos	Os acessos a sistemas críticos estão identificados e são revistos anualmente, mediante obrigatoriedade imposta por políticas internas	Os acessos a sistemas críticos estão identificados e são revistos semestralmente mediante obrigatoriedade imposta por políticas internas. Devido à criticidade destes acessos, estão implementados controlos adicionais em termos de monitorização e registo de eventos (logging)		3
		Revisão de acessos (Geral)	A organização não dispõe de um processo para revisão de acessos, fazendo-o pontualmente e de forma ad-hoc	A organização não dispõe de um processo definido para revisão de acessos, fazendo-o de forma ad-hoc	A organização tem definido um processo para revisão de acessos privilegiados e as soluções que apresentem um maior risco. Esta revisão ocorre anualmente, sendo realizado pela área de gestão de acessos	A organização tem definido um processo que prevê a revisão anual de acessos com maior risco, incluindo acessos de parceiros. Este processo é auditado regularmente. São definidas e avaliadas métricas para o cumprimento destes processos		2
								2,35
Segurança de rede	**Gestão de acessos**	**Acessos à rede interna (acesso físico)**	A organização permite o acesso à rede de qualquer ativo, seja interno ou externo	A organização não permite que sejam ligados ativos externos à organização. A sua proibição é baseada em barreiras físicas	A organização não permite que ativos externos sejam ligados às suas redes, tendo para isso implementado mecanismos que valida o endereço *Mac*, necessitando que este tenha sido previamente aprovisionado	A organização não permite que ativos externos sejam ligados às suas redes, tendo para isso implementado mecanismos que verificam a autenticidade do ativo através de determinados fatores contra a base dados de ativos organizacionais atualizada em tempo real		2

		Acesso remotos para colaboradores	A organização permite a configuração de acessos remotos para colaboradores. A instalação é feita ad-hoc e sem regulação. O acesso é baseado em método de autenticação com fator simples (utilizador e palavra-passe)	A organização permite a configuração de acessos remotos para colaboradores. Contudo, só é permitido o acesso remoto a determinadas soluções/infraestruturas e configurados segundo regras e critérios previamente aprovados. Este acesso é baseado num método de autenticação de múltiplo fator (2FA)	A organização permite a configuração de acessos remotos para colaboradores através de um agente instalado no posto de trabalho e totalmente gerido, Contudo, só é permitido o acesso remoto a um número limitado de soluções/infraestruturas, nomeadamente aquelas que apresentam um risco menor. O acesso é amplamente gerido e monitorizado e requer utilização de múltiplo fator (2FA).	A organização permite a configuração de acessos remotos para colaboradores baseado no perfil e função de cada colaborador. Contudo, só é permitido o acesso remoto a determinadas soluções/infraestruturas e atribuídos segundo regras e critérios previamente aprovados, permitindo apenas determinadas operações e sempre com recurso a 2FA. Sempre que o colaborador inicia uma sessão remota, é executada uma avaliação automatizada e dinâmica que afere o cumprimento de controlos específicos como seja o IP, dispositivo ou a existência de um incidente que foi previamente referenciado e associado ao colaborador		2
		Acesso remoto de parceiros	A organização tem implementado o mesmo modelo de acessos remotos para colaboradores e parceiros	A organização tem definido um modelo de acesso remoto para parceiro segregado do acesso remoto para colaboradores. O acesso é configurado via VPN com recurso à utilização de múltiplo fator (2FA), mas nem sempre estes acessos permitem que os parceiros acedem apenas a aplicações/infraestruturas e serviços por eles geridos	O acesso remoto de parceiro é baseado em postos de trabalho virtualizados disponibilizados pela organização, que após autenticação com 2FA permitem aceder a determinados recursos internos, mediante as permissões configuradas no posto virtualizado. Cada parceiro tem dedicado a si diversos postos virtualizados. O acesso é monitorizado e auditado. Os postos de trabalho dos parceiros nunca são ligados à rede da organização	O acesso remoto é configurado através de VPN que após autenticação com 2FA permite aceder a uma poll de recursos que estão acessíveis ao parceiro, podendo inclusive segregar-se acessos e permissões entre colaboradores do mesmo parceiro, em virtude da segurança e flexibilidade que esta publicação permite. O acesso é monitorizado e auditado. Os postos de trabalho dos parceiros nunca são ligados à rede da organização		3
		Gestão de credenciais administrativas	A organização não tem definido qualquer requisito para gerar e armazenar credenciais usadas na gestão equipamentos	As credenciais usadas para gerir ativos administrativos são definidas pelos gestores dos ativos e guardadas num documento que está partilhado entre todos eles	As credenciais são definidas de acordo com o normativo definido e guardadas de forma segura numa solução implementada para o efeito (Keepass, Key vault,,etc.)	A organização utilização uma solução centralizada para gestão de acessos, que é responsável por gerar palavras-passe, guardar e forçar a sua rotatividade para cumprir com o normativo definido		3

		Disponibilização de acesso a redes sem fios para colaboradores e parceiros	A organização disponibiliza o acesso a redes sem fios sem restrições e de forma aberta a todos os colaboradores e parceiros	A organização disponibiliza o acesso a redes sem fios com protocolos de encriptação pouco robustos a todos os colaboradores e parceiros, embora existe um processo de registo e solicitação de acesso	A organização disponibiliza o acesso a redes sem fios com protocolos de encriptação robustos a todos os colaboradores e parceiros, mas com SSIDs e chaves diferentes. Estes redes sem fios não estão em segmentos de rede distintos	A organização disponibiliza o acesso a redes sem fios com protocolos de encriptação robustos a todos os colaboradores e parceiros, mas com SSIDs e chaves diferentes. Estes redes sem fios estão em segmentos de rede distintos, em que o segmento disponibilizado para parceiros permite unicamente um acesso à internet, monitorizado e auditado		2
	Monitorização e conformidade	**Protecção de eventos de rede (logging)**	Não estão implementados requisitos específicos para proteger os eventos	Os administradores têm acesso total aos eventos, embora o seu acesso fique também auditado	O acesso de escrita/alteração dos eventos está protegida. Apenas é possível realizar operações de leitura	O acesso de escrita/alteração dos eventos está protegida. Apenas é possível realizar operações de leitura. Os eventos estão protegidos contra adulteração ou manipulação		2
		Supervisão, monitorização e restrições sobre comunicações com parceiros e entidades externas	As comunicações internas de e para parceiros não estão definidas e são tratadas de forma informal	As comunicações internas de e para parceiros são documentadas na altura em que são implementadas, mas não é feito um "tracking" deste registo	As comunicações internas de e para parceiros estão documentadas face ao modelo de análise e aprovação em vigor que obriga a seguir um fluxo com determinadas atividades e controlos	As comunicações internas de e para parceiros estão documentadas e atualizadas. Cada comunicação obriga à avaliação de risco e após aprovada a sua implementação são criadas regras de firewall, registadas e implementadas através numa plataforma centralizada. regularmente são recolhidas métricas sobre as regras implementadas, permitindo por exemplo fechar regras que deixaram de ser utilizadas		3

		Gestão de alterações	As alterações preconizadas na rede são realizadas de forma informal pela equipa responsável, não existindo qualquer processo de revisão, autorização e acompanhamento	As alterações preconizadas na rede são realizadas de forma informal pela equipa responsável. Não existe um processo para gestão de alterações e por isso não requerem aprovação. O horário de implementação é definido pela equipa implementadora com base na sua sensibilidade e experiência no que respeita ao potencial impacto que poderá causar	A organização tem definido um processo para gestão de alterações, onde se incluem as alterações nos serviços de rede. Todas as aprovações seguem o seu fluxo de aprovação, existindo um período definido para a sua implementação, tendo em conta o impacto esperado nos utilizadores e serviços. Contudo, a janela de intervenção poderá ser ajustada mediante o parecer da equipa implementadora	A organização tem definido um processo para gestão de alterações, onde se incluem as alterações nos serviços de rede. Todas as alterações são analisadas e aprovadas em reunião de CAB que ocorre semanalmente. Ainda na reunião de CAB é avaliado o impacto e decidida a janela de intervenção mediante o impacto esperado e a criticidade da solução/infraestrutura a ser intervencionada. Para intervenções urgentes é seguido um processo "Agile" aprovado pelos responsáveis aplicacionais/infraestrutura e gestão de serviço		2
		Deteção de ativos na rede (shadown IT)	A organização não dispõe de processos e tecnologia para detetar e identificar postos de trabalho ou outros ativos desconhecidos ou não geridos na rede	A organização de forma pontual avalia a existência de postos de trabalho e outros ativos não geridos na rede. Esta análise é manual	A organização tem definido um processo que é suportado por uma solução tecnológica baseada em varrimentos em tempo real nas diversas redes (cablada e/ou sem fios). Adicionalmente a organização dispõe ainda de uma solução baseada em NAC que autentica o posto através do seu endereço mac	A organização tem definido um processo que é suportado por uma solução tecnológica faz varrimentos em tempo real nas diversas redes (cablada e/ou sem fios). Este processo é revisto anualmente e todos os ativos identificados são alvo de análise. As exceções são registadas em matéria de risco e acompanhadas até à sua mitigação. Adicionalmente a organização dispõe ainda de uma solução para autenticação e autorização de ativos na rede, baseada em RBAC através do registo do ativo na AD, impedindo que qualquer ativo não registado possa conectar-se às redes da organização, inclusive por VPN		3

	Gestão de incidentes na rede	**Identificação, analise, tratamento e monitorização de incidentes envolvendo ativos de comunicação/rede**	Não existe monitorização regular sobre os eventos. O acesso é feito pontualmente e em cenários de incidente	Existe alarmística sobre os eventos gerados através do envio de notificações (ex. por email, SMS,,etc.). Os administradores consultam os eventos mediante os alertas recebidos	A organização possui uma solução de agregação de eventos de ativos, que alem de guardar, também permite correlacionar e notificar. Os administradores acedem aos eventos e iniciam investigação mediante os alertas recebidos	A organização possui um NOC, com equipa dedicada que gere o ciclo de vida do incidente. Esta equipa faz uma primeira análise sobre os alertas e respetivos eventos, apoiando-se na capacidade de inteligência e correlação que a solução disponibiliza . Caso se justifique, o incidente é escalado à equipa de administração dos ativos para tratamento		3
	Arquitectura de rede	**Modelo de segregação de redes**	Os limites das redes não estão definidos, não existindo uma verdadeira segmentação	Existe uma segregação física e lógica entre a rede interna e a rede exposta para o exterior (DMZ)	Existem diversos níveis de segregação na rede (ex. dmz, rede produtiva e rede não produtiva), sendo esta segregação lógica	Encontra-se implementada uma arquitetura de rede transparente onde a rede interna está segregada por zonas, mediante a criticidade dos ativos em cada zona. O modelo de acesso varia por zona, obrigando a mais requisitos de segurança mediante a criticidade da zona		2

	Políticas de rede	**Documentação de rede**	A organização não dispõe de documentação detalhada sobre as suas redes. A informação apenas reside "na cabeça" dos administradores de rede	A organização dispõe de documentação sobre as suas redes e segmentos. Contudo, não existe um processo de atualização e revisão sobre esta documentação	A organização dispõe de documentação detalhada sobre as suas redes e respetivos segmentos. A informação é guardada num repositório central à semelhança da restante informação sobre aplicações e infraestruturas	A organização dispõe de documentação detalhada sobre as suas redes e respetivos segmentos. A informação é guardada num repositório central à semelhança da restante informação sobre aplicações e infraestruturas. Anualmente as equipas de administrações de redes recebem tarefas de revisão sobre a documentação. Sempre que são realizados projecto ou atividade de maior impacto, um fluxo é gerado automaticamente pela solução ITSM e enviado ao executante das alterações para que proceda também à atualização da documentação		2

