Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

AVALIAÇÃO DA MATURIDADE EM CIBERSEGURANÇA DO TECIDO INDUSTRIAL PORTUGUÊS

ANA BEATRIZ NUNES RIBEIRO

Leiria, Março de 2023

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

AVALIAÇÃO DA MATURIDADE EM CIBERSEGURANÇA DO TECIDO INDUSTRIAL PORTUGUÊS

ANA BEATRIZ NUNES RIBEIRO
2202642

Dissertação realizada sob orientação do Professor Doutor Carlos Manuel da Silva Rabadão (carlos.rabadao@ipleiria.pt) e Professor Doutor Leonel Filipe Simões Santos (leonel.santos@ipleiria.pt).

Leiria, Março de 2023

AGRADECIMENTOS

A presente dissertação de mestrado não teria sido concluída com sucesso sem o apoio de diversas pessoas. Esta dissertação foi assumida com muita dedicação, e foi uma experiência enriquecedora.

Primeiramente, queria agradecer à minha família, que sempre me apoiou e incentivou durante o meu percurso académico.

Às associações empresariais que auxiliaram na divulgação do inquérito junto dos seus associados.

Aos especialistas em Cibersegurança que ajudaram a validar as questões e estrutura do inquérito.

Entre todas as pessoas que me apoiaram nesta jornada académica, gostaria de agradecer aos meus orientadores, professor Carlos Rabadão e professor Leonel Santos, pelo acompanhamento, disponibilidade e dedicação durante o decorrer desta dissertação.

A todos que direta ou indiretamente contribuíram para a realização desta dissertação, um grande obrigado!

RESUMO

Tendo em conta que as ameaças cibernéticas são cada vez mais constantes e sofisticadas, é pertinente que administradores e até utilizadores das organizações estejam cientes e preparados para proceder em conformidade no caso de existência de perigos a que poderão estar expostos diariamente. É possível as empresas terem acesso ao seu nível de maturidade em diferentes domínios através de modelos de maturidade. A utilização destes modelos de maturidade providenciam uma avaliação da organização tendo em conta as normas mais utilizadas e boas práticas recomendadas.

Perante este cenário, a preocupação sobre a cibersegurança nas organizações tem aumentado, sendo imprescindível que estas se guiem pelas boas práticas e normas sobre a segurança da informação. A utilização de modelos de maturidade, tornam-se uns aliados das organizações na medida que providenciam uma avaliação da organização.

Assim, o principal foco desta dissertação é averiguar e avaliar o nível de maturidade em cibersegurança no tecido industrial português. De modo a avaliar o nível de maturidade, foi definida uma matriz de avaliação.

Por forma a complementar a investigação foi efetuado um estudo das normas mais utilizadas na área da cibersegurança e segurança de informação. Para aprofundar este assunto foi efetuado um mapeamento tendo como base a associação dos controlos da norma ISO/IEC 27001:2013 (Requisitos e recomendações para o desenvolvimento e operação de um SGSI) e no Roteiro para as Capacidades Mínimas de Cibersegurança do CNCS. Selecionou-se o inquérito como ferramenta para determinar o nível de maturidade em cibersegurança das organizações. Através das correlações dos controlos da norma ISO/IEC 27001:2013 e do Roteiro para as Capacidades Mínimas de Cibersegurança presentes neste mapeamento, surgiram as questões presentes no inquérito.

O caso de estudo efetuado teve como participantes 41 organizações, todas sediadas em território nacional, para determinar o seu nível de maturidade em cibersegurança. Através dos resultados obtidos foi possível averiguar e avaliar o nível de maturidade em cibersegurança do tecido industrial português.

Após analisados os resultados é possível perceber que o nível de maturidade em cibersegurança é Insuficiente.

Com a realização deste estudo, as organizações poderão utilizá-los para melhorar as suas capacidades e na definição de novas estratégias para reforçar o seu nível de

maturidade. Além disso, os resultados obtidos podem também ser vistos como uma forma de sensibilização e consciencialização sobre o tema da cibersegurança.

A metodologia de trabalho seguida é uma vantagem para analisar em que estado se encontram as organizações relativo à cibersegurança.

Palavras-chave: Segurança da Informação, Roteiro para as Capacidades Mínimas da Cibersegurança, ISO/IEC 27001:2013, Maturidade em Cibersegurança

ABSTRACT

Considering that cyber threats are increasingly constant and sophisticated, it is pertinent that administrators and even users of organizations are aware and prepared to proceed accordingly in case of dangers to which they may be exposed daily. Companies can have access to their maturity level in different domains through maturity models. The use of these maturity models provides an evaluation of the organization taking into account the most used standards and good recommended practices.

Given this scenario, the concern about cybersecurity in organizations has increased and they must be guided by good practices and standards for information security. The use of maturity models becomes an ally of the organizations as it provides an evaluation of the organization.

Thus, the main focus of this dissertation is to investigate and evaluate the level of maturity in cybersecurity in the Portuguese industrial fabric. To assess the maturity level, an evaluation matrix was defined.

To complement the research, a study of the most used standards in the area of cyber-security and information security was carried out. To deepen this subject, mapping was carried out based on the association of the controls of the ISO/IEC 27001:2013 standard (Requirements and recommendations for the development and operation of an ISMS) and the CNCS Roadmap for Minimum Cybersecurity Capabilities. A survey was selected as a tool to determine the cybersecurity maturity level of organizations. The questions in the survey emerged through the correlations of the controls of the ISO/IEC 27001:2013 standard and the Roadmap for Minimum Cybersecurity Capabilities present in this mapping.

The case study carried out had participants from 41 organizations, all based in the national territory, to determine their level of maturity in cybersecurity. Through the results obtained, it was possible to verify and assess the cybersecurity maturity level of the Portuguese industrial fabric.

After analyzing the results, it is possible to see that the level of cybersecurity maturity is insufficient.

With the accomplishment of this study, organizations may use them to improve their capacities and in the definition of new strategies to reinforce their level of maturity. Furthermore, the results obtained may also be seen as a way of raising awareness and consciousness on the subject of cybersecurity.

The work methodology followed is an advantage for analyzing the status of organizations regarding cybersecurity.

Keywords: Information Security, Roadmap for Minimum Cybersecurity Capabilities, ISO/IEC 27001:2013, Maturity in Cybersecurity

ÍNDICE

Apêndices

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ADSP	Associação de Segurança de Portugal.
AEF	Associação Empresarial de Felgueiras.
AP2SI	Associação Portuguesa para a Promoção da Segurança da Informação.
BSI	British Standards Institute.
BYOD	Bring Your Own Device.
C2M2	Cybersecurity Capability Maturity Model.
CCD	Centro de Ciberdefesa.
CIS	Center for Internet Security.
CISO	Chief Information Security Officer.
CMDB	Configuration Management DataBase.
CNCS	Centro Nacional de Cibersegurança.
CSIRT	Computer Security Incident Responde Team.
DDoS	Distributed Deniel-of-Service.
DOE	Department of Energy.
DPO	Data Protection Officer.
ENISA	European Union Agency for Cybersecutrity.
EUA	Estados Unidos da América.
HIDS	Host-based Intrusion Detection System.
IBM	International Business Machines.
IG	Implementatation Group.
IP	Internet Protocol.
ISO	International Organization for Standardization.

LIR	Local Internet Registry.
NIS	Network and Information Security.
NIST	National Institute of Standards and Technology.
PDCA	Modelo Plan Do Check Act.
PGP	Pretty Good Privacy.
PII	Personally Identifiable Information.
PIMS	Privacy Information Management System.
PME	Pequena e Média Empresa.
QNRCS	Quadro Nacional de Referência para a Cibersegurança.
RGPD	Regulamento Geral de Proteção de Dados.
SGSI	Sistema de Gestão de Segurança da Informação.
SIEM	Security Information and Event Management.
SINP	Sistema Interno de Normas e Políticas.
SOC	Security Operations Center.
TI	Tecnologia de Informação.
TIC	Tecnologia da informação e Comunicação.
UE	União Europeia.
UNC3T	Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica.

1

INTRODUÇÃO

Para acompanhar a ascensão da evolução da tecnologia e a massificação da Internet [1], toda a sociedade em geral tem sido moldada a novas formas de agir e de comunicar e, por consequência, a forma como as pessoas se relacionam nunca mais foi a mesma. Tendo em conta este crescimento exponencial, a informação e os dados são cada vez mais valorizados e priorizados, consequentemente observou-se um crescimento significativo da competitividade, modernização e inovação [2]. Porém, com este crescimento da tecnologia e da Internet surgiram novas formas de comprometer os dados dos utilizadores e ameaças mais sofisticadas [3].

A situação pandémica que se iniciou em 2020 (Covid-19) forçou a que diversos processos de negócio fossem tratados de forma diferente num plano operacional, como, por exemplo, a questão do trabalho remoto [4]. Esta forma de trabalhar impôs a que fossem implementadas e repensadas novas formas de proteger os ativos e a informação crítica.

Outrora, a preocupação das organizações era permanecerem atualizadas nas últimas tendências tecnológicas, embora que com o tempo, uma das suas inquietações se tenha tornado a cibersegurança. Este cenário da pandemia veio intensificar a operacionalização e consciencialização das organizações para este tema.

Cada vez mais a cibersegurança ganha relevância nas organizações. Com as diversas vulnerabilidades que possam existir numa organização que podem comprometer a informação e os ativos da organização, é fundamental que as organizações estejam preparadas para reagir rapidamente. Considerando estes aspetos significativos, foram desenhados conjuntos de boas práticas por entidades públicas ou privadas que definem estes guias, como, por exemplo, o Roteiro para as Capacidades Mínimas [5] que foi elaborado pelo Centro Nacional de Cibersegurança [6]. Este conjunto de normas e boas práticas podem ser aplicados a qualquer tipo de organização e através deles, ser feita uma análise das falhas existentes e ainda, medir o nível de maturidade em cibersegurança das mesmas.

Uma organização que não cumpra os requisitos mínimos de proteção torna-se um alvo fácil para os atacantes. É importante que as organizações disponham de capacidades de prevenção, deteção e reação, às ocorrências destas ameaças, por forma a prevenir danos maiores resultantes da exploração de vulnerabilidades existentes.

Perante este cenário a presente dissertação ganha relevância, pois é necessário que as organizações conheçam o nível de maturidade de cibersegurança que se encontram para poderem melhorar a sua proteção.

Com este trabalho pretende-se assim averiguar e avaliar o nível de maturidade de cibersegurança em que se encontram as organizações do tecido industrial português, sendo este o principal objetivo da dissertação. Em simultâneo, pretende-se contribuir para que as organizações possam identificar os seus pontos fortes e fracos, para as auxiliar na definição de planos e novas estratégias com intuito à melhoria dos seus níveis de maturidade em cibersegurança. Simultaneamente esta dissertação pode também servir como meio de sensibilização e consciencialização junto das mesmas. É expectável também que sejam desenvolvidas as medidas necessárias para atingirem a conformidade com as boas práticas recomendadas nesta área.

Outro objetivo da realização desta dissertação é efetuar uma caracterização do tecido industrial em Portugal relativamente a este risco supra indicado, da segurança da informação, e perceber quais as práticas que estão já a ser priorizadas e implementadas nas organizações. Para ser efetuada esta caracterização do tecido industrial e ser posteriormente determinado o nível de maturidade em cibersegurança foi selecionado o inquérito como uma ferramenta de diagnóstico com o intuito de avaliar e averiguar o nível de maturidade em cibersegurança das organizações. Após analisados todos os resultados obtidos, existem dados suficientes para se obter uma visão geral do nível de maturidade das organizações.

Conforme o enquadramento efetuado, surgiram algumas questões que orientaram esta investigação:

- Será possível conhecer e aferir a maturidade em cibersegurança do tecido industrial português?
- Como se pode averiguar o nível de maturidade em cibersegurança de uma organização?
- Que normas/boas práticas se podem utilizar no referencial para calcular a maturidade em cibersegurança?
- Qual a melhor ferramenta para averiguar e avaliar o nível de maturidade em cibersegurança das organizações e alcançar o maior número de organizações?
- Qual a melhor forma de apresentar o nível de maturidade em cibersegurança a uma organização?

O interesse por esta área e a preocupação derivado ao elevado número de organizações que sofrem hoje em dia ataques informáticos levaram à realização da presente investigação. Sendo um tema tão relevante e cada vez mais pertinente

para as organizações, esta investigação é um grande suporte para encaminhar as organizações para um nível de segurança cada vez mais elevado.

Esta dissertação está dividida em vários capítulos, com um seguimento lógico. Estes capítulos descrevem a ordem pela qual foi desenvolvido este trabalho.

No Capítulo 2 é efetuado o enquadramento do conceito de cibersegurança e são seguidamente descritas as normas, leis e regulamentos utilizados e relacionados com a segurança da informação.

No Capítulo 3 é apresentada uma definição do termo de maturidade. São apresentados alguns trabalhos relacionados, em que são apresentadas algumas definições e diferentes formas de aferir este termo relacionado com a cibersegurança.

No Capítulo 4 é descrito todo o processo de desenvolvimento desta dissertação, desde o mapeamento das normas acima citadas e mostradas as associações encontradas entre estas duas normas, pois a partir destas associações foram criadas as perguntas que se encontram presentes no inquérito. Encontra-se também a justificação de todas as etapas de construção do inquérito, bem como a metodologia utilizada para a definição das respostas, a seleção da plataforma do inquérito e a forma de divulgação do mesmo. Ainda neste capítulo é descrita a matriz de avaliação para definição do nível de maturidade em cibersegurança.

No Capítulo 5 é apresentada a análise de dados e resultados obtidos das 41 empresas portuguesas que participaram neste estudo.

Por fim, no Capítulo 6 são apresentadas as conclusões, limitações encontradas e trabalho futuro.

2

CIBERSEGURANÇA

Neste capítulo, define-se de forma justificada o conceito de cibersegurança e o seu enquadramento nas normas existentes relativamente a esta temática.

2.1 DEFINIÇÃO DE CIBERSEGURANÇA

A transformação digital provoca a que os indivíduos e organizações se tornem cada vez mais dependentes das Tecnologias de Informação. Por consequência desta transformação a Internet passou a ser imprescindível, dando assim origem ao conceito de Ciberespaço. A vantagem de utilização do Ciberespaço [7] é o facto deste ser livre e aberto, tornando-o assim disponível a qualquer indivíduo ou organização que pretenda usufruir das mais-valias que nele podemos aproveitar.

Segundo o CNCS o conceito de cibersegurança é encarado como um conjunto de medidas e ações indispensáveis para prevenir, detetar e analisar os sistemas de informação. Este conjunto de medidas prevê garantir a integridade, disponibilidade e confidencialidade dos dados [8].

De acordo com a Microsoft, este termo consiste na proteção de informações digitais, dispositivos e recursos [9].

Conforme a APDSI, a cibersegurança consiste num conjunto de meios que aponta para a segurança de programas, computadores, redes e dados, de qualquer intrusão ilícita. Esta segurança baseia-se na Integridade, Confidencialidade e Disponibilidade da Informação [10].

Segundo a IBM, este conceito reflete-se na proteção de sistemas críticos e informação sensível perante incidentes de segurança. As medidas de cibersegurança são desenhadas para travar ameaças contra estes sistemas e dados críticos [11].

Existem diversas propostas para a definição do conceito de cibersegurança, no entanto, provavelmente a melhor definição e mais efetiva seria a fusão de duas ou mais definições.

Para garantir o bom funcionamento das tecnologias e a introdução de novos conceitos foi imperativa a definição de normas visando garantir a segurança a quem utilize o ciberespaço. Estas normas e conjuntos de boas práticas tentam evitar a utilização do ciberespaço de forma menos lícita, e auxiliam as organizações a

desenvolver as medidas necessárias para atingir a conformidade com as melhores práticas de cibersegurança.

Estas normas são instrumentos ao dispor de qualquer organização para lidar com os diversos riscos de segurança e descrevem boas práticas para que estas se tornem mais resilientes. Cada organização deve então avaliar e definir quais as normas que melhor se adequam ao seu negócio, dependendo dos processos que sigam.

Sendo esta uma área preocupante para os seus responsáveis nas organizações, ou deveria impor mais preocupação atualmente, é imprescindível perceber em que nível de maturidade em cibersegurança estas se encontram. Porém, a identificação antecipada de possíveis lacunas e vulnerabilidades existentes através de diversos tipos de testes, é fundamental para a prevenção de possíveis incidentes de segurança.

Para sustentar esta investigação foram estudadas algumas normas e conjuntos de boas práticas.

Normas, Regulamentos e Boas práticas de Cibersegurança
NIST Cybersecurity Framework
Network and Information Security
CIS Controls
ISO - International Organization for Standardization (ISO/IEC 27000)
Roteiro para as Capacidades Mínimas de Cibersegurança
Quadro Nacional de Referência para a Cibersegurança
Regulamento Geral de Proteção de Dados
Lei nº 46/2018 Regime Jurídico da Segurança do Ciberespaço
Decreto-Lei n.º 65/2021

Tabela 1: Boas práticas, regulamentos e normas de Cibersegurança

Na Tabela 1 encontram-se as normas e conjuntos de boas práticas estudadas e sendo cada uma delas apresentadas de seguida.

2.2 NORMAS, LEIS E BOAS PRÁTICAS DA CIBERSEGURANÇA

Perante estes desafios, ameaças existiu a necessidade de ser criado um documento ou guia para habilitar e apoiar as organizações e cidadãos relativamente a boas práticas relacionadas com esta temática.

Foi então publicado em 2016, pelo **National Institute of Standards Technology (NIST)** [12] a primeira versão da NISTIR 7621- "Small Business Information Security: The fundamentals".

Particularmente este guia, é direcionado para as PME, pois estas tendencialmente acreditam que pela sua dimensão reduzida não serão alvo de incidentes de cibersegurança. O foco deste guia é explicar os passos básicos em cibersegurança que as organizações devem adotar para proteger a informação e os seus ativos.

Esta *framework* fornece uma estrutura baseada nos padrões, diretrizes e práticas do setor privado dos Estados Unidos. Permite apoiar as organizações a implementar mecanismos de prevenção, deteção e explica como atuar no caso da existência de um incidente de cibersegurança. Passou a notar-se uma melhoria das comunicações entre as organizações e as entidades a quem devem ser reportados os incidentes.

Figura 1: As cinco funções da framework NIST, adaptado de[13]

Na Figura 1 estão representadas as 5 funções-chave de segurança para organizar os controlos de segurança.

A presente *framework* proposta no documento [14] é constituída por três pontos fulcrais, sendo nomeadamente, o núcleo, o perfil e os níveis de implementação da estrutura.

O núcleo é constituído por um conjunto de atividades e resultados de cibersegurança pretendidos, que permitem manter uma ligação com a gestão de risco, utilizando uma linguagem fácil de entender.

Na componente do perfil são selecionadas uma série de funções, categorias e subcategorias específicas do núcleo, escolhidas para apoiar a organização na gestão de risco de privacidade, ou seja, o perfil pretende melhorar os padrões de segurança e mitigar os riscos duma organização.

Relativamente à última componente, os níveis de implementação auxiliam na tomada de decisão organizacional sobre como deve ser efetuada a gestão de risco de privacidade, sendo determinado o nível de rigor apropriado para a organização. O nível fornece ainda às organizações um contexto sobre a sua robustez relativamente à sua estratégia de cibersegurança.

O propósito desta norma é delinear um conjunto de controlos de segurança básicos direcionados à informação, sistemas e redes. A *framework* é um ponto de referência e de suporte às organizações, pois recorre a um vocabulário de fácil leitura e compreensão.

Diretiva NIS2

A diretiva Network and Information Security (NIS) [15] foi a primeira legislação da União Europeia relativa este tema, da cibersegurança. O propósito desta legislação é atingir um nível sensato nesta matéria em todos os países da Europa e reforçar a cibersegurança em toda a UE. Por ser uma legislação europeia, e com base nesta legislação, cada país desenvolveu as suas próprias regulamentações.

Em Portugal foi criada a lei n.º 46/2018 que estabelece o regime jurídico da segurança do ciberespaço, transpondo a presente diretiva (Diretiva (UE) 2016/1148).

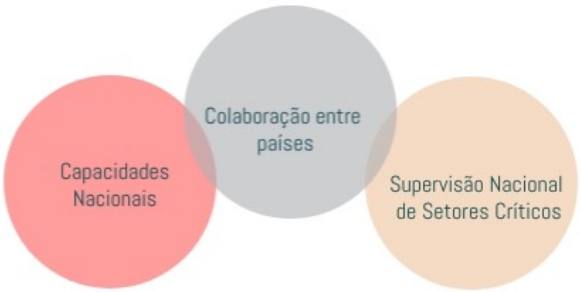


Figura 2: Áreas de atuação da Diretiva NIS, adaptado de [16]

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

Nas capacidades nacionais está mencionado que cada país deve dispor de determinadas capacidades nacionais, como um CSIRT nacional [17], executar simulacros e exercícios de treino para a preparação nesta matéria, entre outros.

Na segunda área é definido que deve existir colaboração entre os países da UE. É recomendado que seja estabelecida uma comunicação com a rede operacional CSIRT da União Europeia ou com o grupo estratégico de cooperação NIS.

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

CIS Controls (Center for Internet Security)

O Center for Internet Securty (CIS) [18] trata-se de um conjunto de boas práticas para a segurança da informação. Foram lançados em 2008 para dar resposta aos desafios de cibersegurança que foram surgindo. O CIS é uma organização sem fins lucrativos, com referência mundial na área da cibersegurança, pois auxilia a encontrar as melhores defesas para os ciberataques.

Constituem um conjunto de 171 controlos, que se podem aplicar em 20 áreas distintas.

Estes controlos estão divididos em três grupos distintos:

- **Controlos Básicos;**
- **Controlos Essenciais;**

- **Controlos Organizacionais.**

A finalidade original era humilde (ajudar as pessoas e as organizações a darem os primeiros passos na área da segurança). Os CIS controls oferecem às empresas um elevado nível de capacitação, e contemplam ainda o mapeamento direto para outras *frameworks* e normas de segurança e conformidade, como a norma ISO 27001. Assumidos e desenvolvidos pelo Center for Internet Security (CIS), os controlos CIS foram a evoluir a larga escala e tornaram-se numa comunidade de indivíduos e instituições voluntários que:

1. **Partilham opiniões e experiências vividas sobre ataques e atacantes, e identificam as causas básicas e as traduzem em classes de ação defensiva;**
2. **Desenvolvem e partilham, ferramentas e soluções de problemas existentes;**
3. **Mapeiam os controlos CIS com estruturas regulatórias, com o intuito de fazer o alinhamento e trazer prioridade e foco para estes;**
4. **Identificam problemas e barreiras comuns (como avaliação inicial e roteiros de implementação).**

Graças à sua capacidade de se ajustar a qualquer tipo de organização independentemente do seu tamanho ou área de negócio, estes controlos são utilizados pelas diversas indústrias, designadamente, a saúde, a educação, o governo, entre outras. Uma característica única que define os CIS controls é a capacidade que estes têm de não se limitarem a bloquear de imediato os sistemas comprometidos, mas também procederem à deteção de equipamentos que já se encontram comprometidos e, ainda, a prevenção e bloqueio de ameaças futuras. Uma organização que decida implementar estes controlos, é uma mais-valia para avaliar e melhorar o seu estado de segurança atual. Permitem, ainda, que a organização perceba o que deve fazer para melhorar o seu nível de segurança.

Estes controlos estão divididos em três grupos de implementação adequados a cada tipo de organização e segundo o seu nível atual de segurança, por exemplo, uma organização que não tenha controlos nenhuns relacionados com a segurança deve começar pela implementação do IG1 e assim sucessivamente.

Na Figura 3 [19] os IGs dos controlos CIS são categorias auto avaliadas para as organizações. Cada IG identifica um subconjunto dos controlos CIS que foram escolhidos e avaliados para serem aplicáveis a uma organização com um perfil de risco e recursos semelhantes para implementação. Estes IGs são uma visão horizontal dos controlos CIS e adaptados a cada tipo de empresa.

O IG1 é designado por "higiene cibernética básica", formado por um conjunto de medidas básicas de segurança e defesa que toda a empresa deve implementar para se proteger dos ataques mais comuns. Cada subgrupo destes de IGs baseia-se no anterior, isto é, o IG2 inclui todas as medidas do IG1 e o IG3 inclui todas as medidas do IG1 e IG2. Para uma organização saber em que grupo está atualmente deve efetuar uma autoavaliação e com o resultado obtido deve enquadrar-se num destes grupos e seguir os seus controlos.

Figura 3: Esquema IG's dos controlos CIS

Uma organização de tamanho pequeno ou médio com experiência reduzida e limitada em TI, em que a segurança é dedicada apenas à proteção de ativos e colaboradores da área de TI, corresponde ao IG1. A principal preocupação destas empresas é manter o negócio operacional, pois não podem ficar muito tempo contínuo sem laborar. A quantidade de dados críticos é relativamente baixa e, na maioria das vezes, trata-se de dados financeiros e dados pessoais de funcionários.

Numa organização onde existem colaboradores responsáveis por manter a infraestrutura e proteção da área de TI, correspondem ao IG2. Estes tipos de organizações dão suporte a vários departamentos com diferentes perfis de risco consoante a missão de trabalho. Normalmente, as organizações pertencentes a este grupo, armazenam informações confidenciais de clientes ou outras empresas, com tolerância para ficar algum tempo sem serviços. Mas um dos maiores receios destas organizações é a má reputação perante um incidente de cibersegurança.

Por fim, uma organização que empregue colaboradores especializados em diferentes áreas da cibersegurança, esta pertence ao IG3. Os ativos e dados pertencentes a este grupo estão sujeitos à supervisão regulatória e de conformidade. Uma organiza-

ção deste grupo está ciente de que um ataque bem-sucedido poderá causar danos significativos.

ISO/IEC 27001:2013

A norma ISO 27001:2013 [20] tornou-se numa referência internacional na área da gestão da Segurança de Informação, pois apresenta os requisitos de auditoria para um Sistema de Gestão de Segurança de Informação.

Da série de normas ISO27XXX, foi esta a primeira a ser publicada pela International Organization for Standardization (ISO) [21], em outubro de 2005. As características desta norma permitem que seja adotada por qualquer tipo de organização independentemente do seu processo de negócio. Sendo um procedente direto do British Standards Institute (BSI) [22], em particular da norma BS799, criada em 1992. Esta norma tem sofrido várias alterações desde que foi criada e milhares de profissionais contribuem com o seu conhecimento para que esta norma alcance um nível estável. A premissa desta norma é que as organizações adotem um conjunto de requisitos, processos e controlos com o intuito de poderem mitigar e gerir adequadamente o risco da organização.

Uma grande parte das organizações tentam obter a certificação ISO, pois é descrito como deve ser implementado um Sistema de Gestão de Segurança da Informação (SGSI). Uma organização que possua esta certificação demonstra que cumpre os requisitos e processos descritos na norma, e demonstra para os seus clientes um nível de confiança mais elevado relativamente à segurança da informação. Com a obtenção da certificação é manifestado o interesse e importância da segurança da informação.

De forma a descrever o processo de implementação de um SGSI, a ISO segue o modelo PDCA (Plan, Do, Check, Act) [23].

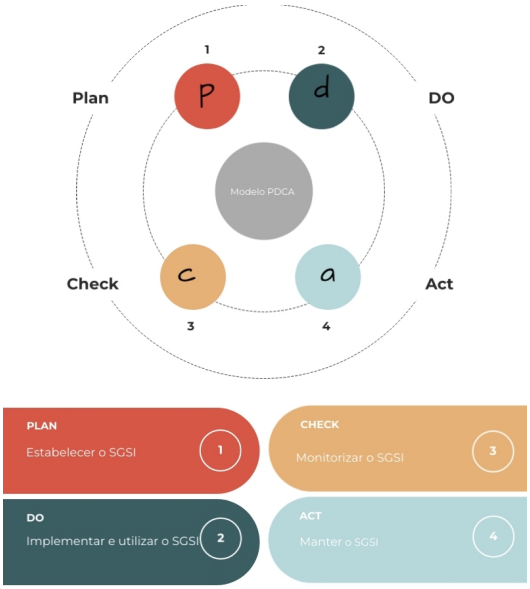


Figura 4: Modelo PDCA, adapatado de [20]

Na Figura 4 está representado o modelo pelo qual esta norma se rege.

1. ***Plan* - Estabelecer o SGSI:** nesta fase é criado o SGSI e planeado. São definidos todos os objetivos e limites do SGSI.
2. ***Do* - Implementar e utilizar o SGSI:** nesta fase vai ser implementado tudo o que foi definido na fase anterior, bem como efetuar a gestão de risco e criar um plano de tratamento do risco. São estabelecidas políticas e os procedimentos necessários de modo a controlar os riscos. Nesta fase dá-se início à formação dos colaboradores e instalação das ferramentas necessárias para monitorizar o que está a ser utilizado na organização.
3. ***Check* - Monitorizar o SGSI:** nesta terceira fase, é feita a monitorização e possíveis melhorias na implementação efetuada, e perceber se os resultados obtidos foram os esperados.
4. ***Act* - Manter o SGSI:** por úlitmo, vão ser aplicadas as medidas necessárias de correção, de maneira que sejam alcançados os objetivos iniciais.

Todos os processos definidos nestas 4 fases acima mencionadas têm de estar documentados e atualizados regularmente para existirem provas de conformidade nos requisitos delineados nestas etapas.

A presente norma é bastante ampla, pois é um modelo de segurança que se adapta a qualquer marca ou fabricante tecnológico. Outro motivo para ser tão utilizada é o facto de estar em conformidade com os mais diversos temas, designadamente, telecomunicações, segurança das aplicações, salvaguarda do meio físico, recursos humanos, continuidade de negócio, licenciamento, entre outros.

A norma ISO 27001 tem os controlos necessários para cumprir os requisitos de risco presentes no anexo A. São 114 controlos agregados em 14 domínios distintos. De acordo com os riscos identificados devem ser tidos em conta os controlos adequados para esses riscos.

Norma ISO/IEC 27701-2019

A norma ISO/IEC 27701 [24] trata-se de uma norma orientada para a gestão de informação privada. Esta define requisitos e fornece orientações que ajudam as empresas a efetuar a gestão de risco de privacidade relacionados com informação de identificação pessoal. Esta norma transmite ainda orientações particulares de como estabelecer, implementar, manter e melhorar continuamente um Privacy Information Management System (PIMS). Este PIMS trata-se de uma extensão do Information Securtiy Management System (ISMS) definido na ISO 27001, para ter em conta os cuidados especiais para o processamento de dados de Personally Identifiable Information (PII) [25].

Tal como a maioria das normas, aplica-se a todos os tipos e tamanhos de organizações, que tenham de manipular dados pessoais, independentemente de serem organizações privadas ou públicas, entidades governamentais e também organizações sem fins lucrativos.

Sendo uma norma que estende da ISO 27001 e ISO 27002, no caso de uma organização pretender obter esta certificação um requisito obrigatório é que possua um sistema de gestão de segurança da informação, implementado segundo a norma ISO 27001.

Uma organização que siga os requisitos desta norma demonstra como faz o tratamento dos dados pessoais, e isto pode ser uma mais-valia em acordos com parceiros de negócios, onde esta questão é extremamente relevante.

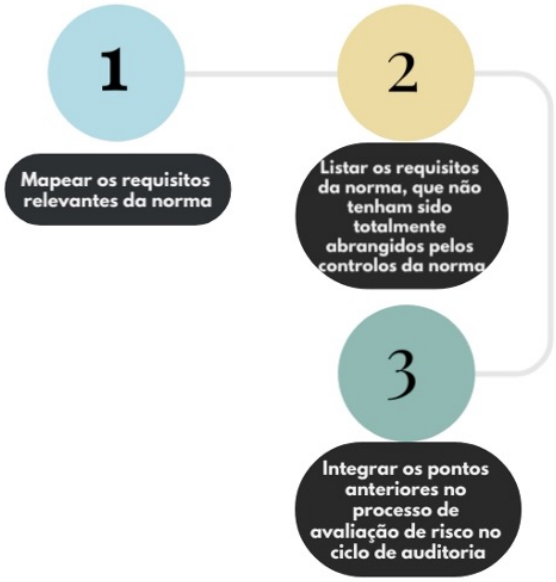


Figura 5: Medidas para avaliar os controlos da norma, adaptado de [24]

Na Figura 5 estão representadas as medidas necessárias para avaliar os controlos da norma.

Os controlos presentes nesta norma fazem mapeamento direto com os requisitos do RGPD (Regulamento Geral de Proteção de Dados).

Esta norma tem uma particularidade perante todas as outras normas ISO, pois necessita de um SGSI implementado através da norma ISO 27001 para se anexar.

Figura 6: Grupos de requisitos da norma ISO 27701, adaptado de [24]

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

Roteiro para as Capacidades Mínimas de Cibersegurança

O Centro Nacional de Cibersegurança definiu este modelo para que as organizações se possam capacitar, tendo como finalidade a melhoria dos processos com foco nas Pequenas e Médias Empresas.

Para fazer face ao aumento do cibercrime foi necessária a criação de Centros Nacionais de Cibersegurança e a delineação de estratégias nacionais. Pelo défice de uma autoridade ou legislação em Portugal nesta área, o país teve que tomar a decisão de implementar uma entidade autoritária nesta área. Por este motivo surgiu assim o Centro Nacional de Cibersegurança.

O CNCS é a autoridade nacional competente capaz de exercer poderes a nível deste assunto relativamente ao Estado e a infraestruturas críticas.

A equipa nacional de resposta de incidentes de cibersegurança, conhecida por CERT.PT [1], funciona no CNCS. As principais funções desta equipa são coordenar a resposta a incidentes, que envolvam entidades pertencentes ao Estado, operadores de serviços de operadoras, serviços críticos e interesses nacionais. O CNCS atua em todo o território português.

Este documento [5] permite que as organizações façam um desenvolvimento gradual, percorrendo cada uma destas 5 fases. O presente documento foi desenvolvido pelo CNCS, e serve como guia de boas práticas para que uma organização esteja em conformidade com os requisitos mínimos de cibersegurança.

Figura 7: Fases do Roteiro das Capacidades Mínimas de Cibersegurança, adaptado de [5]

O roteiro está divido em cinco fases e em cada uma delas, estão presentes um conjunto de ações, como é possível observar na Figura 7. Estas ações auxiliam num desenvolvimento progressivo. Posteriormente vão ser explicadas em detalhe todas as fases, bem como cada ação.

Fase 1 - Preparação Inicial

Nesta primeira fase, estão definidas uma série de ações que servem de guia para a colaboração entre o CNCS e a organização. A colaboração entre o CNCS e a organização é o principal intuito desta etapa.

As ações presentes nesta primeira fase são as seguintes:

- **A 1.1** – Formalização de Protocolo de Colaboração e Adenda
- **A 1.2** – Identificação de RESPONSÁVEL DE SEGURANÇA
- **A 1.3** – Identificação de funções ou atividades críticas
- **A 1.4** – Estabelecimento de canais de comunicação
- **A 1.5** – Registo de endereços de IP no LIR (Local Internet Registry)

1 https://www.cncs.gov.pt/pt/certpt/

- **A 1.6** – Estabelecimento de metodologia de Análise de Risco
- **A 1.7** – Cadeia de responsabilidade: preparação
- **A 1.8** – Definição de política de segurança de informação
- **A 1.9** – Procedimentos de notificação de incidentes

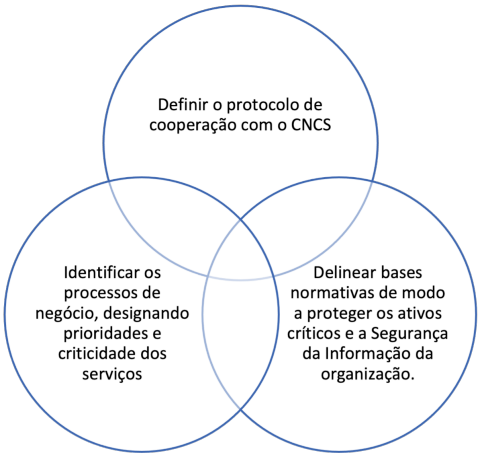


Figura 8: Objetivos para a Fase 1, adaptado de [5]

Os objetivos desta fase, representados na Figura 8, serão detalhados seguidamente.

- **Definir o protocolo de cooperação com o CNCS:** relativamente a esta capacidade é expectável, que seja formalizado o protocolo de colaboração, bem como os canais de comunicação que irão ser utilizados, todos os processos de notificação e deve ser eleito o responsável de Segurança.
- **Identificar os processos de negócio, designando prioridades e criticidade dos serviços:** neste ponto devem ser identificados todos os processos de negócio, determinando quais os processos prioritários e indicando o seu nível de criticidade.
- **Delinear bases normativas de modo a proteger os ativos críticos e a Segurança da Informação da organização:** estas bases normativas têm como finalidade proteger os ativos críticos da organização e toda a informação interna. Para definir estas bases normativas, é necessário definir uma cadeia de responsabilidade interna por sistemas e por ativos, e ainda, adotar uma metodologia de gestão de risco que trate da mitigação de ameaças.

Fase 2 - Arquitetura

Esta fase consiste num leque de ações recomendadas e baseadas na fase anterior, mas ainda contém ações que permitem dotar a organização das capacidades necessárias para uma defesa eficiente dos seus ativos, em diferentes níveis, nomeadamente, o perímetro da sua rede, servidores, postos de trabalho e outros dispositivos. Ainda

nesta etapa é esperado que seja garantida a conformidade essencial da informação com requisitos legais e normativos de acordo com a área de atividade da organização.