		Utilização aceitável e responsável da rede	A organização não tem definidas políticas ou práticas que definem uma correta utilização dos recursos de rede	Estão documentadas as melhores práticas na utilização da rede, embora seja apenas um documento informal servindo de guia de orientação	A organização tem definida e publicada uma política para uso aceitável dos recursos de rede	A organização tem definida e publicada uma política para uso aceitável dos recursos de rede. A cada colaborador é dado conhecimento da política na fase de contratação. Anualmente a política é revista e cada colaborador recebe um fluxo, onde é obrigado a dar conhecimento e aceitação sobre a sua adesão à referida política		3
	Gestão de vulnerabilidades na rede	**Processo de deteção, análise e mitigação**	A organização não possui um processo para deteção de vulnerabilidade na rede. Tem conhecimento apenas quando recebe informação se fontes públicas	A organização não possui um processo para deteção de vulnerabilidade na rede. Contudo, pontualmente executa atividades de scans de vulnerabilidades, sobretudo quando surgem notícias públicas sobre determinados ciberataques que envolvem equipamentos semelhantes aos que a organização utiliza	A organização possui um processo para deteção de vulnerabilidade na rede que assenta na realização de scans de vulnerabilidade anuais a todos os ativos de rede	A organização possui um processo para deteção de vulnerabilidades na rede que assenta na realização de scans de vulnerabilidade mensais a todos os ativos de rede. Estes scans são realizados por equipas internas e externas. São ainda recebidas informações sobre vulnerabilidades diretamente dos fabricantes dos ativos, assim como de outras fontes de *Treath Intel* por forma a serem tratadas o mais urgentemente possível para evitar serem exploradas publicamente		2

		Instalação de atualizações de rede	A organização não tem definido um processo que vise gerir a instalação de atualizações em ativos de rede	O processo de instalação de atualizações não abrange ativos de rede. A aplicação de atualizações é pontual e por norma para corrigir vulnerabilidades	O processo de instalação de atualizações abrange ativos de rede. Contudo, a sua aplicabilidade não é regular em virtude do potencial impacto	O processo de instalação de atualizações abrange também ativos de rede, cuja sua aplicação decorrer de forma regular e contempla todos os ativos de rede de todos os ambientes existentes		3
		Deteção e tratamento de vulnerabilidades em ativos de rede	A organização não tem definido um processo para identificar e acompanhar o tratamento de vulnerabilidades	A organização tem definido um processo para identificar vulnerabilidade, mas o mesmo não tem um acompanhamento até final do ciclo de vida da vulnerabilidade	A organização tem definido um processo para identificar vulnerabilidade e acompanhar o seu tratamento. A vulnerabilidade é registada na base dados de vulnerabilidades e criado um pedido na ferramenta de ITSM para mitigação. Quando a mitigação for confirmada a base dados é manualmente atualizada	A organização tem definido um processo para identificar vulnerabilidade e acompanhar o tratamento de vulnerabilidades. O ciclo de vida da vulnerabilidade é automatizado totalmente materializado através da solução que a identificou		2
								2,44
Gestão de parceiros (fornecedores)	**Políticas, Processos e procedimentos**	**Gestão de contratos**	Os contratos assinados com parceiros são pouco detalhados e clausulados, limitando-se apenas ao que é comum num contrato entre duas partes	Os contratos assinados com parceiros são pouco detalhados, em particular sobre deveres e responsabilidades envolvendo a temática da cibersegurança	Os contratos assinados endereçam cláusulas de deveres, responsabilidade e obrigatoriedade em cumprir todos os requisitos de cibersegurança e privacidade. O contrato prevê ainda que a organização supervisione e audite todas as atividades realizadas	Os contratos assinados endereçam cláusulas de deveres, responsabilidade e obrigatoriedade em cumprir com todos requisitos de cibersegurança, privacidade, práticas de segurança na utilização e configuração de equipamentos e devolução de equipamentos. O contrato é revisto regularmente para garantir a sua atualização e inclusão de novos requisitos e práticas de segurança, que contemplam penalizações por incumprimento. A organização ao abrigo do contrato tem legitimidade para supervisionar, auditar		2

		Cumprimento do normativo interno	A organização não partilha normativo com parceiros/fornecedores, ou partilha, mas não força o seu cumprimento	A organização partilha o seu normativo, incluindo normativo específico para parceiro com o parceiro apenas na fase de contratação de serviços	A organização partilha o seu normativo com o fornecedor na fase de contratação e sempre que existem alterações relevantes	A organização partilha o seu normativo com o fornecedor na fase de contratação e sempre que existem alterações relevantes. A organização monitoriza o cumprimento do normativo por parte dos parceiros e em reuniões de serviço que ocorrem mensalmente, sendo este um ponto na agenda da reunião		3
	Governação	**Processo de contratação**	O processo de contratação de parceiros/fornecedores ocorrem sem formalismos, ocorrendo à medida que é necessário	O processo de contratação não é realizado por departamento de forma informal. Existem algumas orientações para a realização da contratação, mas nem sempre ou nem todos os departamentos seguem essas práticas	A organização dispõe de uma área central de compras, existindo um processo estabelecido que define as regras de contratação	A organização tem definido um processo de contratação com regras e requisitos definidos. Quando é identificada uma necessidade de contratar serviços externos, é seguido um fluxo passando pelas diversas áreas que formalmente estão definidas como sendo parte do processo e outras que variam em função do tipo e natureza dos serviços a contratar, embora a área de segurança participe em todas as contratações que envolvem TIC		2

		Avaliação prévia à contratação	A organização geralmente não executa uma avaliação prévia à contratação (incluindo parceiro e função contratada)	A contratação ocorre ao nível departamental, sendo realizada uma avaliação de prévia, embora por formalizada e não difundida por toda a organização	A análise prévia à contratação do parceiro é uma preocupação e um requisito obrigatório. Os riscos identificados em particular os de maior criticidade são analisados e supervisionados pela organização, tendo sido definidos prazos para a sua mitigação	A avaliação prévia à contratação do parceiro é uma preocupação e um requisito transversal para qualquer contratação, independentemente do valor co contrato. O resultado da avaliação é um fator crítico a ter em conta para fechar a contratação. No caso da contratação ser estabelecida, os riscos identificados são alvo de uma supervisão apertada pela organização, definindo prazos para a sua mitigação e implementados controlos compensatórios. Regularmente são realizadas ações de avaliação de risco pela organização através do seu processo de risco, recorrendo também a avaliação através de ferramentas que avaliam diariamente os riscos e o "rate" de cada parceiro		2
		Gestão de não conformidade de parceiros	A organização não tem definidos processos e procedimentos para monitorizar a conformidade dos seus parceiros. Sempre que uma não conformidade é identificada, a organização trata-a de forma informal	A organização não tem definidos processos formais para gestão de não conformidades envolvendo fornecedores. Apesar de existirem orientações para tratar não conformidades, estas centram-se e tratam-se ao nível departamental	A organização tem definidos processos para gestão de não conformidade de parceiros, sendo tratados e monitorizados ao nível da organização	A organização tem definidos processos para gestão de não conformidade de parceiros, sendo tratados e monitorizados ao nível da organização. O processo é monitorizado e atualizado de forma regular para ter uma maior cobertura para os diversos cenários e diferentes parceiros		3

		Ponto de contato para gestão de pedidos	A organização não tem definido um canal e um contacto formal para interagir com parceiros para as mais diversas situações. As interações ocorrem de forma informal e através de diferentes pessoas	A organização não tem definido um canal e um contacto formal para interagir com parceiros para as mais diversas situações. Contudo, todas as interações ocorrem a nível do departamento ou área responsável pelo serviço prestado pelo parceiro	A organização tem definido um canal e um ponto de contato formal para interação com parceiros	A organização tem definido um canal e um ponto de contato formal para interação com parceiros, tratando da área de gestão de serviço		3
	Gestão de risco de parceiros	**Avaliação de risco a parceiros**	A organização não avalia riscos dos seus parceiros	A organização realiza avaliação de risco de alguns parceiros, sobretudo aqueles que estão envolvidos em soluções com arquitectura mais críticas	A organização tem definidos processos para avaliação de riscos associados a parceiros. A organização monitoriza de forma regular o risco e respetiva classificação dos seus parceiros	A organização tem definidos processos para avaliação de riscos associados a parceiros. A organização monitoriza de forma regular o risco e respetiva classificação de cada parceiro. Estão definidas métricas relativamente ao rate de parceiros, que são monitorizadas e analisadas mensalmente em reuniões de Steering. A organização incentiva ao incremento no rate dos seus parceiros. Em caso de descida de rate, a organização analisa e toma as devidas diligências		2
		Fontes para consulta de classificação de parceiros	A organização não tem definido processos para obter e gerir classificação dos seus parceiros	A organização não tem definido processos para obter e gerir classificação dos seus parceiros. Contudo, obtém classificações através de fontes públicas e contatos próximos	A organização tem definidos processos e soluções (ex.: bitsight, SecurityScoreCard, ,etc.) que fornecem informação sobre classificação de parceiros	A organização tem definidos processos, soluções (ex.: bitsight, SecurityScoreCard,,etc.) que fornecem informação sobre classificação de parceiros. Estas soluções disponibilizam informação coerente, realista e atualizada regularmente. A organização valida os dados obtidos de forma regular e define medidas de melhoria sobre a coerência e audibilidade aos sistemas fonte		2

		Disponibilização de acessos a informação sensível e classificada	A organização não tem implementados controlos específicos para gerir o acesso a informação sensível por parte dos seus parceiros	A organização tem definidos alguns controlos e mecanismos para restringir o acesso a informação sensível pelos parceiros. Estes controlos são implementados de forma ad-hoc e não garantem uma abrangência global	A organização tem implementados controlos centralizados que impedem o acesso a informação sensível. Estes controlos são transversais a toda a organização e também auditam e monitorizam todos os conteúdos acedidos	A organização tem implementados controlos centralizados que impedem o acesso a informação sensível. Estes controlos são transversais a toda a organização e também auditam e monitorizam todos os conteúdos acedidos. A organização tem ainda implementadas políticas e uma solução de classificação de informação, que igualmente impedem o acesso a informações classificadas através da utilização de etiquetas classificativas		2
		Renovação contratual	A renovação de contrato com parceiros é informal, sem qualquer reavaliação	A renovação de contrato é executada tendo por base um questionário interno sobre o qual é obtido pareceres das áreas relevantes, como seja cibersegurança, privacidade ou gestão de serviço	A organização tem um processo formal para renovação contratual, onde são lançados questionários internos sobre a apreciação global do serviço prestado. São ainda lançados alguns questionários base e outros específicos de acordo com o resultado obtido nos questionários base	A organização tem um processo formal para renovação contratual, envolvendo as principais áreas internas, incluindo a área de segurança, que tem obrigatoriamente de emitir um parecer sobre a renovação. São lançados questionários internos sobre a apreciação global do serviço prestado. A classificação do parceiro no que respeita a risco é considerada neste processo		2
		Monitorização sobre a postura de segurança do parceiro	Não são realizadas atividades no decorrer do contrato que visem avaliar a postura, sensibilidade e capacidade do parceiro em matéria de cibersegurança	São realizadas atividades pontuais decorrer do contrato que visam avaliar a postura, sensibilidade e capacidade do parceiro em matéria de cibersegurança. Estas avaliações centram-se em questionários lançados e recolha de pareceres junto dos colaboradores internos	A organização monitoriza de forma regular as atividades do parceiro, retirando daí indicadores. Os parceiros são convidados a participar em formação, exercícios e campanhas de sensibilização para a cibersegurança	A organização monitoriza de forma regular as atividades do parceiro, tendo definidos KPIs. Os parceiros são obrigados a participar em formação, exercícios e campanhas de sensibilização para a cibersegurança. Cada parceiro tem ainda obrigatoriedade de formar os seus quadros para a temática da cibersegurança e dar evidências sobre essas formações		2

		Estratégia de saída	Quando o contrato é assinado com parceiros, não é definida uma estratégia de saída	Os contratos assinados com parceiros, incluem informação sobre a estratégia de saída, embora muito alto nível	Todos os contratos com parceiros definem uma estratégia de saída, onde se inclui informação sobre a gestão do processo de saída no que respeita a passagem de conhecimento, tempo necessário para apoiar a integração de um novo parceiro, formato e moldes em que a passagem de conhecimento deve ocorrer	Todos os contratos com parceiros definem uma estratégia de saída, onde se inclui informação sobre o processo de saída no que respeita a passagem de conhecimento, tempo necessário para apoiar a integração de um novo parceiro, formato e moldes em que a passagem de conhecimento deve ocorre. A organização define uma equipa interna de apoio à saída do parceiro para assegurar que o conhecimento fica também retido no seio da organização e assegurar uma passagem para o novo parceiro sem incidentes, atendendo ao momento sensível que é a substituição de um parceiro		3
								2,33
Monitorização de segurança	**Pessoas/Equipas**	**Equipa de monitorização**	A organização não tem uma equipa dedicada à de monitorização de cibersegurança	A organização não tem uma equipa dedicada para monitorizar e tratar temas de cibersegurança. Sempre que necessário é constituída um grupo de trabalho informal para acompanhar e proceder com as diligências necessárias	A organização tem uma equipa dedicada para monitorizar e tratar temas de cibersegurança	A organização tem uma equipa dedicada para monitorizar e tratar temas de cibersegurança. A equipa é autónoma a tratar todas as situações que envolvem cibersegurança, interagindo com parceiros, grupos de especialidade e entidades legais, regulamentares, supervisoras e setoriais		2
		Capacidade e prontidão	O facto da organização não ter uma equipa dedicada à monitorização e resposta a temas de cibersegurança, a capacidade e qualidade de resposta a qualquer assunto desta natureza não será eficaz	A organização não tem uma equipa dedicada à monitorização e resposta sobre temas de cibersegurança. Contudo, existem informalmente determinadas funções e perfis que respondem a situações que o exigem, embora a resposta seja dada com base no melhor esforço	A equipa de monitorização e resposta a temas de cibersegurança encontra-se definida e com aptidão para responder	A equipa de monitorização e resposta a temas de cibersegurança encontra-se definida e com aptidão para responder. As funções são revistas regularmente de forma a garantir uma total cobertura para temas de cibersegurança, tendo por base análise e tendências sobre novas tipologias de ameaças e ataques cibernéticos		2

		Formação e sensibilização em cibersegurança	As equipas tem uma formação mínima em cibersegurança	As equipas tem alguma formação e sensibilização para lidar com temas de cibersegurança, embora o conhecimento seja muito individualizado	A organização possui equipas dedicadas a temas que envolvem cibersegurança, estando para isso capacitadas com formação que lhes é administrada no início das suas funções e atualizada regularmente	A organização possui equipas dedicadas a temas que envolvem cibersegurança, estando para isso capacitadas com formação que lhes é administrada no início das suas funções e atualizada regularmente de acordo com os seus planos de formação. A organização monitorização a atividades destas equipas e define métricas para avaliar a sua atividade e a partir desses indicadores são definidas formações específicas em determinados domínios consoante as necessidades e a capacidade em conseguir responder correta e eficazmente as todos os temas relacionados com cibersegurança		2
	Processos e procedimentos	**Estratégia de monitorização**	A organização não tem definida uma estratégia para monitorização de cibersegurança	A organização não tem formalizada uma estratégia para monitorização de cibersegurança. Contudo, existe uma equipa que faz monitorização global sobre os ativos e não dedicada a temas de cibersegurança que informa perante a existência de comportamentos anómalos ou alertas associados a cibersegurança	A organização tem definida uma estratégia para monitorização de segurança. Esta monitorização é essencialmente realizada de forma manual e não abrange todos os ativos organizacionais, somente aqueles que tem associado um maior risco devido à sua utilização e exposição	A organização tem definida uma estratégia para monitorização de segurança assente numa total automatização na análise de eventos e resposta a alertas e incidentes. Todos os ativos são alvo de monitorização mediante o nível de risco de cada um. A estratégia de monitorização é avaliada regularmente para aferir a sua eficácia e capacidade de responder às novas ameaças e ataques.		2
		Monitorização e supervisão da estratégia de monitorização	A gestão de topo tem uma reduzida participação e envolvimento no acompanhamento da estratégia de monitorização	A gestão de topo é envolvida e participa no programa de monitorização, embora em alto nível, focando-se apenas nos valores mensais sobre a atividade da área	A gestão de topo é envolvida e participa no programa de monitorização, existindo um comité de segurança que reúne trimestralmente. Este Comité é composto por elementos da gestão de topo e áreas relevantes e que contribuem ativamente para ampliar e melhorar a monitorização de cibersegurança	A gestão de topo é envolvida e participa no programa de monitorização, existindo um comité de segurança que reúne trimestralmente. Este Comité é composto por elementos da gestão de topo e áreas relevantes e que contribuem ativamente para a causa. Este comité serve ainda para analisar modelos, processos e tecnologias imergentes que visem incrementar a segurança da organização, em particular a cibersegurança		2

		Processos de monitorização	A organização não tem definidos nem implementados processos para monitorização de segurança	A organização não tem formalmente definidos processos de monitorização, contudo são executados procedimentos e de forma ad-hoc e manuais	Os processos de monitorização estão formalmente definidos e documentados, embora não sejam totalmente seguidos. A organização tenta manter os processos atualizados e adaptados às novas ameaças	A organização tem os processos formalmente definidos e bastante amadurecidos em virtude da senioridade das equipas de monitorização. Todos os processos são revisto regularmente atualizados em linha com os principais "standards" da indústria		3
		Escalonamentos	A organização não tem definidos nem implementados fluxos de escalonamentos aliados ao processo de monitorização	A organização não tem definidos nem implementados formalmente os fluxos de escalonamentos aliados ao processo de monitorização. Contudo, existe uma lista de contatos informais da área de segurança para onde podem ser escalados temas	A organização tem formalmente definidos e implementados fluxos de escalonamentos aliados ao processo de monitorização, existindo para isso um canal estabelecido para escalonamentos	A organização tem formalmente definidos e implementados fluxos de escalonamentos aliados ao processo de monitorização em modelo 24*7*365. O processo de escalonamentos define as funções e responsabilidades de cada equipa e o procedimento a seguir, bem como os responsáveis de cada equipa		2
		Gestão de exceções	Todas as exceções são tratadas de forma informal à medida que vão surgindo	As exceções são discutidas com a área de segurança e comunicadas informalmente a toda a organização	As exceções são discutidas com a área de segurança, propostas a aprovação, aprovadas e formalmente comunicadas a toda a organização	As exceções são discutidas com a área de segurança, propostas a aprovação, aprovadas e formalmente comunicadas a toda a organização. Regularmente todas as exceções são analisadas entre a área de segurança e as áreas preponderantes para avaliar a sua continuidade		2
		Modelo de reporte interno	Não está definido um modelo de reporte interno	Não está definido um modelo de reporte. Contudo, a equipa de segurança está preparada e responde de forma informal	A organização tem definido um modelo de reporte no que respeita a conteúdos e métricas. Mensalmente são produzidos e partilhados os relatórios	A organização tem definido um modelo de reporte totalmente automatizado. Mensalmente são produzidos e partilhados os relatórios definidos. A gestão de topo recebe os relatórios. Os templates são revistos e atualizados regularmente de forma a contemplarem informação relevante para a gestão de topo		2

		Modelo de reporte externo	Não está definido um modelo de reporte interno	Não está definido formalmente um modelo de reporte externo. A equipa de segurança reporta a entidades externas (supervisores, entidades policiais, regulamentares,,etc.....)	A organização tem definido um modelo de reporte externo. Este modelo define o canal e a área responsável por comunicar com entidades externas (supervisores, entidades policiais, regulamentares,,etc....)	A organização tem definido um modelo de reporte externo automatizado e "standardizado" de forma a responder uniforme e atempadamente às obrigações impostas. Este modelo define todos os detalhes que o reporte deve respeitar, desde a sua conceção, ao envio e reposta a pedidos de provenientes de todas as entidades perante as quais a organização tem essa obrigatoriedade (supervisores, entidades policiais, regulamentares,,etc....)		2
		Processos para monitorização automatizada	A organização não tem definido qualquer processo automatizado para monitorização de segurança	A organização não tem definido qualquer processo automatizado, embora tenha equipas que apoiam na monitorização, mas numa base manual	A organização tem implementado um serviço de monitorização assente em SOC (interno ou externo) que automatiza parcialmente o processo de monitorização de segurança	A organização tem implementado um serviço de monitorização assente em SOC (interno ou externo) que automatiza na íntegra o processo de monitorização de segurança		3
		Processo de reporte de incidentes	A organização não tem definido um processo para reporte de incidentes de segurança. Geralmente são comunicados de forma informal	A organização não tem formalmente definido um processo para reporte de incidentes de segurança, embora estejam informalmente implementados alguns canais, métodos e modelos de comunicação de incidentes	A organização tem definido um processo para reporte de incidentes de segurança. Neste processo estão definidos canais, métodos e modelos de comunicação de incidentes, embora possam ser utilizados outros canais paralelos (email, telefone, chat,,etc.)	A organização tem definido um processo para reporte de incidentes de segurança. Neste processo estão definidos canais, métodos e modelos de comunicação de incidentes. A organização monitoriza regularmente a forma como os incidentes são reportado. De forma regular os colaboradores realizam formação em cibersegurança e simultaneamente são treinados sobre a forma como devem reportar quaisquer incidentes de cibersegurança interna ou externamente		2
		Gestão de incidentes	A gestão de incidentes é executada caso a caso, sem que siga um processo ou fluxo	A gestão de incidentes não está formalmente definida, embora sejam seguidas regras em linha com as características de cada incidente	A organização tem definido e implementado um processo para gestão de incidentes	A organização tem definido e implementado um processo para gestão do ciclo de vida do incidente alinhado com os principais "standards" da indústria		2

		Análise prévia a incidentes de segurança	Não é realizada uma análise prévia a incidentes de cibersegurança de forma a descartar falsos positivos	Formalmente não existe o conceito de análise prévia a incidentes de cibersegurança de forma a descartar falsos positivos. Muitas vezes esta pré-análise é feita com base na experiência da pessoa que recebe o incidente	Em virtude de existirem alguns processos automatizados para análise de incidentes de segurança, a análise prévia é realizada permitindo excluir casos associados a falsos positivos	A organização tem o seu sistema de monitorização de segurança totalmente automatizado, permitindo uma maior e melhor análise a todos os eventos, assim como uma correlação entre eles. Este processo permite uma análise prévia mais eficiente, reduzindo substancialmente o número de falsos positivos que são alvo de análise		2
		Critérios para definição de criticidades	A organização não tem definidos quaisquer critérios para atribuição de criticidade a incidentes de cibersegurança A atribuição é feita caso a caso e sem uma base orientadora	Não estão definidos critérios para atribuição de criticidades a incidentes de cibersegurança, embora sejam seguidas algumas práticas nessa classificação, alinhadas com a criticidade associada ao ativo alvo do incidente	A organização têm definidos critérios para atribuição de criticidade aos incidentes de cibersegurança. Este critério está alinhado com a criticidade do ativo e com o impacto financeiro e reputacional	A organização têm definidos critérios para atribuição de criticidade aos incidentes de segurança. Este critério está alinhado com a criticidade do ativo e com o impacto financeiro e reputacional. O processo de atribuição de criticidade calcula automaticamente a criticidade em função dos casos de uso pré-definidos. Regularmente a organização revê a criticidade de cada ativo, em função dos inputs proveniente da avaliação de risco executada		2
		Tipificação de incidentes e eventos de segurança	Não é seguido qualquer processo ou prática para tipificar incidentes de cibersegurança	Apesar de não existir um processo ou critério para tipificar incidentes, a organização segue um conjunto de práticas que tem por base *standards* ainda que pouco formalizados e nem sempre atualizados	A organização tem definido critérios para tipificação de incidentes de segurança. Esta prática é seguida formal e obrigatoriamente em linha com *standards*	A organização tem definido critérios para tipificação de incidentes de segurança. Esta prática é seguida formal e obrigatoriamente em linha com *standards*. A organização participa regularmente em fóruns da especialidade (ex. CNCS) de forma a garantir que segue as melhores práticas e procedimentos na tipificação de incidentes de segurança		2
		Gestão de eventos de cibersegurança	A organização não tem definido um processo para gestão do ciclo de vida de eventos de cibersegurança	A organização não tem definido um processo para gestão do ciclo de vida de eventos de cibersegurança. Contudo, são recolhidos, analisados e tratados determinados eventos, mas apenas quando sucedem alertas ou incidentes de segurança	A organização tem definido um processo para gestão do ciclo de vida de eventos de cibersegurança. A operacionalização deste processo é realizada pela equipa de cibersegurança	A organização tem definido um processo para gestão do ciclo de vida de eventos de cibersegurança. A operacionalização deste processo é realizada pela equipa de cibersegurança. Este processo é alvo de revisão regular de forma a garantir a sua atualização, adequação e abrangência às ameaças que surgem no dia a dia		3