Nesta fase estão presentes as seguintes ações:

- **A 2.1** – Desenho e implementação da arquitetura e segurança perimétrica
- **A 2.2** – Implementação de sistema de recolha e armazenamento do fluxo de tráfego
- **A 2.3** – Comunicação com o CNCS
- **A 2.4** – Inventariação de ativos / produção de um mapa de rede
- **A 2.5** – Recolha centralizada de registos (logs)
- **A 2.6** – Criação de instrumentos de correção ou mitigação de incidentes
- **A 2.7** – Estabelecimento de conformidade com a legislação aplicável
- **A 2.8** – Estabelecimento de conformidade com normas aplicáveis à área de atividade
- **A 2.9** – Criação de política de uso aceitável
- **A 2.10** – Manutenção de infraestruturas de cópias de segurança e reposição (Backup/Restore)
- **A 2.11** – Mapa de competências e planos de formação
- **A 2.12** – Treino e sensibilização interna: geral
- **A 2.13** – Treino e sensibilização interna: gestão

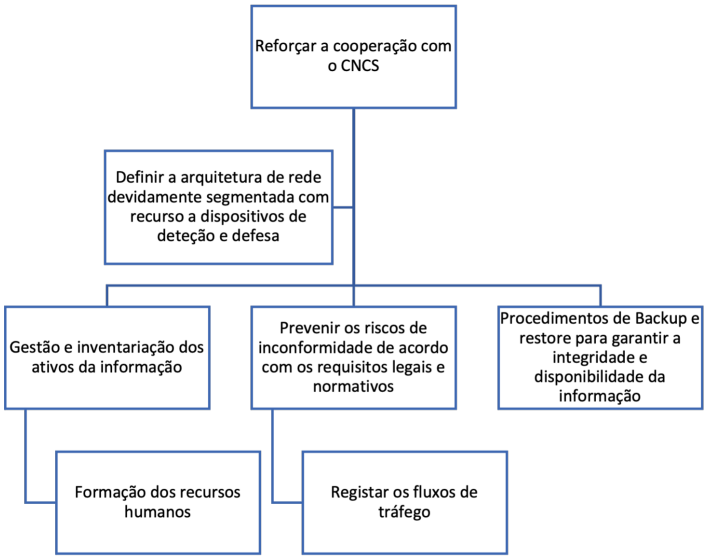


Figura 9: Objetivos para a Fase 2, adaptado de [5]

Seguidamente serão aprofundados os objetivos presentes na Figura 9.

- **Reforçar a cooperação com o CNCS:** neste ponto deve-se reforçar a cooperação com o CNCS através de canais de comunicação definidos na fase anterior.
- **Definir a arquitetura de rede devidamente segmentada recorrendo a dispositivos de deteção e defesa:** a arquitetura da rede deve ser devidamente segmentada, com o auxílio de dispositivos de deteção e defesa para de ameaças externas.
- **Registar os fluxos de tráfego:** todo o tráfego deve ficar registado de modo a permitir uma deteção prévia e ainda, testar o funcionamento dos sistemas internos perante uma deteção de um evento de segurança.
- **Gestão e inventariação dos ativos de informação:** deve ser elaborado um inventário de todos os ativos, pois com este inventário a organização deve conseguir lidar com as eventuais ameaças que possam surgir, ficando assim com uma visão global do panorama interno.
- **Procedimentos de *Backup* e *restore* para garantir a integridade e disponibilidade da informação:** a organização deve ter procedimentos de *backup* e *restore*, para garantir a resiliência da disponibilidade e integridade da informação.
- **Formação dos recursos humanos:** a sensibilização/formação deve transversal a todos os recursos humanos da organização para que a questão da cibersegurança não seja apenas responsabilidade de recursos humanos dedicados a este assunto. Com esta capacidade, todos os colaboradores devem estar atentos e possam implementar determinadas ações no seu quotidiano.

Fase 3 - Segurança dos Dispositivos

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

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

- **A 3.1** – Definição de procedimentos de operação
- **A 3.2** – Instalação e configuração de sensores em dispositivos
- **A 3.3** – Auditoria de segurança e Bases de Dados
- **A 3.4** – Instalação e configuração de controlo de acessos web – (e.g. serviços *proxy*)
- **A 3.5** – Proteção e gestão de equipamentos
- **A 3.6** – Instalação e configuração de mecanismos de monitorização

- **A 3.7** – *Hardening* das configurações
- **A 3.8** – Instalação e configuração de um Security Information and Event Management (SIEM)
- **A 3.9** – Definição de planos de continuidade de negócio
- **A 3.10** – Aquisição de competências técnicas

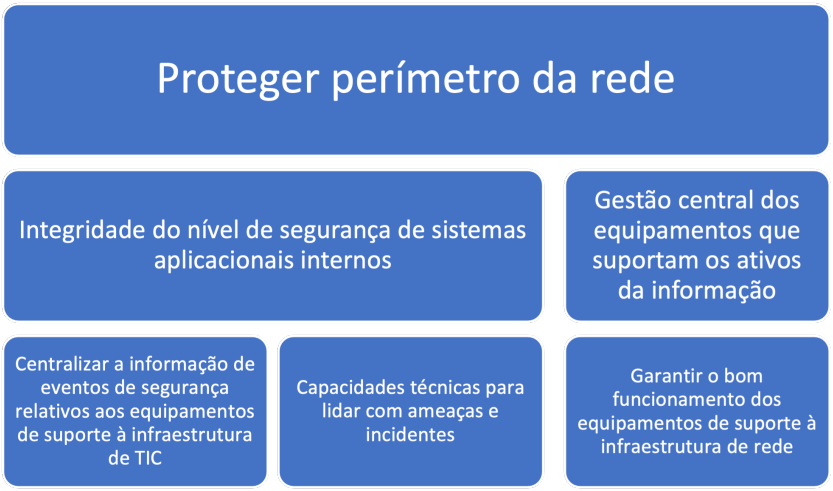


Figura 10: Objetivos para a Fase 3, adaptado de [5]

Seguidamente serão aprofundados os objetivos presentes na Figura 10.

- **Proteger perímetro da rede:** implementar dispositivos que filtrem o tráfego baseados em políticas estabelecidas, bem como em reconhecimento e bloqueio de padrões de ataque.
- **Integridade do nível de segurança de sistemas aplicacionais internos:** através da realização de auditorias e das configurações dos equipamentos, deve ser garantida a integridade de sistemas aplicacionais.
- **Gestão central dos equipamentos que suportam os ativos da informação:** a organização deve dispor de sistemas que detetam e bloqueiam intrusões, como, por exemplo, HIDS e antivírus.
- **Centralizar a informação de eventos de segurança relativos aos equipamentos de suporte à infraestrutura de TIC:** é recomendado que a organização faça a gestão de forma eficaz sobre eventos de segurança, utilizando particularmente um sistema SIEM, com o objetivo de filtrar e organizar estes dados e tornar a informação mais legível em termos de segurança para poderem ser tomadas atitudes e decisões para combater esses incidentes.
- **Capacidades técnicas para lidar com ameaças e incidentes:** cabe à organização contratar recursos humanos e possuir sistemas com as capacidades técnicas necessárias para lidar com as ameaças e incidentes de cibersegurança.

- **Garantir o bom funcionamento dos equipamentos de suporte à infraestrutura de rede:** de modo a garantir o bom funcionamento destes equipamentos indispensáveis, é inevitável que se instale mecanismos de monitorização, supervisão e alarmística.

Fase 4 - Consolidar a Cibersegurança

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

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

- **A 4.1** – Cadeia de responsabilidades: formalização
- **A 4.2** – Definição do Sistema Interno de Normas e Políticas (SINP)
- **A 4.3** – Análise de risco - reavaliação
- **A 4.4** – Simulacro
- **A 4.5** – Definição de procedimentos de reação a incidentes
- **A 4.6** – Treino e sensibilização interna: SINP
- **A 4.7** – Testes de aceitação se serviços
- **A 4.8** – Mecanismos de engodo (honeypots)
- **A 4.9** – Gestão de mudanças e atualizações

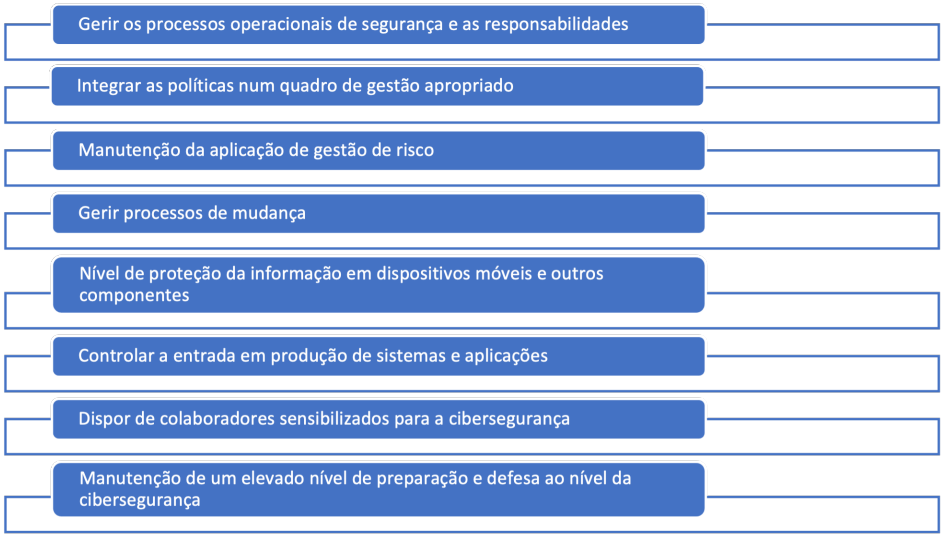


Figura 11: Objetivos para a Fase 4, adaptado de [5]

Seguidamente serão aprofundados objetivos presentes na Figura 11.

- **Gerir os processos operacionais de segurança e as responsabilidades:** para gerir os processos operacionais devem ser estipuladas cadeias de responsabilidades. Estas cadeias de responsabilidades servem para atribuir responsabilidades por processos e ativos de informação internos.
- **Integrar as políticas num quadro de gestão apropriado:** este quadro de gestão apropriado tem como principal missão agregar políticas e normativos definidos em fases precedentes.
- **Manutenção da aplicação de gestão de risco:** a manutenção da aplicação de gestão de risco deve ser garantida.
- **Gerir processos de mudança:** processos como a aplicação de *patches* e atualizações de segurança, devem ser geridos num sistema que garanta a compatibilidade destas alterações com o bom funcionamento dos sistemas aplicacionais e que mantenha um nível elevado de proteção dos ativos.
- **Nível de proteção da informação em dispositivos móveis e outros componentes:** deve ser contemplada a segurança de dispositivos móveis e outros componentes em rede para garantir um elevado nível de segurança.
- **Controlar a entrada em produção de sistemas e aplicações:** a entrada em produção de sistemas e aplicações apenas deve ser permitida após testes de segurança e consequente aceitação por parte de uma equipa especializada.
- **Dispor de colaboradores sensibilizados para a Cibersegurança:** é essencial que qualquer colaborador, independentemente das suas funções, esteja sensibilizado para este tema, garantindo a aplicação de boas práticas no seu quotidiano.
- **Manutenção de um elevado nível de preparação e defesa ao nível da Cibersegurança:** este ponto destaca a importância da manutenção de um elevado nível de preparação e defesa ao nível da cibersegurança, assegurando a manutenção e melhoria contínua dos sistemas.

Fase 5 - Equipa de Cibersegurança

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

- **A 5.1** – Nomear um CISO
- **A 5.2** – Estabelecer um serviço de gestão de vulnerabilidades
- **A 5.3** – Estabelecer e implementar um plano de auditorias
- **A 5.4** – Definir a missão, a comunidade servida e o portfólio de serviços do CSIRT

- **A 5.5** – Elaborar e fazer aprovar o plano e o orçamento para o CSIRT
- **A 5.6** – Montar e anunciar o CSIRT
- **A 5.7** – Estabelecer um sistema de gestão de Crise
- **A 5.8** – Afiliação nas comunidades nacionais e internacionais de CSIRT
- **A 5.9** – Participação num exercício nacional de cibersegurança

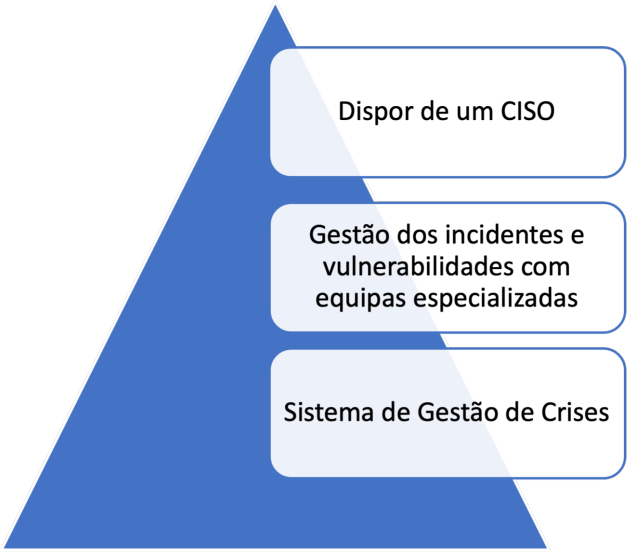


Figura 12: Objetivos para a Fase 5, adaptado de [5]

Seguidamente vão ser aprofundados os objetivos presentes na Figura 12.

- **Dispor de um CISO:** um CISO é o responsável máximo pela segurança de informação, é esta figura que controla a cibersegurança e as equipas de deteção e resposta a incidentes.
- **Gestão dos incidentes e vulnerabilidades com equipas especializadas:** as equipas de SOC ou CSIRT são responsáveis pela gestão dos incidentes e vulnerabilidades.
- **Sistema de Gestão de crises:** um sistema desta natureza auxilia na redução do tempo de reação e aumentam a eficácia de combate a incidentes de uma magnitude que possa causar um impacto catastrófico na organização.

Quadro Nacional de Referência para a Cibersegurança

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

103 medidas que correspondem a 5 objetivos de segurança, e que, correspondem a 3 níveis de capacidade.

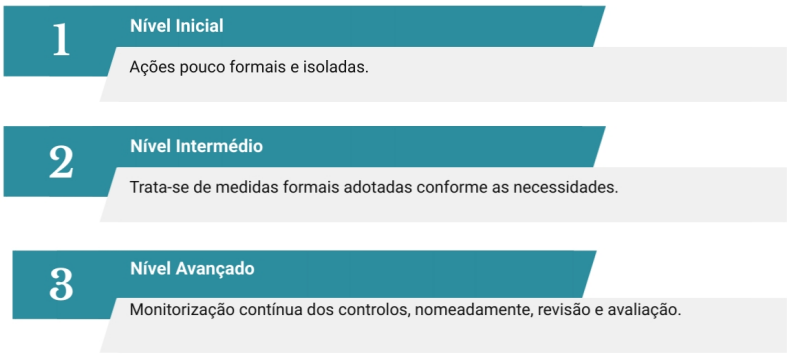


Figura 13: Níveis de Capacidade, adaptado de [26]

Na Figura 13 são apresentados os níveis de capacidade descritos no documento.

Em [26] estão reunidos um conjunto de boas práticas, cuja finalidade é reduzir os riscos das ameaças a que as organizações estão expostas. Este conjunto de boas práticas permite que qualquer organização cumpra os requisitos mínimos de segurança.

Estes requisitos traduzem-se em 5 objetivos que são, nomeadamente, a identificação, proteção, deteção, resposta e recuperação de incidentes de segurança.

Este guia é transversal a qualquer tipo de organização, independentemente da sua dimensão ou processo de negócio. O QNRCS contém ainda uma série de recomendações extra de maneira que as organizações cumpram a legislação em vigor e, simultaneamente, possam efetuar a gestão de risco e mitigar o impacto dos incidentes.

Figura 14: Objetivos de Segurança, adaptado de [26]

Estes objetivos representados na Figura 14 estão organizados em categorias e subcategorias.

De seguida são indicados os objetivos de segurança e uma breve descrição de cada um deles.

- **Identificar -** São identificados os ativos e serviços críticos da organização e os seus riscos associados. Assim a organização sabe o que deve priorizar tendo em conta a sua estratégia de gestão de risco.
- **Proteger -** São aplicadas as medidas necessárias para proteger os serviços críticos e ativos identificados no objetivo anterior. Estão incluídas três dimensões: Pessoas, Processos e Tecnologia.
- **Detetar -** São definidas e implementadas as medidas para efetuar a deteção antecipada de incidentes.
- **Responder -** São definidas e implementadas as medidas para atuar quando for detetado um incidente.
- **Recuperar -** São definidas e implementadas as medidas para efetuar a recuperação de incidentes.

Este documento não deve ser apelidado de norma, mas sim sendo uma referência que permite identificar as normas, padrões e boas práticas existentes em diversos domínios da segurança da informação.

Estas medidas de segurança presentes neste documento podem ser mapeadas diretamente com diversas normas. No final do documento, está descrita a função de um CISO, o qual é uma figura relevante na organização.

Regulamento Geral de Proteção de Dados

Cada vez mais os dados têm um valor significativo e tornou-se assim uma preocupação, pois não existia forma de proteger a informação sensível, e garantir a integridade dos dados. Atualmente pode-se afirmar que os dados são o ativo de maior valor para uma organização, e estes podem-se tornar determinantes para o sucesso ou não duma organização.

Assim, em abril de 2016 o Parlamento Europeu chegou à conclusão que seria necessário substituir a Diretiva 95/46/CE, que usaria até então para proteger os dados. Para garantir a salvaguarda da informação, este adotou o Regulamento Geral de Proteção de Dados (RGPD) [27]. Este regulamento trouxe o equilíbrio relativamente às regras de segurança da informação.

Este regulamento foi criado tendo em vista resolver e definir regras na questão da privacidade e à segurança da informação. Com a implementação deste regulamento, as organizações tiveram de redefinir todos os seus processos por forma a garantir a segurança da informação.

O Regulamento Geral de Proteção de Dados assenta em dois conceitos-chave:

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

Apesar da sua importância, os dados, se não forem devidamente tratados e analisados, não valem de nada. Sendo assim, tornando os dados um ativo vital, é a sua gestão que deve ser efetuada por um indivíduo com formação para desempenhar tal função.

Segundo este regulamento é expectável que exista um responsável para efetuar a manipulação dos dados para garantir que este processo corresponde com as regras deste regulamento. Este responsável desgina-se de Data Protection Officer (DPO).

O DPO deve estar presente nas organizações em que exista uma grande manipulação de dados. Este responsável pelo tratamento de dados tem o dever de informar e aconselhar a organização da qual faz parte, sobre a conformidade da proteção de dados e monitorizar a conformidade deste regulamento. Este também tem a função de dar formação aos restantes colaboradores que desempenhem funções, que estejam associadas a esta área, e fazem a ponte de ligação com as autoridades de proteção de dados.

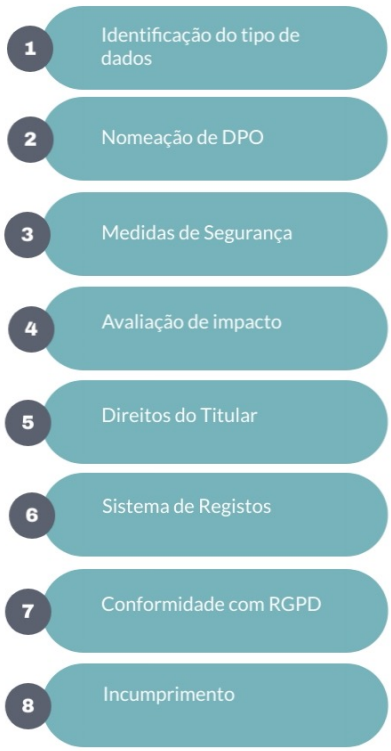


Figura 15: Etapas para implementação do RGPD, adaptado de [27]

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

Relativamente aos dados guardados nas bases de dados, estas terão que ter uma camada adicional de proteção. Desta forma, dependendo da natureza dos dados pessoais e também a sua finalidade, tem que ser garantida a sua confidencialidade, integridade, disponibilidade e resiliência permanente dos sistemas que tratam os dados.

Este regulamento tornou-se mandatório em Portugal no dia 25 de maio de 2018.

Lei nº 46/2018 Regime Jurídico da Segurança do Ciberespaço

Esta lei vem no seguimento da Diretiva 2016/1148 da União Europeia, do Parlamento Europeu e do Conselho e julho de 2016 [28]. Este regime veio estabelecer e transpor um conjunto de requisitos presentes na diretiva anteriormente referida. Entrou em vigor em Portugal em 13 de agosto de 2018.

O propósito deste regime é garantir um elevado nível comum de segurança das redes e dos sistemas da UE. Com a aplicação deste regime nas organizações, estas têm de cumprir os deveres presentes neste regime.

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

Tabela 2: Entidades abrangidas por este regime

As entidades listadas na Tabela 2 têm a obrigatoriedade de cumprir este regime e de igual forma, respeitar os deveres que estão associados.

Estes deveres são os seguintes:

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

No final desta lei são descritas as sanções aplicadas para quando esta lei não é cumprida.

Decreto-Lei n.º 65/2021

A lei da segurança do ciberespaço [29] aplica-se a todas as organizações que usem redes e sistemas de informação.

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

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

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

- **Fase 1: Formação inicial e identificação de catálogos da CIM-TTM e Associações de Municípios;**
- **Fase 2: Inventário de Ativos;**
- **Fase 3: Elaboração de um Plano de Segurança das entidades envolvidas;**
- **Fase 4: Avaliação intermédia e plano de melhoria;**
- **Fase 5: Notificação de incidentes;**
- **Fase 6: Análise de riscos de ativos;**

- **Fase 7: Medidas técnicas para monitorização;**
- **Fase 8: Revisão do Plano de Segurança.**

Este assunto emprega-se em especial no âmbito da comunicação voluntária de incidentes.

No segundo capítulo deste documento está estabelecido que o CNCS é a Autoridade Nacional de Cibersegurança e o CERT, como equipa nacional de gestão de incidentes de segurança de informação.

O terceiro capítulo estabelece que as entidades abrangidas pelos regimes jurídicos de cibersegurança são obrigadas a implementar pré-requisitos de segurança e informar o CNCS de incidentes que possam afetar a segurança das redes e sistemas de informação.

No quarto capítulo do documento está definido qual o regime de fiscalização e sanção.

No último capítulo, encontram-se as disposições finais, destacando o regime de identificação de operadores de serviços essenciais e prestadores de serviços digitais.

2.3 SÍNTESE

Neste capítulo foi apresentada a definição de cibersegurança presente no glossário do CNCS que consiste num conjunto de medidas e ações fundamentais para prevenir, detetar e analisar os sistemas de informação. Foram, também, apresentadas diversas normas, leis e documentos que sugerem um conjunto de boas práticas direcionadas às organizações.

De todas as normas e melhores práticas que devem ser aplicadas às organizações destacam-se, nomeadamente:

- **ISO/IEC 27001:2013**;
- **Roteiro para as Capacidades Mínimas da Cibersegurança**.

Evidencia-se a norma ISO/IEC 27001:2013 por esta ser um referencial nacional e internacionalmente. O Roteiro para as Capacidades Mínimas da Cibersegurança destaca-se por se tratar de um manual de boas práticas definido pelo CNCS, que deve ser tido em consideração para a definição do nível de maturidade em cibersegurança de uma organização.

3

MATURIDADE DA CIBERSEGURANÇA

Neste capítulo será apresentado o conceito de maturidade de uma forma global e ajustado à cibersegurança, a relação do contexto organizacional aliando com a cibersegurança.

3.1 DEFINIÇÃO

De um ponto de vista geral, a expressão maturidade representa um estado de maturidade e um pressuposto de desenvolvimento pleno.

Em setembro de 2019, o autor José Almeida definiu de forma breve o termo de maturidade num documento publicado pela APDSI (Associação para a promoção e desenvolvimento da Sociedade da Informação) [30]. Esse documento apresenta uma explicação de alto nível sobre este mesmo conceito, sendo apresentado um enquadramento relativo à maturidade organizacional. Por fim, é definida a relação da maturidade com a cibersegurança.

O conceito de maturidade é definido como um conjunto de características ou atributos que representam a evolução num determinado domínio.

Tendo em conta que as organizações possuem controlos (ou deveriam possuir) por forma a controlar as ameaças de segurança da informação, estes devem ser coordenados com os processos de gestão internos e de operacionalização do negócio. Cada organização deve, então, avaliar com regularidade em que medida está implementada uma efetiva segurança de informação na sua organização.

Por forma a ser efetuada esta avaliação é necessário recorrer a modelos de maturidade. Estes modelos consistem numa melhoria progressiva de boas práticas, para que as organizações possam evoluir por fases, percorrendo um caminho até à maturação de segurança desejada. Estes modelos de maturidade representados por fases pretendem descrever o caminho de maturação, levando assim a uma melhoria contínua da segurança da informação numa organização.

Um modelo de maturidade é constituído por objetivos, sendo estes objetivos os seguintes:

- **Descritivo** - é aplicado para avaliar a situação atual da organização e avaliar as capacidades existentes;

- **Prescritivo** - para identificar o nível de maturidade desejado;
- **Comparativo** - caso seja utilizado um *benchmarking* externo ou interno entre organizações, onde se podem comparar dados históricos de empresas similares;
- **Holístico** - são integrados todos os objetivos acima descritos num quadro de melhoria.

Tendo em conta que os modelos de maturidade indicam as capacidades desejáveis numa organização relativamente a uma determinada dimensão, cabe aos cargos de gestão escolher o modelo de maturidade que melhor se adequa ao seu processo de negócio e corresponde aos seus objetivos.

Um modelo de maturidade de cibersegurança, descreve uma orientação para a organização sobre como alcançar o próximo nível. Sempre que a organização considere relevante, pode recorrer a estes modelos de maturidade para averiguar o estado de maturidade.

3.2 TRABALHOS RELACIONADOS

Seguidamente serão apresentados trabalhos relacionados com a maturidade, maturidade em cibersegurança e com a cibersegurança em contexto empresarial.

Deteção de Incidentes de Cibersegurança: Capacidades Mínimas

Em outubro de 2017, Catarina Sousa Rego em [31], criou um modelo de maturidade direcionado para as autoridades de cibersegurança nacionais e cargos de gestão de uma organização.

Este modelo de maturidade é constituído por quatro pilares, técnica, humana, processual e organizacional, definindo um conjunto de ações para cada nível do modelo de maturidade. Estas ações foram estabelecidas conforme diversos documentos, experiências efetuadas por outros investigadores ou fóruns. Os cinco níveis presentes neste modelo de maturidade são os seguintes:

- **Nível 1** - Preparação;
- **Nível 2** - Arquitetura;
- **Nível 3** - Segurança de Dispositivos e Aplicações;
- **Nível 4** - Procedimentos de cibersegurança;
- **Nível 5** - Centro de Operações;

O modelo criado poderá ser aplicado em qualquer tipo de organização independentemente do seu processo de negócio ou dimensão e permite ainda obter o nível de maturidade na deteção de incidentes por organização.

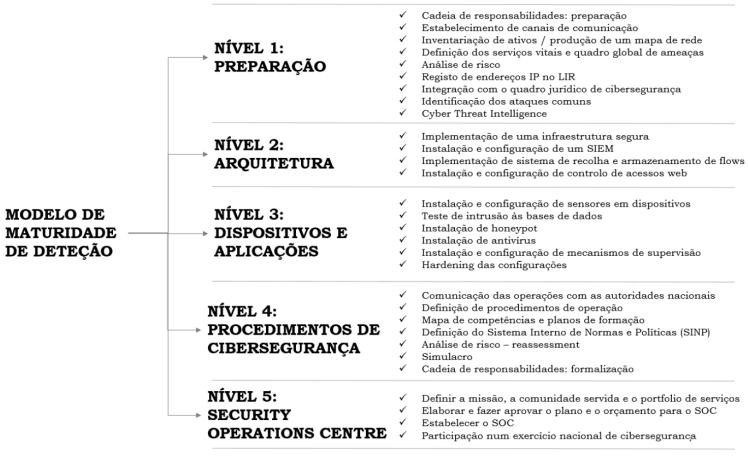


Figura 16: Resumo dos níveis e ações presentes no modelo de maturidade

É expectável que este modelo representado na Figura 16 seja utilizado para obter um nível de maturidade nacional. Segundo este modelo, foi definido um orçamento para cada nível proposto, de modo a orientar os órgãos de gestão das organizações. A colaboração e comunicação com o CNCS são temas com grande destaque neste trabalho. Foram consideradas normas como a NIST Cybersecurtity Framework e a norma ISO/IEC 27001:2013, sendo feito um estudo comparativo entre estas.

A aplicação deste modelo é feita por três fases distintas, sendo que primeira fase tem um propósito de desenvolver uma autoavaliação de modo a situar o panorama da organização, a segunda fase visa calcular as lacunas entre o panorama inicial e o panorama pretendido. Já a última fase, o seu propósito é o desenho do plano para melhorar o nível de maturidade.

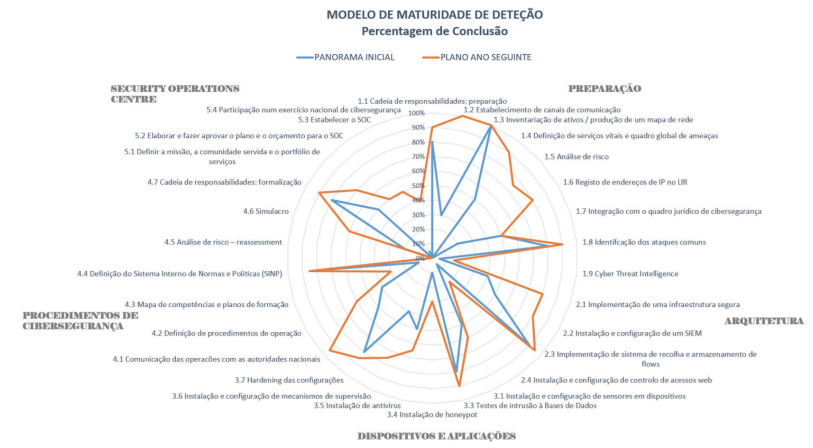


Figura 18 – Exemplo de visualização Maturidade Deteção de Incidentes

Figura 17: Exemplo de visualização da aplicação do modelo

O modelo apresenta um modelo de maturidade que auxilia as organizações e as autoridades nacionais, com o intuito de avaliar a maturidade nacional. Neste estudo apenas foi desenvolvido um modelo de maturidade, não tendo sido testado. Na Figura 17 pode-se observar um exemplo de visualização da aplicação do modelo. É apresentado um explicativo de como deve ser aplicado na prática, porém como não foi efetuado algum teste, não existem resultados.

Modelo de maturidade de segurança cibernética para os órgãos da administração pública federal

Na sua investigação de 2020, António João Gonçalves de Azambuja e João Souza Neto [32], delinearam um modelo de maturidade de segurança da informação, direcionado para os órgãos da administração pública federal do Brasil.

Foi então desenvolvido um estudo qualitativo por forma a analisar os modelos de maturidade já existentes na literatura, servindo estes como base para a definição deste modelo desenvolvido. Na Figura 18 pode-se observar a relação entre os domínios definidos no modelo e os seus objetivos.

Quadro 7| Domínios do modelo vs Objetivos da Estratégia de SIC e SegCiber

Domínios	Objetivos
Gestão de riscos	Elevar o nível de maturidade de SIC e de SegCiber na APF;
Gestão de ativos	
Gestão de acesso	
Gestão de ameaças e vulnerabilidades	
Gestão de continuidade	Valorizar e ampliar ações que fortaleçam a segurança das infraestruturas críticas da informação;
Compartilhamento de informações	Garantir continuamente a pesquisa, o desenvolvimento e a inovação em SIC e SegCiber na APF; Ampliar e fortalecer ações colaborativas em SIC e SegCiber com a academia, setores público, privado e terceiro setor no país e no exterior;
Capacitação, conscientização e cultura	Garantir continuamente o aprimoramento do quadro de pessoal da APF em SIC e SegCiber de forma qualitativa e quantitativa; Promover mecanismos de conscientização da sociedade sobre SIC e SegCiber;
Infraestrutura tecnológica	Valorizar e ampliar ações que fortaleçam a segurança das infraestruturas críticas da informação;
Governança de segurança cibernética	Instituir modelo de Governança Sistêmica de SIC e de SegCiber na APF; Alinhar o planejamento de SIC e de SegCiber ao planejamento estratégico dos órgãos da APF.

Figura 18: Relação dos Domínios e Objetivos do modelo

Para analisar tudo o que já existia na literatura sobre este tema, foi feito um questionário online. Este questionário teve a participação de 35 órgãos da administração pública federal.

Como conclusão desta investigação, os autores entenderam que existe um nível baixo de maturidade na amostra estudada. Esta pesquisa teve como finalidade aumentar o nível de maturidade de Segurança da Informação na administração pública federal, e uma melhoria da segurança no Brasil.

Este inquérito é dirigido a um público-alvo específico, neste caso os órgãos da administração pública federal, de modo a avaliar o seu nível de maturidade de

acordo com o modelo de maturidade desenvolvido pelos autores. Este trabalho está apenas direcionado a um público-alvo, ficando assim limitado a este setor e não podendo ser estendido a mais indivíduos.

Modelo de Maturidade C2M2

Por forma a auxiliar o maior número de organizações possíveis, foi criado pelo Departamento de Energia dos Estados Unidos da América (DOE) um Modelo de Maturidade de Capacidade de Cibersegurança [33] que permite avaliar, privilegiar e melhorar as capacidades de cibersegurança.

O modelo C2M2 está divido por dez domínios, sendo que cada domínio é constituído por práticas de cibersegurança. Estas práticas de cibersegurança estão associadas à operação e utilização da tecnologia e ativos da organização.

Domínio
Gestão de risco
Gestão de ativos, mudança e configuração
Gestão de identidade e acesso
Gestão de ameaças e vulnerabilidades
Consciência Situacional
Partilha de informações e comunicações
Resposta a eventos e Incidentes, Continuidade das Operações
Supply chain e gestão das dependências externas
Gestão dos trabalhadores
Gestão do Programa de Cibersegurança

Tabela 3: Domínios do modelo C2M2

Na Tabela 3 estão representados os domínios que compõem este modelo de maturidade, tendo como finalidade melhorar as boas práticas e capacidades de cibersegurança presentes nas organizações. As organizações podem usar este modelo para fortalecer as capacidades de SegCiber, permitir a avaliação de forma eficaz e consistente do estado atual da SegCiber, compartilhar conhecimento, melhores práticas e referências de SegCiber e permitir a priorização das ações e investimentos para melhorar a SegCiber.

A maturity framework for cybersecurity governance in organizations

No seu trabalho de 2021, Yassine Maleh, Abdelkebir Sahid e Mustapha Belaissaoui salientou os problemas que surgiram na atual era da digitalização [34].

O documento citado salienta que a existência de normas e governança neste tema é fundamental para lidar com todos os riscos presentes em todos os sistemas de informação. Os autores deste artigo apresentam uma estrutura de maturidade que permite avaliar e melhorar a gestão da cibersegurança nas organizações.

A finalidade desta estrutura é auxiliar as organizações a melhorar e ampliar a segurança da informação em todos os seus sistemas e infraestruturas físicas, pois podem sempre avaliar os seus recursos relacionados com este tema.

O foco deste estudo foi definir uma estrutura de maturidade, não tendo sido testada esta estrutura, com um inquérito, por exemplo.

Inquérito Aberto à Segurança da Informação nas Instituições em Portugal

A investigação feita pela Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI) [35], foi desenvolvida sob a forma de um inquérito por forma a avaliar a realidade portuguesa. Este estudo não se baseou simplesmente nos responsáveis de TI, mas sim a outras funções dentro das empresas, por forma a entender-se de que forma os restantes inquiridos lidam com este assunto. O inquérito foi desenhado para abranger diversos temas, nomeadamente:

- O compromisso da gestão de topo;
- A formação de competências;
- A existência de uma unidade organizacional dedicada;
- O papel da auditoria e controlo;
- A gestão de incidentes de segurança;
- A gestão do orçamento para Segurança da Informação;
- A gestão dos recursos humanos com funções na Segurança de Informação;
- A existência de incidentes e eventuais perdas relacionadas;
- As preocupações de segurança dos órgãos de topo;
- A perceção da exposição da instituição às ameaças.

Os resultados deste questionário foram recolhidos entre julho de 2015 e setembro de 2015, sendo direcionado a qualquer indivíduo que exercesse funções em território português.

Neste estudo foi averiguado como é que as organizações encaram a cibersegurança e de que forma estão protegidos. Com a realização deste inquérito espera-se que sejam alteradas mentalidades relativas à cibersegurança, e seja dada a importância a este tema que, na verdade, é-lhe que merecida.

Com este inquérito foi possível a AP2SI analisar de que modo é que as empresas se importam com esta temática e de que forma o colocam em prática a proteção devida. A principal ambição deste trabalho foi intensificar a consciencialização para esta questão da cibersegurança. Numa primeira fase o inquérito foi respondido por 169 indivíduos.

De acordo com os resultados obtidos nesta investigação, constatou-se que tanto as organizações como os seus colaboradores estão conscientes de alguns riscos a que estão expostos. Foi comprovado que, os cargos de gestão ainda não estão conscientes o suficiente dos riscos a que estão inerentes, acreditam que ainda não se justifica a adoção de medidas específicas, por exemplo, a contratação de recursos humanos com formação específica nesta área.

Este estudo foi desenvolvido em parceria com o Departamento de Matemática da Escola de Tecnologias e Arquitetura do ISCTE-IUL para uma análise profunda dos resultados. A divulgação do inquérito foi efetuado pela Associação de Empresas Familiares (AEF) e pela Associação de Segurança de Portugal (ADSP).

Este estudo não avalia o nível de maturidade das organizações inquiridas através do inquérito. A AP2SI apenas desenvolveu e disponibilizou o inquérito para se perceber como as organizações lidam com este tema e, desta forma, fosse possível sensibilizar as organizações sobre este tema.

Gestão da Cibersegurança em empresas Transnacionais relacionadas com Transações Financeiras Críticas de espectro Macroeconómico

No seu trabalho de 2018, Cláudia Maria Félix Leite de Faria [36] baseou-se nos controlos da norma ISO/IEC 27001:2013 para construir uma matriz de avaliação de cibersegurança.

Esta matriz foi desenvolvida através do mapeamento entre as regulamentações obrigatórias e opcionais, bem como pelos requisitos requeridos no contexto da atividade das empresas envolvidas nesta investigação. Foi desenvolvido em ambiente

empresarial e teve como objetivo avaliar os riscos de segurança de informação e verificar a conformidade com a ISO/IEC 27001:2013.

Esta avaliação foi efetuada sob a forma de inquérito, em que participaram 13 equipas. Estas equipas que participaram no estudo, estavam associadas, de alguma forma, à criação e desenvolvimento dos sistemas de informação submetidos a esta avaliação. Esta matriz vem apoiar o setor que participou no estudo, a verificar em que nível de conformidade se encontra na identificação de medidas de segurança, para reduzir os riscos de segurança.

Esta matriz de avaliação baseia-se nos controlos da norma ISO/IEC 27001:2013, obtida através do mapeamento feito entre normas e regulamentações.

Depois da análise dos inquéritos é possível definir apenas em que nível de conformidade se encontra a organização de modo a serem reduzidos os riscos de segurança. Para testar esta matriz foi desenvolvido um inquérito, estando este direcionado apenas para o setor financeiro e não estando preparado para ser generalizado e alargado a todas as organizações independentemente do seu processo de negócio.

Avaliação da maturidade em cibersegurança

O CNCS disponibilizou um inquérito online disponível a qualquer indivíduo, para ser possível averiguar em que nível de maturidade se encontra [37]. Este inquérito foi desenvolvido com base no Quadro de Avaliação de Capacidades de Cibersegurança, publicado em janeiro de 2020. Este documento serve como complemento ao QNRCS para auxiliar as organizações a melhorar o seu nível de maturidade.