		Seleção de eventos de segurança	A organização não tem instituída uma norma ou guia que defina quais os eventos de segurança que devem ser produzidos e recolhidos	A organização não tem formalmente instituída uma norma ou guia que defina quais os eventos de segurança que devem ser produzidos e recolhidos como objeto de "alimentar" a monitorização de cibersegurança, embora algumas fontes estejam configuradas para produzir eventos de segurança por defeito, mas não existe um *standard*	A organização tem formalmente instituído normativo define quais os eventos de segurança que devem ser produzidos e recolhidos como objeto de monitorização de segurança	A organização tem formalmente instituído uma norma que define quais os eventos de segurança que devem ser produzidos e recolhidos como objeto de monitorização de cibersegurança. Esta norma "mapeia" os casos de uso implementados na monitorização, sendo assim alvo de atualizações constantes por forma a refletir todos os casos de uso que vão sendo implementados		3
		Frequência definida para revisão de eventos de segurança	Não existe uma frequência ou regularidade definida para revisão de eventos de segurança	Não está definida uma frequência ou regularidade formal para rever eventos de segurança. Esta revisão ocorre de forma ad-hoc em resultado de alertas ou incidentes de cibersegurança ocorridos	A organização tem implementado um processo de revisão dos eventos de segurança produzidos e recebidos com objetivo de cumprirem com os casos de uso existentes	A organização tem implementado um processo de revisão dos eventos de segurança produzidos e recebidos de forma regular para assegurar que cada de uso definido na monitorização tem os eventos necessária para uma avaliação completa e assertiva		2
		Acesso e envio seguro aos eventos de segurança	A organização não recolhe eventos de segurança de ativos O acesso a estes eventos é feito através dos gestores de infraestrutura	A organização não recolhe eventos de segurança dos ativos. Contudo, sempre que necessário essa recolha, a mesma é processada de forma segura. O acesso a estes eventos é feito através dos gestores de infraestrutura, ficando auditado todas as operações realizadas	A organização tem definido um processo para recolha e envio de eventos de segurança de forma segura, seja para análise interna (ex. equipa de segurança, SOC,,etc...), seja para entidades externas (ex. Reguladores, entidades judiciárias,...,etc.). Os ativos (fontes) que produzem eventos, registam qualquer ação ocorrida sobre eles	A organização tem definido um processo para recolha e envio de eventos de segurança de forma segura e por meio de um canal previamente definido, seja para análise interna (ex. equipa de segurança, SOC,,etc...), seja para entidades externas (ex. Reguladores, entidades judiciárias,...,etc.). Os ativos (fontes) que produzem eventos, registam qualquer ação ocorrida sobre estes		3
		Informação sensíveis em eventos de segurança	A organização não tem definida qualquer norma ou guia que indique a informação deve ou não constar nos eventos de segurança	A organização não tem definida qualquer norma ou guia para definição da informação que deve ou não constar nos eventos de segurança. Contudo, existe sensibilização por parte das equipas em não guardar dados pessoais ou sensíveis nos eventos de segurança	A organização tem definidas normas ou guias que indicam que tipologia de informação deve ou não constar nos eventos de segurança, mediante os requisitos que constam em regulamentos como seja o RGPD, instruções da CNPD ou outros *standards*	A organização tem definidas normas que indicam que tipologia de informação deve ou não constar nos eventos de segurança dos ativos fonte, mediante os requisitos que constam em regulamentos como seja o RGPD, instruções da CNPD ou outros *standards*. Os eventos gerados são alvo de auditorias regulares para assegurar que cumprem com as normas e orientações definidas		2

		Prazos de retenção e conservação	A organização não define nem aplica prazos de retenção nos eventos de segurança	A organização não define nem aplica prazos de retenção nos eventos de segurança. Cada ativo é configurado de forma ad-hoc e de acordo com a pessoa que o configurou	A organização tem formalmente definidos prazos para retenção e conservação de eventos de segurança, quer ao nível dos ativos fonte quer ao nível do armazenamento central	A organização tem formalmente definidos prazos para retenção e conservação de eventos de segurança, quer ao nível dos ativos fonte quer ao nível do armazenamento central. Estes prazos estão alinhados com os requisitos de negócio e legais/regulamentares. Anualmente ou sempre que surjam alterações formais, estes prazos são revistos e o normativo atualizado		2
		Threat Intelligence	A organização não tem quaisquer fontes de TI internas ou externas. Apenas obtém informações públicas	A organização não tem quaisquer fontes formais de TI internas ou externas. De forma ad-hoc a equipa de segurança tem conhecimento de algumas fontes	A organização tem definido um processo de TI baseado em informações públicas do setor onde está inserida, dos diversos reguladores e de um serviço contratado	A organização tem definido um processo de TI baseado em informações públicas do setor onde está inserida, dos diversos reguladores e de um serviço contratado. Regularmente a organização revê o processo de forma a aferir a consistência do serviço contratado, procurando de forma ativa melhorá-lo e aumentar o seu âmbito		2
		Threat Hunting	A organização não tem implementado qualquer serviço de TH	A organização não tem implementado qualquer serviço de TH. Contudo, a equipa de segurança faz pequenas investigações com base em informação pública ou que recebe de forma informal	A organização tem implementado serviços de TH, contratados externamente	A organização tem implementado serviços de TH formado por equipas internas e um serviço contratado externamente, funcionando em plena articulação		2
	Tecnologia	**Ferramenta de Análise e correlação de eventos (SIEM)**	A organização não tem implementada qualquer solução baseada em SIEM	A organização não tem formalmente implementada qualquer solução baseada em SIEM. Contudo, são utilizadas de forma pontual e informal mecanismos que permitem fazer análises automatizadas e correlação de eventos de segurança	A organização tem implementada uma solução de SIEM (interna ou externalizada) que operacionaliza a automatização da monitorização de cibersegurança	A organização tem implementada uma solução de SIEM (interna ou externalizada) que operacionaliza a automatização da monitorização de cibersegurança. Regularmente são realizadas auditorias à solução e ao processo que a sustenta de forma a assegurar a sua correta operação e melhoria contínua		2

		Alarmística	A organização não tem implementada qualquer solução que permite enviar alertas/notificações ou outros meios de informar acerca de incidentes de segurança	A organização tem implementados mecanismos para o envio de alertas/notificações sobre incidentes de segurança, embora predomine um elevado valor de falsos positivos atendendo que não é realizada qualquer triagem	A organização tem implementados mecanismos para o envio de alertas/notificações sobre incidentes de cibersegurança.	A organização tem implementados mecanismos para o envio de alertas/notificações sobre incidentes de cibersegurança. Estes alertas de criticidade mais reduzida são automatizados, sendo os restantes procedidos de um contato pela equipa de monitorização. A organização revê regularmente os casos de uso que despoletam os alertas/notificações de forma a torná-los mais assertivos e evitar que as equipas percam o foco perante casos realmente importantes e críticos		2
		Armazenamento de eventos de segurança	A organização não recolhe quaisquer eventos dos ativos que os produzem	A organização não recolhe formalmente eventos de segurança dos ativos. Num cenário de incidente os eventos são recolhidos de forma ad-hoc e armazenados em localizações temporárias e depois removidos	Os eventos de segurança são recolhidos dos ativos e encaminhados para um repositório centralizado, onde é possível fazer pesquizas rápidas	Os eventos de segurança recolhidos dos ativos e encaminhados para um repositório centralizado, onde é possível fazer pesquizas rápidas sobre qualquer evento de qualquer fonte, caso ainda não tenha sido ultrapassado o prazo de retenção. A solução de armazenamento de eventos é monitorizada em modelo 24x7x365 para assegurar a sua permanente disponibilidade assim como o espaço disponível/ocupado		2
		Monitorização ativa de cibersegurança em postos de trabalho, servidores e ativos de rede	A organização não possui qualquer solução para deteção de comportamento anómalo nos seus ativos	A organização não possui qualquer solução para deteção de comportamento anómalo nos seus ativos. Em cenários de alerta ou incidentes de cibersegurança são executadas algumas aplicações (muitas vezes baseadas em *freeware* ou *shareware) para análise dos ativos*	A organização possui parte do seu parque tecnológico dotado de uma solução que permite a monitorização e reposta em tempo real para comportamentos anómalos de colaboradores e respetivos equipamentos (XDR)	A organização possui o seu parque tecnológico dotado de uma solução que permite a monitorização e reposta em tempo real para comportamentos anómalos dos colaboradores e respetivos equipamentos (XDR) no caso de postos de trabalho e servidores. Para equipamentos de rede são utilizados IDS, WAF e firewall		3

		Cobertura na monitorização de cibersegurança	A organização não tem uma cobertura formal de todos os seus ativos no que respeita à monitorização de cibersegurança	A organização não tem uma cobertura formal de todos os seus ativos no que respeita à monitorização de segurança, embora existam ativos é dado um maior foco e importância pela criticidade que representam	A organização tem uma monitorização total dos seus ativos, embora não tenha uma equipa a suportar essa monitorização em 24x7x365	A organização tem uma monitorização total dos seus ativos com uma equipa dedicada a suportar essa monitorização em 24x7x365		3
		Segurança no correio eletrónico	A organização não tem implementado qualquer controlo de segurança sobre os emails recebidos pelos seus colaboradores	A organização tem implementado alguns controlos de segurança para melhorar a segurança sobre os emails recebidos pelos seus colaboradores	A organização tem definidas e implementadas políticas e mecanismos para bloqueio/reter emails que representam uma ameaça para a organização	A organização tem definidas e implementadas políticas e mecanismos para bloqueio/retenção de emails que representem uma ameaça para a organização, impedindo que estes chegam aos colaboradores. Estes mecanismos são atualizados automaticamente com informação proveniente de fontes de Threat Intelligence e Threat Hunting		2
		Gestão e monitorização de impressoras	A organização não tem implementado controlos com objetivo de gerir e monitorizar o parque de impressão	A organização não tem implementado controlos com objetivo de gerir e monitorizar o parque de impressão. Contudo, os administradores de sistemas implementam de forma ad-hoc determinados controlos, mas não de forma formal nem abrangem todos os servidores de impressão	A organização tem implementado controlos com objetivo de gerir e monitorizar o parque de impressão. As impressoras são geridas centralmente e atualizadas assim que surjam atualizações pelos fabricantes. Os servidores de impressão são alvo de monitorização e atualizados de acordo com o ciclo pré-definido	A organização tem implementado controlos com objetivo de gerir e monitorizar o parque de impressão. As impressoras são geridas centralmente e atualizadas assim que surjam atualizações pelos fabricantes. Os servidores de impressão são alvo de monitorização e atualizados de acordo com o ciclo pré-definido. A utilização de impressoras locais não está autorizada por defeito		2
		Análise aos ficheiros na rede e pastas partilhadas	A organização não tem implementado qualquer controlo de segurança para identificar e analisar ameaças na rede e em pastas partilhadas	A organização não tem implementado qualquer controlo de segurança para identificar e analisar ameaças na rede e pastas partilhadas. Perante um cenário de ameaça, são utilizadas soluções ad-hoc	A organização tem definidas e implementadas políticas e mecanismos que permitem monitorizar em tempo real atividade maliciosas na rede em concreto nas pastas partilhadas	A organização tem definidas e implementadas políticas e mecanismos que permitem monitorizar em tempo real atividades maliciosas na rede em concreto nas pastas partilhadas. Estes mecanismos são atualizados automaticamente com informação proveniente de fontes de Threat Intelligence e Threat Hunting		2
								2,22