Este inquérito permite a qualquer indivíduo perceber em que nível de maturidade se encontra.

It Won't Happen to Me: Surveying SME Attitudes to Cyber-security

Após analisar o artigo de maio de 2022 de Martin Wilson, Sharon McDonald, Dominic Button e Kenneth McGarry [38], é possível constatar que foi desenvolvido e disseminado um inquérito online dirigido a PME com sede no Reino Unido, onde foram efetuados vários testes de exploração de ameaças.

Foram realizadas diferentes simulações de ataques, mais concretamente a simulação de um ataque à rede, roubo de dados ou a encriptação de dados, distribuição de *malware*, comprometer alguns dispositivos móveis e ataques de *phishing* por email.

Os resultados obtidos mostram que as PME envolvidas revelam um baixo nível de risco de ataque. Porém, foi possível concluir que apesar de o risco ser baixo, a probabilidade de ocorrência resultava num impacto muito alto para a empresa. Relativamente às medidas para combater estes riscos, os inquiridos referiram que estas eram de baixo custo e eficazes. Relativamente aos dispositivos móveis, as medidas de prevenção não são assim tão eficazes, tal como, os ataques de *phishing* por email.

Tal como a maioria dos trabalhos acima referidos, este inquérito está idealizado apenas para PME, não tendo como objetivo obter o nível de maturidade da empresa, mas sim conhecer o nível de risco a que estão expostas e a probabilidade de ocorrência de problemas.

A Comprehensive Review on the Cyber Security Methods in Indian Organisation

Também em 2022, Dr. Deepshikha Bhatia [39], foca-se na questão da cibersegurança das organizações e na importância que este tema tem para todas as organizações.

No artigo supramencionado mencionada uma aplicação que permite às organizações protegerem e controlar todos os sistemas, redes ou dados pertencentes à organização. O estudo indicado focou-se em organizações da Índia, efetuado através de um inquérito desenvolvido que permite compreender quais os métodos e desafios da cibersegurança em vigor na organização.

A partir dos resultados do inquérito citado, foi possível averiguar qual a melhor forma de proteger os dados sensíveis e eventualmente, podem ser definidos modelos de avaliação de risco e educação/formação neste tema.

Após a realização do estudo supra indicado, é expectável que a maioria dos riscos sejam ultrapassados e que seja possível desenvolver um pensamento preventivo relativamente a esta temática.

Neste artigo foi utilizado como instrumento e método de avaliação um inquérito, os resultados serviram para se perceber a importância deste tema na questão da cibersegurança.

3.3 SÍNTESE

Neste capítulo foi apresentada uma definição do conceito de maturidade e a relação deste conceito a nível organizacional e com a cibersegurança. Para complementar esta definição foram introduzidos alguns trabalhos relacionados onde são abordados estes temas da maturidade e da cibersegurança.

Após a revisão do estado da arte, foi possível constatar-se que foram efetuados diversos estudos para compreender qual o estado das empresas ao nível de cibersegurança, nomeadamente o seu nível de maturidade.

A maioria dos estudos anteriormente descritos utilizou como ferramenta a construção e disponibilização de inquéritos para averiguar as capacidades existentes nas empresas e também para aferir o nível de maturidade ou capacidades de uma organização. Nos restantes estudos existentes verificou-se que foram desenvolvidos diferentes modelos de maturidade, mas não foram testados em casos reais, uma forma de testar estes modelos criados, talvez o desenvolvimento de um inquérito, fosse uma ferramenta adequada para testar estes modelos. Estes trabalhos em que foram criados modelos de maturidade podem justificar uma nova abordagem de maneira a testar o modelo.

O inquérito do CNCS [40] permite notar em que nível de maturidade a empresa se encontra, porém, tendo como base um diferente manual de boas práticas. Este inquérito pode ser um exemplo a considerar para uma nova abordagem sobre este tema.

4

DESENVOLVIMENTO

Neste capítulo é descrito o desenvolvimento da dissertação, com o objetivo de apresentar todas as etapas e decisões que constituem esta dissertação. Primeiro é apresentada a abordagem, utilizada para se obter o nível de maturidade das organizações e a escolha da ferramenta para ser medida a maturidade. De seguida apresenta-se o trabalho realizado e a justificação das escolhas tomadas, sendo apresentada a matriz de maturidade com a fundamentação das opções adotadas.

4.1 ENQUADRAMENTO

Para elaborar esta investigação estudaram-se as normas anteriormente referidas, para que se pudesse verificar quais as normas ou boas práticas a utilizar. Neste estudo foram feitos alguns mapeamentos entre estas normas, mas todos têm em comum a associação com a norma ISO/IEC 27001:2013, sendo esta uma norma fixa para o desenvolvimento da dissertação por ser uma norma muito abrangente e por se adaptar a qualquer tipo de organização. As restantes normas escolhidas para se fazer associação com esta foram, o Regulamento Geral de Proteção de Dados, CIS Controls, Quadro Nacional de Referência para a Cibersegurança e Roteiro para as Capacidades Mínimas da Cibersegurança. Com estes mapeamentos é possível aferir as suas semelhanças e de que forma se podem complementar. Estes mapeamentos podem ser consultados no Apêndice A. Relativamente a estes mapeamentos todos têm associações com controlos da norma ISO/IEC 27001:2013.

Após este estudo, o mapeamento escolhido para suportar a presente investigação foi o mapeamento entre o Roteiro para as Capacidade Mínimas da Cibersegurança e a norma ISO/IEC 27001:2013. Este mapeamento foi o que pareceu mais adequado para se considerar para o desenvolvimento deste trabalho.

Mapeamento entre o Roteiro para as Capacidades Mínimas da Cibersegurança e a norma ISO 27001:2013

Neste mapeamento são descritas as ações do roteiro e os controlos da norma ISO/IEC 27001:2013 que se correlacionam, e o mesmo é apresentado graficamente.

Ação	Descrição da Ação	Controlo ISO27001	Descrição do Controlo
A1.1	Formalização do protocolo de comunicação entre o CNCS e a organização.	**A16.1.1**	Definir os responsáveis para efetuar a gestão e implementar os procedimentos necessários para a gestão dos incidentes.
A1.2	Identificar o responsável de segurança da organização. Esta figura dentro da organização é aquela que é competente para responder às questões postas pelas autoridades competentes nesta área (equipa operacional do CNCS, mais concretamente, CERT.PT).	**A6.1.4** **A16.1.1**	A organização deve manter contacto com grupos de interesse, especializados na área de segurança da informação, de maneira a ampliar os seus conhecimentos e atualizações. Definir os responsáveis para efetuar a gestão e implementar os procedimentos necessários para a gestão dos incidentes.
A1.3	Descrição dos serviços críticos prestados pela organização. Esta ação tem como principal foco apurar os principais serviços críticos para a organização, e isto implica, que sejam ordenados por criticidade, possíveis ameaças e impactos que daí possam advir. Após estas informações deve ser elaborado um quadro global de ameaças da organização.	**A8.2.1**	Garantir que a informação sobre os ativos receba um nível adequado de acordo com a sua importância, valor, requisitos legais e sensibilidade.

A1.4	Estabelecer qual o canal de comunicação para a troca de informação sensível, sempre que seja necessário comunicar com o CNCS. É recomendado que este canal seja cifrado para garantir a integridade da informação enviada.	**A10.1.1** **A10.1.2**	Especificar uma política que especifique quais os ativos que devem ser encriptados. Tudo o que for encriptado deve ser documentado o tipo de documentado qual o tipo de encriptação que foi utilizado, de que forma é gerida, e a identificação do responsável desta área. Deve ser utilizado um certificado digital. Este certificado deve ser emitido por uma entidade certificadora e possui um prazo de validade.
A1.5	A organização deve possuir uma base de dados no Local Internet Registry (LIR). Os dados presentes nesta bases permitem, em caso de incidente, o CNCS fazer a associação de endereços IP a entidades.	Sem associação.	Sem associação.
A1.6	A gestão de risco tem um conjunto de etapas que inclui a identificação, avaliação e resposta ao risco. A organização deve ainda identificar a probabilidade de um evento ocorrer, bem como o seu impacto.	**A12.6.1**	Explorar e identificar possíveis vulnerabilidades de ativos, de forma a minimizar ou eliminar riscos.
A1.7	A organização deve eleger um órgão/equipa ou pessoa responsável pela deteção de incidentes de segurança que ocorram na organização.	**A6.1.1** **A16.1.1**	Devem ser definidas as responsabilidades dos funcionários na organização. Definir os responsáveis para efetuar a gestão e implementar os procedimentos necessários para a gestão dos incidentes.

A1.8	A organização criar uma política de segurança de informação sendo um elemento estruturante para a governação da cibersegurança.	**A5.1.1**	Devem ser definidas políticas para a segurança da informação.
A1.9	Deve ser criado um procedimento de notificação de incidente de cibersegurança relativo às funções que são identificadas como críticas.	**A16.1.2** **A16.1.3** **A16.1.4**	Os eventos de segurança devem ser comunicados através de canais próprios. Os funcionários devem ser instruídos a detetar e reportar qualquer ponto fraco identificado nos sistemas ou serviços. Os eventos de segurança devem ser avaliados de acordo com parâmetros definidos, nomeadamente, a prioridade e a classificação, pois podem ser cruciais para auxiliar na identificação do impacto e na abrangência desse incidente.

Tabela 4: Justificação do Mapeamento das ações da Fase 1 do Roteiro das Capacidades Mínimas para a Cibersegurança

Mapeamento das ações presentes na Fase 2 - Arquitetura

Ação	Descrição da Ação	Controlo ISO27001	Descrição do Controlo
A2.1	Deve ser desenhada uma nova arquitetura de cibersegurança para a organização. Esta arquitetura deve contemplar novas áreas de segurança e identificar	**A12.2.1** **A13.1.3**	Criar controlos para detetar, prevenir e recuperar em caso de existir alguma perda ou danos de informação. Devem ser proibidos o uso de softwares não autorizados. Deve ser feita uma divisão das redes. Esta segregação das redes permite a proteção das informações de cada uma das redes virtuais. Entre estas redes deve ser criada uma Firewall que permite filtrar o tráfego ou, restringir o fluxo de dados entre redes.
A2.2	Recolher os metadados de comunicações durante um período mínimo de 1 ano. Esta recolha deve ser feita a partir dos routers/ switch ou qualquer equipamento com acesso à Internet.	Sem associação.	Sem associação.
A2.3	Definir um procedimento de comunicação operacional entre a organização e o CNCS. Este procedimento deve ser analisado e aprovado pelo departamento jurídico e administração.	**A6.1.4**	A organização deve manter contacto com grupos de interesse, especializados na área de segurança da informação, de maneira a ampliar os seus conhecimentos e atualizações.
A2.4	Efetuar uma inventariação dos ativos.	**A8.1.1**	Fazer um inventário de todos os ativos da organização.

A2.5	Os logs produzidos pelos sistemas e pelas aplicações devem ser recolhidos para posterior análise em caso de incidente de segurança. Deve existir um repositório centralizado destes logs de um período.	**A12.4.1** **A12.4.2**	Registos como os logs, atividades de utilizadores ou falhas, devem ser documentados e analisados regularmente. Esta informação presente nos logs deve estar protegida de acessos não autorizados, de maneira a poder garantir a sua integridade.
A2.6	Após se identificar a origem de um incidente é necessário aplicar medidas para corrigir ou mitigar o mesmo.	**A16.1.5**	A organização deve definir procedimentos de resposta aos incidentes de segurança.
A2.7	A organização deve estar ciente dos quadros legais e regulatórios a que está sujeita.	**A18.1.1**	A organização tem o dever de conhecer quais as legislações ou regulamentações que abrangem o seu processo de negócio, para laborar de acordo com as leis. Deve estar de acordo com todas as normas relativas à segurança da informação e RGPD.
A2.8	A organização deve estar em conformidade com normas ou certificações exigidas por lei, que estejam impostas às atividades da organização. Este deve ser considerado pela organização um fator prioritário.	**A18.1.1**	A organização tem o dever de conhecer quais as legislações ou regulamentações que abrangem o seu processo de negócio, para laborar de acordo com as leis. Deve estar de acordo com todas as normas relativas à segurança da informação e RGPD.
A2.9	É recomendado que a organização defina uma Política de Uso Aceitável (PUA), onde são definidas as linhas orientadoras para uma boa e segura utilização dos recursos.	**A8.1.3**	Definir regras para a utilização dos ativos por parte de todos os colaboradores.

A2.10	A organização deve possuir mecanismos para recuperar de possíveis incidentes e garantir assim a salvaguarda de informação classificada como crítica e prioritária, garantindo assim a sua recuperação.	**A12.3.1**	Realizar e testar as cópias de segurança regularmente. Estes testes garantem a sua integridade.
A2.11	Identificar as responsabilidades para cada colaborador, um plano de formação adequado para atingir os objetivos esperados na função a desempenhar.	**A7.2.2**	Disponibilizar formação e treino durante todo o período que o colaborador desempenhe funções na organização.
A2.12	Realizar ações internas de sensibilização a nível de cibersegurança. Estas ações devem ser transversais a todos os colaboradores da organização.	**A7.2.2**	Disponibilizar formação e treino durante todo o período que o colaborador desempenhe funções na organização.
A2.13	Os colaboradores pertencentes aos órgãos de gestão devem ter formação específica dos principais mecanismos de governação interna, e também à metodologia de gestão de risco e a sua aplicação na prática.	**A7.2.2**	Disponibilizar formação e treino durante todo o período que o colaborador desempenhe funções na organização.

Tabela 5: Justificação do Mapeamento das ações da Fase 2 do Roteiro das Capacidades Mínimas para a Cibersegurança

Mapeamento das ações presentes na Fase 3 - Segurança dos Dispositivos

Ação	Descrição da Ação	Controlo ISO27001	Descrição do Controlo
A3.1	Definir procedimentos para a deteção de incidentes e atualização de ativos. Identificar as responsabilidades e funções para estes procedimentos.	**A16.1.1**	Definir os responsáveis para efetuar a gestão e implementar os procedimentos necessários para a gestão dos incidentes.
A3.2	Instalação de Host-Based Intrusion Detection System (HIDS) de maneira a garantir uma proteção adicional de deteção em comparação com os sistemas tradicionais. Estes sistemas devem ser instalados nos sistemas críticos da organização.	Sem associação.	Sem associação.
A3.3	Registar todos os acessos efetuados às bases de dados que contém informação sensível para evitar acessos não autorizados. É oportuno que estes registos sejam mantidos durante o período de um ano. Desta forma torna-se possível fazer uma auditoria e análise forense se existir um incidente.	**A12.4.2**	Registos como os logs, atividades de utilizadores ou falhas, devem ser documentados e analisados regularmente.
A3.4	Instalar e efetuar a devida configuração de controlos de acesso web, nomeadamente, um serviço proxy.	**A13.1.1**	Utilizar softwares para registar eventos e monitorizar a rede para analisar o tráfego.
A3.5	Instalar antivírus em todos os equipamentos que contenham serviços críticos. É conveniente que a organização defina uma política BYOD que deve ter em conta diversos aspetos dos dispositivos móveis.	**A6.2.1** **A6.2.2**	Definir políticas específicas para os dispositivos móveis. Estabelecer políticas especiais para o teletrabalho e todos os equipamentos que saem da estrutura física da organização.

A3.6	Instalar sistemas de monitorização dos principais ativos de rede e sistemas de suporte às principais atividades da organização. Estes sistemas devem estar aptos para medir diversos parâmetros, nomeadamente, disponibilidade e qualidade dos equipamentos lançando alertas sempre que necessário.	**A13.1.2**	Implementar serviços de proteção e monitorização da rede da organização.
A3.7	Definir um processo de Hardening. Este processo fornece um robustecimento de acordo com as ameaças, ações de mitigação dos riscos e execução de atividades corretivas.	**A13.1.1**	Utilizar softwares para registar eventos e monitorizar a rede para analisar o tráfego.
A3.8	A organização deve investir num Security Information and Event Management (SIEM). Este sistema tem como principal função efetuar a gestão e correlação de eventos e dados. Armazena informações como registos (logs) mais relevantes.	**A13.1.1**	Utilizar softwares para registar eventos e monitorizar a rede para analisar o tráfego.

A3.9	Definir um plano de continuidade de negócio. Este plano permite que a organização continue a laborar mesmo em caso de desastre ou incidente.	**A17.1.1** **A17.1.2** **A17.1.3**	Determinar quais os requisitos de segurança da informação, tendo em conta a continuidade da informação em situações de desastre ou incidente, e simultaneamente, manter a informação íntegra. Devem ser estabelecidos, mantidos, documentados e implementados, todos os processos ou procedimentos para assegurar o nível requerido de continuidade para a segurança da informação. O plano de continuidade de negócio ou plano de recuperação de desastres/incidentes devem estar guardados fora da empresa. É recomendado ainda, que sejam verificados e testados periodicamente, de forma a garantir que são eficazes e robustos sempre que necessário.
A3.10	As pessoas com conhecimentos técnicos devem estar aptas para efetuar a análise de artefactos informáticos e devem receber formação concreta nesta área. Para serem bem sucedidas nas investigações forenses que forem necessárias de realizadas.	**A7.2.2**	Disponibilizar formação e treino durante todo o período que o colaborador desempenhe funções na organização.

Tabela 6: Justificação do Mapeamento das ações da Fase 3 do Roteiro das Capacidades Mínimas para a Cibersegurança

Mapeamento das ações presentes na Fase 4 - Consolidar a Cibersegurança

Ação	Descrição da Ação	Controlo ISO27001	Descrição do Controlo
A4.1	Formalizar a cadeia de responsabilidades e traçar os privilégios de acesso individual. Estes privilégios devem ser de conhecimento geral e aprovados pela administração da empresa.	**A9.4.1**	O acesso à informação deve ser restrito por utilizador.
A4.2	Normalizar e regular os termos de funcionamento internos da empresa, através da criação de boas práticas e políticas (Sistema Interno de Normas e Políticas), o qual deve ser seguido por todos os colaboradores.	**A5.1.1** **A9.1.1**	Devem ser definidas políticas para a segurança da informação. Desenvolvimento de políticas de controlo de acesso. Estas políticas devem ser delineadas pelo proprietário dos ativos e este determina as regras do controlo de acesso.
A4.3	Avaliação do processo de gestão de risco.	**A17.1.3**	O plano de continuidade de negócio ou plano de recuperação de desastres/incidentes devem estar guardados fora da empresa. É recomendado ainda, que sejam verificados e testados periodicamente, de forma a garantir que são eficazes e robustos sempre que necessário.
A4.4	É aconselhada a realização de simulacros com uma periodicidade anual, com o objetivo de entender o grau de preparação para incidentes dos especialistas existentes e testar as capacidades mínimas.	**A17.1.3**	O plano de continuidade de negócio ou plano de recuperação de desastres/incidentes devem estar guardados fora da empresa. É recomendado ainda, que sejam verificados e testados periodicamente, de forma a garantir que são eficazes e robustos sempre que necessário.

A4.5	Identificar os tipos de ataques mais comuns e criar métodos de mitigação. Esta informação deve ser documentada e aprovada pela administração da organização. E ainda, é recomendado que seja implementado um sistema de notificações para que qualquer colaborador saiba como atuar em caso de incidente.	**A16.1.6**	Devem-se tirar lições e aprendizagens de todos os incidentes que ocorram na organização, de forma a reduzir a probabilidade ou impacto de incidentes possam vir a acontecer no futuro.
A4.6	Sensibilizar todos os colaborares e órgãos da administração sobre o SINP. A sensibilização deve ser feita por especialistas na área para que sejam explicadas as normas que devem ser implementadas no quotidiano da organização.	**A7.2.2**	Disponibilizar formação e treino durante todo o período que o colaborador desempenhe funções na organização.
A4.7	Adotar práticas que se foquem no princípio da segurança. Para adotar este princípio, é indispensável que todos os serviços que são baseados em recursos de TIC sejam submetidos a uma bateria de testes de segurança, antes de serem postos em funcionamento.	**A14.2.9**	Devem ser definidos testes de aceitação, bem como os critérios de aceitação para eventuais sistemas de informação que surjam futuramente.
A4.8	É recomendado que exista uma postura defensiva na organização. Uma sugestão é a utilização de honeypots, em que a sua função é basicamente reproduzir algumas atividades comuns praticadas pela organização e assim atrair atacantes para que se fique a conhecer os seus métodos.	Sem associação.	Sem associação.

A4.9	Deve ser feita uma boa gestão de patching e atualizações para manter um nível razoável de segurança.	**A14.2.4** **A14.2.9**	Dissuadir as alterações no software. As alterações devem ser apenas as necessárias, e devem ser totalmente controladas. Devem ser definidos testes de aceitação, bem como os critérios de aceitação para eventuais sistemas de informação que surjam futuramente.

Tabela 7: Justificação do Mapeamento das ações da Fase 4 do Roteiro das Capacidades Mínimas para a Cibersegurança

Mapeamento das ações presentes na Fase 5 - Equipa de Cibersegurança

Ação	Descrição da Ação	Controlo ISO27001	Descrição do Controlo
A5.1	Nomeação de um responsável máximo da segurança da informação. Esta etapa apenas faz sentido numa organização com algum grau de complexidade ou de grande dimensão.	**A16.1.1**	Definir os responsáveis para efetuar a gestão e implementar os procedimentos necessários para a gestão dos incidentes.
A5.2	Deve ser criado um serviço de gestão de vulnerabilidades, para englobar as componentes de deteção e mitigação de incidentes. É aconselhado que seja executado com a regularidade necessária, para detetar vulnerabilidades na rede da organização.	**A12.6.1**	Explorar e identificar possíveis vulnerabilidades de ativos, de forma a minimizar ou eliminar riscos.
A5.3	Todos os controlos de segurança da organização devem ser postos à prova, através da realização de auditorias. Estas auditorias devem ser externas e internas, é recomendável que sejam feitas anualmente e por especialistas da área.	**A12.7.1**	As atividades de auditoria que sirvam para verificar os sistemas de produção devem ser projetadas de forma a minimizar interrupções no processo de negócio.
A5.4	Deve ser traçada a missão e visão do SOC/CSIRT na organização. Esta missão passa por definir a comunidade que vai usufruir destes serviços e ainda, a panóplia de serviços adequados para atingir os objetivos sugeridos.	**A12.6.1**	Explorar e identificar possíveis vulnerabilidades de ativos, de forma a minimizar ou eliminar riscos.
A5.5	Deve ser elaborado e aprovado o plano e orçamento do SOC/CSIRT.	Sem associação.	Sem associação.

A5.6	Para implementar um CSIRT é necessário preparar canais de comunicação, mecanismos de encriptação e ferramentas de suporte à análise forense de incidentes de segurança. Esta equipa deve ter presença assídua em fóruns de cibersegurança.	Sem associação.	Sem associação.
A5.7	Implementar a gestão de crise para lidar com grandes incidentes de segurança.	**A17.1.2**	Devem ser estabelecidos, mantidos, documentados e implementados, todos os processos ou procedimentos para assegurar o nível requerido de continuidade para a segurança da informação.
A5.8	O CSIRT deve estar integrado em diversas comunidades de cibersegurança para que o seu desempenho seja bem sucedido.	Sem associação.	Sem associação.
A5.9	A equipa CSIRT deve participar em exercícios de cibersegurança, de forma a testar os seus conhecimentos e capacidades de resposta a incidentes. Esta participação deve ser executada uma vez por ano.	**A17.1.3**	O plano de continuidade de negócio ou plano de recuperação de desastres/incidentes devem estar guardados fora da empresa. É recomendado ainda, que sejam verificados e testados periodicamente, de forma a garantir que são eficazes e robustos sempre que necessário.

Tabela 8: Justificação do Mapeamento das ações da Fase 5 do Roteiro das Capacidades Mínimas para a Cibersegurança

Foi selecionado este mapeamento como fundamento deste estudo por ter presente a norma ISO27001:2013 e as boas práticas presentes no Roteiro para as Capacidades Mínimas, ambas têm vários controlos que podem ser associados. Nas fases do roteiro

a maioria das ações têm associação direta com um ou vários controlos do roteiro, como, por exemplo:

- **Fase 1** - 89% de associação;
- **Fase 2** - 92% de associação;
- **Fase 3** - 90% de associação;
- **Nível 4** - 89% de associação;
- **Nível 5** - 66% de associação.

De uma forma geral, a percentagem total de associação entre o Roteiro para as Capacidades Mínimas da Cibersegurança e a norma ISO27001:2013 é de 83%. O Roteiro para as Capacidades Mínimas pode ser utilizado como referencial para as organizações portuguesas e com este mapeamento ficam a saber quais os controlos da norma ISO27001:2013 e que ações do roteiro têm implementadas ou ainda estão em falta. Este mapeamento serviu para estruturar as questões do inquérito com a finalidade de obter o nível de maturidade.

Após o estudo das normas e das suas associações, ponderou-se que através da análise de respostas de um inquérito dadas pelas organizações se conseguiria obter o nível quantitativo e qualitativo de maturidade das organizações inquiridas. Neste sentido, desenvolveu-se um inquérito para esse efeito, disseminou-se a solicitação do preenchimento do mesmo, sendo analisados os resultados para obter o nível de maturidade das organizações.

Seguidamente passou-se à fase de definição e construção do inquérito, considerando que era necessário ter como referência este mapeamento citado.

Mapeamento ações do roteiro CNCS - Controlos ISO 27001

Ações	A1.1	A1.2	A1.3	A1.4	A1.5	A1.6	A1.7	A1.8	A1.9	A2.1	A2.2	A2.3	A2.4	A2.5	A2.6	A2.7	A2.8	A2.9	A2.10	A2.11	A2.12	A2.13	A3.1	A3.2	A3.3	A3.4	A3.5	A3.6	A3.7	A3.8	A3.9	A3.10	A4.1	A4.2	A4.3	A4.4	A4.5	A4.6	A4.7	A4.8	A4.9	A5.1	A5.2	A5.3	A5.4	A5.5	A5.6	A5.7	A5.8	A5.9
Seção																																																			
A5.1																																																			
A5.1.1								X																									X																
A6.1																																																		
A6.1.1							X																																										
A6.1.4		X										X																																					
A6.2.1																											X																						
A6.2.2																											X																						
A7.2.2																				X	X	X										X					X												
A8.1.1													X																																					
A8.1.3																		X																																
A8.2.1			X																																														
A9.1.1																																		X															
A9.4.1																																	X															
A10.1.1				X																																													
A10.1.2				X																																													
A12.1.1										X																																						
A12.3.1																			X																															
A12.4														X																																			
A12.4.1														X																																			
A12.4.2																									X																								
A12.6.1						X																																					X		X				
A12.7.1																																												X					
A13.1.1																										X			X	X																		
A13.1.2																											X																						
A13.1.3										X																																							
A14.2.4																																											X						
A14.2.9																																											X		X				
A16.1.1	X	X					X		X														X																				X					
A16.1.2									X																																								
A16.1.3									X																																								
A16.1.5															X																																		
A16.1.6																																								X								
A17.1.1																															X																
A17.1.2																															X																
A17.1.3																															X																
A18.1.1																X	X																																

Sem correlação encontrada

Figura 19: Tabela de mapeamento Roteiro para as Capacidades Mínimas da Cibersegurança - ISO 27001:2013

4.2 MODELO DE MATURIDADE

Considerando que a maturidade um conjunto de 5 etapas, em que cada uma delas é composta por capacidades mínimas/ações que devem ser desenvolvidas e implementadas pelas organizações. Este modelo tem como base 3 pilares fundamentais, que são, a prevenção, a deteção e a reação.

O nível de maturidade é avaliado tendo em conta 5 fases (fase 1 a fase 5). Estes níveis foram definidos da seguinte forma:

- **Nível 1** - deve ser definido um ponto de contacto com o CNCS e devem ser definidas as áreas críticas bem como a gestão de ativos destas;
- **Nível 2** - devem ser recolhidos os metadados de comunicações e outros registos para análise de incidentes e devem existir ferramentas para a mitigação de incidentes de segurança;
- **Nível 3** - a presença de recursos humanos com formação nesta área, com as capacidades para analisar incidentes e que estabeleçam a comunicação com o CNCS;
- **Nível 4** - processos internos de resposta a incidentes, e que esteja definida a cadeia de responsabilidades no que toca a resposta a incidentes de segurança, e ainda, que sejam realizados simulacros de cibersegurança.
- **Nível 5** - deve existir uma equipa dedicada à cibersegurança (CSIRT ou SOC), e que esta equipa esteja envolvida em projetos e partilha de informação na comunidade nacional de CSIRT.

Visto que a maturidade é constituída por estas 5 fases, decidiu-se que esta se conseguiria obter através de um inquérito como instrumento para esse efeito. Por forma a definir as melhores questões que poderiam levar à obtenção do nível de maturidade, as questões foram construídas com base no mapeamento citado e a estrutura do inquérito teve por base este modelo de maturidade.

4.3 INQUÉRITO

Seguidamente vão ser apresentados os detalhes do desenvolvimento da dissertação após os mapeamentos, onde é apresentada todo o processo de implementação e da estrutura do inquérito, e justificação das escolhas tomadas.

Figura 20: Etapas do desenvolvimento do inquérito

Na Figura 20 onde se pode observar as etapas necessárias para o desenvolvimento do inquérito.

Após a recolha das respostas ao inquérito, quem assim o indicar receberá um relatório individual personalizado com o seu nível de maturidade, que contém algumas sugestões de melhoria para aumentar o nível de maturidade da organização em cada uma das fases.

Metodologia de Construção do inquérito

A construção de um inquérito não é uma tarefa trivial, pois requer dedicação e tempo despendido por parte de quem está o desenvolver. Durante o processo de construção do inquérito é necessário ter em conta a linguagem e como se aborda o inquirido, como são formuladas as questões e a apresentação do questionário.

As questões do questionário seguem os seguintes princípios:

- **Princípio da Clareza** - deve ser claro e conciso;
- **Princípio da Coerência** - devem corresponder à intenção da pergunta;
- **Princípio da Neutralidade** - não deve induzir a uma determinada resposta.

Na construção deste inquérito foi definido apenas um tipo de respostas, as respostas estruturadas (fechadas).

Este tipo de respostas permite simplificar a quantificação e efetuar o tratamento estatístico posteriormente. As respostas fechadas permitem, ainda, comparar de forma mais transparente as respostas dadas dos diferentes inquiridos. Porém, este tipo de respostas, as quais são previamente determinadas e selecionadas pelo investigador, podem limitar a expressão do sujeito, e este não responder da forma que pretendia. Isto significa, que podemos ficar sem conhecer se existem variações no nível das respostas dadas.

Enquanto um inquérito composto por respostas estruturadas permite conhecer a variabilidade de comportamentos, atitudes e opiniões dos inquiridos, e dispõe-se de total controlo sob as respostas dadas.

A construção deste inquérito baseou-se na utilização de duas escalas, do tipo Likert [41] e em respostas dicotómicas.

O facto de serem disponibilizados diferentes tipos de resposta permite obter diferentes pontos de vista sobre este tema, bem como facilitar a comparação entre as respostas dadas, e desta forma tirar conclusões mais concretas. As respostas dicotómicas são compostas apenas por duas opções de resposta, nomeadamente, Sim ou Não. Estas respostas, tornam-se exclusivas, pois o inquirido está "sujeito"a uma das possibilidades de resposta, e devem ser, exaustivas, pois todos os sujeitos devem poder enquadrar-se numa das duas hipóteses de resposta. Com estas respostas é possível formar-se dois grupos distintos de resposta e comparar se existem diferenças significativas entre elas.

Nas respostas de escala, permitem obter conclusões quantitativas e obter opinião sobre este tema da cibersegurança.

A escala do tipo Likert, permite que o inquirido escolha a opção entre dois extremos, escolhendo o ponto que mais se adequa ao seu caso. Com a utilização desta escala é possível perceber as atitudes ou comportamentos dos inquiridos.

No presente inquérito foram utilizadas duas escalas de Likert, de frequência e de importância.

A escala de frequência foi aplicada para se entender qual a frequência que determinadas ações são efetuadas na organização, tal como a escala de importância foi utilizada para se aferir qual o nível de importância que este tema representa na organização.

Quando são utilizados estes tipos de escalas é necessário contemplar um nível de equilíbrio, nomeadamente em relação à quantidade de níveis positivos e níveis negativos, e entre estes deve existir um nível neutro. De acordo com este princípio, utilizou-se um nível totalmente positivo, um parcialmente positivo, um neutro, um parcialmente negativo e por fim, um nível totalmente negativo.

A escala de frequência, é composta pelos seguintes níveis:

- **Muito frequente**
- **Frequente**
- **Ocasionalmente**
- **Raramente**
- **Nunca**

A escala de importância, é composta pelos seguintes níveis:

- **Muito Importante**
- **Importante**
- **Indiferente**
- **Pouco Importante**
- **Nada Importante**

A utilização deste tipo de escala na construção de um inquérito tem várias vantagens e desvantagens.

As principais vantagens da utilização desta escala são as seguintes:

- Trata-se de um processo fácil de construção e colocá-la em prática, pois existem várias possibilidades de respostas, garantindo assim uma resposta mais clara à pergunta efetuada

- Minimiza a hipótese de respostas amplas ou ambíguas, por exemplo, as respostas de "Sim ou Não", que se tornam mais complexas para responder e pode prejudicar os resultadas do inquérito;
- Esta escala é visualmente fácil de entender e o inquirido entende sem dúvida a lógica desta.

Porém, existem pontos fracos na utilização desta escala, que vão ser descritos seguidamente:

- Para o indivíduo que vai efetuar a análise das respostas dadas, torna-se difícil definir e lidar com as respostas neutras, concretamente o "indiferente", pois este tipo de resposta fornece poucas informações aplicáveis de forma prática;
- Se o inquirido responder de forma "automática"à questão, a resposta pode ser impulsiva e não expressa o seu verdadeiro sentimento segundo a realidade.

Este tipo de escala é bastante utilizada apesar dos seus contras, mostra-se altamente eficiente quando se pretende analisar a satisfação ou experiência dos indivíduos.

Questões do Inquérito

As perguntas presentes no inquérito, surgiram após a análise das associações encontradas no mapeamento efetuado entre o Roteiro para as Capacidades Mínimas da Cibersegurança e a norma ISO 27001:2013.

Tendo em conta as fases presentes no Roteiro para as Capacidade Mínimas, o inquérito encontra-se dividido por secções com o intuito de se medir o nível de maturidade em cada fase, e foi posteriormente definido um modelo de maturidade.

As secções presentes no inquérito, correspondem com as fases presentes no nível de maturidade implementado e as restantes correspondem a questões gerais sobre este tema.

As primeiras questões deste inquérito são genéricas sobre a organização.

Informações Gerais sobre a organização
Qual é o setor de atividade da organização?
Qual é o número de colaboradores da organização?
Qual é o número de colaboradores da organização?
Que tipo de tecnologias são utilizadas pela organização?
Em que região está sediada a organização?

Tabela 9: Questões da primeira secção do inquérito - parte I

Na Tabela 9, estão presentes as questões que permitem fazer uma caracterização geral da organização.

As perguntas seguintes, ainda presentes nesta secção, são genéricas sobre a cibersegurança, numa lógica de alto nível, sem entrar em grande detalhe.

Informações Gerais sobre a organização
Qual o grau de importância da segurança a informação para a organização?
A organização tem preocupação com os danos reputacionais em caso de incidente de segurança?
Qual é o tipo de informação processada pela organização?
A sua empresa tem algum seguro contratado para cobrir incidentes de segurança?
A sua empresa tem colaboradores certificados na área de Cibersegurança?
Qual(is) das seguintes certificações possi(uem) os colaboradores ou a organização?
Qual o orçamento anual para investir em Cibersegurança:

Tabela 10: Questões da primeira secção do inquérito - parte II

Na Tabela 10 estão presentes as questões que permitem fazer uma caracterização de alto nível sobre a cibersegurança na organização.

Fase 1 - Preparação Inicial
Está definida uma forma de comunicação com o CNCS?
Quais são os canais de comunicação que estão definidos com o CNCS?
Existe um inventário de ativos e serviços críticos da organização?
De que forma é feita a inventariação dos ativos?
Os ativos da organização são encriptados?
São efetuados testes de penetração aos ativos da organização?

Tabela 11: Questões presentes na segunda secção do inquérito

Na Tabela 11 estão apresentadas as questões relativas à primeira fase do nível de maturidade.

Fase 2 - Arquitetura
Quais das seguintes soluções de segurança estão disponíveis na organização para lidar com possíveis ameaças?
As soluções de segurança indicadas na questão anterior são utilizadas nos sistemas e postos de trabalho onde é tratada informação crítica?
Na organização é utilizada alguma tecnologia com a capacidade de analisar tráfego malicioso?
Quais dos seguintes procedimentos de backup/restore estão implementados na organização?
A organização é conhecedora dos quadros legais e regulatórios a que está sujeita (nacionais e europeus)?
Existem relatórios de auditorias que comprovem a conformidade com a legislação e regulamentação?
É efetuado o registo de eventos como logs e atividades de utilizadores?
Qual o número de horas de ações de formação e sensibilização de colaboradores em matéria de cibersegurança na organização?
A quem se destinam estas ações de formação disponibilizadas na organização?
Na organização são utilizados alguns dos seguintes lembretes relativamente a boas práticas de cibersegurança?

Tabela 12: Questões presentes na segunda secção do inquérito

Na Tabela 12 estão apresentadas as questões relativas à segunda fase do nível de maturidade.

Fase 3 - Segurança dos Dispositivos
Com que regularidade são auditadas as configurações dos dispositivos?
A organização tem uma política BYOD (Gestão de Dispositivos Móveis Pessoais)?
De que forma é feita a gestão de eventos de segurança?
Existe algum sistema de monitorização dos principais ativos de rede e sistemas que dão suporte às atividades da organização?
Os colaboradores têm conhecimento de como utilizar informação crítica?

Tabela 13: Questões presentes na terceira secção do inquérito

Na Tabela 13 estão apresentadas as questões relativas à terceira fase do nível de maturidade.

Fase 4 - Consolidar a Cibersegurança
Com que regularidade são feitas as atualizações de software?
Quais os procedimentos de segurança, que estão definidos na política de dispositivos móveis?
Antes da entrada em produção, os sistemas e aplicações são submetidos a testes de cibersegurança?
Por quem são efetuados os testes de cibersegurança indicados na questão anterior?
Já foi efetuado algum simulacro de Cibersegurança na organização?
Com que frequência são efetuados estes simulacros?
Existe uma equipa capaz de dar resposta a incidentes de cibersegurança na sua organização?

Tabela 14: Questões presentes na quarta secção do inquérito

Na Tabela 14 estão apresentadas as questões relativas à quarta fase do nível de maturidade.

Fase 5 - Equipa de Cibersegurança
Foi nomeado um (Responsável de Segurança de Informação) CISO na organização?
A organização possui algum destes serviços?
Alguma vez a organização foi alvo de um ataque informático?
Estes ataques foram documentados?
Que tipo(s) de ataque sofreu?
Considera que qualquer colaborador sabe como atuar em caso de ataque informático?
Existe um processo para que todos os colaboradores possam reportar possíveis incidentes de segurança?

Tabela 15: Questões da quinta secção do inquérito

Na Tabela 15 estão apresentadas as questões relativas à quinta fase do nível de maturidade.

Relatório de Maturidade da Organização
Pretende que lhe seja posteriormente enviado um relatório de maturidade da organização via e-mail?
Forneça por favor, o e-mail que pretende receber o relatório de maturidade de Cibersegurança:

Tabela 16: Questões da última secção do inquérito sobre o Relatório de Maturidade da Organização

Na tabela 16 estão apresentadas as questões da última secção do inquérito. Este grupo destina-se a perceber se as organizações pretendem receber posteriormente um relatório com dados detalhados sobre o seu nível de maturidade.

De salientar que todas as questões presentes nas Tabelas 9, 10, 11, 12, 13, 14, 15 e 16 sofreram várias alterações desde a sua primeira versão, até à versão final. Todo o inquérito foi validado e teve o parecer de especialistas da área.

Plataforma onde o inquérito foi disponibilizado

Antes de se escolher a plataforma final, foram feitos diversos testes noutras plataformas destinadas à construção de inquéritos como, por exemplo, a plataforma Survey Mokney [1], Lime Survey [2] e ainda, Google Forms [3].

Figura 21: Plataformas onde foram testados os inquéritos

A plataforma Survey Monkey inicialmente, não foi escolhida por não permitir atribuir pontuação a cada pergunta da forma pretendida e não ser tão transparente para o utilizador. Esta plataforma não permitiu dividir o inquérito em secções.

Não se optou pela plataforma Google Forms, por não possuir um *backoffice* que auxiliasse na análise de resultados, e concluiu-se que era bastante limitado no tipo de respostas que se poderia colocar. Porém, trata-se de uma plataforma conhecida para grande parte dos indivíduos e bastante simples na ótica do utilizador.

A plataforma Lime Survey não foi considerada para implementar este inquérito, pois para definir as perguntas com condições não se mostrou trivial e eficaz. Esta plataforma também não possui um *backoffice* para auxiliar na análise de resultados.

1 https://pt.surveymonkey.com/
2 https://www.limesurvey.org/pt/
3 https://docs.google.com/forms/

Após esta análise exaustiva de plataformas de inquéritos concluiu-se que a plataforma Question Pro [4] respondia a todas as necessidades necessárias. Ao contrário das outras plataformas testadas, esta mostrou ter uma interface bastante simplista para o utilizador, a nível das perguntas com condições revelou ser bastante eficaz e simples, e ainda permite obter uma panóplia de gráficos e resultados formatados e de fácil compreensão para quem está a desenvolver o estudo e chegar a conclusões concretas de forma mais cómoda. Trata-se de uma plataforma online e gratuita.

Disseminação do inquérito

Como forma de disseminação do inquérito, foi elaborado um email em tom de convite para os órgãos de administração de diversas organizações.

"Com o objetivo de avaliar a maturidade da Cibersegurança das empresas em Portugal, estou a coordenar um estudo intitulado "Avaliação da maturidade em Cibersegurança do tecido industrial português". O estudo conta com apoio da estudante Ana Beatriz Ribeiro do Mestrado em Cibersegurança e Informática Forense do Politécnico de Leiria. Assim, venho, por este meio, solicitar a vossa colaboração na divulgação de um inquérito online junto dos vossos associados para recolher o seu valioso contributo para este estudo que, no final, caso assim pretendam, poderão receber um relatório com o grau de maturidade em que se encontram as suas organizações."

https://questionpro.com/t/AU1HIZtYO3

"O questionário é anónimo, e não requer muito esforço. Antecipadamente gratos pela vossa colaboração!"

No texto acima apresentado pode-se observar o email enviado organizações com o link para acesso do inquérito para se obter as respostas pretendidas.

Para garantir um preenchimento dos inquéritos e obter o maior número de respostas, foram reforçados os pedidos de resposta por email, e em alguns casos, presencialmente.

Seguidamente encontram-se a lista de associações representativas de diversos setores para os quais foram enviadas mensagens a solicitar a divulgação deste estudo pelos seus associados:

- **CEFAMOL**
- **APIP**
- **NERLEI**

4 https://www.questionpro.com/pt-br/?

- **clustermineralresources**
- **AFIA - Associação de Fabricantes para a Indústria Automóvel**
- **AIMMAP - Associação dos Industriais Metalúrgicos, Metalomecânicos e Afins de Portugal**
- **AIMMP - Associação das Indústrias de Madeira e Mobiliário de Portugal**
- **AIN - Associação das Indústrias Navais**
- **ANEME - Associação Nacional das Empresas Metalúrgicas e Eletromecânicas**
- **ANETIE - Associação Nacional das Empresas de Tecnologia de Informação**
- **ANICP - Associação Nacional dos Industriais de Conservas de Peixe**
- **ANIET - Associação Nacional da Indústria Extrativa e Transformadora**
- **ANIVEC/APIV - Associação Nacional das Indústrias de Vestuário e Confeção**
- **APCOR - Associação Portuguesa da Cortiça**
- **APF - Associação Portuguesa de Fundição**
- **APIC - Associação Portuguesa dos Industriais de Curtumes**
- **APICCAPS - Associação Portuguesa dos Industriais de Calçado, Componentes e Artigos de Pele e os seus Sucedâneos**
- **APICER - Associação Portuguesa da Indústria da Cerâmica**
- **APIFARMA - Associação Portuguesa da Indústria Farmacêutica**
- **APIMA - Associação Portuguesa das Indústrias de Mobiliário e Afins**

4.4 MATRIZ DE MATURIDADE

Tendo em conta a finalidade do inquérito e, considerando que se decidiu organizar as perguntas e o questionário segundo o mapeamento e o modelo de maturidade, tornou-se necessário definir uma matriz de avaliação para ser possível calcular o nível de maturidade das organizações inquiridas.

Para estudar a maturidade de uma organização através de um inquérito, foram atribuídos diferentes pesos a cada questão pertencente na Fase 1 à Fase 5. Nos dois conjuntos de questões gerais não foram definidos quaisquer pesos nem foram considerados para o cálculo da maturidade, pois são questões de caracterização geral e recolha de informação de alto nível sobre este tema.

Foram atribuídos diferentes pesos tendo em conta a importância da questão e desta forma poder distinguir as empresas que têm determinadas capacidades. Se as organizações tiverem conhecimento do nível de maturidade, é o primeiro passo para poderem delinear estratégias para o melhorar.

O nível de maturidade coincide com cada uma das fases presentes no mapeamento efetuado e no modelo de maturidade, em que cada uma destas fases estão associadas capacidades avaliadas através do inquérito.

Pergunta	**Peso**
Está definida uma forma de comunicação com o CNCS?	2
Quais são os canais de comunicação que estão definidos com o CNCS?	0.5*5
Existe um inventário de ativos e serviços críticos da organização?	1
De que forma é feita a inventariação dos ativos?	1
Os ativos da organização são encriptados?	1
São efetuados testes de penetração aos ativos da organização?	1
Total	8.5

Tabela 17: Pesos de cada questão da Fase 1 - Preparação Inicial

Na Tabela 17 estão indicados os pesos de cada questão da Fase 1 do modelo de maturidade. Na segunda questão são apresentados por defeito 4 canais de comunicação, por esse motivo atribuiu-se o peso de 0,5 a cada um. Como é dada a opção do inquirido escrever outra opção, e caso esta seja válida, é de igual forma contabilizada como 0,5.

Pergunta	Peso
Quais das seguintes soluções de segurança estão disponíveis na organização para lidar com possíveis ameaças?	0.5*4
As soluções de segurança indicadas na questão anterior são utilizadas nos sistemas e postos de trabalho onde é tratada informação crítica?	1
Na organização é utilizada alguma tecnologia com a capacidade de analisar tráfego malicioso?	1
Quais dos seguintes procedimentos de backup/restore estão implementados na organização?	0.5*4
A organização é conhecedora dos quadros legais e regulatórios a que está sujeita (nacionais e europeus)?	1.5
Existem relatórios de auditorias que comprovem a conformidade com a legislação e regulamentação?	1
É efetuado o registo de eventos como logs e atividades de utilizadores?	1.5
Qual o número de horas de ações de formação e sensibilização de colaboradores em matéria de cibersegurança na organização?	0.5; 0.75; 1
A quem se destinam estas ações de formação disponibilizadas na organização?	0.5*4
Na organização são utilizados alguns dos seguintes lembretes relativamente a boas práticas de cibersegurança?	0.5*4
Total	15

Tabela 18: Pesos de cada questão da Fase 2 - Arquitetura

Na Tabela 18 estão indicados os pesos de cada questão da Fase 2 do modelo de maturidade. Na questão sobre as horas de ação de formação fornecidas, são apresentados por defeito 4 opções temporais, que se designam por, "Sem ações de formação", "Entre 1 a 5 horas", "Entre 6 a 10 horas"e "Mais de 10 horas", foi atribuída uma gama de pesos entre, 0 que corresponde à opção "Sem ações de formação", 0.5, 0.75 e 1 respetivamente.

Pergunta	Peso
Com que regularidade são auditadas as configurações dos dispositivos?	0.5; 0.75; 1
A organização tem uma política BYOD (Gestão de Dispositivos Móveis Pessoais)?	1.5
De que forma é feita a gestão de eventos de segurança?	1.5
Existe algum sistema de monitorização dos principais ativos de rede e sistemas que dão suporte às atividades da organização?	1
Os colaboradores têm conhecimento de como utilizar informação crítica?	1
Total	6

Tabela 19: Pesos de cada questão da Fase 3 - Segurança dos Dispositivos

Na Tabela 19 estão indicados os pesos de cada questão da Fase 3 do modelo de maturidade. Na questão a regularidade em que são auditadas as configurações dos dispositivos, são apresentados por defeito 4 opções de frequência, que se designam por, "Nunca"e "Raramente", "Ocasionalmente", "Frequente"e "Muito Frequente", foi atribuída uma gama de pesos entre, 0 que corresponde à opção "Nunca e Raramente", 0.5, 0.75 e 1 respetivamente.

Pergunta	Peso
Com que regularidade são feitas as atualizações de software?	0.5; 0.75; 1
Quais os procedimentos de segurança, que estão definidos na política de dispositivos móveis?	0.5*4
Antes da entrada em produção, os sistemas e aplicações são submetidos a testes de cibersegurança?	1
Por quem são efetuados os testes de cibersegurança indicados na questão anterior?	0.5*4
Já foi efetuado algum simulacro de Cibersegurança na organização?	1
Com que frequência são efetuados estes simulacros?	0.5; 0.75; 1
Existe uma equipa capaz de dar resposta a incidentes de cibersegurança na sua organização?	1.5
Total	10.5

Tabela 20: Pesos de cada questão da Fase 4 - Consolidar a Cibersegurança

Na Tabela 20 estão indicados os pesos de cada questão da Fase 4 do modelo de maturidade. Na questão a regularidade em que são feitas as atualizações de software, são apresentados por defeito 4 opções de frequência, que se designam por, "Nunca"e

"Raramente", "Ocasionalmente", "Frequente"e "Muito Frequente", foi atribuída uma gama de pesos entre, 0 que corresponde à opção "Nunca e Raramente", 0.5, 0.75 e 1 respetivamente. A penúltima questão segue a mesma lógica da primeira questão, pois as opções também são de frequência.

Pergunta	Peso
Foi nomeado um (Responsável de Segurança de Informação) CISO na organização?	1.5
A organização possui algum destes serviços?	1
Alguma vez a organização foi alvo de um ataque informático?	1
Estes ataques foram documentados?	1
Que tipo(s) de ataque sofreu?	0.5*4
Considera que qualquer colaborador sabe como atuar em caso de ataque informático?	1
Existe um processo para que todos os colaboradores possam reportar possíveis incidentes de segurança?	1
Total	8.5

Tabela 21: Pesos de cada questão da Fase 5 - Equipa de Cibersegurança

Na Tabela 21 estão indicados os pesos de cada questão da Fase 5 do modelo de maturidade. Na questão sobre o tipo de ataques, são apresentados por defeito 4 exemplos de ataques mais comuns, por esse motivo atribuiu-se o peso de 0,5 a cada um.

Devido à discrepância do número de perguntas por grupo e à pontuação atribuída a cada questão, existe a diferença de totais entre todos os grupos.

Tendo em conta os pesos definidos para cada questão, por exemplo, uma empresa que tenha os pontos máximos numa das fases, corresponde a uma percentagem de 100%, e assim sucessivamente, de acordo com os pontos obtidos foi calculada a percentagem obtida.

Para transmitir uma mensagem mais clara às empresas sobre o seu nível de maturidade em cibersegurança, e tornar os resultados mais intuitivos e de fácil interpretação, foi definido um intervalo quantitativo e qualitativo segundo a escala de percentagens de 0 a 100%.

Percentagem	Nível Maturidade
0-39%	Insuficiente
40-49%	Suficiente
50-59%	Bom
60-79%	Muito Bom
80-100%	Excelente

Tabela 22: Definição quantitativa do nível de maturidade

Na Tabela 22 estão representados os níveis quantitativos de cada nível de maturidade.

De acordo com os níveis de maturidade definidos, uma organização num nível Insuficiente de maturidade, significa que tem um conjunto de práticas básicas de cibersegurança, e que os processos já implementados são informais, incompletos ou inconsistentes. Neste nível, a organização está preocupada em cumprir leis e normas.

No nível Suficiente são consideradas as organizações em que têm uma maior preocupação com os seus hábitos, de maneira a reduzir os riscos para a organização.

No nível Bom são aquelas em que os procedimentos estão completos, devidamente documentados e implementados e a consciencialização junto dos funcionários é contínua.

As organizações em que os procedimentos existentes são analisados regularmente para se verificar a eficácia dos controlos implementados, encontram-se no nível Muito Bom.

No nível Excelente, estão presentes as organizações em que existe um processo de melhoria contínua e a implementação de controlos mais robustos.

4.5 EXEMPLO DE UM RELATÓRIO ENVIADO PARA UMA DAS EMPRESAS

As organizações inquiridas que solicitaram este feedback individual e personalizado no final do inquérito irão recebê-lo via email, e tem como finalidade que a organização possa perceber em que nível de maturidade em cibersegurança se encontra em cada uma das cinco fases do modelo de maturidade para perceber onde pode melhorar. Ainda recebe algumas indicações/sugestões de ações para melhorar o seu nível de maturidade em cibersegurança em cada uma das fases, sendo destacadas as ações mais importantes de cada uma das fases que se encontram em falta, e que desta forma possa melhorar o seu nível de maturidade em cibersegurança.

De seguida serão apresentados alguns exemplos destes relatórios enviados.

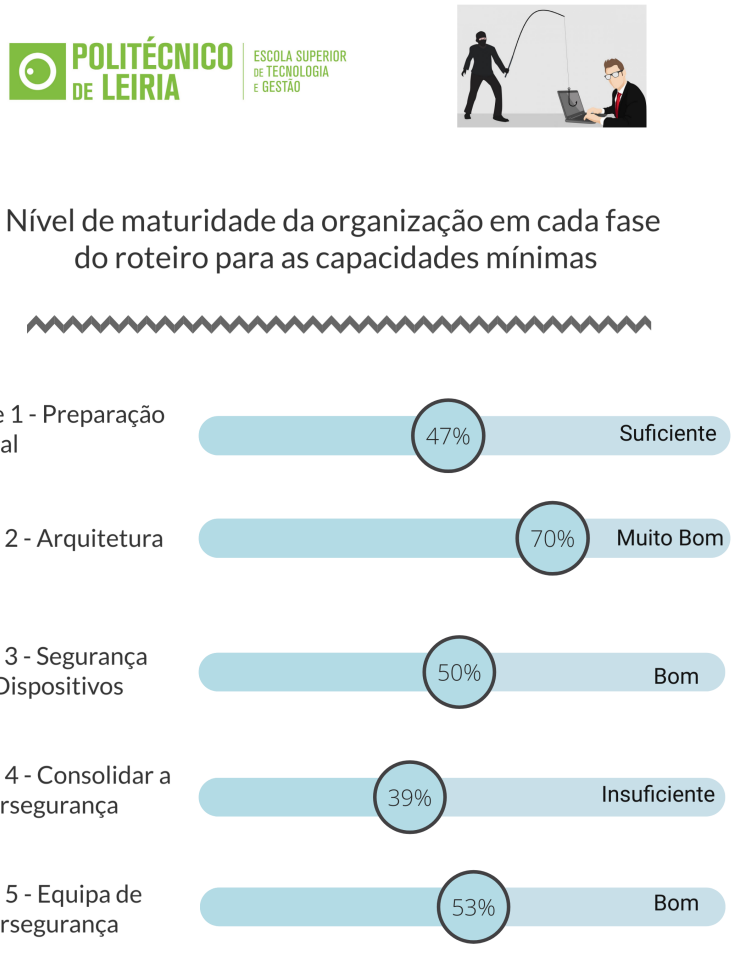


Figura 22: Exemplo de relatório personalizado disponibilizado - Parte I

Figura 23: Exemplo de relatório personalizado disponibilizado - Parte II

Nas Figuras 22 e 24 pode-se observar um exemplo de relatório personalizado disponibilizado para os inquiridos que indicaram que gostariam de receber este relatório personalizado.

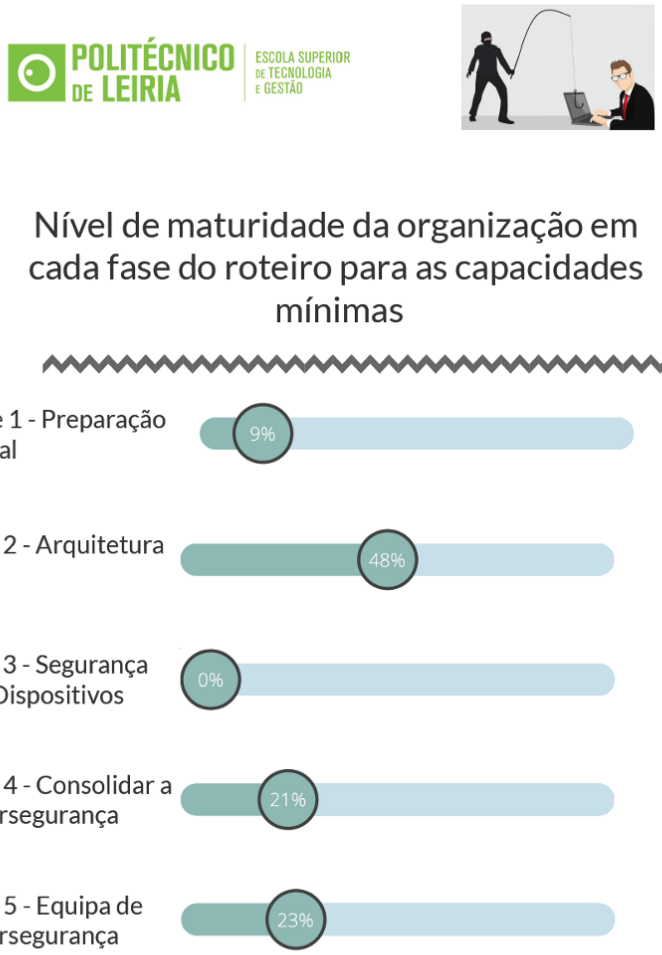


Figura 24: Exemplo de relatório personalizado disponibilizado - Parte I

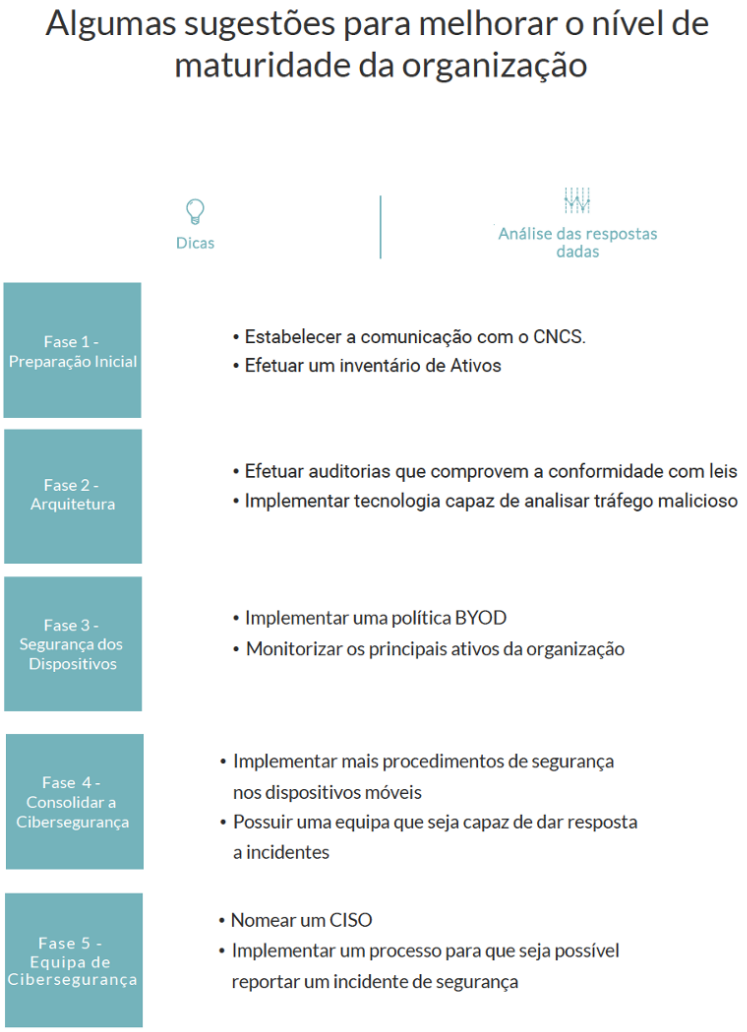


Figura 25: Exemplo de relatório personalizado disponibilizado - Parte II

Nas Figuras 24 e 25 pode-se observar outro exemplo de relatório personalizado disponibilizado para os inquiridos que indicaram que gostariam de receber este relatório personalizado.

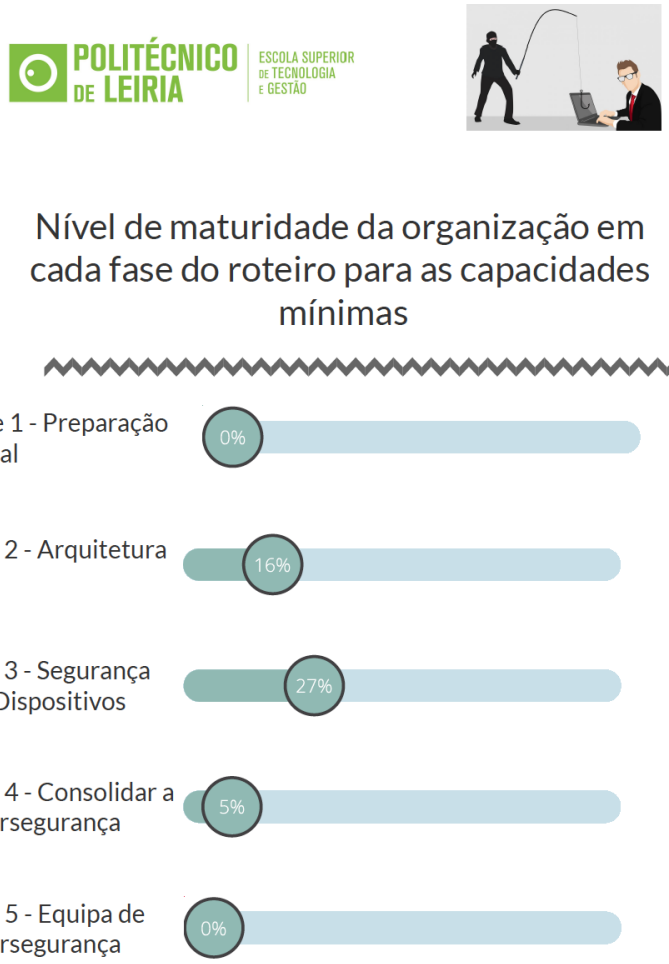


Figura 26: Exemplo de relatório personalizado disponibilizado - Parte I

Figura 27: Exemplo de relatório personalizado disponibilizado - Parte II

Nas Figuras 26 e 27 pode-se observar outro exemplo de relatório personalizado disponibilizado para os inquiridos que indicaram que gostariam de receber este relatório personalizado.

4.6 SÍNTESE

Este trabalho pretende que as organizações percebam em que nível de maturidade em cibersegurança se encontram e quais os próximos passos que devem ser efetuados para melhorar o seu nível de maturidade.

Neste capítulo foi apresentado todo o processo de desenvolvimento desta dissertação, bem como a justificação das opções tomadas. De salientar que o mapeamento efetuado entre o Roteiro para as Capacidades Mínimas da Cibersegurança e a norma ISO27001:2013 foi a base de todo o trabalho e foi a partir deste que surgiu o modelo de maturidade e a estrutura e questões do inquérito.

5

APRESENTAÇÃO E ANÁLISE DE RESULTADOS

Neste capítulo são apresentados os resultados obtidos após a disseminação do inquérito, através do qual se obtiveram no total 41 respostas de diversas organizações sediadas em território nacional.

Para análise e discussão de resultados foram contabilizadas apenas 41 respostas, por estas se encontrarem totalmente concluídas. De todas as respostas foram excluídas apenas 1, a qual foi preenchida por uma autarquia local e não se enquadrava neste estudo. Porém, constatou-se um elevado número de desistências/respostas incompletas, contabilizadas em 81.

Este inquérito foi disponibilizado a diferentes tipos de organizações, independentemente da sua dimensão ou processo de negócio, com o intuito de tornar este estudo o mais global possível. Com esta análise de resultados pretende-se ter uma visão geral de como as organizações encaram este tema e quais as medidas que estão implementadas para fazer face aos incidentes de segurança, e ainda, determinar o nível de maturidade em que se encontram em cada uma das fases do mapeamento.

Após a divulgação do inquérito, no intervalo de tempo entre a disseminação do inquérito e o seu término, antes do tratamento das respostas dadas, verificou-se que existiram 81 respostas no total. Destas 81 apenas foram completas 41, das quais 1 não foi considerada para o este estudo, pois se tratava de uma autarquia local.

Das 40 respostas das empresas inquiridas consideradas para o estudo, verificou-se que 11 trata-se de microempresas, por terem até 10 funcionários, 21 organizações, são consideradas pequenas e médias empresas e 8 são grandes empresas por terem mais de 250 funcionários. Pode-se afirmar que cerca de 80% dos inquiridos são pequenas e médias empresas (pelo facto de terem até 250 colaboradores).

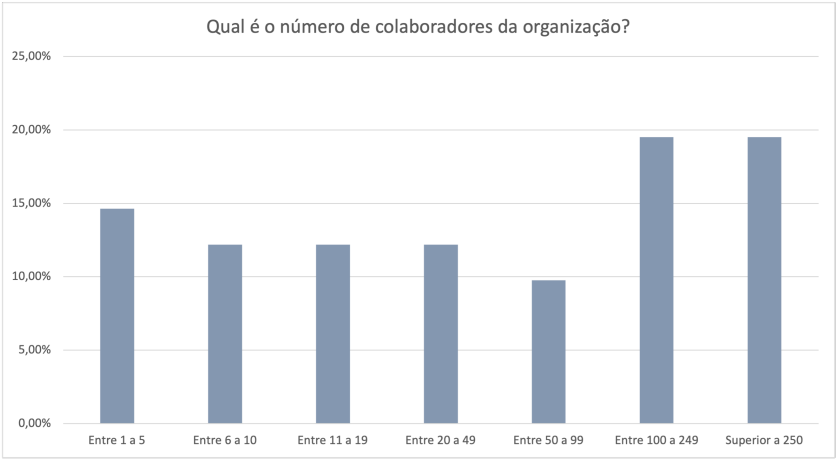


Figura 28: Resultados sobre o número de colaboradores das empresas

Na Figura 28, observa-se o número de colaboradores dos inquiridos.

Cerca de 70% destas empresas encontram-se sediadas no Centro de Portugal, sendo que as restantes estão localizadas na zona Norte, Área Metropolitana de Lisboa e Alentejo.

Os setores de negócio afetos aos inquiridos são bastante diversos, tais como, comércio, divulgação cientifica, ambiente, informática e tecnologias, financeiro, consultoria, serviços administrativos, transformação de rochas ornamentais e associação empresarial.

Caracterização geral das organizações

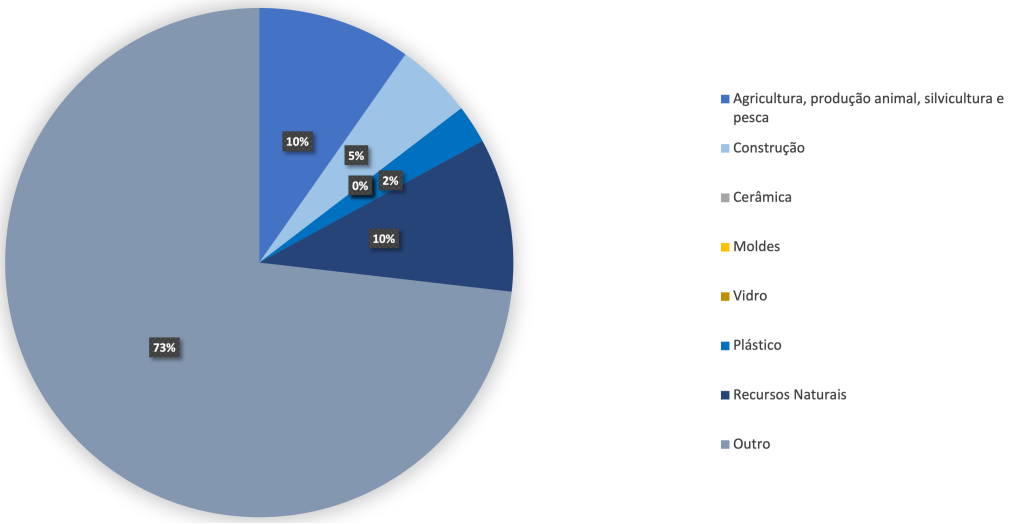


Figura 29: Resultados sobre o setor de atividade das empresas

Como se pode observar na Figura 29 as empresas que participaram neste estudo têm uma diversidade enorme relativamente ao seu processo de negócio, sendo que

73% não se enquadravam nas opções pré-preenchidas, e desta forma selecionaram a opção "Outro"para especificar a sua área de negócio.

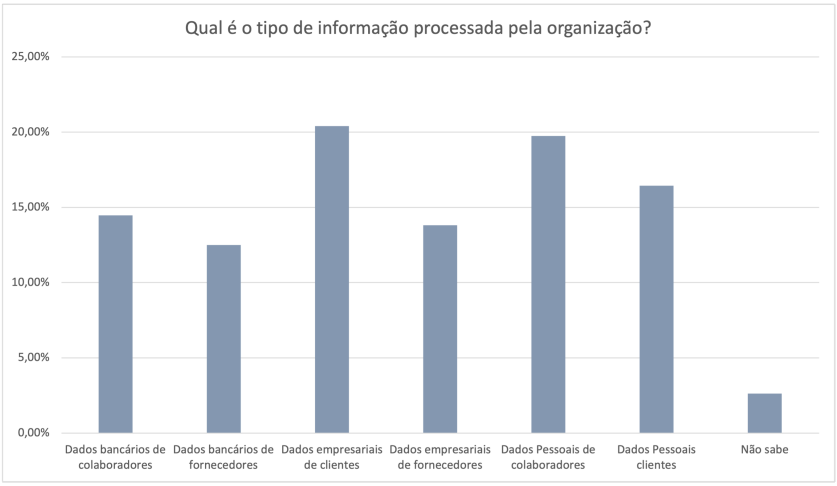


Figura 30: Resultados sobre quais os tipos de dados processados pela organização

Sendo os dados um dos ativos com mais valor de qualquer empresa, foi interessante apurar quais os tipos de dados processados pelas organizações. Na Figura 30, pode-se observar os tipos de dados processados pelas empresas, tendo maior destaque os dados empresariais de clientes e dados pessoais de colaboradores.

Figura 31: Resultados sobre quais as tecnologias presentes na empresa

Para se aprofundar este tema, era importante perceber quais os tipos de tecnologias que estão presentes no quotidiano das organizações, e sendo assim, foi colocada a questão presente na figura 31. Pode-se afirmar que todas as tecnologias apresentadas têm uma forte presença na maioria das empresas, sendo que o email corporativo é a que mais se destaca. A Cloud Pública não é muito utilizada pelas empresas.

Sendo este um tema tão atual e pertinente, é curioso perceber, sendo bastante evidente que a maioria dos inquiridos entende que do ponto de vista da empresa o tema da segurança da informação, é muito importante. E de forma coerente, pode-se afirmar que existe preocupação com a reputação da empresa no caso de ocorrer um incidente de segurança, pois 98% das empresas responderam de forma positiva relativamente a esta questão.

Apesar de todas as precauções tomadas e medidas, qualquer empresa contínua exposta ao risco de sofrer um ciberataque, e desta forma, as organizações podem contratar seguros para que estes incidentes tenham um impacto menor. A contratação de um seguro para este tipo de eventos ainda não é muito comum nas empresas portuguesas, e isso está refletido nos dados que se obtiveram com este estudo, pois apenas 24% das organizações afirmaram ter um seguro contratado.

Com os resultados obtidos é curioso perceber que cerca de 24% das organizações tem um orçamento anual previsto para esta questão, isto demonstra que estas organizações dão grande relevância a este tema e preocupam-se com a proteção das mesmas. Porém, consegue-se perceber que a grande maioria (56%) não sabe se existe algum orçamento previsto para a segurança da informação, pode-se deduzir que esta informação não seja do conhecimento de todos os colaboradores, e apenas órgãos da administração ou gestores saibam mais detalhes sobre esta questão.

Resultados obtidos na secção: Fase 1 - Preparação Inicial

Relativamente a esta primeira fase do inquérito e coincide com a primeira fase do modelo de maturidade, vão ser analisadas as respostas obtidas das empresas inquiridas e vão ser demonstradas as devidas conclusões. As Figuras 32, 33, 34, 35, 36 e 36 apresentam os resultados globais em valor percentual das respostas obtidas a estas questões.

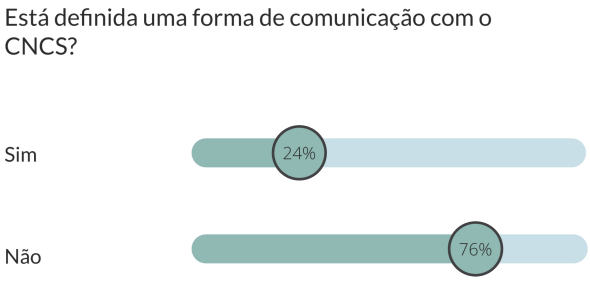


Figura 32: Resultados sobre se existe comunicação com o CNCS

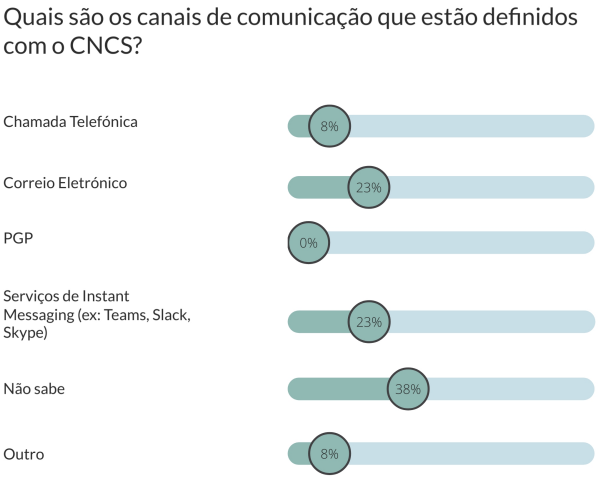


Figura 33: Resultados sobre quais os canais de comunicação existentes

Quanto aos resultados obtidos, verifica-se na Figura 32 que a grande maioria das empresas respondeu de forma negativa (76%) em como não tem nenhuma forma de comunicação definida com o CNCS. Porém, apenas 10 organizações assumem cumprir este critério. Ter uma comunicação direta com o CNCS é bastante relevante, pois em caso de incidente ou suspeita de incidente, este é reportado mais facilmente.

Das 10 organizações que afirmaram ter uma comunicação, todas utilizam os canais de comunicação pré-definidos nas respostas, à exceção do canal de comunicação PGP, sendo que os canais mais utilizados são o correio eletrónico e serviços de Instant Messaging (Teams, Slack ou Skype). Uma das empresas descreveu outro canal de comunicação com o CNCS, salientando que o CNCS colabora regularmente com a organização, na Figura 33 estão apresentados os resultados obtidos.

Figura 34: Resultados sobre se existe um inventário de ativos

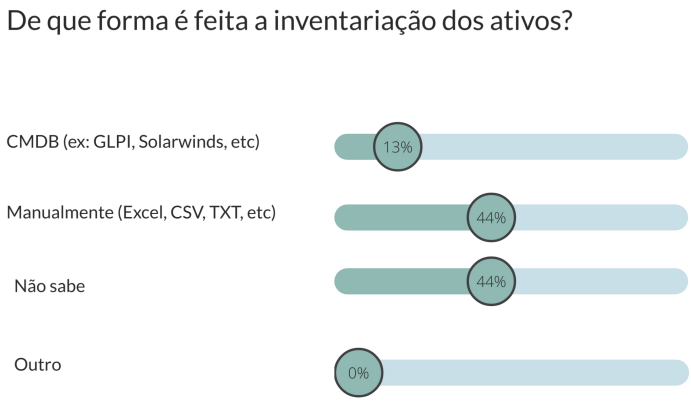


Figura 35: Resultados sobre qual a forma de realizar a inventariação de ativos

Relativamente ao inventário de ativos, em que os resultados podem ser observados na Figura 34, é possível afirmar que a generalidade das empresas, tem este cuidado de inventariar todos os ativos e serviços críticos da empresa. Sendo que, apenas nove empresas assume não efetuar nenhuma inventariação dos ativos. Outra conclusão que se pode tirar, é que a percentagem de inquiridos que não sabe se este processo é efetuado é igual à quantidade de empresas que o faz. Para perceber melhor o processo de inventariação de ativos e de que forma este é feito, a pergunta seguinte está

dependente da anterior e apenas é mostrada para quem respondeu positivamente, sendo assim, foi possível concluir que a maioria faz este processo de forma manual, e que apenas duas o fazem de forma automática utilizando o CMDB, como se pode observar na Figura 35.