Gestão de vulnerabilidades técnicas	**Normativo de suporte**	**Formalização de um processo para gestão de vulnerabilidades**	A organização não tem formalizado um processo para gestão de vulnerabilidades	A organização não tem formalizado um processo para gestão de vulnerabilidades. Contudo, existe documentação e procedimentos que servem de guia orientador e suportam as atividades associadas à gestão de vulnerabilidades	A organização tem formalizado um processo para gestão de vulnerabilidades documentado em políticas, normas, processos e procedimentos	A organização tem formalizado um processo para gestão de vulnerabilidades documentado em políticas, normas, processos e procedimentos. Este processo é alvo de monitorização regular para garantir a sua abrangência e adequação aos requisitos de segurança organizacionais		3
		Operacionalização do processo	A organização não segue um processo formal para operacionalizar a gestão de vulnerabilidades. As vulnerabilidades são geridas caso a caso sem qualquer formalismo	A organização não segue um processo formal para operacionalizar a gestão de vulnerabilidades. Contudo, são seguidas orientações e procedimentos informais para operacionalizar a identificação, analisar/classificação, tratamento, revalidação, monitorização de vulnerabilidades	A organização têm formalizado e instituído um processo para operacionalizar a identificação, análise/classificação, tratamento revalidação, monitorização de vulnerabilidades	A organização têm formalizado e instituído um processo para operacionalizar a identificação, análise/classificação, tratamento revalidação, monitorização de vulnerabilidades. Este processo é alvo de monitorização regular para garantir a sua adequação e abrangência transversal a toda a organização, incluindo novos ativos que vão sendo desenvolvidos e integrados no seio da organização		3
		Repositório centralizado de vulnerabilidades	A organização não possui um repositório centralizado para gestão de vulnerabilidades	A organização não possui um repositório centralizado para gestão de vulnerabilidades. Existem diversos repositórios não formais que armazenam diversos tipos de vulnerabilidades	A organização possui um repositório centralizado para gestão de vulnerabilidades, embora possam existir outros repositórios para vulnerabilidades específicas	A organização possui um repositório único e centralizado para gestão de vulnerabilidades		3
	Identificação	**Processo de identificação**	A organização não tem formalizado um processo específico para identificação de vulnerabilidades	A organização não tem formalizado um processo específico para identificação de vulnerabilidades. Contudo, existem procedimentos que servem de guia orientador e suportam as atividades associadas à identificação de vulnerabilidades	A organização tem formalizado um processo específico para identificação de vulnerabilidades	A organização tem formalizado um processo específico para identificação de vulnerabilidades. Este processo é alvo de monitorização e avaliação regular para garantir a sua abrangência e adequação aos requisitos de segurança organizacionais		3

		Tecnologias IOT	A organização não executa testes específicos para identificar vulnerabilidades em tecnologias IOT	A organização não executa formalmente testes para identificar vulnerabilidades em tecnologias IOT. Contudo, participa e consulta fóruns da especialidade e dos respetivos fabricantes para obter informação sobre vulnerabilidades. Com base na informação recolhida, são realizados testes ad-hoc para identificar vulnerabilidades	A organização executa de forma regular testes para identificar vulnerabilidades em tecnologias IOT	A organização executa de forma regular testes para identificar vulnerabilidades em tecnologias IOT. Regularmente a organização avalia a forma como as tarefas são executadas para assegurar a sua adequação e abrangência		2
		Tecnologias *Cloud*	A organização não executa testes específicos para identificar vulnerabilidades em tecnologias cloud	A organização não executa formalmente testes específicos para identificar vulnerabilidades em tecnologias *cloud*. Contudo, são executados testes ad-hoc para identificação de vulnerabilidades semelhantes às que são realizadas nas restantes tecnologias	A organização tem definidos critérios e tarefas especificas para identificar vulnerabilidades em tecnologias *cloud*	A organização tem definidos critérios e tarefas especificas para identificar vulnerabilidades em tecnologias *cloud.* Anualmente são realizadas reuniões com os fornecedores dos serviços de *cloud* para avaliar a adequação nos processos implementados para identificar vulnerabilidades nestas tecnologias		3
		Equipamentos de rede (routers, switches,	A organização não executa testes específicos sejam externos ou internos para identificar vulnerabilidades em tecnologias e ativos de rede	A organização não executa formalmente testes específicos, externos ou internos para identificar vulnerabilidades em tecnologias e ativos de rede. Contudo, são executados testes ad-hoc, embora sem uma regularidade ou âmbito definido	A organização executa de forma regular testes internos e externos para identificar vulnerabilidades em tecnologias e ativos de rede	A organização executa de forma regular testes internos e externos para identificar vulnerabilidades em tecnologias e ativos de rede. Regularmente a organização avalia a forma como os testes são executados para assegurar a sua adequação e abrangência		3
		Equipamentos móveis (telemóveis, smartphones, tablets,,etc.)	A organização não executa testes específicos para identificar vulnerabilidades em tecnologias móveis	A organização não executa formalmente testes específicos para identificar vulnerabilidades em tecnologias e ativos móveis. Contudo, são executados testes ad-hoc para identificação, embora de carácter mais geral como seja em cenário de incidente de segurança, ou mediante conhecimento de uma(s) vulnerabilidade(s) crítica	A organização executa de forma regular testes para identificar vulnerabilidades em tecnologias e equipamentos móveis	A organização executa de forma regular testes para identificar vulnerabilidades em tecnologias e ativos móveis. Regularmente a organização avalia a forma como os testes são executados para assegurar a sua adequação e abrangência		2

		Equipamentos sem fios (WiFi)	A organização não executa testes específicos para identificar vulnerabilidades em tecnologias sem fios	A organização não executa formalmente testes específicos para identificar vulnerabilidades em tecnologias e ativos sem fios. Contudo, são executados testes ad-hoc para identificação, embora de carácter mais geral como seja em cenário de incidente de segurança, ou mediante conhecimento de vulnerabilidade(s) crítica	A organização executa de forma regular testes para identificar vulnerabilidades em tecnologias e ativos sem fios	A organização executa de forma regular testes para identificar vulnerabilidades em tecnologias e ativos sem fios. Regularmente a organização avalia a forma como os testes são executados para assegurar a sua adequação e abrangência		3
		Novas vulnerabilidades (0-day)	A organização não executa testes para identificar novas vulnerabilidades em qualquer dos seus ativos	A organização não executa formalmente e com uma regularidade definida testes para identificar novas vulnerabilidades em qualquer dos seus ativos. Pontualmente são executados testes com vista a identificar vulnerabilidades novas em ativos com maior criticidade e exposição	A organização tem implementado um processo contempla a realização de testes regulares com objetivo de identificar novas vulnerabilidades nos seus ativos	A organização tem implementado um processo que contempla a realização de testes regulares com objetivo de identificar novas vulnerabilidades nos seus ativos. Este processo é alvo de revisão periódica para avaliar a sua adequação e abrangência em função da criticidade de cada ativo		3
		Equipas executantes	A organização não tem uma equipa interna ou externa para realização de testes com vista a identificar vulnerabilidades nos ativos	A organização não tem uma equipa interna ou externa para realização de testes com vista a identificar vulnerabilidades nos ativos. Pontualmente são solicitados testes de vulnerabilidades a parceiros	A organização dispõe de uma equipa para realizar testes para deteção de vulnerabilidades nos ativos	A organização possui uma equipa interna dedicada a realizar testes para identificar vulnerabilidades nos ativos. Existe ainda uma equipa externa contratada para realizar testes de específicos em determinados domínios e em ativos que requerem uma maior especificidade/complexidade. As equipas internas e externas interagem entre si para melhor articulação das tarefas		2

		Desenvolvimento interno	A organização não tem definido um processo formal para realização de testes sobre vulnerabilidades nas aplicações desenvolvidas internamente	A organização não tem definido um processo formal para realização de testes sobre vulnerabilidades nas aplicações desenvolvidas internamente. Contudo, as soluções mais críticas são alvo de testes antes de serem colocadas em produção	A organização tem definido um processo formal para realização de testes a vulnerabilidades nas aplicações desenvolvidas internamente antes que sejam colocadas em produção	A organização tem definido um processo formal para realização de testes sobre vulnerabilidades nas aplicações desenvolvidas internamente antes que sejam colocadas em produção. O processo é revisto regularmente de forma a assegurar a sua adequação, abrangência e inclusão de novos métodos		2
		Desenvolvimento externo	A organização não tem definido um processo formal para realização de testes a vulnerabilidades nas aplicações desenvolvidas por terceiros para uso na organização	A organização não tem definido um processo formal e regular para realização de testes a vulnerabilidades nas aplicações desenvolvidas por terceiros para uso na organização. Contudo, pontualmente são realizados testes embora só aos ativos de maior criticidade	A organização tem definido um processo formal para realização de testes sobre vulnerabilidades nas aplicações desenvolvidas por terceiros para uso na organização. Contudo, o âmbito dos testes está bem definido, previamente acordado e aceite pelo parceiro. A realização destes testes ocorrem obrigatoriamente antes da entrada em produção	A organização tem definido um processo formal para realização de testes sobre vulnerabilidades nas aplicações desenvolvidas por terceiros para uso na organização. Contudo, o âmbito dos testes está bem definido, previamente acordado e aceite pelo parceiro. A organização revê periodicamente este processo de forma a estar alinhado com a criticidade dos ativos e requisitos de segurança, sendo também definidas métricas para avaliar o processo. A realização destes testes ocorrem obrigatoriamente antes da entrada em produção		2
		Análise aplicacional periódica	A organização não tem definido um processo formal para regularmente executar de testes sobre vulnerabilidades aplicacionais	A organização não tem definido um processo formal para regularmente executar de testes sobre vulnerabilidades aplicacionais. Os testes são realizados de forma ad-hoc e apenas em ativos classificados com maior criticidade	A organização tem definido um processo formal para regularmente executar de testes sobre vulnerabilidades aplicacionais em linha com o normativo existente para o efeito. Os testes realizados incluem análise estática e dinâmica de código	A organização tem definido um processo formal para regularmente executar de testes sobre vulnerabilidades aplicacionais em linha com o normativo existente para o efeito. Periodicamente a organização revê o processo de forma a assegurar a sua adequação, abrangência e eficácia, sendo também definidas métricas que para avaliar o processo. Os testes realizados incluem análise estática e dinâmica de código		2
		Tecnologia para deteção de vulnerabilidades	A organização não utiliza soluções especificas para identificar vulnerabilidades	A organização não tem formalmente definidas soluções para identificar vulnerabilidades. Contudo, utiliza de forma ad-hoc soluções gratuitas (shareware, freeware) para deteção e análise	A organização tem formalmente definidas e implementadas soluções para identificar vulnerabilidades	A organização tem formalmente definidas e implementadas soluções para identificar vulnerabilidades. regularmente são avaliadas todas as soluções utilizadas para identificar soluções para garantir que cumprem com os requisitos de segurança, abrangentes e adequadas face aos ativos organizacionais		3