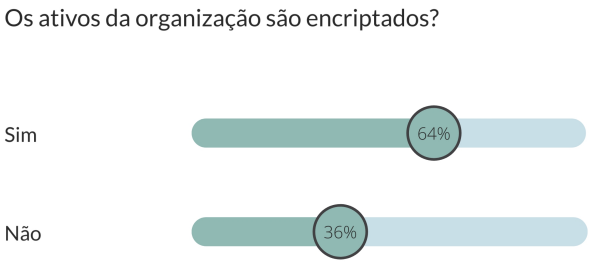


Figura 36: Resultados sobre se os ativos são encriptados

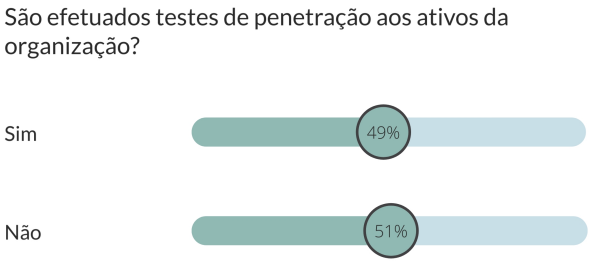


Figura 37: Resultados sobre se são efetuados testes de penetração aos ativos

É de realçar que de acordo com a Figura 36, mais de metade das empresas afirma que os seus ativos encontram-se encriptados.

Quanto aos testes de penetração aos ativos da organização, pode-se observar na Figura 37, que mais de metade não efetua nenhum teste de penetração aos seus ativos, de maneira a detetar e antever possíveis vulnerabilidades.

Face aos resultados globais desta primeira fase do inquérito, e visando aumentar o nível de maturidade das empresas, destacam-se alguns pontos importantes, nomeadamente, a definição da comunicação com o CNCS, visto que tem uma elevada percentagem de respostas negativas e é o pilar desta fase. Nesta primeira fase percebe-se que há um elevado número de inquiridos que não sabe responder ou não pretende responder às questões propostas. Ainda existem várias capacidades que devem ser revistas e devem ser tidas em conta pelas empresas. E, sendo esta uma fase inicial, estas capacidades aqui previstas são os primeiros passos para estabelecer

a cooperação com o CNCS e a empresa.

Resultados obtidos na secção: Fase 2 - Arquitetura

Seguidamente vão ser apresentados das empresas inquiridas os resultados obtidos nesta segunda fase do inquérito e que coincide com a segunda fase do modelo de maturidade. As Figuras 38, 39, 40, 41, 42, 43, 41, 44, 45, 46 e 47 apresentam os resultados globais em valor percentual das respostas obtidas a estas questões.

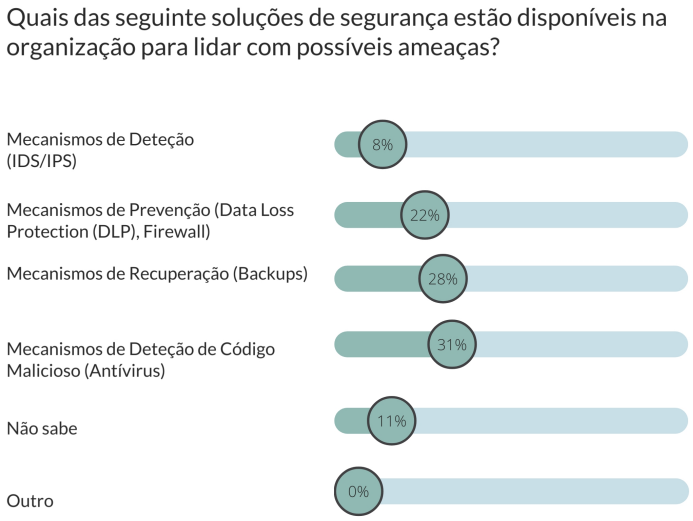


Figura 38: Resultados sobre as soluções existentes para lidar com ameaças

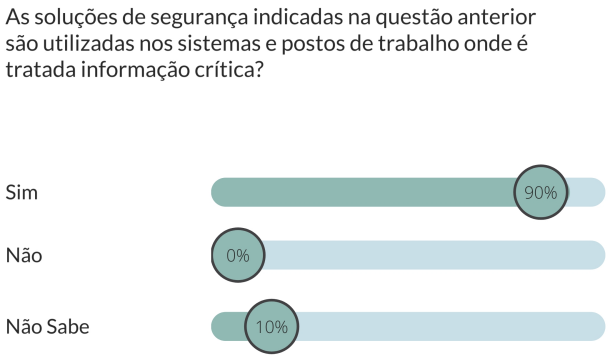


Figura 39: Resultados sobre onde é que as soluções da questão anterior estão implementadas

Tendo em conta os resultados obtidos nesta segunda fase do inquérito, pode-se comprovar que 89% dos inquiridos respondeu de forma afirmativa em como as empresas a que são afetos utilizam os mecanismos de segurança pré-definidos no

conjunto de respostas, sendo que a solução de segurança que mais se destaca é os Mecanismos de Deteção de Código Malicioso (Antívirus). Pode-se também observar que um pequeno grupo de empresas tem implementados Mecanismos de Deteção (IDS/IPS), estes dados estão representados na Figura 38.

Sendo a questão seguinte dependente da primeira e apenas estaria visível para as empresas que tenham alguma solução de segurança implementada, representada na Figura 39, é possível concluir que 90% destes mecanismos estão presentes nos postos de trabalho onde é manipulada informação sensível e em sistemas onde é armazenada esse tipo de informação.

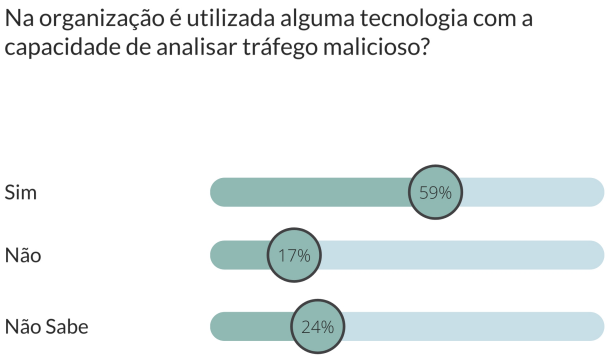


Figura 40: Resultados sobre se existe uma tecnologia capaz de analisar tráfego malicioso

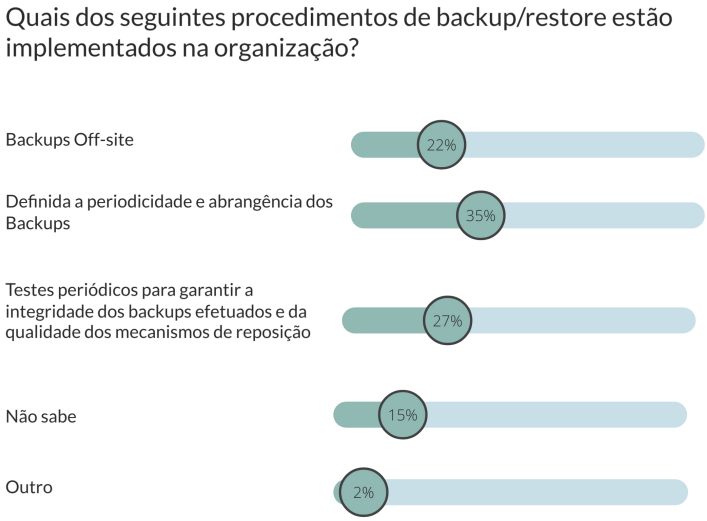


Figura 41: Resultados sobre quais os procedimentos de backup ou restore

Pode-se verificar que pouco mais de metade das empresas tem tecnologias com capacidade para analisar tráfego malicioso, segundo a Figura 40. Isto significa que

muitas empresas estão expostas a determinados riscos, como, por exemplo, sofrer algum ataque cibernético.

Sendo os *backups* e procedimentos de *restore* uma implementação fundamental e imprescindível a qualquer empresa, com os resultados obtidos, consegue-se perceber que a grande maioria, cerca de 85% dos inquiridos, corrobora que estão implementados procedimentos para esta questão, como pode ser observado na Figura 41.

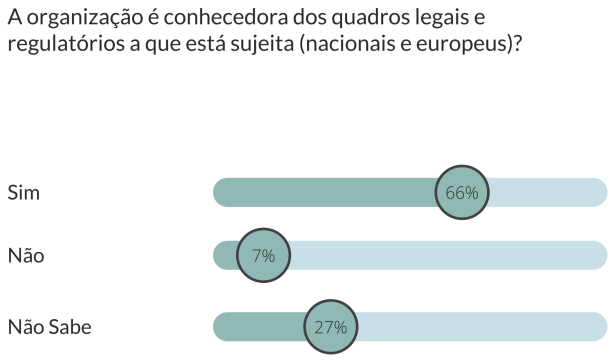


Figura 42: Resultados sobre se a organização é conhecedora das leis a que está sujeita

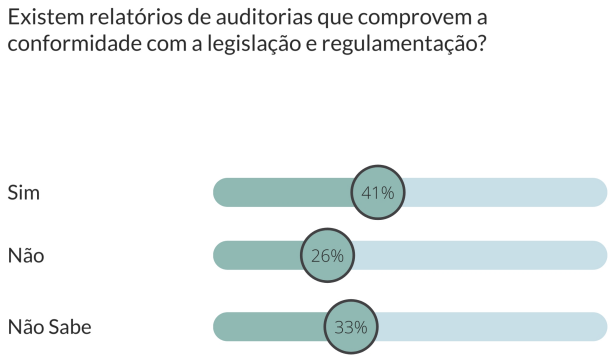


Figura 43: Resultados sobre se existem auditorias que comprovem a conformidade com as leis

Sabendo que existem e quadros legais e regulatórios que devem ser cumpridos pelas organizações dependendo da sua área de negócio, mas também em nível de cibersegurança, foi relevante perceber se as organizações estão cientes deste facto. Os resultados estão apresentados na Figura 42, através da qual se conclui que 66% tem conhecimento destas normas, mas existe uma elevada percentagem que não sabe se a empresa está ciente das legislações. Para os inquiridos que responderam de

forma positiva a esta questão, era importante perceber se conhecendo as legislações, se existem auditorias que pudessem comprovar o seu cumprimento, observável na Figura 43. De acordo com os resultados, apenas 11 empresas possuem auditorias que comprovam a implementação destas normas.

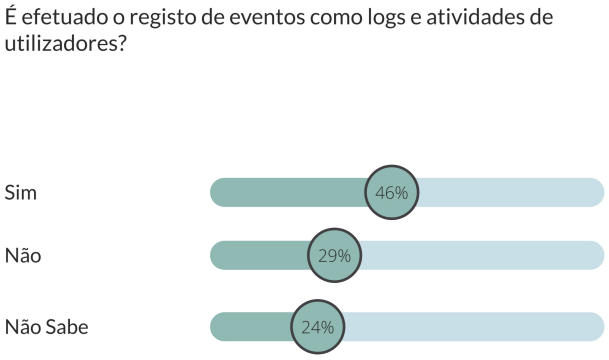


Figura 44: Resultados sobre se existe registo de eventos como logs ou atividades de utilizadores

Os logs tornam-se grandes aliados quando ocorre um incidente, pois têm informação fulcral. Ainda existe uma grande percentagem de empresas que não tem este mecanismo implementado, sendo que apenas 46% o pratica, como está representado na Figura 44.

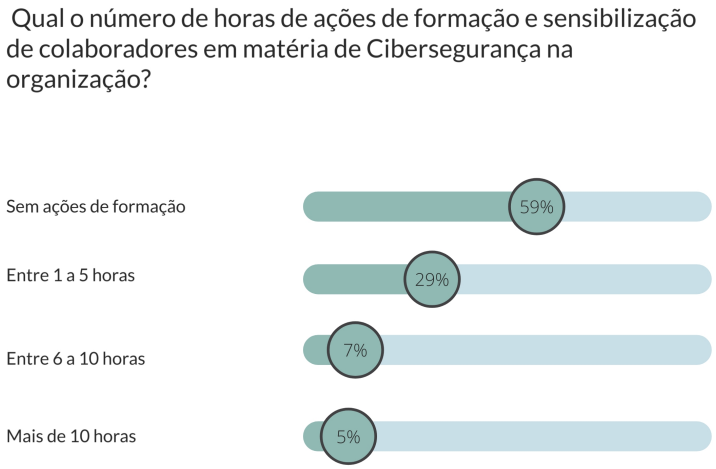


Figura 45: Resultados sobre a quantidade de horas de formação sobre este tema

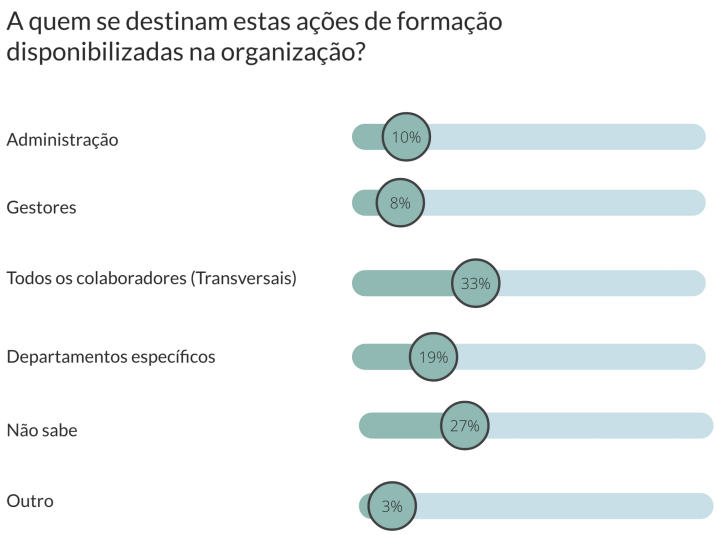


Figura 46: Resultados sobre a quem se destinam as ações de formação existentes

De acordo com a Figura 45, é possível concluir que 59% das empresas não proporciona horas de formação em cibersegurança para os seus colaboradores. Das restantes, cerca de 41% com este processo implementado, a maioria disponibiliza estas ações de formação para todos os colaboradores da organização, como está demonstrado na Figura 46.

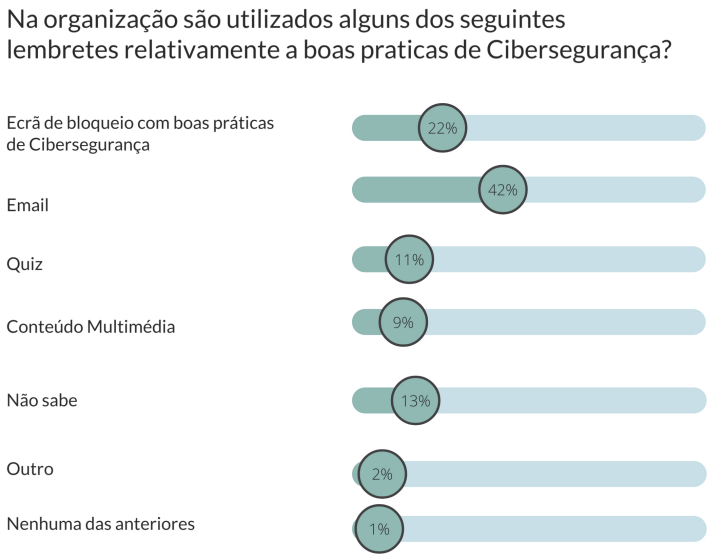


Figura 47: Resultados sobre quais os lembretes utilizados sobre este tema

Com os dados obtidos, pode-se afirmar que 86% faz questão de relembrar este tema aos colaboradores através de diferentes tipos de lembretes, como está representado

na Figura 47, isto mostra que as empresas têm interesse que os seus funcionários tenham sempre este tema presente de diversas formas.

De acordo com os resultados completos desta segunda fase do inquérito, é possível afirmar que existem competências fundamentais em falta nas empresas para que estas estejam melhor preparadas, e possam ter um nível de maturidade mais elevado. De todas as competências, podem ser destacadas algumas, nomeadamente, devem ser implementadas mais soluções de segurança, a política de *backups* e *restore* deve ser revista e reforçada. Também os logs deveriam ser registados para que possam ser utilizados como ferramenta de suporte em caso de incidente de segurança. Outro aspeto que deve ser implementado pelas empresas é disponibilizar algum tempo de formação a todos os colaboradores da organização, visto que se todos tiverem souberem como reconhecer algum evento estranho possa ser possível antecipar ou prevenir incidentes.

Resultados obtidos na secção: Fase 3 - Segurança dos Dispositivos

Seguidamente vão ser apresentados das empresas inquiridas os resultados obtidos nesta terceira fase do inquérito e que coincide com a terceira fase do modelo de maturidade, as Figuras 48, 49, 50, 51 e 52, onde são mostrados esses resultados.

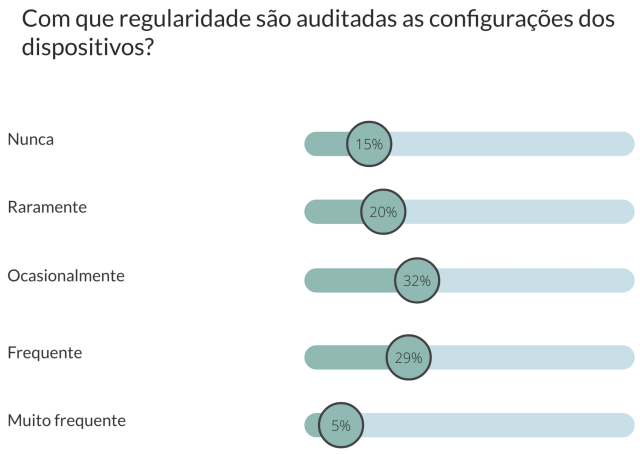


Figura 48: Resultados sobre com que frequência são auditadas as configurações dos dispositivos

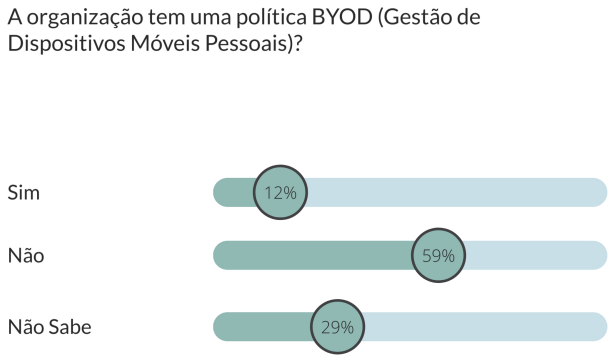


Figura 49: Resultados sobre se existe política BYOD

Verifica-se através da Figura 48, que não é prática comum as configurações dos dispositivos serem auditadas regularmente para manter os dispositivos atualizados e protegidos de possíveis falhas existentes, sendo que a maioria das empresas assume que faz este processo ocasionalmente.

Relativamente às políticas de dispositivos móveis, cerca de 59% dos inquiridos responderam de forma negativa a esta questão, como se pode observar na Figura 49. Apenas 5 empresas têm esta política implementada.

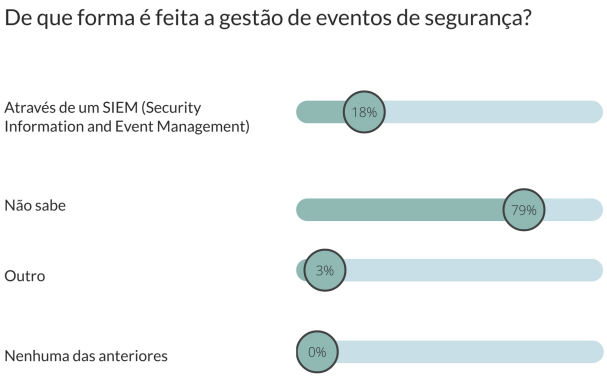


Figura 50: Resultados sobre de que forma é que é feita a gestão de eventos de segurança

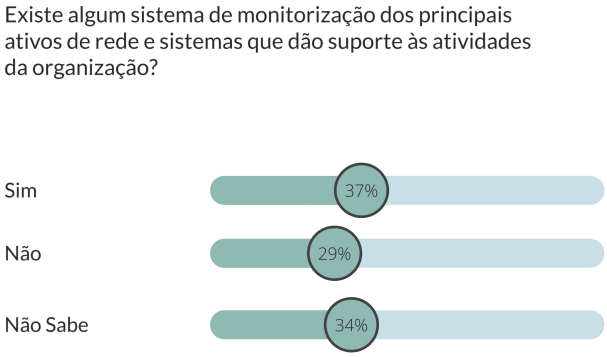


Figura 51: Resultados sobre se os principais são monitorizados

Relativamente à gestão de eventos de segurança, pois apenas 18% das empresas efetuam esta gestão através de um SIEM e a outra recorre a uma empresa externa de informática para o fazer, como se pode observar na Figura 50.

No que toca à monitorização de sistemas críticos e ativos das empresas, apenas 37% responderam de forma afirmativa em como têm esta capacidade, pode-se constatar na Figura 51. Porém, a maioria não tem conhecimento se este processo se efetua, ou então não tem mesmo este procedimento implementado.

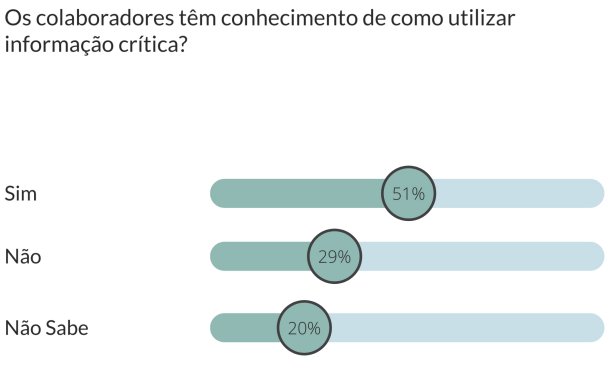


Figura 52: Resultados sobre se os colaboradores sabem processar informação crítica

Sendo que é importante que todos os colaboradores saibam como lidar em caso de incidente, os resultados obtidos permitem perceber que apenas 21 dos inquiridos respondeu de forma positiva a esta questão. Porém, 29

Devido à elevada percentagem de respostas negativas desta secção, pode-se confirmar que ainda existem muitas capacidades em falta que precisam de ser implementadas nas empresas, nomeadamente, verificar as configurações de dispositivos,

implementar políticas BYOD e ainda, dotar os colaboradores de conhecimento para saberem como agir em caso de incidente.

Resultados obtidos na secção: Fase 4 - Consolidar a Cibersegurança

Seguidamente vão ser apresentados das empresas inquiridas os resultados obtidos nesta quarta fase do inquérito e que coincide com a quarta fase do modelo de maturidade. Os resultados gerais podem ser visualizados nas Figuras 53, 54, 55, 56, 57, 58 e 59.

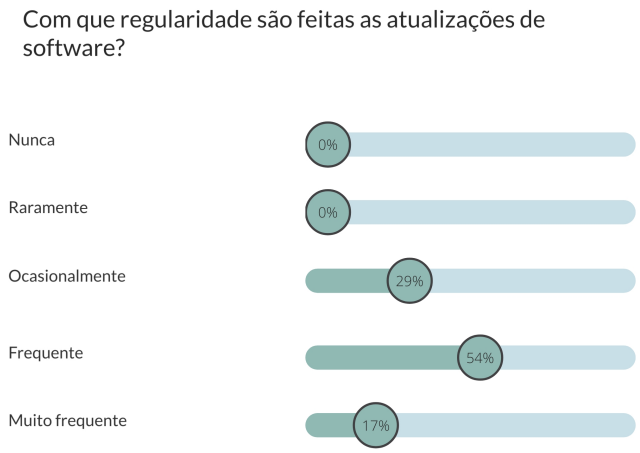


Figura 53: Resultados sobre com que frequência são feitas as atualizações de software

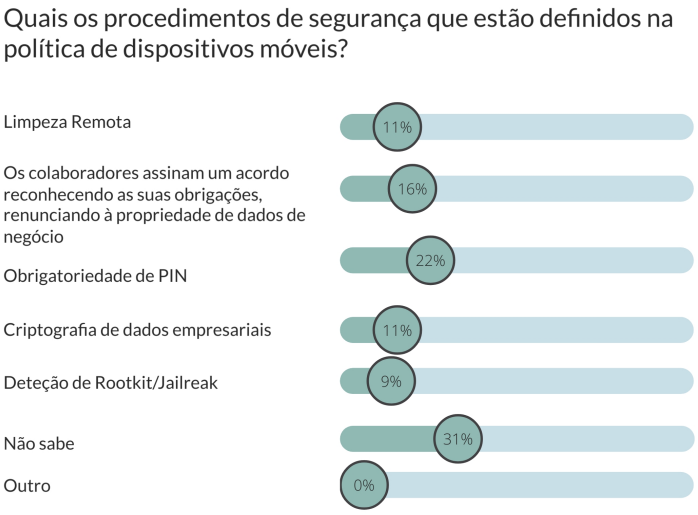


Figura 54: Resultados sobre quais os procedimentos de segurança definidos na política de dispositivos móveis

É imperativo que qualquer empresa mantenha os seus softwares atualizados, para manter as aplicações atualizadas. Apesar da maioria dos inquiridos ter afirmado que é frequente estas atualizações serem feitas, não houve nenhuma empresa que desse uma resposta negativa a esta questão, como pode ser comprovado na Figura 53.

Relativamente aos procedimentos de segurança referentes aos dispositivos móveis, foi possível concluir que 69% das empresas utiliza pelo menos 1 dos procedimentos pré-definidos nas respostas, conforme a Figura 54.

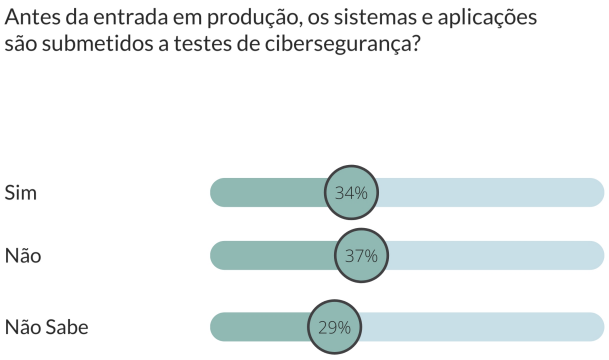


Figura 55: Resultados sobre se os sistemas e aplicações são submetidos a testes de segurança antes da entrada em produção

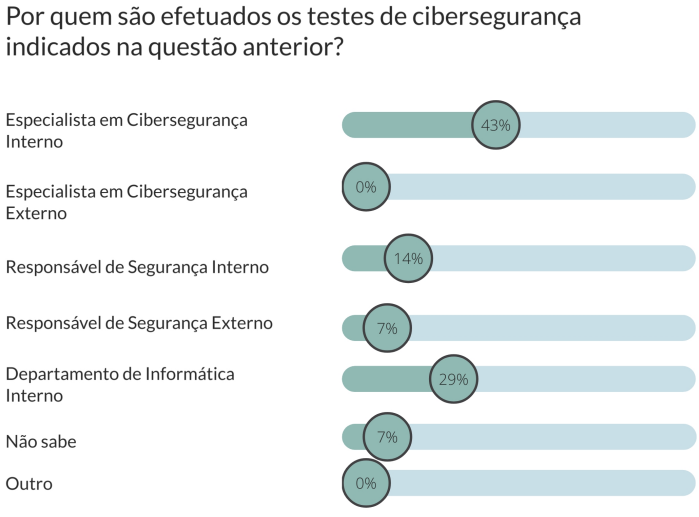


Figura 56: Resultados sobre quem efetua os testes de segurança indicados na questão anterior

De acordo com os resultados obtidos, observou-se que a percentagem de empresas que testa as aplicações e sistemas antes da entrada em produção é ligeiramente inferior, comparativamente às empresas que não testam, mais concretamente, 15

empresas responderam de forma negativa e 14 afirmaram efetuar este procedimento, tal como pode ser verificado na Figura 55. Sabendo que esta pergunta é dependente da anterior e apenas está visível para quem respondeu de forma afirmativa, é possível verificar estes testes de segurança são efetuados pelas entidades disponíveis nas respostas, disponível na Figura 56.

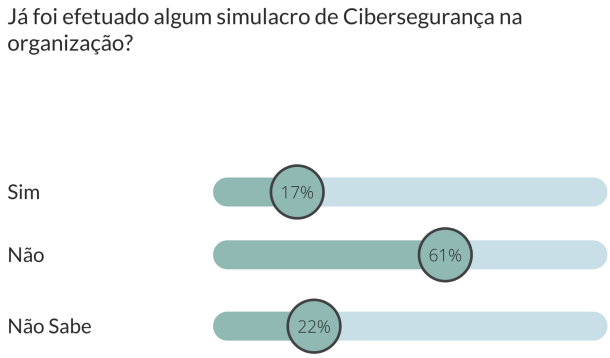


Figura 57: Resultados sobre se já foi efetuado um simulacro de cibersegurança

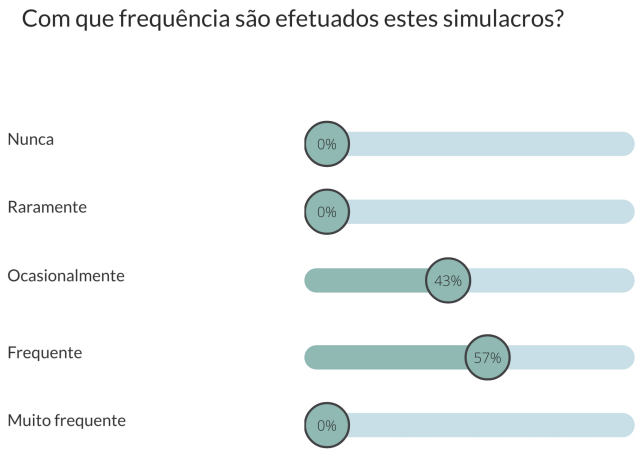


Figura 58: Resultados sobre qual a frequência que estes simulacros são efetuados

Relativamente à questão se já foi efetuado algum simulacro nas empresas inquiridas, a grande maioria das respostas foi negativa (cerca de 61%), apenas 7 empresas já fizeram um evento deste tipo. A próxima questão em que o seu objetivo é perceber a frequência destes simulacros, permitiu determinar que estes ocorrem de forma frequente ou ocasional, os resultados podem ser vistos nas Figuras 57 e 58.

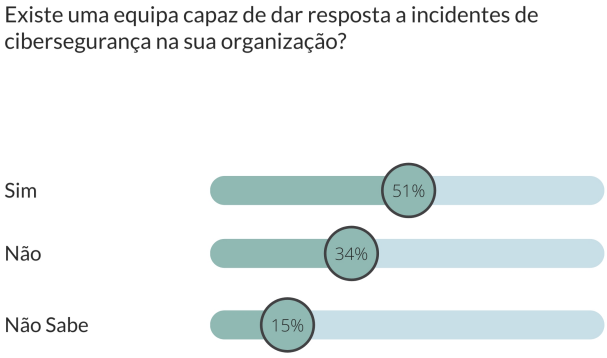


Figura 59: Resultados sobre se existe uma equipa capaz de dar resposta a incidentes de segurança

Pode-se afirmar que 51% das empresas indica que tem uma equipa capaz de lidar com incidentes de segurança, como pode ser constatado na Figura 59.

Tal como nas fases anteriores, ainda existem várias arestas para limar nesta fase, para que o nível de maturidade seja mais elevado e robusto.

Resultados obtidos na secção: Fase 5 - Equipa de Cibersegurança

Seguidamente vão ser apresentados das empresas inquiridas os resultados obtidos nesta quinta fase do inquérito e que coincide com a quinta fase do modelo de maturidade. Os resultados gerais podem ser visualizados nas Figuras 60, 61, 62, 63, 64, 65 e 66 onde são visíveis os dados obtidos através do inquérito.

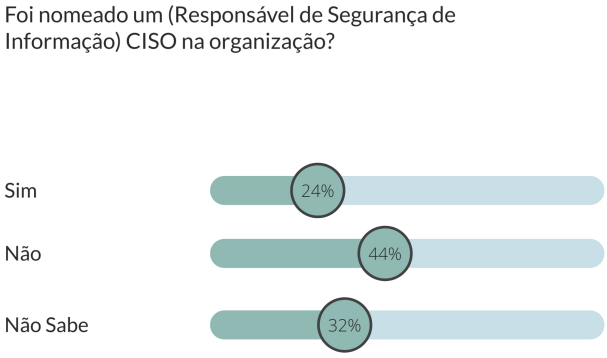


Figura 60: Resultados sobre a existência de um CISO na organização

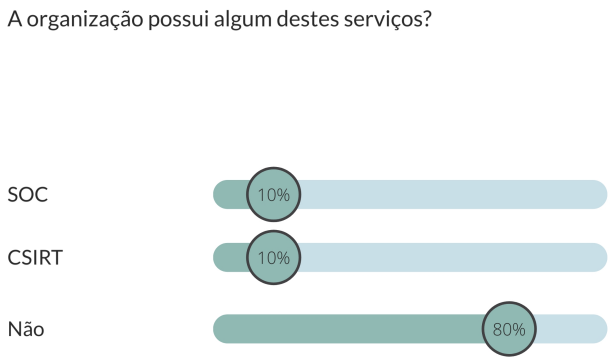


Figura 61: Resultados sobre a existência de algum destes serviços

De acordo com os resultados obtidos, 32% das empresas respondeu de forma negativa em como não tem um CISO presente na empresa, por outro lado, existem 10 empresas que dispõe desta entidade, como pode ser confirmado na Figura 60. Na totalidade, apenas 8 empresas possui algum destes serviços (SOC ou CSIRT), as restantes não têm nenhum destes serviços, estes dados estão representados na Figura 61.

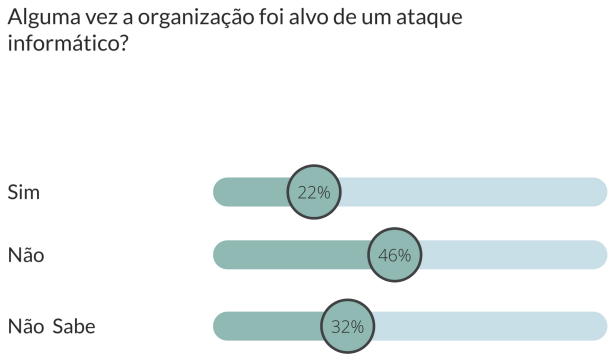


Figura 62: Resultados sobre se a organização já foi alvo de um ataque informático

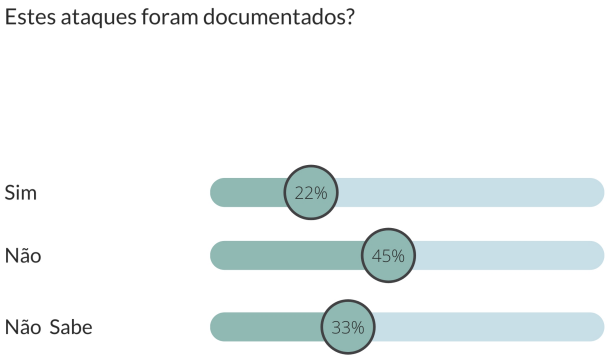


Figura 63: Resultados sobre se os ataques foram documentados

Relativamente à questão sobre se a empresa já foi algo de algum ataque, apenas 22% confirma ter sido alvo de um ataque, e 47% ainda não sofreu algum ataque informático, os resultados estão visíveis na Figura 62. Para as empresas que responderam positivamente a esta questão faz sentido perceber se os ataques sofridos foram documentados, para eventuais ocorrências futuras. Cerca de 44% dos ataques não foram documentados, e em apenas 2 empresas os ataques sofridos foram documentados, como pode ser observado na Figura 63.

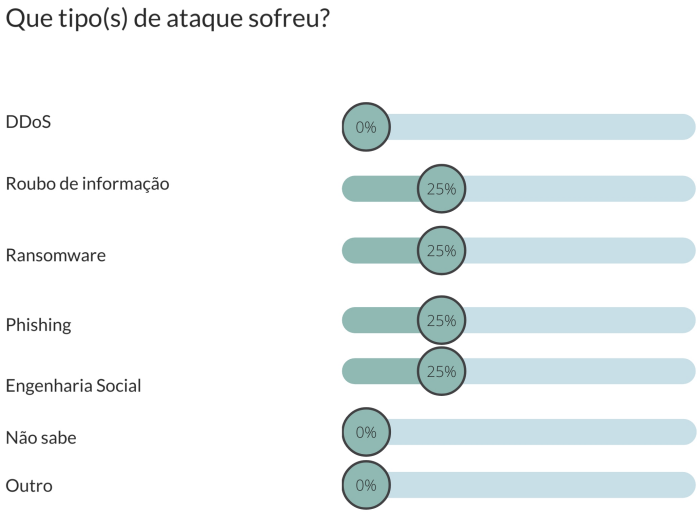


Figura 64: Resultados sobre qual o tipo de ataque sofrido

Os tipos de ataques mais sofridos são o Roubo de Dados, Engenharia Social, *Ransomware* e *Phishing*, de acordo com os dados presentes na Figura 64.

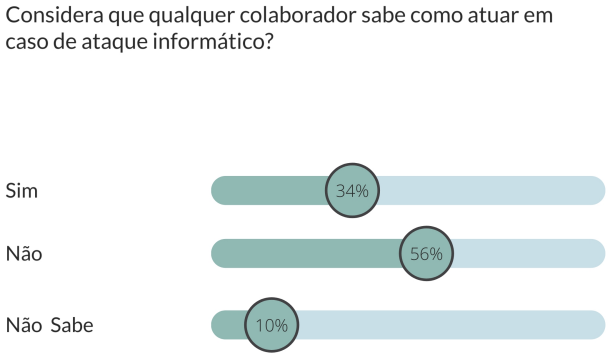


Figura 65: Resultados sobre se qualquer colaborador sabe como atuar em caso de ataque informático

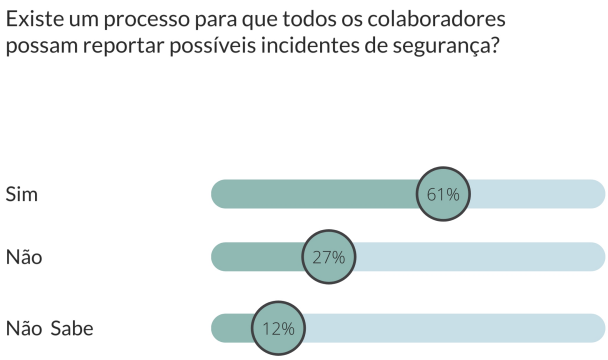


Figura 66: Resultados sobre se existe um processo para reportar possíveis incidentes de segurança

Relativamente aos dados obtidos, pode-se observar que 56% dos colaboradores não sabem como atuar em caso de incidente de segurança na organização. Na última questão deste grupo consegue-se verificar que 61% dos inquiridos admite que existe um processo para reportar possíveis incidentes de segurança. Os resultados de ambas as questões podem ser comprovados através das Figuras 65 e 66.

No geral desta fase e visto que é a fase com menor nível de maturidade, as empresas deveriam apostar em mais algumas capacidades pertencentes a esta fase do inquérito.

Resultados globais obtidos em cada organização

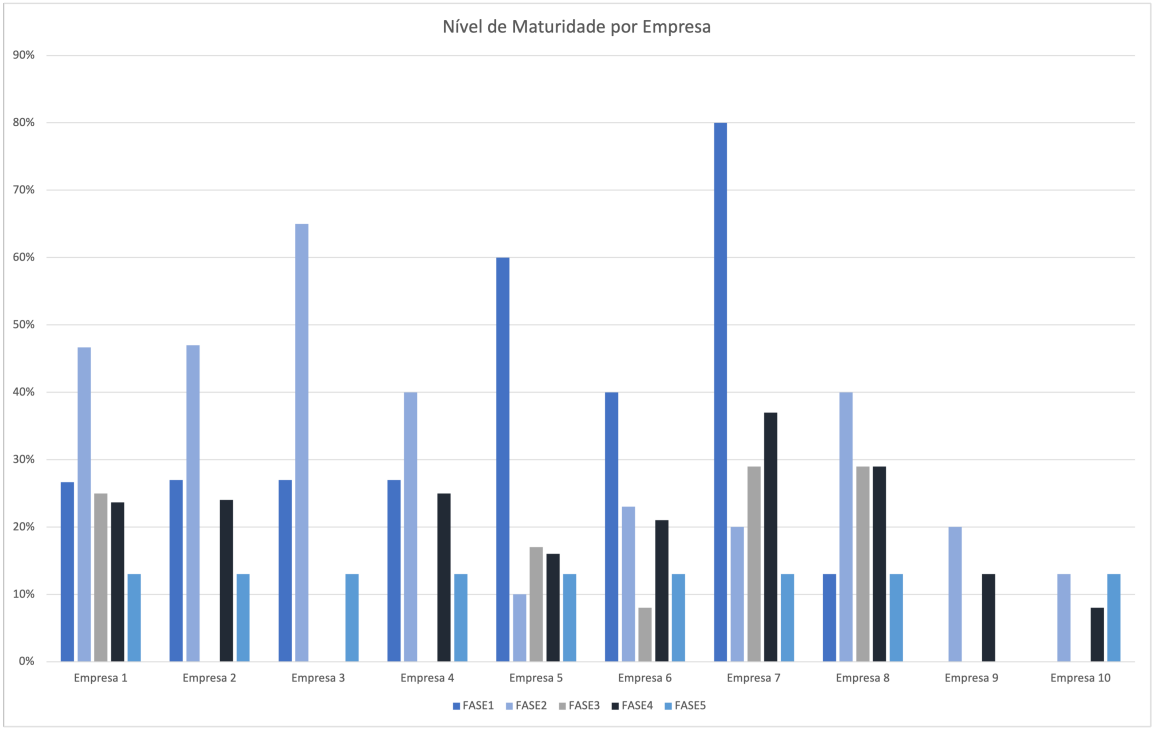


Figura 67: Resultados do Nível de Maturidade em cada fase nas primeiras 10 empresas

Como se pode observar na Figura 67, foram agrupados os resultados obtidos por empresa em cada fase, de maneira a ter-se uma visão mais pormenorizada de cada empresa que respondeu ao inquérito.

Relativamente a estas 10 empresas e aos resultados obtidos, é possível salientar que algumas delas não têm nenhum requisito preenchido em algumas fases do inquérito, nomeadamente, nas fases 1, 3 e 4, tendo assim um nível de maturidade nestas fases de **Insuficiente**.

Quanto aos resultados atingidos existe uma empresa que se destaca no cumprimento das capacidades da fase 1 do inquérito, tendo atingido os 80%, correspondendo ao nível **Excelente**. Nas restantes empresas e, nas correspondentes fases apresentam resultados, na maioria abaixo dos 50%, ou seja, houve uma elevada quantidade de respostas negativas e capacidades que não são cumpridas, o que significa que ainda existem muitas falhas para colmatar em todas as fases do inquérito nestas empresas.

Pode-se observar, ainda, que existe um longo processo a ser implementado para garantir que estas empresas estejam minimamente preparadas para fazer face a questões de cibersegurança.

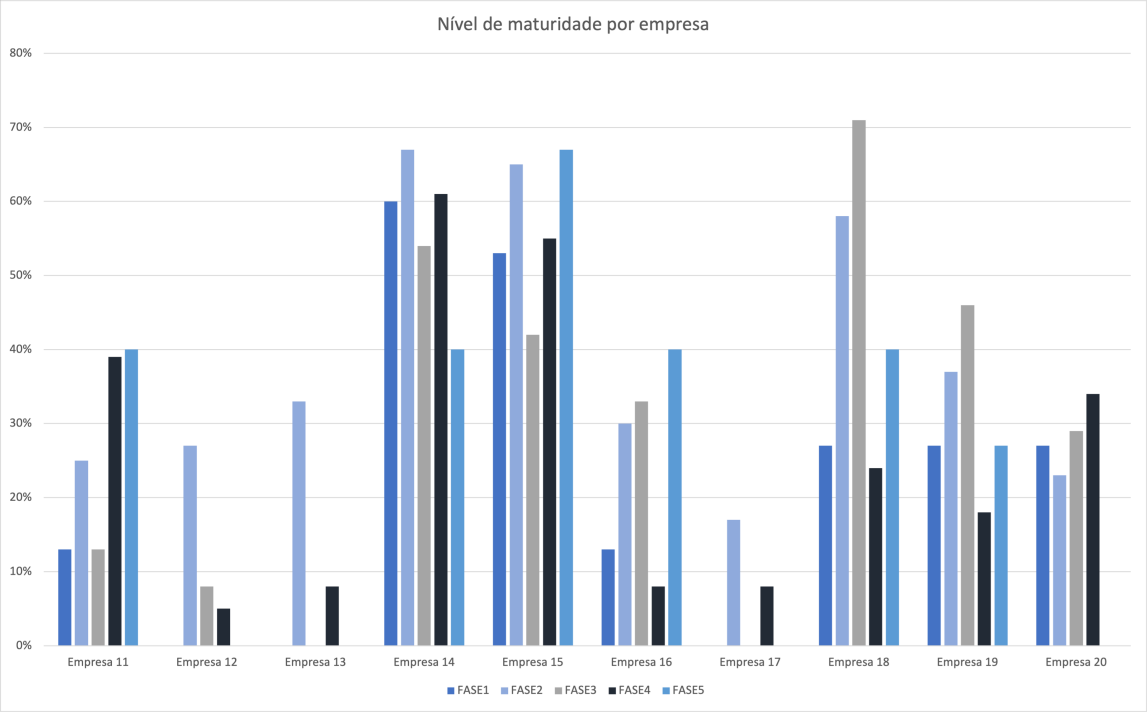


Figura 68: Resultados do Nível de Maturidade em cada fase da empresa 11 à 20

Sobre estes dados obtidos neste grupo de empresas, pode-se observar na Figura 68 que existem lacunas nas fases 1, 3 e 5 do inquérito.

Neste grupo de empresas, estão em destaque 2, pois ao analisar os dados obtidos, é notório que na maioria das fases ultrapassaram os 50% de percentagem e possuem desta forma algumas capacidades mínimas para a cibersegurança. É evidente que existe preocupação e têm algumas capacidades de cibersegurança.

Relativamente às restantes empresas, continua-se a observar que existem muitas capacidades em falta, e desta forma, estão mais vulneráveis a qualquer questão de cibersegurança.

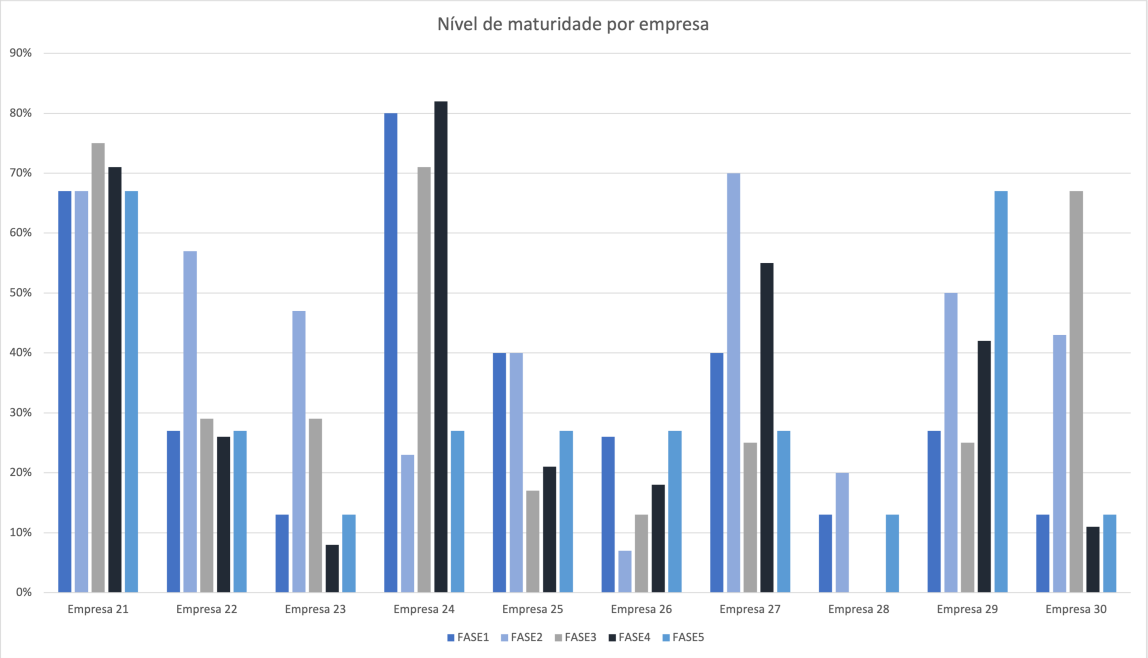


Figura 69: Resultados do Nível de Maturidade em cada fase da empresa 21 à 30

Na Figura 69 é possível afirmar que apenas uma empresa não cumpre de todo as capacidades relativas à fase 3 do inquérito. Porém, apenas empresa 21 tem grande destaque relativamente às outras, pois em todas as fases do inquérito tem um valor percentual acima dos 50%, estando assim entre o nível **Bom** e **Muito Bom**.

Nas restantes empresas, após analisadas as respostas, concluí-se que em algumas das fases estão abaixo dos 50%, coincidindo com níveis de **Suficiente**, ou em alguns casos, nível **Insuficiente**, mostrando assim que têm algumas destas capacidades avaliadas no inquérito.

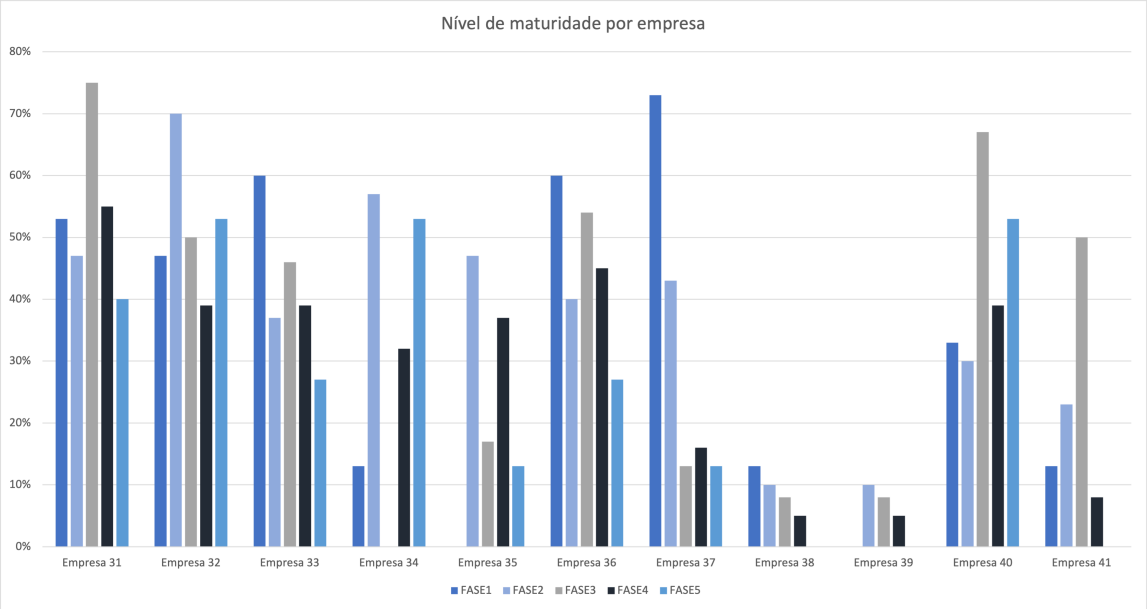


Figura 70: Resultados do Nível de Maturidade em cada fase da empresa 31 à 41

Nos resultados do último conjunto de empresas representados na Figura 70 destacam-se as 2 primeiras empresas, que se pode afirmar que na maioria das fases têm um nível de maturidade médio. Relativamente às restantes, observa-se que existem 2 empresas que na fase 1 e 3 não têm nenhuma capacidade, isto significa que se encontram num nível **Insuficiente**.

É de destacar que a fase 2 em algumas empresas tem um nível de maturidade acima dos 50%, que corresponde ao nível **Muito Bom** e **Bom**, bem como a fase 1 que em alguns casos, está perto dos 50% ou um pouco acima.

Face aos resultados obtidos com este inquérito pode concluir-se que existe uma necessidade urgente de corrigir as lacunas existentes nas empresas de maneira a melhorar o nível de maturidade existente, e para possuírem as capacidades mínimas presentes no modelo de maturidade, e, consequentemente, que estejam mais resilientes perante este tema tão pertinente.

Nível Médio de Maturidade Geral - Microempresas

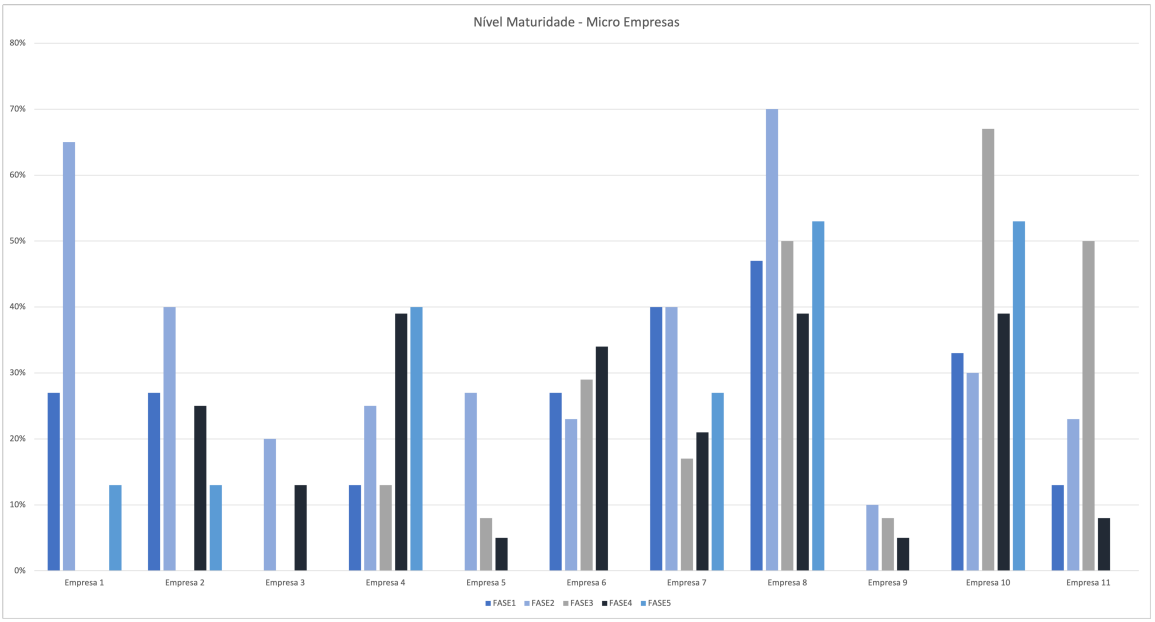


Figura 71: Resultados do Nível de Maturidade das Micro Empresas

Na Figura 71 está representado o nível de maturidade das microempresas que responderam ao questionário. Nesta figura destacam-se 2 empresas, com um nível **Muito Bom** de maturidade. A empresa 1 e 3 não tem qualquer capacidade na fase 3, correspondendo assim a um nível **Insuficiente**. A empresa 3, 5 e 9 não tem nenhuma capacidade da fase 1 implementada.

Nível Médio de Maturidade Geral - PME

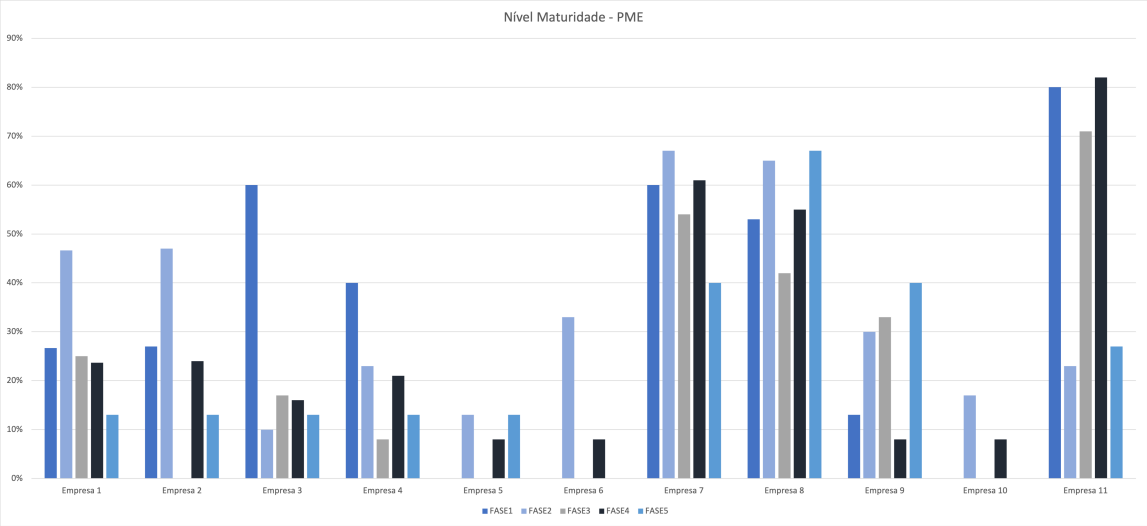


Figura 72: Resultados do Nível de Maturidade das PME - Parte I

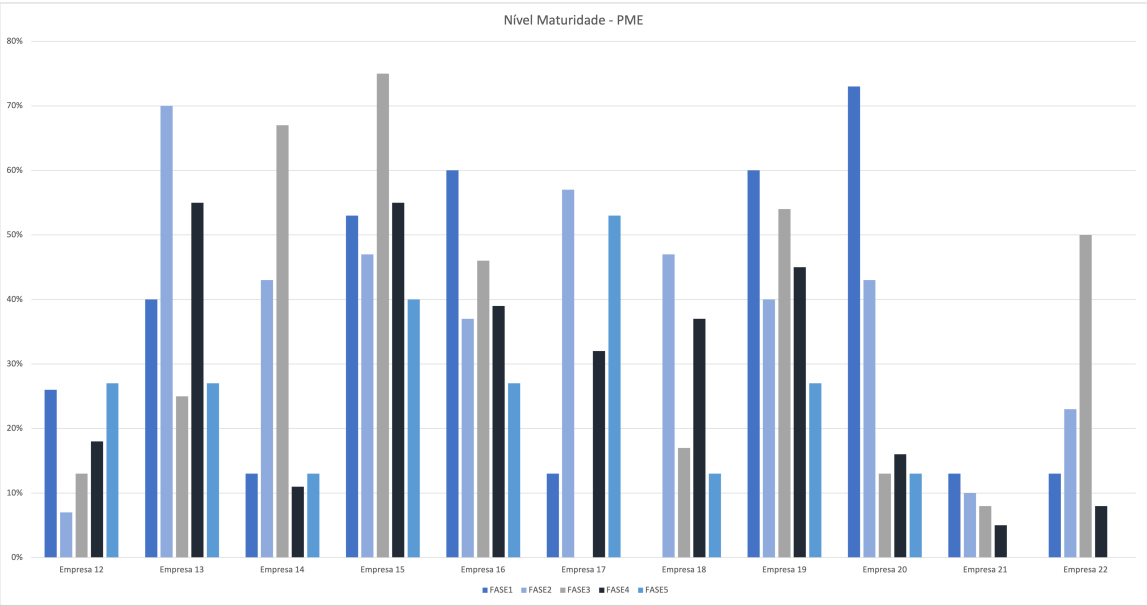


Figura 73: Resultados do Nível de Maturidade das PME - Parte II

Nas Figuras 72 destaca-se a empresa 11 tendo na fase 1 e 4 um nível **Excelente** de maturidade, destaca-se ainda de forma positiva as empresas 7 e 8 que são as que têm mais capacidades implementadas em todas as fases.

De salientar que as empresas 5, 6 e 10 apresentam várias falhas em diversas fases do nível da maturidade.

Na Figura 73 a empresa 12 e a empresa 21 apresentam um nível de maturidade **Insuficiente**. Pode-se observar que em 5 destas empresas a fase 3 tem grande

destaque, sendo que num dos casos tem um nível de maturidade **Muito Bom**.

Nível Médio de Maturidade Geral - Grandes Empresas

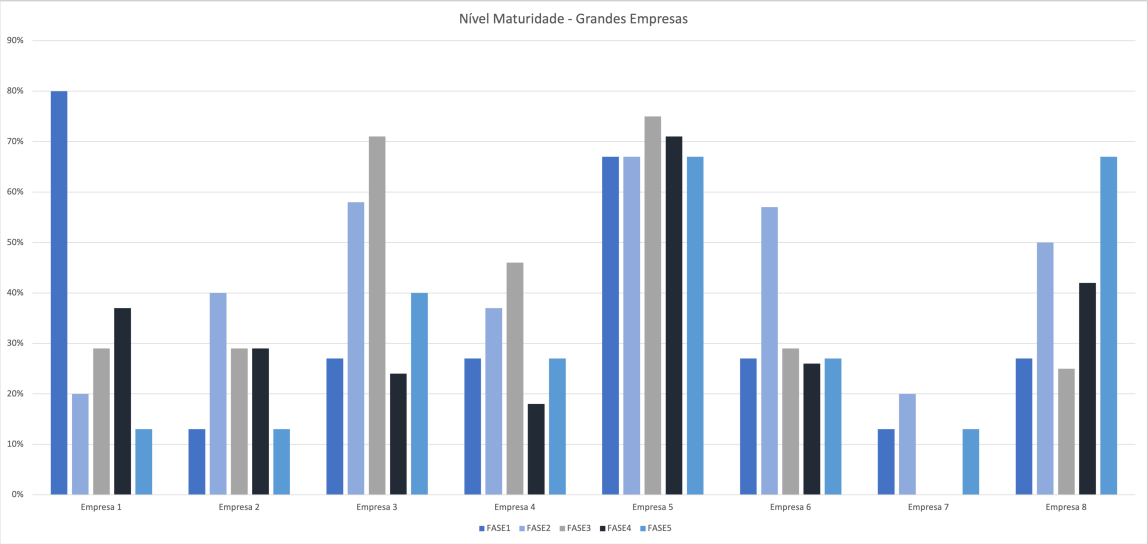


Figura 74: Resultados do Nível de Maturidade das Grandes Empresas

Na Figura 74 a empresa 5 tem grande destaque relativamente às restantes, pois em todas as fases têm um nível de maturidade **Muito Bom**. Pode-se observar que a empresa 1 na fase 1 tem um nível de maturidade **Excelente**, porém nas restantes fases tem um nível de maturidade **Insuficiente**. A empresa 7 não tem qualquer controlo implementado nas fases 3 e 4. Na maioria das fases têm todas um nível de maturidade **Insuficiente**.

Nível Médio de Maturidade Geral - Região Norte

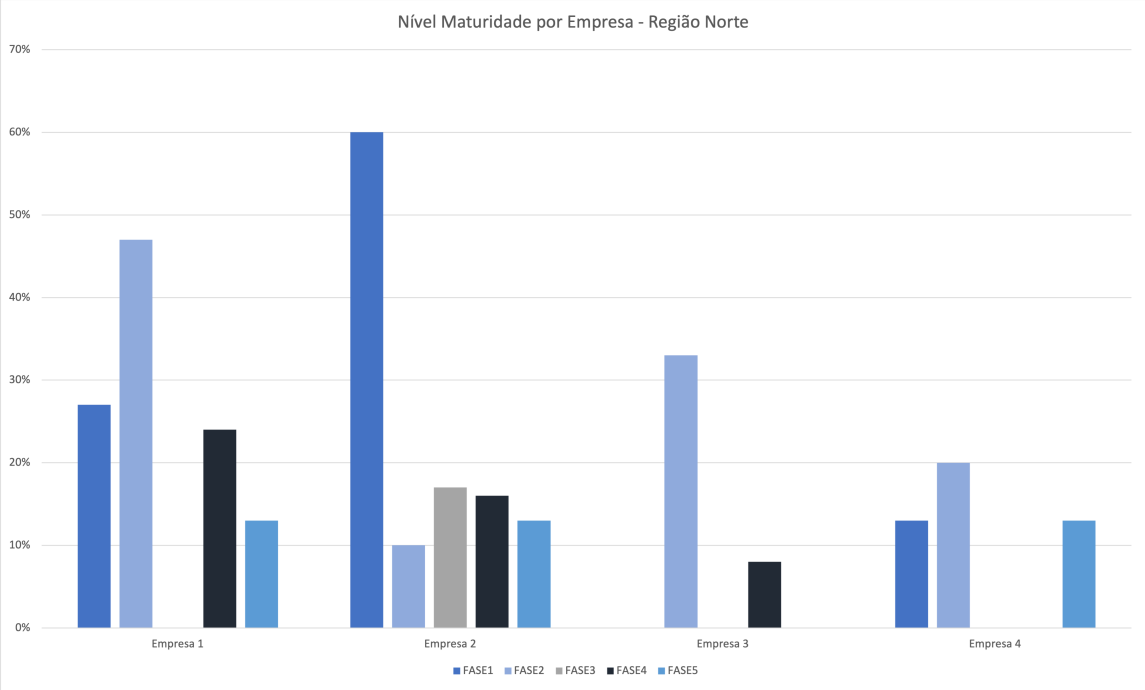


Figura 75: Resultados do Nível de Maturidade das organizações - Região Norte

Na Figura 75 é possível observar o nível da maturidade em cada fase das empresas inquiridas sediadas na Região Norte de Portugal. A empresa 2 destaca-se na fase 1 por ter um nível **Muito Bom**, porém nas restantes fases tem um nível **Insuficiente**. Na fase 2 da empresa 1 tem um nível de maturidade **Suficiente**. As restantes empresa têm um nível de maturidade **Insuficiente** ou até nulo em algumas fases.

Nível Médio de Maturidade Geral - Região Centro

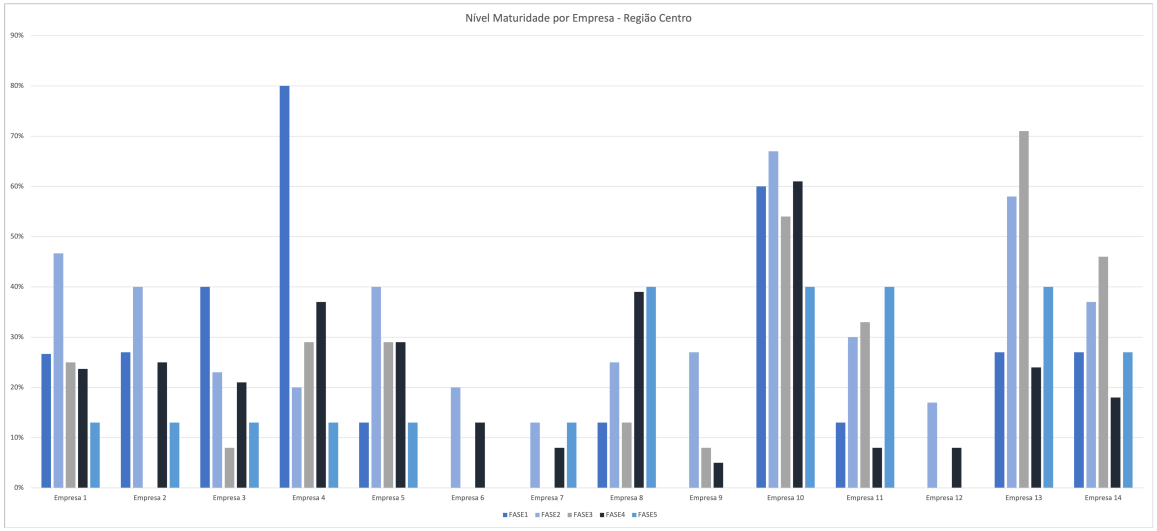


Figura 76: Resultados do Nível de Maturidade das organizações - Região Centro

Na Figura 76 pode-se observar o nível de maturidade em cada uma das fases das empresas inquiridas sediadas nesta região. A empresa 10 evidencia-se, pois apenas na fase 5 encontra-se num nível de maturidade **Suficiente** e nas restantes fases encontra-se num nível de maturidade **Bom** e **Muito Bom**. A empresa 4 apresenta um nível de maturidade **Excelente** na fase 1. As restantes empresas apresentam um nível de maturidade **Insuficiente** e em alguns casos, não apresentam qualquer capacidade em algumas fases.

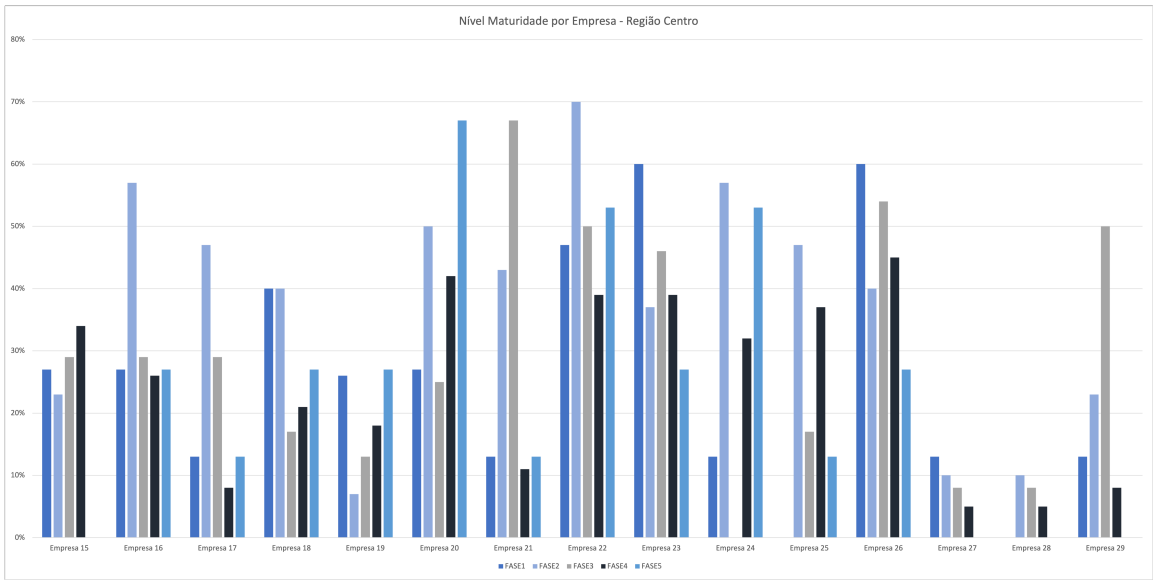


Figura 77: Resultados do Nível de Maturidade das organizações - Região Centro

Na Figura 77 pode-se observar os resultados do nível da maturidade das restantes empresas sediadas na região Centro de Portugal. Pode-se afirmar que as empresas 20, 22 e 26 em 2 ou mais fases têm um nível de maturidade acima de **Suficiente**, sendo que a maioria apresenta um nível de maturidade **Insuficiente**.

Nível Médio de Maturidade Geral - Área Metropolitana de Lisboa

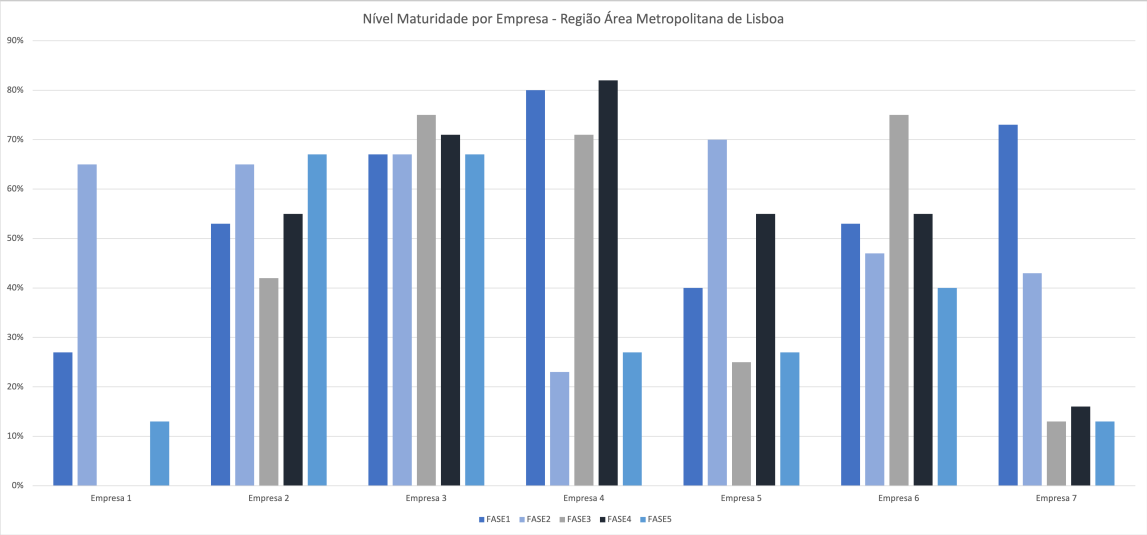


Figura 78: Resultados do Nível de Maturidade das organizações - Região Área Metropolitana de Lisboa

Na Figura 78 são apresentados os resultados dos níveis de maturidade por fase das empresas sediadas na área Metropolitana de Lisboa. A empresa 3 evidencia-se pela positiva, pois apresenta um nível de maturidade **Muito Bom** em todas as fases. As empresas 2 e 6 têm um nível de maturidade **Suficiente** ou superior em todas as fases. Relativamente à empresa 1 não apresenta qualquer competência nas fases 3 e 4, as restantes apresentam um nível de maturidade **Insuficiente** na maioria das fases.

Nível Médio de Maturidade Geral - Região Alentejo

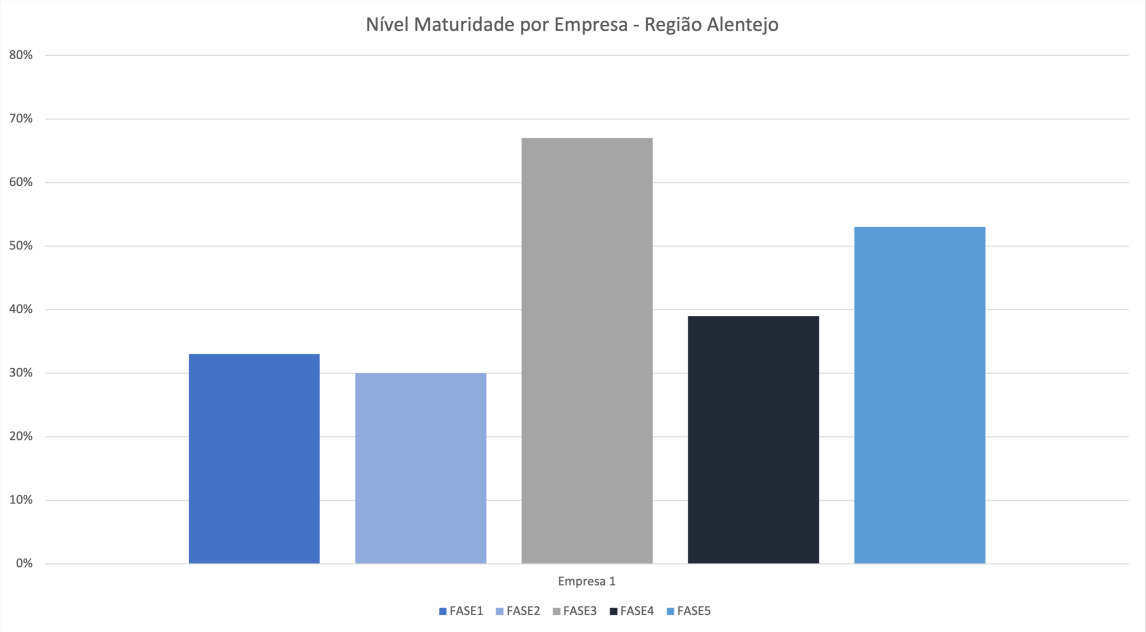


Figura 79: Resultados do Nível de Maturidade das organizações - Região Alentejo

Na Figura 79 estão apresentados os níveis de maturidade da única empresa inquirida sediada no Alentejo. Como se pode observar, a fase 3 tem um nível de maturidade **Muito Bom** e a fase 5 um nível **Bom**, sendo que as restantes têm um nível **Insuficiente** de maturidade.