	Classificação	**Escala de classificação**	A organização não tem adotada uma *framework* para classificação de vulnerabilidades	A organização não tem adotada uma *framework* para classificação de vulnerabilidades. Para as vulnerabilidades identificadas internamente é atribuída uma classificação com base na criticidade do ativo	A organização utiliza uma *framework* para classificação de vulnerabilidades	A organização utiliza uma *framework* para classificação de vulnerabilidades. Periodicamente é feita uma revisão assim como uma comparação com outras *frameworks* de forma a assegurar que são utilizados os mais corretos critérios. Sempre que uma framework é atualizada a organização reflete isso nos seus processos internos		2
		Reclassificação de vulnerabilidades	A organização não tem formalizado um processo para rever e reclassificar vulnerabilidades	A organização não tem formalizado um processo para rever e reclassificar vulnerabilidades . Contudo, informalmente é feita uma análise às vulnerabilidades de maior criticidade que pode resultar numa reclassificação	A organização tem formalizado um processo para rever e reclassificar vulnerabilidades mediante a não materialização e/ou aplicabilidade ao contexto organizacional	A organização tem formalizado um processo para rever e reclassificar vulnerabilidades mediante a não materialização e/ou aplicabilidade ao contexto organizacional podendo envolver áreas internas e externas à organização mediante o ativo em causa. O processo é avaliado regularmente sendo analisados os critérios de reclassificação		2
	Mitigação e fecho	**Identificação do plano de mitigação**	A organização tem instituído um processo para apoiar na definição do plano de mitigação adequado a cada vulnerabilidade	A organização não tem instituído um processo para apoiar na definição do plano de mitigação adequado a cada vulnerabilidade. Contudo, para as vulnerabilidades de maior criticidade é definida de forma ad-hoc uma solução de mitigação	A organização tem instituído um processo para apoiar na definição do plano de mitigação adequado a cada vulnerabilidade. A solução é discutida com a área de segurança em linha com o normativo interno no que respeita ao prazo definido para cada criticidade	A organização tem instituído um processo a seguir para apoiar na definição do plano de mitigação adequado a cada vulnerabilidade. A solução é discutida com a área de segurança em linha com o normativo interno no que respeita ao prazo definido para cada criticidade. Este processo é alvo de monitorização e avaliação regular para garantir a sua adequação, abrangência e cumprimento com o normativo em vigor e requisitos de segurança instituídos		2
		Processo de mitigação	A organização não tem formalizado um processo específico para mitigação de vulnerabilidades	A organização não tem formalizado um processo específico para mitigação de vulnerabilidades. Contudo, existem procedimentos que servem de guia orientador e suportam as atividades associadas à mitigação de vulnerabilidades	A organização tem formalizado um processo específico para mitigação de vulnerabilidades. Somente após a confirmação da resolução, é executado o fecho da vulnerabilidade	A organização tem formalizado um processo específico para mitigação de vulnerabilidades. Este processo é alvo de monitorização e avaliação regular para garantir a sua abrangência e adequação aos requisitos de segurança organizacionais. Somente após se confirmar a resolução, a vulnerabilidade é fechada		2

		Responsabilidade pela mitigação	A organização não tem definido um processo que apoie na identificação e atribuição de um responsável pelo tratamento de cada vulnerabilidade identificada	A organização não tem formalmente definido um processo que suporte a identificação e atribuição de um responsável pelo tratamento de cada vulnerabilidade identificada. Contudo, é feita uma atribuição ad-hoc em função da área onde o ativo se localiza	A organização tem definido um processo para apoiar na identificação e atribuição de um responsável pelo tratamento de cada vulnerabilidade identificada	A organização tem definido um processo para identificação e atribuir de um responsável (interno ou externo) pelo tratamento de cada vulnerabilidade identificada. Periodicamente o processo é revisto e atualizado		2
		Objetivos e métricas de mitigação	A organização não tem definidos objetivos nem métricas para mitigação de vulnerabilidades	A organização não tem formalmente definidos objetivos nem métricas para mitigação de vulnerabilidades. Contudo, para as de maior criticidade é dado um maior foco e urgência na sua mitigação	A organização tem definidos objetivos e métricas mensais para mitigação de vulnerabilidades	A organização tem definidos objetivos e métricas mensais para mitigação de vulnerabilidades. Estas métricas são formalizadas transversalmente por cada área que tem envolvimento na mitigação de vulnerabilidades. Os contratos com parceiros preveem SLAs para assegurar que os prazos de tratamento mapeiam as métricas organizacionais. Sempre que existe atualização nos tempos de mitigação, estes são partilhados e discutidos com os diversos parceiros de forma a existir concordância com o seu cumprimento		2
	Monitorização	**Processo**	A organização não tem definido um processo ou procedimento para reavaliação de vulnerabilidades após a sua mitigação e assim garantir que podem ser fechadas	A organização não tem definido um processo ou procedimento para reavaliação de vulnerabilidades após a sua mitigação e assim garantir que podem ser fechadas. A revalidação é executada de forma ad-hoc e sem seguir um processo formal	A organização tem definido um processo ou procedimento para reavaliação de vulnerabilidades após a sua mitigação e assim garantir que podem ser fechadas. Neste processo são estipulados as forma de revalidação a utilizar, bem como os prazos para ocorrerem	A organização tem definido um processo ou procedimento para reavaliação de vulnerabilidades após a sua mitigação e assim garantir que podem ser fechadas. Estão definidos testes específicos a realizar, tais como testes de regressão. Caso o tratamento não tenha sido o mais eficaz, o mesmo é avaliado num fórum específico (CAB). Regularmente o processo é analisado, sendo também definidas métricas que permitem aferir a eficácia dos planos de tratamento		3

		Revalidação automatizada de vulnerabilidades	A organização não utiliza uma solução que automatiza a revalidação de vulnerabilidades	A organização não utiliza uma solução que automatiza a revalidação de vulnerabilidades. Contudo, pontualmente são realizadas revalidações com recurso a ferramentas gratuitas apenas para as vulnerabilidades de maior criticidade	A organização tem operacionalizada uma solução que automatizam a revalidação de vulnerabilidade. Somente após a confirmação, é executado o fecho da vulnerabilidade	A organização tem operacionalizadas diversas soluções que automatizam a revalidação de vulnerabilidades, mediante a tipologia do ativo onde a mesma foi identificada. O processo é totalmente automatizado, através de fluxo que são criados automaticamente quando a vulnerabilidade é registada. Somente após a confirmação, é executado o fecho da vulnerabilidade	2
		Exceções	A organização não tem instituído um processo formal para monitorização de vulnerabilidades que não foram alvo de mitigação	A organização não tem instituído um processo formal para monitorização de vulnerabilidades que não foram alvo de mitigação, apenas as vulnerabilidades de maior criticidade são alvo de monitorização	A organização tem instituído um processo formal para monitorização de vulnerabilidades que não foram alvo de mitigação por assim se ter decidido	A organização tem instituído um processo formal para monitorização de vulnerabilidades que não foram alvo de mitigação por assim se ter decidido. Este processo é revisto periodicamente e avaliada a sua adequação e abrangência em linha com a gestão de risco nos sistemas de informação	3
							2,46
Resposta a incidentes de segurança	**Governação**	**Política, norma e processo**	A organização não tem definida uma política, norma ou processo para resposta a incidentes de segurança	A organização não tem definida uma política, norma ou processo para resposta a incidentes de segurança. Informalmente são seguidos procedimentos e guias para apoiar na resposta a incidentes de segurança	A organização tem definida uma política, norma e processo para formalizar a resposta a incidentes de segurança	A organização tem definida uma política, norma e processo para formalizar a resposta a incidentes de segurança. Periodicamente é feita uma revisão ao normativo de forma a manter a sua adequação ao contexto organizacional e às novas tipologias de incidentes	2
	Equipa	**Equipa dedicada para resposta a incidentes**	A organização não tem constituída uma equipa para responder a incidentes de segurança	A organização não tem constituída uma equipa para responder a incidentes de segurança. A resposta é dada de forma individual e ad-hoc	A organização dispõe de uma equipa dedicada (CSIRT) para dar resposta a incidentes de segurança	A organização dispõe uma equipa dedicada (CSIRT) para dar resposta a incidentes de segurança elementos com competências variadas e capazes de responder às mais diversas tipologias de incidentes de segurança.	2
		Análise forense	A organização não tem constituída uma equipa com capacidade de realizar uma análise forense	A organização não tem constituída uma equipa com capacidade de realizar uma análise forense. Na eventualidade de ser necessário, é contratado um serviço externo específico para a situação em causa	A organização não tem constituída uma equipa com capacidade de realizar uma análise forense. Contudo, está contratado um serviço externo que é invocado quando necessário	A organização tem constituída uma equipa com capacidade de realizar uma análise forense	1

		Funções e responsabilidades	A organização não tem formalizada nem materializada a definição de funções e responsabilidades para responder a incidentes de segurança	A organização não tem formalizada nem materializada a definição de funções e responsabilidades para responder a incidentes de segurança. A equipa é de pequena dimensão, informal e sem segregação de funções entre os elementos da equipa	A organização tem formalizada e materializada a definição de funções e responsabilidades para responder a incidentes de segurança	A organização tem formalizada e materializada a definição de funções e responsabilidades para responder a incidentes de segurança. A equipa está estruturada de forma redundante para assegurar a disponibilidade permanente de elementos nas diferentes tipologias de incidentes	2
		Formação da equipa	O conhecimento da equipa é limitado para responder a incidentes de segurança	A equipa detém os conhecimentos mínimos para responder a incidentes de segurança	A equipa de resposta a incidentes possui conhecimentos e formação para execução das suas atividades especificas, possuindo um conhecimento generalizado em todos os domínios de segurança	A equipa de resposta a incidentes possui conhecimentos e formação para execução das suas atividades especificas, possuindo conhecimento generalizado em todos os domínios de segurança. Cada elemento da equipa é obrigado a definir um plano de formação anual para atualizar e reciclar os seus conhecimentos	2
		Simulacros e exercícios	Não são realizados simulacros ou outros exercícios que permitam à equipa adquirir e testar conhecimentos e práticas a seguir na resposta a incidentes de cibersegurança	Pontualmente são realizados simulacros ou outros exercícios que permitam à equipa adquirir e consolidar conhecimentos e práticas na resposta a incidentes de cibersegurança	Anualmente a organização realiza um simulacro anualmente envolvendo toda a equipa de resposta a incidentes de cibersegurança	Anualmente a organização realiza um simulacro e diversos exercícios(table top cybersecurity exercises) envolvendo toda a equipa de resposta a incidentes de cibersegurança. Estes exercícios envolvem também equipas externas que tenham sido contratadas para apoiar a organização na sua missão de responder eficientemente. Os exercícios e simulacros são revisto de forma a contemplar os diversos e mais recentemente tipologias de ciberataques	2
	Operação e execução	**Playbooks, workbooks e planos de resposta a incidentes**	A organização não tem definidos procedimentos e outros documentos que apoiam na resposta a incidentes de cibersegurança	A organização não tem definidos procedimentos e outros documentos que apoiam na resposta a incidentes de cibersegurança, embora de forma informal sejam seguidos procedimentos definidos e atualizados com base na experiência da equipa	A organização tem definidos procedimentos e outros documentos como sejam *playbooks, workbooks,,etc..,* que apoiam na resposta a incidentes de cibersegurança	A organização tem definidos procedimentos e outros documentos como sejam *playbooks, workbooks,,etc..,* que apoiam na resposta a incidentes de cibersegurança. Regularmente estes procedimentos são revistos e atualizados para abranger todos os tipos de incidentes	1

		Critérios para identificação de incidentes	A organização não tem instituído um processo com critérios definidos que permitam identificar o que são incidentes de cibersegurança. A identificação é feita ad-hoc com base com conhecimento individual	A organização não tem instituído um processo com critérios definidos que permitam identificar o que são incidentes de cibersegurança. A equipa de segurança faz a identificação com base na partilha de experiências em situações semelhantes	A organização tem instituído um processo com critérios definidos que permitam identificar o que são incidentes de cibersegurança, permitindo fácil e rapidamente distinguir de outra tipologia de incidentes	A organização tem instituído um processo com critérios definidos que permitam identificar o que são incidentes de segurança, permitindo fácil e rapidamente distinguir de outra tipologia de incidentes. Os critérios são revistos regularmente e atualizados para abranger novas tipologias de incidentes que surgem de forma constante	2
		Classificação de incidentes	A organização não tem definido critérios para atribuição de criticidade a incidentes de cibersegurança. A atribuição é feita caso a caso e baseado na experiência individual	A organização não tem definido um critério para atribuição do nível de criticidade a incidentes de cibersegurança, embora sejam seguidas algumas boas práticas nessa classificação com base na partilha de conhecimento da equipa e no historial de incidentes de características semelhantes. Por norma a criticidade do incidente está mapeada com a criticidade e exposição do ativo ou dos ativos associados ao incidente	A organização têm definidos critérios para atribuição de criticidade aos incidentes de cibersegurança. Este critério está alinhado com a criticidade do ativo e com o impacto financeiro e reputacional que o mesmo poderá ter para a organização	A organização têm definidos critério claros para atribuição de criticidade aos incidentes de cibersegurança. Este critério está alinhado com a criticidade do ativo e com o impacto financeiro e reputacional. O processo de atribuição de criticidade calcula automaticamente a criticidade em função dos casos de uso pré-definidos. Regularmente a organização revê a criticidade de cada ativo, em função dos inputs provenientes da avaliação de risco executada para cada ativo, atualizando com base nesta informação os critério	2
		Reclassificação de incidentes	A organização não tem definido critérios para reclassificar a criticidade de um incidente de cibersegurança. A classificação atribuída inicialmente é mantida até que o incidente seja fechado	A organização não tem definido critérios para reclassificar a criticidade de um incidente de cibersegurança, embora existam procedimentos informais que a equipa de resposta segue para o fazer, mas esta reclassificação ocorre pontualmente e de forma ad-hoc	A organização tem definido critérios para reclassificar a criticidade de um incidente de cibersegurança. Na fase de análise ao incidente, está prevista a sua reclassificação caso seja aplicável	A organização tem definido critérios para reclassificar a criticidade de um incidente de cibersegurança. Na fase de análise ao incidente, está prevista a sua reclassificação caso seja aplicável. Regularmente os critérios são revistos para que estejam alinhados com a criticidade dos ativos e o impacto para a organização (financeiro, reputacional,,etc.)	2