Nível Médio de Maturidade Geral

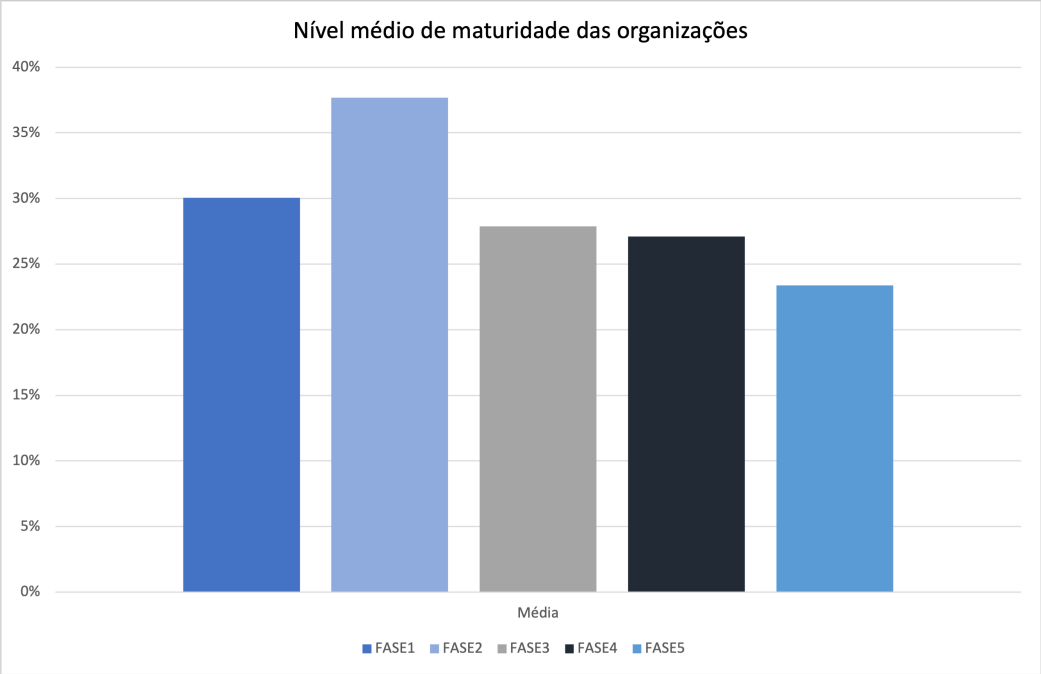


Figura 80: Resultados Gerais do Nível de Maturidade por fase

Tal como pode ser observado na Figura 80 que representa o nível médio de maturidade das empresas inquiridas, é notório que na fase 2 do nível de maturidade, de acordo com os resultados obtidos, é onde as empresas possuem mais competências implementadas. Porém, pode-se afirmar que nenhuma destas 5 fases alcança os 50% de valor percentual, e assim, pode-se constatar que ainda existem muitas competências a serem implementadas por parte das organizações, para melhorar assim este nível médio de maturidade em todas as fases do modelo de maturidade, e simultaneamente, poderem antecipar e estarem mais bem preparadas para enfrentar possíveis incidentes de segurança.

De acordo com os resultados obtidos, pode-se concluir que todas as empresas, em média, têm um nível de maturidade **Insuficiente**, visto que em nenhuma das fases ultrapassam os 40%.

Pode-se observar, também, que a fase com mais respostas negativas, é a fase 5 do inquérito. Pela ausência da figura de um CISO (Responsável de Segurança de Informação) nas organizações e equipas SOC ou CSIRT, é a justificação mais plausível para que esta apresentação de resultados.

Nível Médio de Maturidade Geral - Microempresas

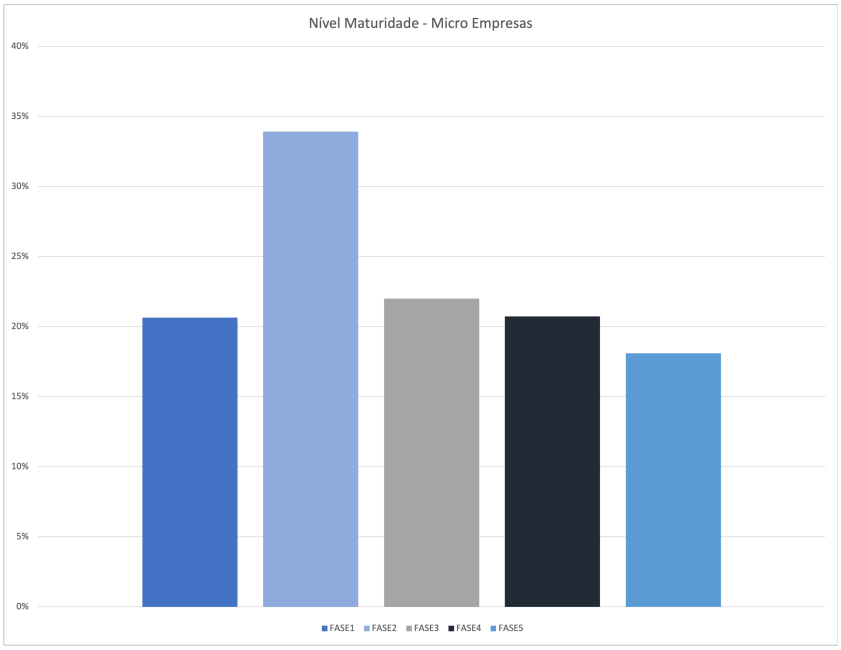


Figura 81: Resultados Gerais do Nível de Maturidade das Micro Empresas

Relativamente ao nível médio de maturidade em cibersegurança das microempresas, que se pode observar na Figura 81 tem destaque a fase 2, sendo a que tem mais competências implementadas, nomeadamente, o antivírus por ser um mecanismo para lidar com possíveis ameaças, ainda assim, pode-se afirmar que as microempresas têm um nível de maturidade **Insuficiente**.

Nas fases 1, 3 e 4, também existem várias falhas de competências implementadas. Na fase 1 poderá ser explicada pelo facto de a maioria não estabelecer comunicação com o CNCS. A ausência de recursos com formação nesta área, pode explicar o baixo nível de maturidade na fase 3 do inquérito. Na fase 4 do inquérito tem de igual forma um nível **Insuficiente**, e isto pode ser explicado pela falta de recursos humanos com capacidade de dar resposta a incidentes, e que não exista formação para dar aos colaboradores nesta área.

Pode-se observar que a fase com menos competências implementadas é a fase 5, isto pode ser explicado eventualmente pela ausência da figura de um CISO, e sendo microempresas poderá não fazer sentido existirem equipas SOC ou CSIRT.

Nível Médio de Maturidade Geral - PME

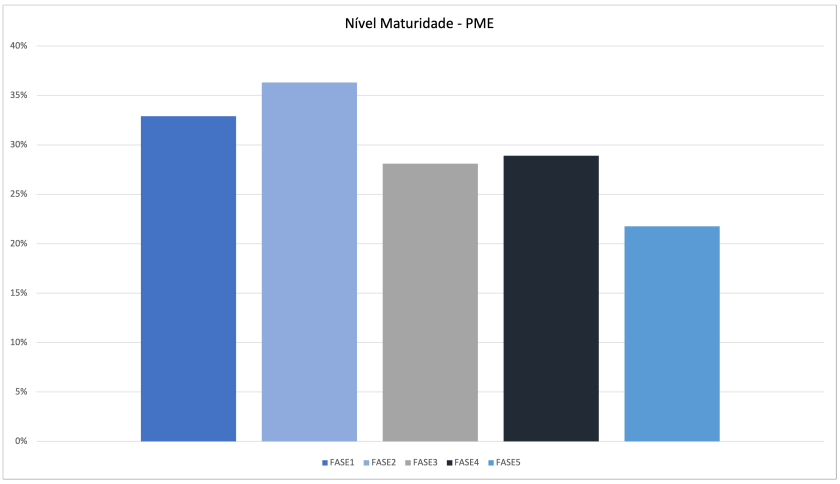


Figura 82: Resultados Gerais do Nível de Maturidade das PME

Relativamente ao nível médio de maturidade em cibersegurança das pequenas e médias empresas, que se pode observar na Figura 82 as fases 1 e 2 são as que apresentam mais competências implementadas como, por exemplo, a comunicação com o CNCS está implementada em várias das empresas inquiridas e fazem a gestão de ativos, existem formas mais diversificadas de *backup* e *restore*, são recolhidos metadados de comunicações para ser mais fácil analisar os incidentes de segurança, mas não as capacidades suficientes para ultrapassar os 40% e desta forma, encontram-se num nível **Insuficiente**.

Nas fases 3 e 4, respetivamente, na maioria das empresas ainda se verifica alguma escassez de recursos humanos com formação nesta área, e ainda faltam implementar mecanismos internos de resposta a incidentes.

Tal como foi verificado anteriormente nas microempresas, a fase 5 é a que tem um nível de maturidade mais baixo, pois a maioria não possui equipas SOC e CSIRT.

Nível Médio de Maturidade Geral - Grandes Empresas

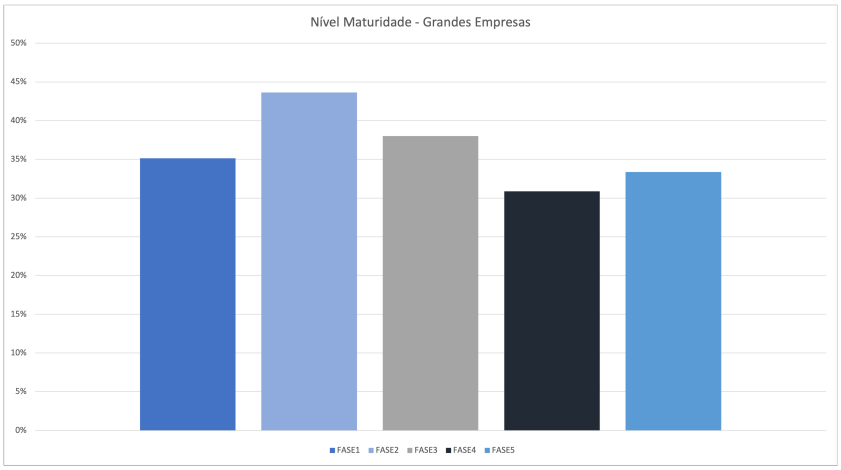


Figura 83: Resultados Gerais do Nível de Maturidade das Grandes Empresas

Relativamente ao nível médio de maturidade em cibersegurança das grandes empresas, que se pode observar na Figura 83 a fase 2 destaca-se, pois encontra-se num nível **Suficiente**, enquanto, todas as outras fases têm um nível de maturidade superior relativamente às PME e microempresas. Relativamente às grandes empresas a fase 4 é a que apresenta menos competências comparativamente às restantes fases, isto pode ser justificado pela ausência de alguns mecanismos de resposta a incidentes e falta de realização de simulacros.

Nas fases 1 e 2, as grandes empresas afirmam fazer uma gestão de ativos e estabelecer uma comunicação com o CNCS, e ainda apresentam ferramentas de mitigação de incidentes, por exemplo.

Nas fases 3 e 5, estão presentes recursos humanos com formação nesta área e com capacidade de analisar incidentes de segurança, e ainda, por existir na maioria delas, uma equipa dedicada à cibersegurança. Estes factos podem-se explicar por se tratar de grandes empresas e terem mais orçamento disponível para investir nesta área.

Relativamente às microempresas, apesar de terem um orçamento para esta área inferior, destacam-se pela positiva na fase 2 do inquérito, e não se verifica uma aposta na formação dos seus colaboradores, porque não existem na maioria delas colaboradores com formação na área.

Independentemente de ser microempresas ou pequenas e médias empresas, verifica-se que na fase 2 do inquérito estão bastante equivalentes, e de igual forma na fase 5 do inquérito.

Na fase 1 e 4 do inquérito as pequenas e médias empresas apresentam um nível de maturidade bastante parecido com as grandes empresas.

Na fase 5 do inquérito, as grandes empresas destacam-se na fase 5 e isto pode-se justificar pelo facto de terem um orçamento mais elevado para esta área e a sua dimensão justificar a existência de uma equipa dedicada à cibersegurança.

Nível de Maturidade em 3 setores distintos

Para se efetuar uma caracterização mais pormenorizada das organizações participantes deste estudo, foram selecionados os 3 setores distintos e com maior número de respostas, sendo calculado o seu nível de maturidade em cibersegurança. Estes 3 setores são o setor da informática e tecnologia, do qual fazem parte 8 empresas, o setor da agricultura, produção animal, silvicultura e pesca, que fazem parte 4 empresas, e por fim, o setor dos recursos naturais, também com 4 empresas.

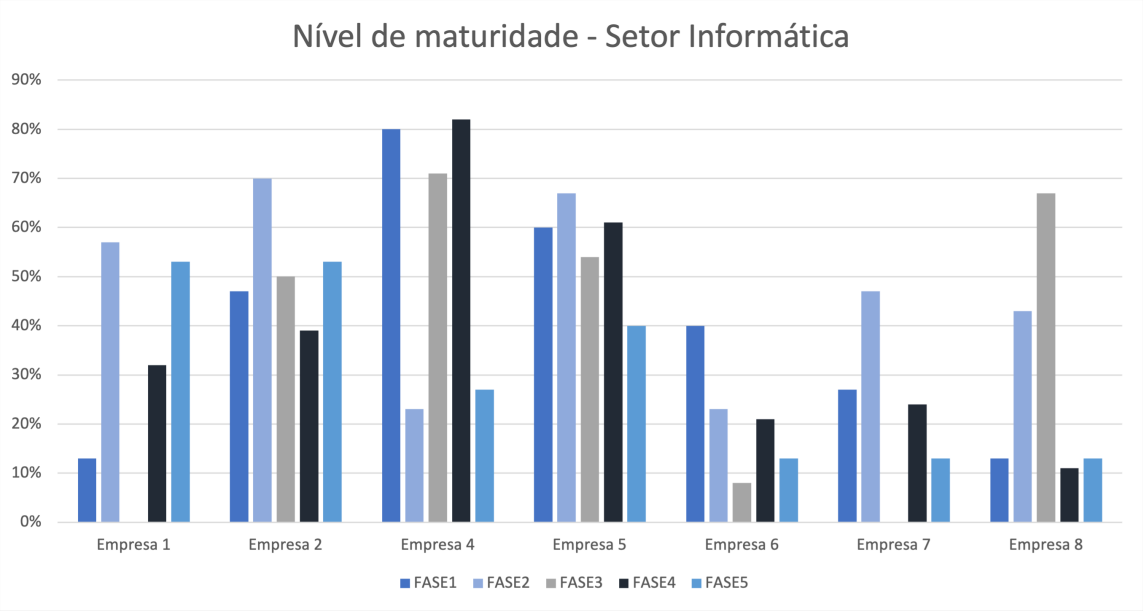


Figura 84: Nível de Maturidade por empresa do setor Informática e Tecnologia

Na Figura 84 pode-se observar o nível de maturidade em cibersegurança por empresa no setor da informática e tecnologia, na fase 1 as empresas 1, 7 e 8 têm um nível **Insuficiente** de maturidade. As empresas 2 e 6 encontram-se num nível **Suficiente**. A empresa 6 está num nível **Muito Bom**, com exceção da empresa 4 que se encontra num nível **Excelente**.

Relativamente à fase 2, destacam-se as empresas 2 e 5 que se encontram num nível **Muito Bom**. A empresa 1, encontra-se num nível **Bom**. As empresas 7 e 8 têm um nível de maturidade **Suficiente**. As restantes empresas têm um nível de maturidade **Insuficiente**.

Na fase 3 o nível de maturidade **Muito Bom** tem destaque nas empresas 4 e 8. A empresa 2 apresenta um nível de maturidade **Bom**, enquanto que a empresa 6 tem um nível de maturidade **Insuficiente**.

Na fase 4, a maioria das empresas apresenta um nível de maturidade **Insuficiente**. Face aos resultados obtidos é visível que a empresa 5 tem um nível de maturidade **Muito Bom**, e nesta fase a empresa 4 tem grande destaque tendo um nível de maturidade **Excelente**.

Relativamente à fase 5, metade das empresas tem um nível de maturidade **Insuficiente**. As empresas 1 e 2 encontram-se no nível **Bom**. As restantes encontram-se num nível **Suficiente**.

De realçar que a empresa 1 e 7 não tem qualquer capacidade implementada da fase 3.

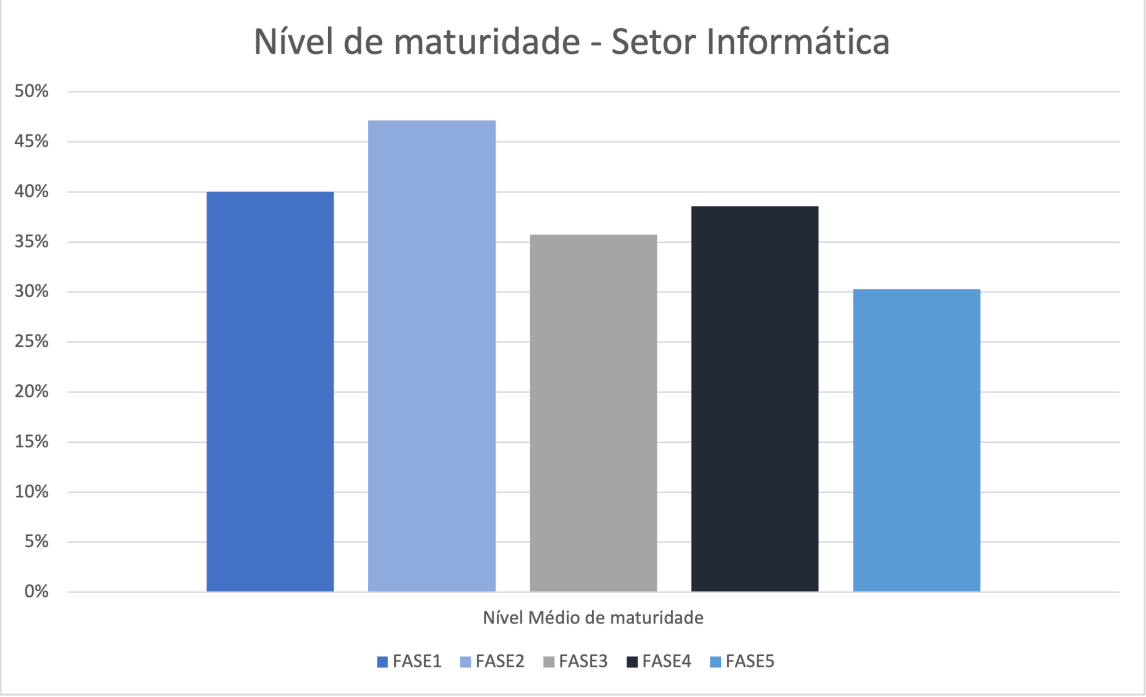


Figura 85: Nível de Maturidade por fase do setor Recursos Naturais

Para se ter uma visão mais geral deste setor, avaliou-se o nível de maturidade por fase. A partir da Figura 85 que representa o nível médio de maturidade em cibersegurança do setor da informática e tecnologia, observa-se que neste setor todas as fases encontram-se num nível **Insuficiente**, com exceção da fase 2 que se

encontra num nível **Suficiente**.

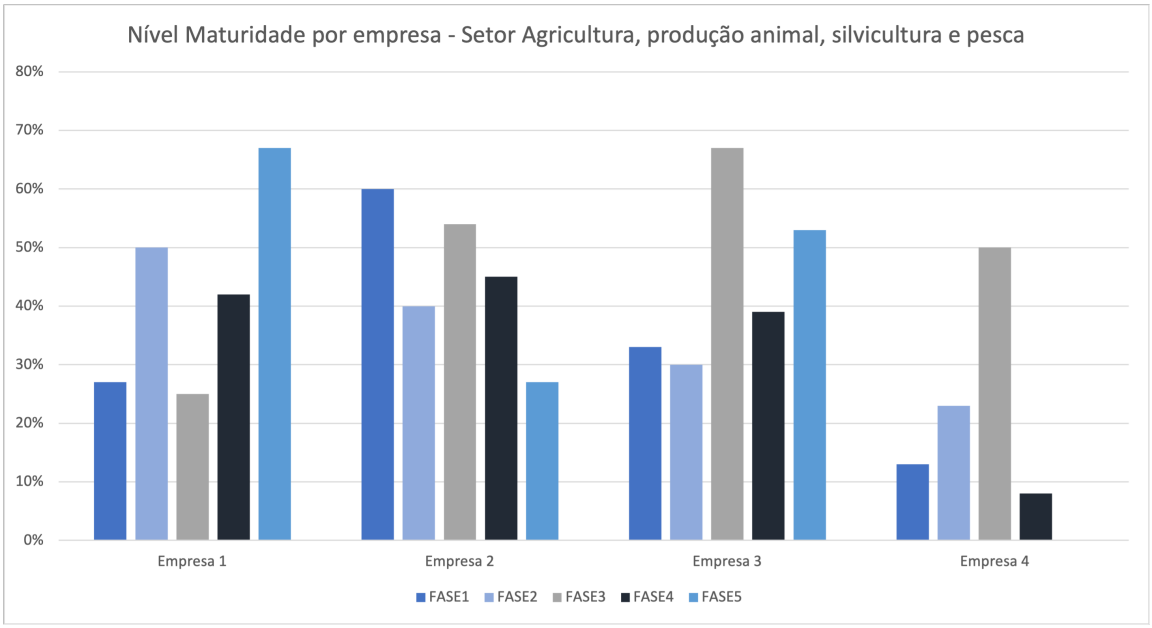


Figura 86: Nível de Maturidade por empresa do setor Agricultura, produção animal, silvicultura e pesca

Como se pode observar na Figura 86 que representa o nível de maturidade em cibersegurança por empresa no setor da agricultura, na fase 1 todas as empresas têm um nível **Insuficiente** de maturidade, exceto a empresa 2 que se encontra num nível **Muito Bom**.

Relativamente à fase 2, as empresas 3 e 4 encontram-se num nível **Insuficiente**. As restantes empresas, encontram-se num nível **Suficiente** e **Bom**, respetivamente.

As empresas 2, 3 e 4 apresentam 2 diferentes níveis de maturidade na fase 3, sendo eles **Bom** e **Muito Bom** na empresa 4.

Na fase 4, destacam-se as empresas 2 e 4 por terem um nível de maturidade **Bom**, e a empresa 3 por ter um nível **Muito Bom**.

A empresa 5 não tem qualquer capacidade pertencente à fase 5. Quanto às empresas 1, 2 e 3, apresentam diferentes níveis de maturidade, **Muito Bom**, **Insuficiente** e **Bom**.

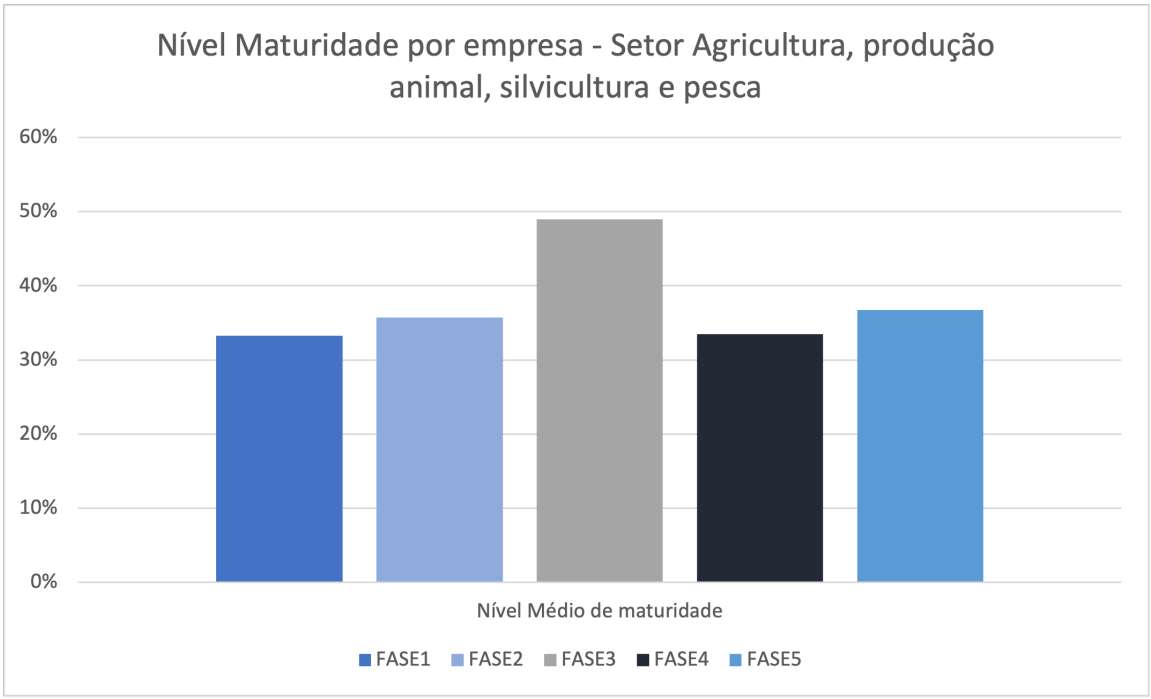


Figura 87: Nível de Maturidade por fase do setor Agricultura, produção animal, silvicultura e pesca

Para se ter uma visão mais geral deste setor, avaliou-se o nível de maturidade por fase. A partir da Figura 87 que representa o nível médio de maturidade em cibersegurança por empresa no setor da agricultura, conclui-se que neste setor todas as fases encontram-se num nível **Insuficiente**, exceto a fase 3 que se encontra num nível **Suficiente**.

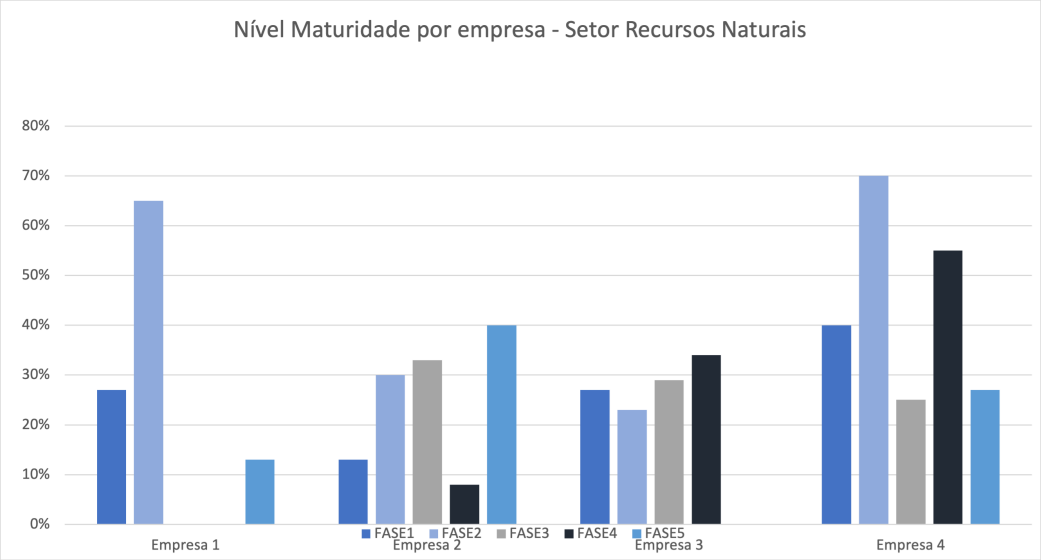


Figura 88: Nível de Maturidade por empresa do setor Recursos Naturais

Como se pode observar na Figura 86 que representa o nível de maturidade em cibersegurança das empresas deste setor, na fase 1 todas as empresas têm um nível **Insuficiente** de maturidade, exceto a empresa 4 que se encontra num nível **Suficiente**.

Relativamente à fase 2, as empresas 2 e 3 encontram-se num nível **Insuficiente**. As restantes empresas, encontram-se num nível **Muito Bom**.

Na fase 3 existe um nível de maturidade **Insuficiente**.

Na fase 4, as empresas 2 e por terem um nível de maturidade **Insuficiente**, e a empresa 3 tem um nível **Bom**.

A empresa 3 não tem qualquer capacidade pertencente à fase 5. Quanto às empresas 1, 2 e 3, apresentam diferentes níveis de maturidade, **Muito Bom**, **Insuficiente** e **Bom**.

De realçar que a empresa 1 não tem qualquer capacidade implementada das fases 3 e 4.

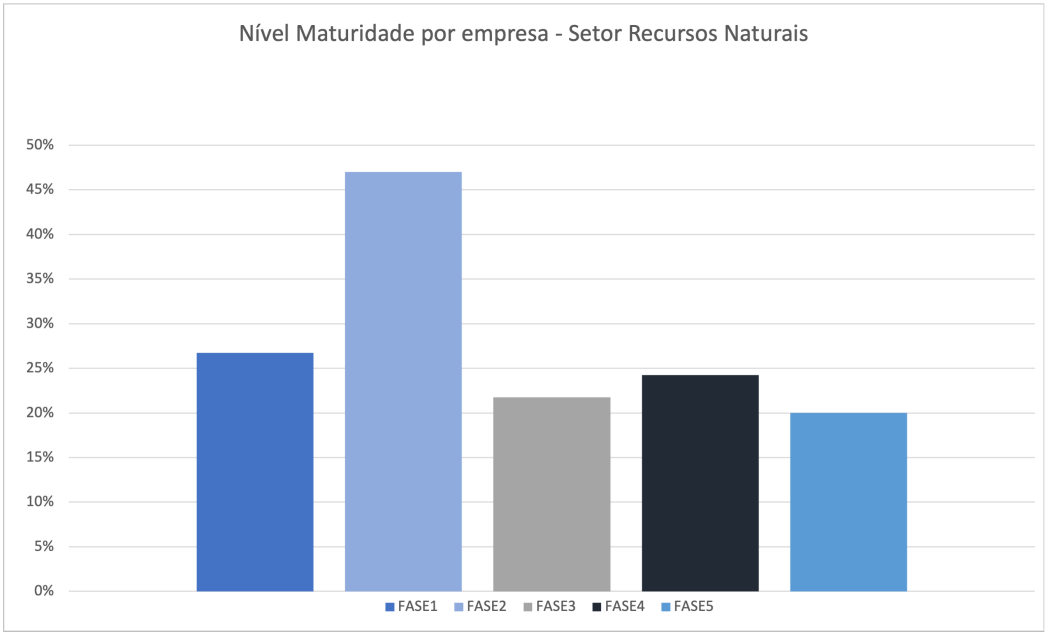


Figura 89: Nível de Maturidade por fase do setor Recursos Naturais

Para se ter uma visão mais geral deste setor, avaliou-se o nível de maturidade por fase. A partir da Figura 89 que representa o nível médio em cibersegurança do setor dos recursos naturais, conclui-se que neste setor todas as fases encontram-se num nível **Insuficiente**, com exceção da fase 2 que se encontra num nível **Suficiente**.

Por se tratar do setor da tecnologia e informática seria expectável que o seu nível de maturidade fosse mais elevado, e em termos de panorama geral pode significar que os restantes setores também não tenham uma maturidade elevada.

Verifica-se que a fase 2 do setor da informática e dos recursos naturais têm ambos um nível de maturidade em cibersegurança **Suficiente**.

O setor da agricultura é o que apresenta um maior nível de maturidade em cibersegurança na fase 3 do inquérito, sendo uma das fases com mais lacunas nos outros setores.

Existem setores que podem ter mais propensão para investir mais nesta área e na tecnologia do que os restantes, também por ser mais necessária a tecnologia nesses setores, e isso é visível nos gráficos citados. O setor da agricultura, dos recursos naturais e até da construção, são setores que em termos tecnológicos não necessitam de tanto investimento, exceto se se tratem de grandes empresas para investir em infraestrutura tecnológica.

Empresas que se destacam positivamente pelo seu nível de maturidade em cibersegurança

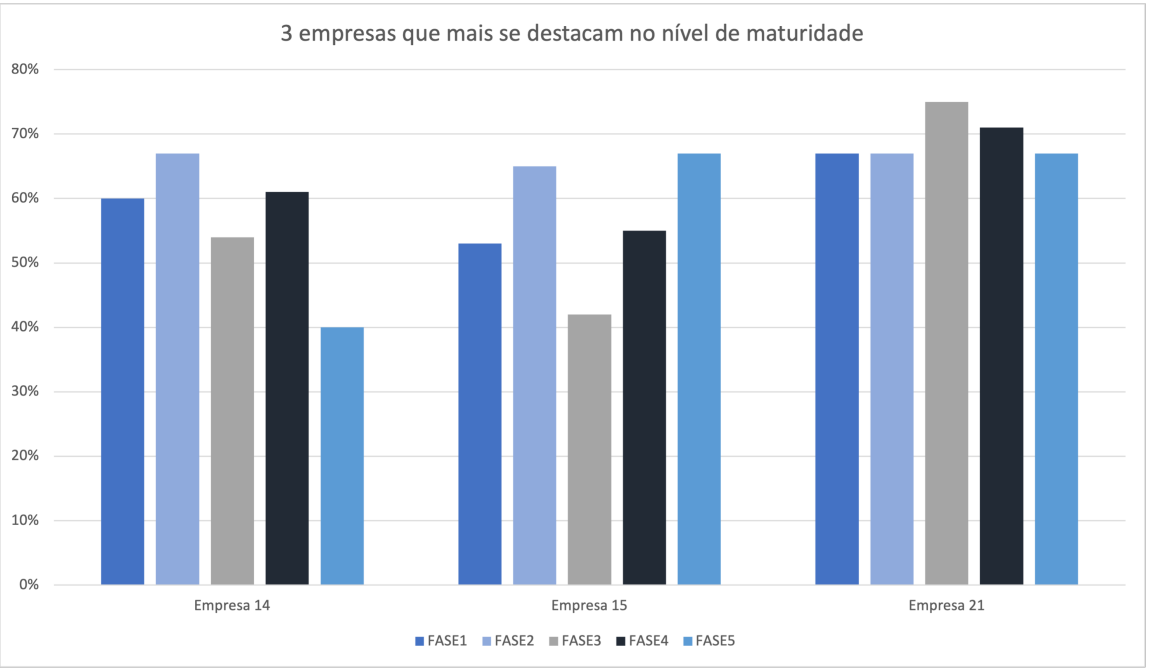


Figura 90: 3 empresas com um nível de maturidade em cibersegurança mais elevado

Na Figura 90 estão representadas as 3 empresas que se destacam positivamente tendo em conta o seu nível de maturidade em cibersegurança.

A empresa 1 pertence ao setor da informática, sendo considerada uma grande organização visto que conta com mais de 250 colaboradores, e está sediada na região Centro de Portugal. Esta empresa tem um seguro contratado para cobrir incidentes de segurança, com colaboradores com certificações na área, nomeadamente, CCNA CyberOps, CEH e SSCP. Quanto ao grau de importância da segurança da informação e à preocupação com os danos reputacionais em caso de incidente, esta revela ter grande preocupação com estes temas. Porém, o inquirido não tem conhecimento se existe orçamento anual para investir nesta área.

A empresa 2, pertence ao setor de Consultoria tal como a anterior, é considerada uma grande organização devido à quantidade de colaboradores existentes, e encontra-se sediada na Área Metropolitana de Lisboa. Tal como a empresa anterior, esta possui seguro para cobrir possíveis incidentes de segurança e a empresa possui a certificação ISO27001. O inquirido não tem conhecimento se existe um orçamento anual para investir nesta área. O inquirido revela também grande preocupação com os danos reputacionais e afirma que é um tema muito importante, no entanto, não sabe se existe algum orçamento anual destinado à cibersegurança.

O setor de atividade da última empresa destacada é Serviços, também se pode considerar uma grande organização pela quantidade de colaboradores, e está sediada na Área Metropolitana de Lisboa. Tal como as anteriores, tem um seguro para cobrir possíveis incidentes de segurança. Revela ainda grande preocupação com a reputação e revela que este tema tem grande importância para a empresa, mas também desconhece se existe algum orçamento anual para investir nesta área.

Empresas que se destacam negativamente pelo seu nível de maturidade em cibersegurança

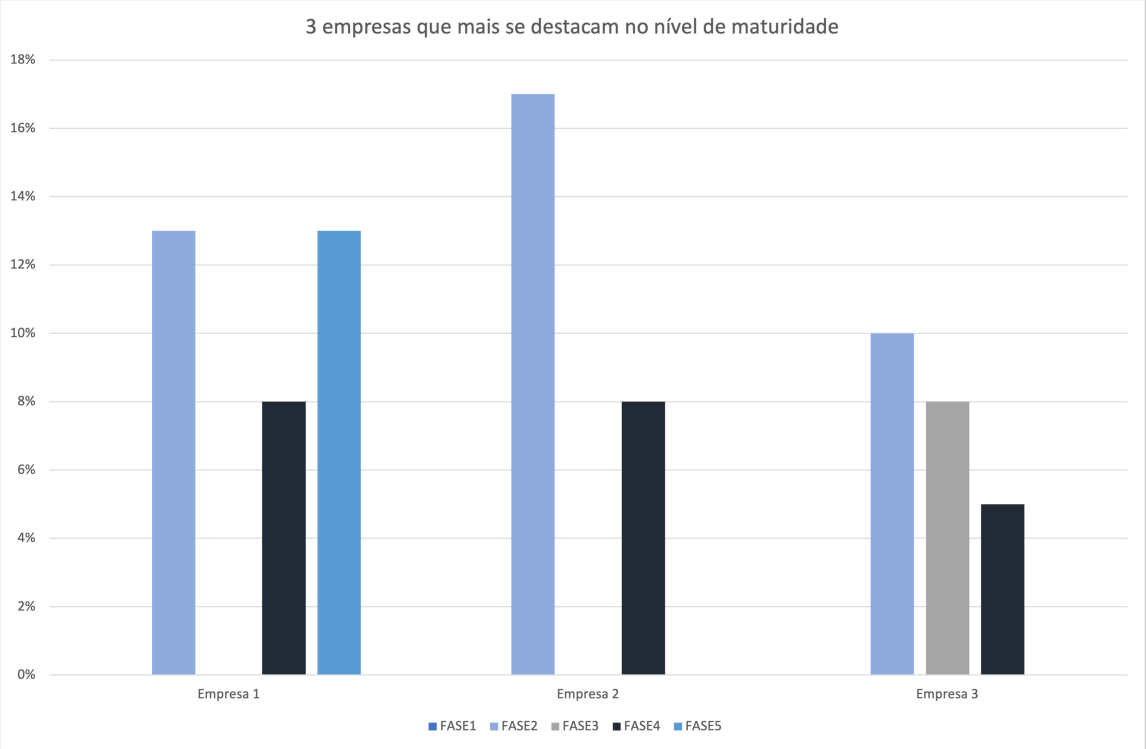


Figura 91: 3 empresas com um nível de maturidade mais baixo

Na Figura 91 estão representadas as 3 empresas que se destacam negativamente tendo em conta o seu nível de maturidade em cibersegurança.

A empresa 1, pertence ao setor da Construção, considerada uma PME visto que tem entre 6 a 10 colaboradores, e está sediada na região Centro de Portugal. O inquirido não sabe se existe algum seguro contratado nesta área, mas indica que existe um orçamento anual para investir em cibersegurança. Revela ainda que a organização tem preocupação com possíveis danos causados em caso de incidente e que este tema é muito importante. Como pode ser observado ainda tem por implementar na totalidade capacidades da fase 1 e da fase 3.