		Interação com parceiros/fornecedores	A organização não tem definido um procedimento para interagir com os seus parceiros relativamente a incidentes de cibersegurança	A organização não tem definido um procedimento para interagir com os seus parceiros relativamente a incidentes de cibersegurança. Contudo, perante um cenário de incidente é estabelecido um canal informar para comunicação entre as duas partes	A organização tem definido um procedimento para interagir com todos os seus parceiros para reporte de incidentes de cibersegurança. Este procedimento define o canal de comunicação, quem reporta o incidente e em que circunstâncias deve ser reportado	A organização tem definido um procedimento para interagir com todos os seus parceiros para reporte de incidentes de cibersegurança. Este procedimento define o canal de comunicação, quem reporta o incidente e em que circunstâncias deve ser reportado. Este procedimento é visitado e revisto regularmente e comunicado a todos os parceiros		2
	Tecnologia de suporte	**Deteção e resposta automatizada**	A organização não dispõe de tecnologia para automatizar a resposta a incidentes de cibersegurança. O processo é totalmente manual e reativo	A organização tem implementada alguma tecnologia que operacionaliza uma resposta automatizada em algumas tipologias de incidentes de cibersegurança, embora em formato 9x5	A organização tem implementada tecnologia (SOAR) que automatiza as fases do processo de resposta a incidentes de cibersegurança, embora existam ainda alguns procedimentos que não estejam totalmente integrados num formato 24x7x365	A organização tem implementada tecnologia (SOAR) que automatiza todas as fases do processo de resposta a incidentes de cibersegurança com cobertura 24x7x365		2
	Reporte	**Reporte a reguladores e supervisores**	A organização não tem definido um procedimento para reporte de incidentes de cibersegurança a entidades legais, supervisores ou setoriais. Todas as solicitações são tratadas de forma ad-hoc e sem um critério definido	A organização não tem definido um procedimento para reporte de incidentes de cibersegurança a entidades legais, supervisores ou setoriais. A comunicação é feita de forma ad-hoc, mas segue um padrão pré-definido que vem sendo atualizado ao longo do tempo	A organização tem definido critérios e procedimentos para reportar incidentes de cibersegurança a entidades legais, supervisão ou setoriais. A comunicação é feita por meio de um canal pré-definido através do responsável da segurança	A organização tem definido critérios e procedimentos para reportar incidentes de cibersegurança a entidades legais, supervisão ou setoriais. A comunicação é feita por meio de um canal pré-definido através do responsável da segurança. Os critérios assim como os procedimentos são revistos, atualizados e comunicados regularmente		1
		Recolha e envio de evidências	A organização não tem especificado um procedimento para recolha, análise e envio de evidências associadas a um pedido de entidades legais, supervisão ou setoriais. Quando existem pedidos de evidências, a organização responde de forma ad-hoc de acordo com as instruções da entidade requisitante	A organização não tem especificado um procedimento para recolha, análise e envio de evidências associadas a um pedido de entidades legais, supervisão ou setoriais. Cada pedido é processado de forma ad-hoc e enviado pelo colaborador que procedeu ao seu tratamento	A organização tem especificado um procedimento para recolha, análise e envio de evidências associadas a um pedido de entidades legais, supervisão ou setoriais. O pedido é processado de acordo com o procedimento definido, sendo avaliado e validado pelo responsável pela segurança que trata do seu envio pelo canal e da forma definida	A organização tem especificado um procedimento para recolha, análise e envio de evidências associadas a um pedido de entidades legais, supervisão ou setoriais. O pedido é processado de acordo com o procedimento definido e por uma equipa especifica a responder a esta tipologia de pedidos, sendo avaliado e validado pelo responsável pela segurança, que trata do seu envio pelo canal e da forma definida. Este procedimento é revisto e atualizado regularmente e partilhado internamente		2
								1,79

Arquitetura de segurança	**Classificação de ativos relativamente à segurança**	**Definições de segurança**	A organização não tem um processo para classificação de ativos onde se inclua a vertente de cibersegurança nas suas características	A organização não tem um processo para classificação de ativos onde se inclua a vertente de cibersegurança nas suas características, apenas classifica-os quanto à criticidade e nível de exposição ao risco	Todos os ativos organizacionais são classificados tendo em conta a vertente de cibersegurança e risco	Todos os ativos organizacionais são classificados tendo em conta a vertente de cibersegurança, risco e operação. Regularmente a classificação é revista e atualizada para refletir o valor do risco que é aferido anualmente em cada ativo, a probabilidade e o impacto resultante de um potencial incidente de segurança	1
	Detalhes sobre os ativos	**Responsável pelo ativo**	A organização não atribui um responsável aplicacional a todos os ativos	A organização não atribui formalmente um responsável aplicacional aos seus ativos, apenas aqueles que apresentam maior criticidade, fazendo-o de forma ad-hoc e sem um critério de regularidade	Todos os ativos organizacionais tem associado um responsável aplicacional que em primeira instância é quem deve assegurar que o mesmo cumpre com os requisitos de cibersegurança definidos	Todos os ativos organizacionais tem associado um responsável aplicacional que em primeira instância é quem deve assegurar que o mesmo cumpre com os requisitos de cibersegurança definidos. Regularmente a organização faz uma revisão de forma a assegurar que exista um mapeamento correto entre o responsável e o ativo	3
		Renovação de ativos	A organização não tem instituídas políticas para renovação de ativos	A organização não tem instituídas políticas para renovação de ativos, embora existam preocupações e controlos compensatórios sobre os ativos que se encontram obsoletos	A organização tem definidas políticas para renovação de ativos	A organização tem definidas políticas para renovação de ativos. Os critérios são revistos com regularidade para assegurar que qualquer ativo é renovado atempadamente, tendo por base a dificuldade, tempo necessário e impacto causado direta e indiretamente em outros ativos	3
		Isolamento de ativos obsoletos	A organização não tem instituídos processos para definir e implementar uma arquitetura que permita isolar ou implementar controlos compensatórios para ativos que se encontrem obsoletos ou vulneráveis	A organização não tem instituídos processos para definir e implementar uma arquitetura que permita isolar ou implementar controlos compensatórios para ativos que se encontrem obsoletos ou vulneráveis. Contudo, é feita uma análise de risco aos ativos nesta situação e implementados mecanismos ad-hoc que visem aumentar a segurança e robustez dos mesmos	A organização não tem instituídos processos para definir e implementar uma arquitetura que permita isolar ou implementar controlos compensatórios para ativos que se encontrem obsoletos ou vulneráveis, cuja substituição ou mitigação não seja possível sem a sua total substituição. É definida uma arquitectura especifica e temporária para estes ativos	A organização não tem instituídos processos para definir e implementar uma arquitetura que permita isolar ou implementar controlos compensatórios para ativos que se encontrem obsoletos ou vulneráveis, cuja substituição ou mitigação não seja possível sem a sua substituição. É definida uma arquitectura especifica e temporária para estes ativos. Periodicamente a organização revê e atualiza as arquitectura definidas para estes casos e força a substituição dos mesmos e assim terminar com estas soluções temporárias	2

		Soluções e ativos de terceiros	A organização não define, verifica ou valida arquiteturas de segurança sobre soluções e ativos de parceiros	A organização não define, verifica ou valida arquiteturas de segurança sobre soluções e ativos de parceiros. Contudo, guarda informação sobre estas arquiteturas. Este controlo não se aplica a soluções em modelo SaaS ou PaaS	Antes de ser contratada uma solução externa, a arquitetura é analisada pela organização de forma a cumprir com os requisitos definidos. Este controlo não se aplica a soluções em modelo SaaS ou PaaS	Antes de ser contratada uma solução externa, a arquitetura é analisada pela organização de forma a cumprir com os requisitos definidos. Periodicamente a organização solicita aos parceiros informação atualizada sobre estas arquiteturas. Este controlo não se aplica a soluções em modelo SaaS ou PaaS	2
		Políticas, normas e procedimentos	A organização não tem instituído um quadro normativo orientado a suportar a definição e implementação de arquiteturas de referência em diversas vertentes, incluindo a de cibersegurança	A organização não tem definido um quadro normativo orientado a suportar a definição e implementação de arquiteturas de referência em diversas vertentes, incluindo a de cibersegurança. Contudo, durante a fase de implementação de umas novas arquiteturas são incluídos alguns controlos	A organização tem definido um quadro normativo orientado a suportar a definição e implementação de arquiteturas de referência em diversas vertentes, incluindo a de cibersegurança	A organização tem definido um quadro normativo orientado para suportar a definição e implementação de arquiteturas de referência em diversas vertentes, incluindo a de cibersegurança. O quadro normativo é revisto e atualizado regularmente e publicado para toda a organização e parceiros	2
	Arquiteturas de referência	**Requisitos de segurança**	A organização não tem definida uma arquitetura de referência que contemple requisitos de cibersegurança	A organização não tem definida uma arquitetura de referência que contemple requisitos de cibersegurança, embora sejam definidos de forma ad-hoc determinados requisitos sobretudo quando envolve ativos de maior criticidade	A organização tem definida uma arquitetura de referência que contempla requisitos de cibersegurança	A organização tem definida uma arquitetura de referência que contempla requisitos de cibersegurança. periodicamente a organização revê e atualiza a arquitetura de referência para contemplar os mais recentes requisitos de segurança face a novos ciberataques e ameaças	1
		Arquiteturas diversificadas (cloud, onprem,,etc.)	A organização não tem definidas diferentes arquiteturas, tendo em conta o ambiente, contexto e localização das mesmas	A organização não tem definidas diferentes arquiteturas, tendo em conta o ambiente, contexto e localização das mesmas. Contudo, no que respeita a requisitos de cibersegurança são definidos alguns de forma informal	A organização tem definidas arquiteturas de referência diversificadas, mediante o contexto onde são aplicadas	A organização tem definidas arquiteturas de referência diversificadas, mediante o contexto onde são aplicadas. Regularmente são revistas, atualizadas e difundidas por todos os parceiros da organização de forma a garantir a conformidade com o requisito	2

		Acompanhamento de segurança	A organização não tem definido requisitos que obrigue ao acompanhamento e supervisão de um arquiteto de cibersegurança durante o ciclo de implementação de uma arquitetura aplicacional	A organização não tem definido requisitos que obrigue ao acompanhamento e supervisão de um arquiteto de cibersegurança durante todo o ciclo de implementação de uma arquitetura aplicacional, embora participe pontualmente e mediante solicitação da equipa aplicacional	A organização tem definido requisitos que obrigue ao acompanhamento de um arquiteto de cibersegurança durante o ciclo de implementação de uma arquitetura aplicacional. A equipa de cibersegurança tem definida uma lista de requisitos e verificações para as diferentes arquiteturas	A organização tem definido requisitos que obrigue ao acompanhamento e supervisão de um arquiteto de cibersegurança durante o ciclo de implementação de uma arquitetura aplicacional. A equipa de cibersegurança tem definida uma lista de requisitos e verificações de segurança, seguida pelos arquitetos de segurança e atualizada regularmente para contemplar novas ameaças e arquiteturas	1
		Ambientes produtivos e não produtivos	A organização tem definido um único ambiente, sobre o qual estão localizados todos os ativos e aplicações	A organização tem definido um ambiente produtivo e um ambiente não produtivo onde são desenvolvidas e testadas algumas aplicações antes de entrarem em produção	A organização tem definido e implementado quatro ambientes (desenvolvimento, pré-Produção, produção e d*isaster recover),* embora nem todas as aplicações estejam configuradas em todos eles	A organização tem definido e implementado quatro a ambientes (desenvolvimento, pré-Produção, produção e d*isaster recover).* Todas as soluções aplicacionais tem obrigatoriamente um ambiente de desenvolvimento, pré-produção e produção, sendo o ambiente de d*isaster recover* configurado apenas para as soluções com RTO e RPO mais críticos. As exceções são registadas e revistas regularmente	3
		Segregação entre ambientes	Não existe segregação lógica e física entre ambientes	Não existe segregação lógica e física entre ambientes em termos de arquitetura, embora determinados componentes estejam segregados entre o que é produtivo e não produtivo	A arquitetura define requisitos de segregação entre cada um dos ambientes, embora possam existir componentes comuns, sobretudo ao nível físico	A arquitetura define requisitos de segregação entre cada um dos ambientes. Exceções estão previstas e são devidamente avaliadas. Periodicamente é feita de revisão para assegurar uma revalidação do risco e necessidade em manter as exceções	3
	Alta disponibilidade e resiliência	**Redundância**	A organização não têm definidos requisitos ou critérios para avaliar a necessidade de implementar redundância aplicacional	A organização não têm definidos requisitos ou critérios para avaliar a necessidade de implementar redundância aplicacional. Contudo, existe consciencialização sobre a criticidade de algumas aplicações, levando à implementação de controlos compensatórios para assegurar redundância dessas aplicações	A organização têm definidos requisitos ou critérios para avaliar a necessidade de implementar redundância aplicacional com base no resultado dos BIA (Business Impact Analysis) realizados às aplicações	A organização têm definidos requisitos ou critérios para avaliar a necessidade de implementar redundância aplicacional com base no resultado dos BIA (Business Impact Analysis) realizados às aplicações. Regularmente a organização procede à atualização dos BIA de forma a assegurar que refletem a verdadeira criticidade da solução no decorrer do seu ciclo de vida	3
							2,17

Segurança do software	**Conformidade**	**Políticas, normas, processos e procedimentos**	Não existe normativo associado à segurança do software, em particular sobre aquele que é desenvolvimento internamente	Não existe normativo associado à segurança do software, em particular sobre aquele que é desenvolvimento internamente. Contudo, são seguidas boas práticas, como seja a não utilização de protocolos inseguros, cifras fracas ou bibliotecas obsoletas	Existe normativo associado à segurança do software, seja desenvolvido internamente ou adquirido	Existe normativo associado à segurança do software, seja desenvolvido internamente ou adquirido. Este normativo é revisto e atualizado regularmente e partilhado com todos os parceiros e fornecedores de forma a cumprirem com os requisitos definidos	2
		Prevenção contra exfiltração de dados	Não está definido um processo com controlos para prevenir a exfiltração de dados	Não está definido um processo com controlos para prevenir a exfiltração de dados. O controlo é feito sob uma perspetiva teórica e com alguns controlos implementados ad-hoc	Encontra-se definido um processo com controlos para prevenir a exfiltração de dados	Encontra-se definido um processo com controlos para prevenir a exfiltração de dados, incluindo o acesso a portais que permitam identificar e corrigir bugs no código desenvolvido	3
		Aquisição de software de terceiros	Não é seguido nenhum processo para análise e avaliação prévia à aquisição de software a terceiros	Não existe um processo formal para avaliação a softwares de terceiros. Esta avaliação é feita ad-hoc e essencialmente teórica e baseada em informação pública sobre o software em causa	Existe um processo formal para avaliação a softwares de terceiro assim como o próprio fornecedor. Esta avaliação é feita através de diversos questionários que avaliam em diferentes vertentes a aplicação com particular foco na cibersegurança. Estes questionários são atualizados de forma regular para refletirem novos requisitos em matéria de cibersegurança.	Existe um processo formal para avaliação a softwares de terceiro assim como o próprio fornecedor. Esta avaliação é feita através de diversos questionários que avaliam em diferentes vertentes a aplicação com particular foco na cibersegurança. Estes questionários são atualizados de forma regular para refletirem novos requisitos em matéria de cibersegurança. Em certos casos podem ser realizados testes de segurança à aplicação em causa mediante um acordo formal entre as partes. Geralmente é realizado um piloto (prova de conceito) interna que permite testar as funcionalidades da aplicação antes de se avançar com a aquisição	2
		Repositório centralizado para código	Não existe um repositório centralizado onde é armazenado todo o código aplicacional desenvolvido internamente	Não existe um repositório centralizado onde é armazenado todo o código aplicacional desenvolvido internamente. Contudo, estão implementados controlos compensatórios que visam assegurar que o código desenvolvido não sai da organização	Existe um repositório centralizado onde é armazenado todo o código aplicacional desenvolvido internamente. Este repositório é abrangido pela política de gestão de acessos, ficando o registo de cada acesso realizado	Existe um repositório centralizado onde é armazenado todo o código aplicacional desenvolvido internamente e sobre o qual ocorrem testes regulares. Este repositório é abrangido pela política de gestão de acessos, ficando o registo de cada acesso realizado. Adicionalmente, todos os desenvolvimentos são realizados nos ativos internos de forma a evitar qualquer exfiltração	3

		Metodologia de desenvolvimento	Não é seguida uma metodologia de desenvolvimento de software	Não é seguida uma metodologia formal para desenvolvimento de software. Contudo, são seguidos critérios e práticas que cobrem todo o ciclo de vida de um software	É seguida uma metodologia para desenvolvimento que contempla todas as fases do SDLC	É seguida uma metodologia para desenvolvimento que contempla todas as fases do SDLC. A metodologia é revista regularmente para assegurar que a área de cibersegurança tem participação ativa neste processo através da definição de requisitos e realização de testes de segurança	3
		Desenvolvimento interno e externo	O desenvolvimento aplicacional pode ser realizado por equipas internas ou externas à organização sem que haja um processo definido que regula esse desenvolvimento	O desenvolvimento aplicacional pode ser realizado por equipas internas ou externas à organização sem que haja um processo formal definido que regula esse desenvolvimento, embora estejam definidos alguns procedimentos e regras sobre a forma como a equipas externas devem realizar o seu trabalho	O desenvolvimento aplicacional pode ser realizado por equipas internas ou externas à organização com base num processo definido que estipula regras e procedimentos	O desenvolvimento aplicacional pode ser realizado por equipas internas ou externas à organização com base num processo definido que estipula regras e procedimentos. Este processo é revisto e atualizado regularmente e partilhado com todas as partes interessadas	2
		Segurança e privacidade por omissão e por desenho	Não existem cláusulas ou requisitos que obriguem à implementação de mecanismos de segurança e privacidade por omissão e desenho	Não existem cláusulas ou requisitos que obriguem à implementação de mecanismos de segurança e privacidade por omissão e desenho, embora sejam adotados de forma ad-hoc procedimentos que contemplam segurança e privacidade por omissão e defeito nas soluções de maior criticidade	Existem cláusulas ou requisitos que obrigam à implementação de mecanismos de segurança e privacidade por omissão e desenho	Existem cláusulas ou requisitos que obrigam à implementação de mecanismos de segurança e privacidade por omissão e desenho. As cláusulas e requisitos são revistos e atualizados regularmente para assegurar a sua adequação e abrangência, sendo partilhados com todas as partes interessadas	3
	Gestão de alterações	**Entradas e saídas de produção**	Não está definido um processo para gerir as alterações preconizadas nas aplicações	Não está definido um processo para gerir as alterações preconizadas nas aplicações. Contudo, para as alterações em ambiente de produção é seguido um fluxo de aprovações que avaliam o risco da alteração em causa	Está definido um processo para gestão de alterações, suportado por um pedido formal em ITSM	Está definido um processo um processo para gestão de alterações, tendo obrigatoriamente de passar por um pedido formal em ITSM que é levado a um CAB semanal com todas as áreas relevantes para rever e aprovar a sua implementação	1
	Testes de segurança Aplicacionais	**Análise estática e dinâmica ao código**	Não é formalmente realizada análise estática e/ou dinâmica ao código tanto em fase de desenvolvimento como produção	Não é formalmente realizada análise estática e/ou dinâmica ao código quer em fase de desenvolvimento nem em produção. Apenas são realizadas análises e verificações de forma ad-hoc	Na metodologia SDLC seguida estão definidos requisitos para realizar análise estática e/ou dinâmica ao código tanto em fase de desenvolvimento como produção, embora nem todas as aplicações sejam alvo desta análise	Na metodologia SDLC seguida estão definidos requisitos para realizar análise estática e/ou dinâmica ao código tanto em fase de desenvolvimento como produção a todas as soluções aplicacionais desenvolvidas internamente. Exceções estão previstas mediante justificação e tendo o risco sido aceite	2

		Testes de penetração (pentesting)	Não são realizados testes de penetração às aplicações durante a fase de desenvolvimento ou pós entrados em produção	Não são formalmente realizados testes de penetração às aplicações durante a fase de desenvolvimento. Contudo, os ativos e soluções de maior criticidade sejam alvo de testes depois da entrada em produção e de forma regular	Na metodologia SDLC seguida estão definidos requisitos para a realização de testes de penetração quer em fase de desenvolvimento quer depois da entrada produção, embora nem todas as aplicações sejam alvo de testes, somente as aplicações com maior criticidade e exposição. Exceções estão previstas mediante justificação e tendo o risco sido aceite	Na metodologia SDLC seguida estão definidos requisitos para a realização de testes de penetração quer em fase de desenvolvimento quer depois da entrada em produção a todas as soluções aplicacionais. Exceções estão previstas mediante justificação e tendo o risco sido aceite		3
		Testes a API	Não são realizados testes às API invocadas pelas aplicações durante a fase de desenvolvimento ou depois da entrada em produção	Não são realizados testes às API invocadas pelas aplicações durante a fase de desenvolvimento ou depois da entrada em produção , embora sejam realizadas avaliações ad-hoc a algumas API	Na metodologia SDLC seguida estão definidos requisitos para a realização de testes às API quer em fase de desenvolvimento quer depois da entrada em produção, embora nem todas as API sejam alvo de testes, somente as aquelas que apresentem uma maior criticidade e exposição	Na metodologia SDLC seguida estão definidos requisitos para a realização de testes a todas as API desenvolvidas ou alteradas para utilização nas aplicações quer em fase de desenvolvimento quer depois da entrada em produção a todas as soluções aplicacionais. Exceções estão previstas mediante justificação e tendo o risco sido aceite		2
		Testes em modelo black box e white box	Não são realizados testes em modo black e white box às aplicações desenvolvidas pela internamente	Não são realizados testes em modo black e white box às aplicações desenvolvidas internamente. Contudo, para as soluções de maior risco e exposição são realizados testes pontuais	Estão definidos requisitos para a realização de testes em modo black e white box às soluções desenvolvidas internamente embora nem todas as soluções sejam alvo desta tipologia de testes, somente aquelas que apresentem uma maior criticidade e exposição. Estão testes em aplicações de parceiros sempre que a organização o pretenda fazer, embora requeira obrigatoriamente uma autorização prévia e formal	Na metodologia SDLC seguida estão definidos requisitos para a realização de testes em modo black e white box a todas as aplicações desenvolvidas ou que tenham sido alvo de alterações, embora nem todas as aplicações sejam alvo desta tipologia de testes. Estão testes em aplicações de parceiros sempre que a organização o pretenda fazer, embora requeira obrigatoriamente uma autorização prévia e formal. Exceções estão previstas mediante justificação e tendo o risco sido aceite		3
								2,42

Maturidade por Domínio	
Domínios	**Maturidade**
0	**2,17**
0	**2,42**
0	**3,18**

0	2,35
0	2,44
0	2,33
0	2,22
0	2,46
0	1,79
0	2,17
0	2,42
Maturidade Global	2,36