A empresa 2 trata-se de uma organização de serviços, que se encontra sediada na região Centro de Portugal, com 100 a 249 colaboradores. O inquirido refere que este é um tema importante para a organização, e ainda que, não existe preocupação com possíveis danos reputacionais causados por incidentes de segurança. É referido que não existe nenhum seguro contratado, e não existem certificações feitas na área. Através do gráfico conclui-se que não tem qualquer capacidade implementada referente à fase 1, 3 e 5.

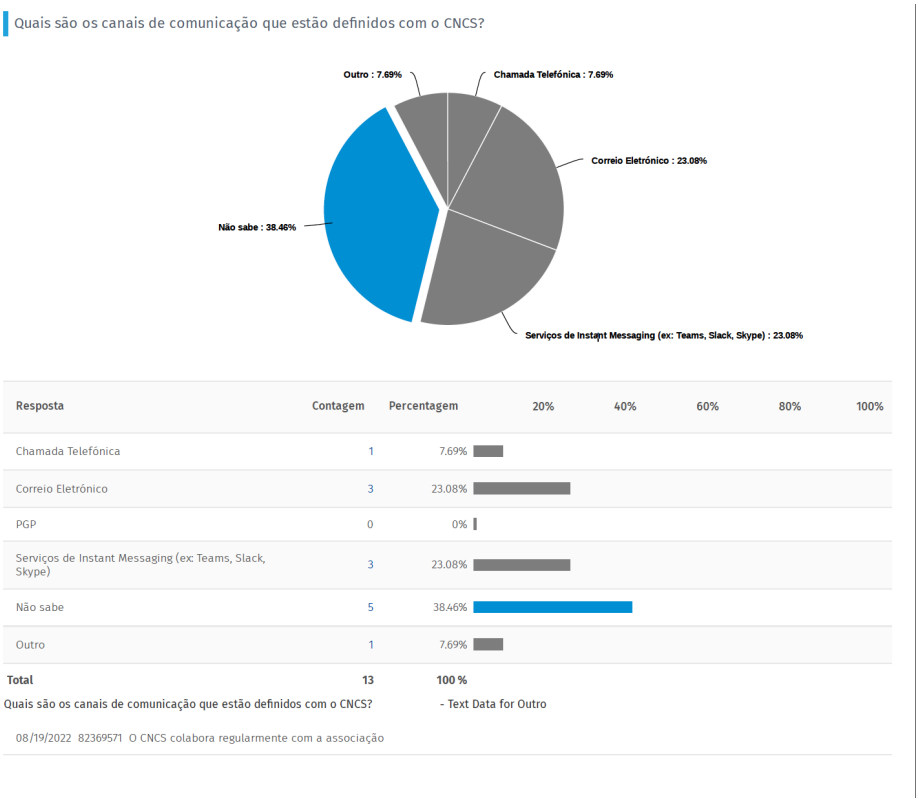
A última empresa representada no gráfico, trata-se de uma organização cuja área de negócio é o comércio. É considerada uma PME visto que tem entre 6 a 10 colaboradores, e está sediada na região Centro de Portugal. Revela que este tema é muito importante, e refere que tem preocupação com a reputação em caso de incidente de segurança. O inquirido afirma não saber se existe algum seguro contratado e não existe nenhum orçamento para investir nesta área.

Comparando os resultados obtidos, pode-se observar que as empresas com um nível de maturidade em cibersegurança mais elevado são todas grandes empresas, embora de setores diferentes, sendo o setor da informática, consultoria e serviços. Estes resultados podem ser justificados pelo facto de se tratar de grandes empresas e por esse motivo existir um orçamento maior e um maior investimento do que as restantes empresas para esta área.

Seria expectável que as 3 empresas com um nível de maturidade em cibersegurança mais baixo fossem microempresas, mas trata-se de pequenas e médias empresas, com diferentes áreas de negócio, nomeadamente, a área da construção, serviços e comércio. Estes setores do comércio, serviços podem apresentar este nível de maturidade tão baixo, por não possuírem infraestrutura tecnológica e a maioria dos serviços tecnológicos serem *outsourcing*.

Destaques dos Resultados

Durante a análise de resultados foi possível detetar algumas contradições por parte dos inquiridos, na medida em que existe preocupação com esta área, mas depois não há investimento e não são tomadas as ações necessárias para se proteger.



Resposta	Contagem	Percentagem
Chamada Telefónica	1	7.69%
Correio Eletrónico	3	23.08%
PGP	0	0%
Serviços de Instant Messaging (ex: Teams, Slack, Skype)	3	23.08%
Não sabe	5	38.46%
Outro	1	7.69%
Total	**13**	**100 %**

Quais são os canais de comunicação que estão definidos com o CNCS? - Text Data for Outro

08/19/2022 82369571 O CNCS colabora regularmente com a associação

Figura 92: Questão sobre a comunicação com o CNCS

Na Figura 92 pode-se observar que uma das organizações afirmou que colabora regularmente com o CNCS.

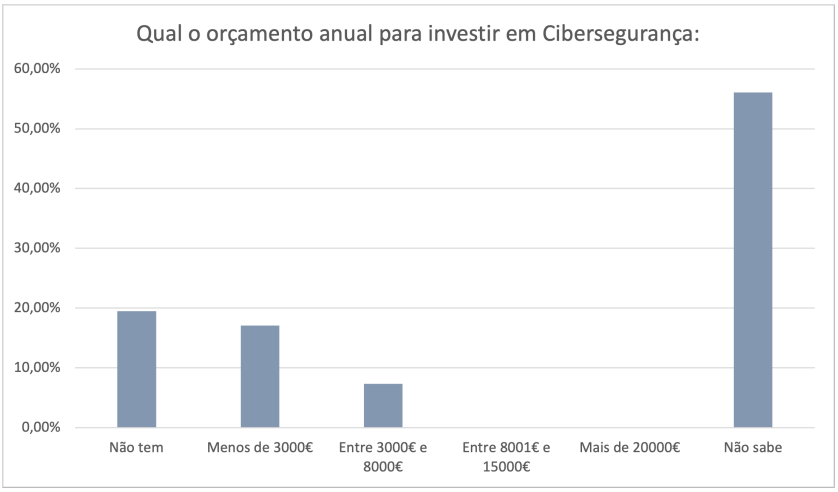


Figura 93: Resultados sobre qual o orçamento anual para investir em Cibersegurança

Na Figura 93 que representa o orçamento anual disponível para investir em cibersegurança, em que cerca de 24% das organizações têm algum orçamento anual definido para esta área da Cibersegurança.

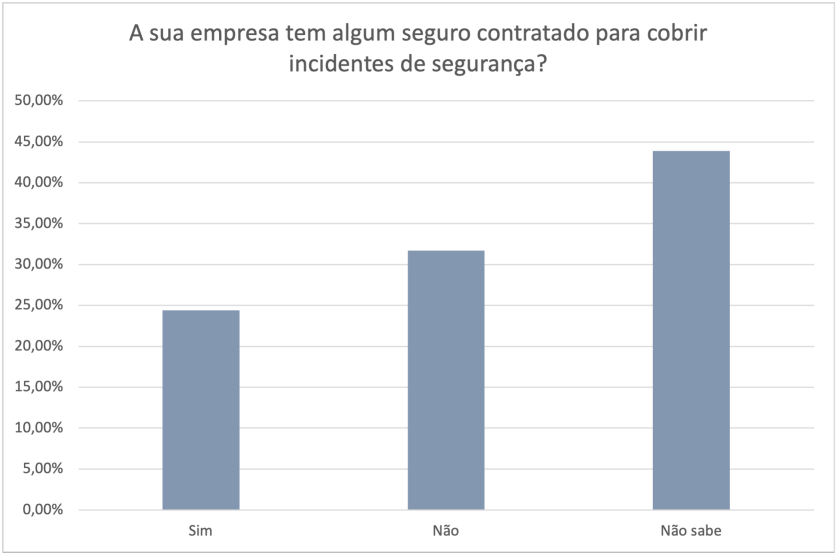


Figura 94: Resultados sobre se existe seguro contratado para cobrir incidentes de segurança

Relativamente à existência de seguro que possa cobrir futuros incidentes de segurança, pode-se afirmar que ainda não está presente em muitas empresas, tal como se pode observar na Figura 94, e que apenas 24% das empresas têm um seguro para estas ocorrências. Mas é possível constatar-se que a grande maioria não tem conhecimento se existe ou não seguro contratado.

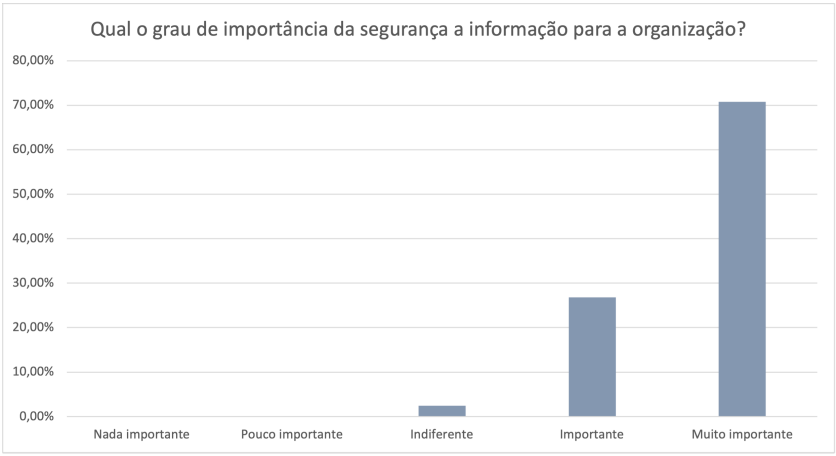


Figura 95: Resultados sobre a importância deste tema para a empresa

Quando se questiona o grau de importância da cibersegurança para a empresa é visível na Figura 95, que para 71% das empresas este tema é muito importante, e que para apenas 2%, é classificado como um assunto indiferente.

Figura 96: Resultados sobre se existe preocupação com os danos reputacionais em caso de incidente de segurança

Para se averiguar a preocupação existente com eventuais danos reputacionais em caso de incidente de segurança, pode ser observado na Figura 96 que 98% dos inquiridos respondeu de forma positiva a esta questão.

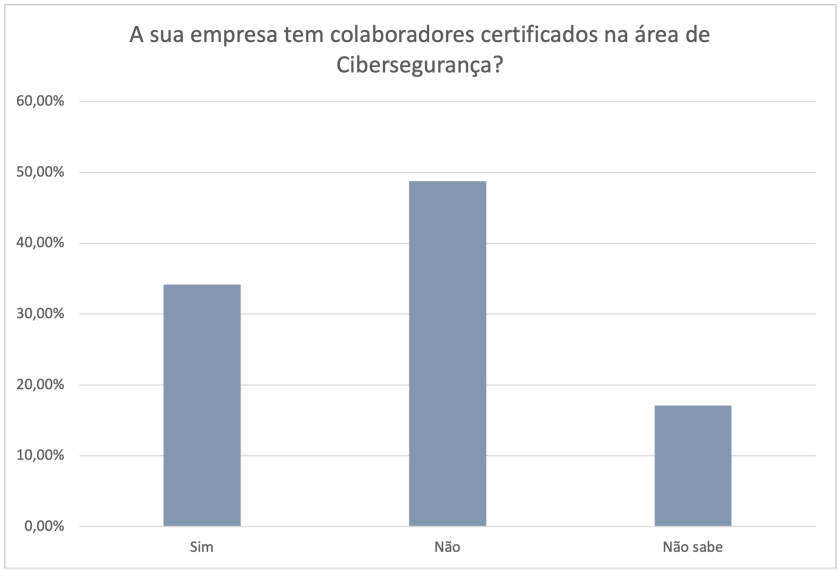


Figura 97: Resultados sobre se existem colaboradores certificados

Com os resultados obtidos nesta questão, presentes na Figura 97, é evidente que quase metade das empresas não tem qualquer colaborador com certificação em alguma norma standard da área da cibersegurança.

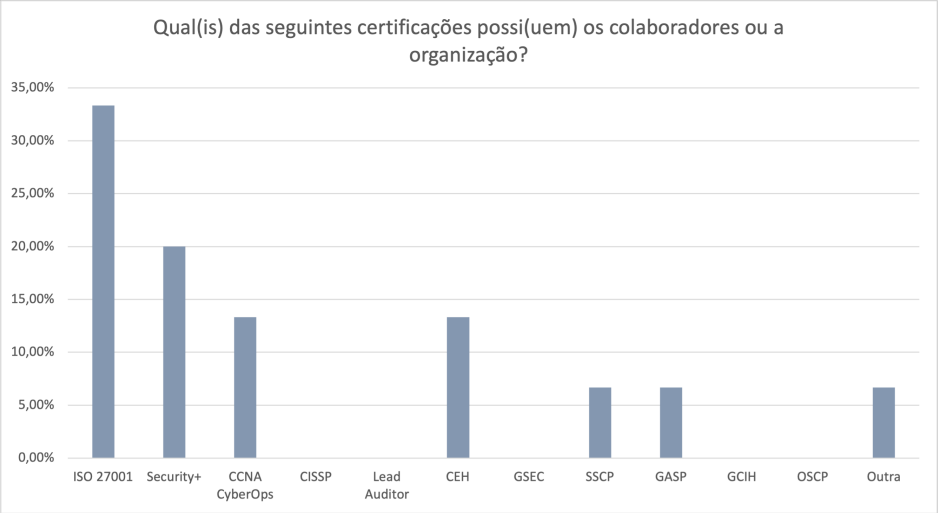


Figura 98: Resultados sobre as certificações que possuem os colaboradores/empresa

Dos 34% de colaboradores certificados, a maioria tem certificação nas seguintes normas representadas na Figura 98. É possível concluir que a certificação na norma ISO 27001 é a que tem maior percentagem.

Como se pode observar na Figura 95 e 96 os inquiridos afirmam que existe grande preocupação com este tema e que este tema é deveras importante para a organização, mas, por outro lado, apenas 24% das empresas têm um seguro contratado para cobrir estes riscos e também apenas 24% tem um orçamento anual definido para investir nesta área. Também está evidenciada uma grande preocupação com danos reputacionais devido a incidentes de segurança.

Através destes dados, pode-se afirmar que existe consciência de que a cibersegurança é uma área muito importante, porém a maioria das organizações ainda não têm competências suficientes nesta área e observa-se alguma resistência no investimento nesta área, por este motivo inúmeras empresas está aquém do que era esperado.

De acordo com a Figura 99, pode-se concluir que os controlos da norma ISO 27001:2013 em estudo, A.10.1.1 e A.10.1.2, A.13.1.1 e A.14.2.4 e A14.2.9 são os que são mais cumpridos nas empresas que participaram neste estudo. Porém, existe o controlo A.12.2.1, A.13.1.3 e o A.12.3.1, estão perto ou parcialmente a serem cumpridos. Nenhuma das empresas cumpre todos os controlos da ISO. De notar que nos relatórios disponibilizados às empresas vão ser destacados quais os pontos da norma ISO27001:2013 que já estão cumpridos ou parcialmente cumpridos.

Os controlos A.10.1.1 e A.10.1.2 recomenda que seja especificada uma política que especifique quais os ativos que devem ser encriptados. Tudo o que for encriptado deve ser documentado, qual o tipo de encriptação que foi utilizada, de que forma é gerida, e a identificação do responsável desta área. Deve ser utilizado um certificado digital. Este certificado deve ser emitido por uma entidade certificadora e possui um prazo de validade.

O controlo A.12.2.1 cita que se deve criar controlos para detetar, prevenir e recuperar em caso de existir alguma perda ou danos de informação. Devem ser proibidos o uso de softwares não autorizados.

O controlo A.12.3.1 sugere que de devem realizar e testar as cópias de segurança regularmente. Estes testes garantem a sua integridade.

O controlo A.13.1.1 recomenda que se deve utilizar softwares para registar eventos e monitorizar a rede para analisar o tráfego.

O controlo A.13.1.3 cita que deve ser feita uma divisão das redes. Esta segregação das redes permite a proteção das informações de cada uma das redes virtuais. Entre estas redes deve ser criada uma Firewall que permite filtrar o tráfego ou, restringir o fluxo de dados entre redes.

Os controlos A.14.2.4 e A.14.2.9 recomendam que se devem dissuadir as alterações no software. As alterações devem ser apenas as necessárias, e devem ser totalmente controladas. E, devem ser definidos testes de aceitação, bem como os critérios de aceitação para eventuais sistemas de informação que surjam futuramente.

P	Controlo Parcialmente cumprido
x	Controlo cumprido
	Sem associação

Empresa	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
Questão/Controlo																																									
Fase 1 - Preparação Inicial																																								
Q1/A.16.1.1							x		x							x	x						x			x						x		x			x	x		
Q1.1/A.10.1.1 - A.10.1.2							x																			x								x			x			
Q3/A.8.2.1	x			x		x	x								x						x	x		x	x	x	x					x		x			x	x		x	
Q3.4 - Sem associação																																									
Q5/A.10.1.1 - A.10.1.2		x	x		x	x	x	x					x	x	x			x	x	x	x		x	x	x	x	x	x	x	x	x	x			x	x				
Q6- Sem associação																																									
Fase 2 - Arquitetura																																									
Q1/A.12.2.1 - A.13.1.3	P	P	P	P		P		P	P	P	P	P	P	P	P	P	P	P	x		X	P	P		P		X		P	P	P	x		P	P	P			P	P	P
Q1.1- Sem associação																																									
Q3/Sem associação																																									
Q3/A.12.3.1	P	P	P		P	P	P	P	P	P	P	P			P	P		P	P	P	P	P	P	P	P		P			P		P	P	x	x	x	x		P	P	
Q4/18.1.1			x	x		x	x						x	x	x	x		x			x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x		x	
Q5/A.10.1.1 - A.10.1.2																																									
Q6/A12.4.1 A12.4.2			x	x				x						x	x		x	x	x	x	x	x					x		x	x	x	x	x	x					x	
Q7/7.2.2	x		x								x			x	x			x			x	x		x		x	x	x	x		x			x		x			x	
Q8/Sem associação																																									
Q9/Sem associação																																									
Fase 3 - Segurança dos Dispositivos																																								
Q1/13.1.1	x					x	x	x			x	x		x	x			x	x	x	x	x	x	x		x	x		x		x	x	x		x	x	x	x	x	x	x
Q2/A.6.2.1 - A.6.2.2														x			x				x									x					x					
Q3/A.13.1.1																														x	x	x			x				x	
Q4/A.13.1.2	x													x	x			x	x	x	x	x		x			x			x	x	x	x		x				x	
Q5/A.7.2.2					x		x	x						x	x	x		x	x		x		x	x	x			x	x	x	x		x		x	x			x	x
Fase 4 - Consolidar a Cibersegurança																																									
Q1/A14.2.4 A14.2.9	x	x	x				x	x		x	x		x	x	x	x	x	x	x	x	x	x	x	x		x	x		x	x	x	x	x			x	x			x	
Q2/Sem associação																																									
Q3/A14.2.9											x			x	x					x	x			x			x				x	x	x	x	x	x	x			x	
Q4/Sem associação																																									
Q5/A17.1.3							x														x			x			x		x		x					x					
Q6/Sem associação																																									
Q7/A16.1.1	x				x	x					x			x	x	x		x	x		x	x		x		x	x		x		x	x	x	x		x			x	
Fase 5 - Equipa de Cibersegurança																																									
Q1/A16.1.1	x														x	x		x	x		x								x			x		x					x	
Q2/A12.6.1														P							P			P		x			P		P	P									
Q3/Sem associação																																									
Q4/Sem associação																																									
Q5/Sem associação																																									
Q6/Sem associação																																									
Q7/Sem associação																																									

Figura 99: Tabela de mapeamento Respostas - ISO

6

CONCLUSÕES

Com o crescente número de ataques informáticos, cada vez mais a temática Cibersegurança está presente na maioria das organizações derivado aos dados atualmente serem algo a proteger, não só pela questão da continuidade de negócio em caso de ataque mas também pela obrigatoriedade de proteção de dados imposta pela União Europeia a todas as organizações.

Sabendo que as organizações estão altamente dependentes da tecnologia, estas deverão cumprir requisitos de segurança até a nível tecnológico, para evitar ao máximo que haja um incidente pois, quando o há é bastante preocupante pois na realidade a maior parte das vezes acaba por trazer repercussões negativas, sejam perdas de dados ou até paragem do negócio.

Por este motivo é crucial que os órgãos de administração das organizações estejam mais sensibilizados para este assunto, para poderem aprovar a execução das devidas melhorias. A prevenção é o primeiro passo que uma organização deve tomar para garantir a segurança da informação, onde nessa fase devem analisar os riscos ao qual estão expostas e depois sim, traçar estratégias e implementar melhorarias para garantir a robustez da sua Cibersegurança.

Assim, no enquadramento deste problema, a realização deste estudo verificou-se o nível de maturidade das empresas inquiridas através do inquérito que permite estudar que mecanismos são utilizados e como este tema da cibersegurança é encarado, e ainda, perceber em que nível de maturidade se encontra.

Ao responder a este inquérito, é possível que a organização conheça em que nível de maturidade se encontra, pois ao ter esta informação e se se encontrar num nível de maturidade intermédio também é uma forma de transmitir mais confiança e fiabilidade a todos os seus parceiros com quem trabalha diretamente.

As questões iniciais afetas a esta dissertação foram respondidas, nomeadamente, foi possível conhecer e aferir o nível de maturidade em cibersegurança do tecido industrial português, através do estudo das normas e do modelo de maturidade definido. O estudo inicial das normas e conjuntos de boas práticas permitiu perceber quais os controlos ou ações que as organizações se devem guiar. Considerou-se que o inquérito seria a melhor ferramenta para abordar as organizações e consequen-

temente obter o maior número de resultados possível. Optou-se por disponibilizar posteriormente um relatório personalizado individual para as organizações que manifestassem esse interesse com o seu nível de maturidade em cada uma das fases do inquérito, e ainda, com algumas sugestões de melhorias das suas capacidades que podem ser implementadas, auxiliando as organizações a aumentar a robustez neste tema.

Através das perguntas iniciais foi possível obter uma caracterização do tecido industrial português, e desta forma teve-se a oportunidade de perceber quais as práticas que já estão implementadas e a ser priorizadas nas organizações.

Com a realização desta investigação foi possível alcançar o principal objetivo, aferir que o nível de maturidade das organizações é Insuficiente e desta forma pode-se afirmar que existem várias lacunas que precisam de ser colmatadas e as organizações têm um longo caminho a percorrer para melhorar o seu nível de maturidade.

Paralelamente, foi feito um estudo para perceber quais os controlos da norma ISO27001:2013 já se encontram totalmente implementados ou parcialmente, e foi possível concluir que ainda existe um longo caminho a percorrer neste aspeto, pois ainda existem muitos controlos desta norma por implementar.

Foi feita a comparação de 3 setores com mais respostas dadas, e percebeu-se que o setor de Informática é o que demonstra ter um nível de maturidade mais elevado que os restantes. Relativamente à comparação entre os diferentes tipos de empresa, tendo em conta o seu número de funcionários, tornou-se evidente que as grandes empresas têm um nível de maturidade em cibersegurança superior.

Ao serem analisados os resultados, foi observado uma grande número de respostas "Não Sei", esta elevada quantidade pode ser pelo facto do inquirido não possuir as devidas competências técnicas na área para responder com exatidão às questões colocadas.

Esta dissertação permite orientar e apoiar as organizações para poderem aumentar a segurança da informação e estejam melhor preparadas para atuar em caso de incidente de segurança, e que as organizações preencham todos os requisitos das capacidades mínimas para a cibersegurança. Através dos resultados alcançados com este estudo, estes podem ser utilizados de maneira que as organizações possam definir novas estratégias para reforçar o seu nível de maturidade. Estes resultados podem ainda ser vistos como uma forma de sensibilização sobre o tema da cibersegurança.

As principais recomendações deste estudo são as seguintes:

- *Primeira fase do modelo de maturidade*

Que as organizações colaborem com o CNCS de forma sistemática e estabelecer um ponto de contacto com esta entidade.

- Segunda fase do modelo de maturidade

Que a organização deve estar elucidada das normas e quadros legais e regulatórios a que está sujeita, sejam nacionais ou internacionais;

Devem ser registadas as atividades de utilizadores e registo de eventos como os logs.

- Terceira fase do modelo de maturidade:

Que seja definida uma política BYOD (Gestão de Dispositivos Móveis Pessoais); Efetuar uma estão dos eventos de segurança utilizando um SIEM ou outro sistema semelhante;

- Quarta fase do modelo de maturidade:

Definir um plano de formação nesta área para capacitar os colaborares sobre este tema;

Verificar se existe necessidade de criar uma equipa capaz de dar resposta a incidentes;

- Quinta fase do modelo de maturidade:

Consoante a dimensão da empresa, nomear um Responsável de Segurança da Informação (CISO);

Para se alcançar um nível de maturidade em cibersegurança **Suficiente**, devem ser tidas em conta estas recomendações citadas.

Durante o desenvolvimento desta investigação existiram algumas limitações que desaceleraram este processo, nomeadamente, a análise das diversas normas estudadas e a escolha da plataforma para a implementação e disponibilização do inquérito, pois no fim de várias tentativas de plataformas percebeu-se que nem todas teriam as funcionalidades pretendidas para o efeito.

O inquérito foi sujeito a parecer de especialistas e alvo de bastantes alterações e melhorias. Tendo em conta o contexto do inquérito e a quantidade de perguntas presentes, pode ter sido um fator para o elevado número de desistências.

Tendo em conta que a disseminação do inquérito foi via e-mail demorou-se algum tempo a obter respostas e foi necessário o reenvio de emails para reforçar este pedido, considera-se que este tenha sido um motivo para que este processo tenha sido mais demorado como seria desejável.

Como trabalho futuro, seria um óptimo complemento o desenvolvimento uma plataforma onde o questionário seria disponibilizado e no final do mesmo seria facultado automaticamente o relatório com o nível de maturidade. Futuramente, também, as questões que compõe o inquérito também poderiam ser ajustadas, de forma a que se tornasse mais genérico. Poderiam também ser definidos mais

matrizes de avaliação, com base em normas diferentes, por forma a perceber quais os controlos das normas que estão implementados nas empresas, e poder assim, detetar mais falhas para prevenir incidentes de segurança.

BIBLIOGRAFIA

[1] F. Cozinheiro, *Atualmente, viver sem a Internet é simplesmente impensável!*, visitado em 06-2022. URL: https://www.fccn.pt/blog/30-anos-internet-portugal-fernando-cozinheiro.

[2] I. N. Okuma, *A importância dos dados no mundo corporativo*, visitado em 04-2022. URL: https://www.linkedin.com/pulse/import%5C%C3%5C%A2ncia-dos-dados-mundo-corporativo-isabelle-nedilha-okuma/?originalSubdomain=pt.

[3] A. R. Costa, *A cibersegurança é um tema premente em qualquer negócio*, visitado em 04-2022. URL: https://www.distribuicaohoje.com/retalho/a-ciberseguranca-e-um-tema-premente-em-qualquer-negocio/.

[4] F. Macias, *COVID-19: Cibersegurança e força de trabalho remota*, visitado em 06-2022. URL: https://www2.deloitte.com/pt/pt/pages/risk/articles/covid19-ciberseguranca-e-forca-de-trabalho-remoto.html.

[5] CNCS, *Roteiro das Capacidades Mínimas para a Cibersegurança*, visitado em 12-2021. URL: https://www.cncs.gov.pt/docs/cncs-roteiro-capacidades-minimas-ciberseguranca.pdf.

[6] F. Macias, *Centro Nacional de Cibersegurança*, visitado em 12-2021. URL: https://www.cncs.gov.pt/.

[7] CNCS, *Conceito de Ciberespaço*, visitado em 06-2022. URL: https://www.cncs.gov.pt/pt/sobre-nos/.

[8] ——, *Conceito de Cibersegurança*, visitado em 06-2022. URL: https://www.cncs.gov.pt/pt/glossario/linhasobservacao.

[9] Microsoft, *Conceito de Cibersegurança*, visitado em 06-2022. URL: https://support.microsoft.com/pt-pt/topic/o-que-C3A9-a-ciberseguranC3A7a-8b6efd59-41ff-4743-87c8-0850a352a390.

[10] APDSI, *Conceito de Cibersegurança*, visitado em 06-2022. URL: https://apdsi.pt/glossario/c/ciberseguranca/.

[11] IBM, *Conceito de Cibersegurança*, visitado em 06-2022. URL: https://www.ibm.com/topics/cybersecurity.

[12] N. I. of Standards e Technology, *NIST*, Website, visitado em 12-2021. URL: https://www.nist.gov/.

[13] G. .-. S. de Segurança da Informação, *Funções NIST*, visitado em 12-2021. URL: https://www.gat.digital/blog/implementacao-do-nist-cybersecurity-framework/.

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

[15] E. Parliament, *Directive on security of Network and Information Systems*, Website, visitado em 12-2021. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.

[16] ENISA, *Áreas de atuação NIS*, visitado em 12-2021. URL: https://www.enisa.europa.eu/topics/nis-directive/nis-visualtool.

[17] RNCSIRT, *Rede Nacional CSIRT*, Website, visitado em 02-2021. URL: https://www.redecsirt.pt/.

[18] CIS, *Center for Internet Security (CIS)*, Website, visitado em 12-2021. URL: https://www.cisecurity.org/controls.

[19] ——, *CIS Controls v8*, visitado em 01-2022. URL: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-privacy-companion-guide-portuguese-translation.

[20] Integrity, *ISO 27001 - Sistema de Gestão de Segurança da Informação*, Website, visitado em 12-2021. URL: https://www.27001.pt/.

[21] ISO, *ISO/IEC 27001 - INFORMATION SECURITY MANAGEMENT*, Website, visitado em 12-2021. URL: https://www.iso.org/isoiec-27001-information-security.html.

[22] S. N. V. (Schweizerische, «Information technology-Security techniques-Information security management systems-Requirements. ISO/IEC International Standards Organization.»,

[23] E. Ramos, E. Cordeiro, G. Martins, N. Silva e E. Duarte, *Orientações para implementação do Sistema de Gestão de Segurança da Informação com base na ISO 27001 e o Ciclo PDCA. In FatecSeg-Congresso de Segurança da Informação*. 2021, October.

[24] ISO, *ISO27701*, Website, visitado em 12-2021. URL: https://www.27701.pt/.

[25] APCER, *APCER - ISO27701*, Website, visitado em 12-2021. URL: https://www.apcergroup.com/pt/certificacao/pesquisa-de-normas/1571/iso-iec-27701?highlight=WyJpc28iLCJpc28ncyIsImllYyIsMjc3MDEsImlzbyBpZWMiLCJpc28gaW

[26] CNCS, *Quadro Nacional de Referência para a Cibersegurança*, visitado em 12-2021. URL: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf.

[27] G. D. P. i. c. 2. Regulation, visitado em 12-2021. URL: https://gdpr-info.%20eu..

[28] CNCS, *Regime Jurídico*, visitado em 12-2021. URL: https://www.cncs.gov.pt/pt/regime-juridico/.

[29] D.-L. n.º 65/2021, *Decreto-Lei n.º 65/2021*, Documento, visitado em 01-2022. URL: https://dre.pt/dre/detalhe/decreto-lei/65-2021-168697988.

[30] APDSI, *Maturidade da Cibersegurança*, Website, visitado em 01-2022, 2019. URL: https://apdsi.pt/wp-content/uploads/2019/10/APDSI_Maturidade-em-Ciberseguran%C3%A7a_23072019.pdf/.

[31] C. S. Rego, *Deteção de Incidentes de Cibersegurança: Capacidades Mínimas*, Website, 2017. URL: https://fenix.tecnico.ulisboa.pt/downloadFile/844820067125424/Thesis.pdf.

[32] A. J. G. D. (Azambuja, «Modelo de maturidade de segurança cibernética para os órgãos da administração pública federal.», 2020, ISSN: 2357-8017. DOI: 10.21874/rsp.v71i3.3210.

[33] C2M2, *Cybersecurity Capability Maturity Model C2M2*, visitado em 03-2022. URL: https://c2m2.doe.gov/C2M220Version202.120June202022.pdf.

[34] M. Yassine, S. Abdelkebir e M. B. (2021)., «A maturity framework for cyber-security governance in organizations.», *EDPACS*, DOI: 10.1080/07366981.2020.1815354.

[35] AP2SI, *Inquérito Aberto à Segurança da Informação nas Instituições em Portugal*, Website, visitado em 12-2021, 2015. URL: https://ap2si.org/iniciativas-ap2si/inquerito/.

[36] C. M. F. L. (de Faria, *Gestão da Cibersegurança em empresas Transnacionais relacionadas com Transações Financeiras Críticas de espectro Macroeconómico.* Website, visitado em 03-2022, 2018. URL: https://hdl.handle.net/10216/118687.

[37] CNCS, *AVALIAÇÃO DE CAPACIDADES DE CIBERSEGURANÇA*, Website, visitado em 12-2021, 2020. URL: https://cibercheckup.cncs.gov.pt/.

[38] W. Martin, M. Sharon, B. Dominic e M. Kenneth, «It Won't Happen to Me: Surveying SME Attitudes to Cyber-security», 2022. DOI: 10.1080/08874417.2022.2067791.

[39] D. (Bhatia, «A Comprehensive Review on the Cybersecurity Methods in Indian Organisation. International Journal of Advances in Soft Computing and Its Applications, 14(1).», ISSN: 2074-8523. DOI: 10.15849/IJASCA.220328.08.

[40] CNCS, *AVALIAÇÃO DE CAPACIDADES DE CIBERSEGURANÇA*, Website, visitado em 12-2021. URL: https://cibercheckup.cncs.gov.pt/.

[41] M. Miners, *Entenda a escala Likert e saiba como aplicá-la em sua pesquisa*, visitado em 02-2022. URL: https://mindminers.com/blog/entenda-o-que-e-escala-likert/.

APÊNDICES

A

APÊNCICE A - MAPEAMENTOS EFETUADOS

Este apêndice corresponde aos restantes mapeamentos efetuados, com o objetivo de perceber a ligação entre diferentes normas e a norma ISO/IEC 27001:2013.

Mapeamento entre a norma ISO/IEC 27001:2013 e Regulamento Geral de Proteção de Dados

Justificação do mapeamento entre o RGPD e os controlos da ISO/IEC 27001:2013

Através do estudo efetuado entre o RGPD e a norma ISO 27001, pode-se constatar que os controlos da norma ISO/IEC 27001:2013 tem como princípio a redução do risco e aumentar a proteção da informação de uma organização, e assim sendo, é notória a semelhança com os objetivos do RGPD, que se foca na privacidade e proteção dos dados pessoais de qualquer individuo da União Europeia e Espaço Económico Europeu. Desta forma, é possível fazer uma correlação direta da grande maioria dos artigos do RGPD com os controlos da norma ISO/IEC 27001:2013.

Capítulo I - Disposições Gerais

Neste primeiro conjunto de artigos do RGPD é explicado que este regulamento pretende defender os direitos e liberdades dos titulares dos dados, ao serem definidas regras relativas à proteção e tratamento de dados pessoais e à livre circulação desses mesmos dados. É definido ainda o âmbito de aplicação material do mesmo, isto é, é definida a abrangência territorial da legislação apresentada. Devido à diferença de objetivos tanto do regulamento como dos controlos da norma ISO/IEC 27001:2013, nem todos os artigos do regulamento são diretamente mapeáveis para a norma, porém é necessário destacar o controlo A.18.1.4 da norma ISO/IEC 27001:2013, onde é dito de forma clara que deve ser assegurada a privacidade e proteção de informação que permita a identificação pessoal do individuo. Este controlo reforça a ideia de que sempre que exista legislação ou regulamentação que exija a privacidade e proteção de informação, esta tem de ser respeitada, e o RGPD é um exemplo de um desses regulamentos a cumprir. Várias organizações definem os seus próprios termos relativamente, tornando assim relevante efetuar a verificação de que estes não entram em conflito com os que estão contemplados no artigo 4 do RGPD.

Artigo	Controlos ISO/IEC 27001:2013
1	A18.1.4
2	Correspondência com vários controlos da norma ISO 27001
3	A18.1.4
4	Controlo 3

Tabela 23: Associação dos artigos do Capítulo I do RGPD com os controlos da norma ISO/IEC 27001:2013

Capítulo II - Princípios

Neste capítulo é explicada a forma como os dados pessoais devem ser tratados pelas organizações. Este tratamento deve ser lícito, leal e completamente transparente, e os dados pessoais devem ser recolhidos apenas para finalidades explícitas e legítimas. É citado que os dados devem ser os mais exatos possíveis e apenas devem ser guardados pelo tempo necessário. Existem exceções especificas como por exemplo, os dados referentes a dados pessoais pertencentes a crianças, o processamento de dados particularmente sensíveis como a religião, sexualidade, informação genética e biométrica. Estes dados são proibidos de serem fornecidos a não ser que exista uma razão válida para o seu processamento ou caso seja dado o consentimento por parte do titular dos dados.

Esta análise serve para identificar e classificar a informação tratada pelo sistema. Com esta análise é possível saber onde são tratados os dados sensíveis.

Artigo	Controlos ISO/IEC 27001:2013
5	Este artigo tem correspondência direta com quase todos os controlos da norma ISO 27001

6	**A.6.1.2 A.14.1.1 A.18.1.1**
7	**A.8.2.3 A.12.1.1 A.13.2.4 A.18.1.3 A.6.1.2 A.14.1.1 A.8.3.2 A.13.2**
8	**A.8.2.3 A.12.1.1 A.13.2.4 A.18.1.3 A.6.1.2 A.14.1.1 A.8.3.2 A.13.2**
9	**A.8.2.1 A.8.2.3 A.14.1.1**
10	**A.7.1 A.8.2.1 A.8.2.3 6.1.2 A.7.1 A.14.1.1**
11	**A.8.2.1 A.8.2.3 6.1.2 A.14.1.1**

Tabela 24: Associação dos artigos do Capítulo II do RGPD com os controlos da norma ISO/IEC 27001:2013

Capítulo III - Direitos do titular dos dados

Neste capítulo são definidos quais os direitos dos titulares dos dados.

É descrito que o responsável pelos dados é obrigado a fornecer qualquer informação ao titular dos dados de forma transparente, clara e compreensível. O titular dos dados deve ser informado do uso dos dados no momento em que são recolhidos e pedidos, e ainda, deve ser elucidado sobre a responsabilidade do seu tratamento, bem como o responsável pelo seu tratamento.

O titular dos dados pode ainda, exigir que estes sejam apagados, ou que não sejam mais utilizados, ou limitar o seu uso.

Artigo	**Controlos ISO/IEC 27001:2013**
12	**A.12.1.1 A.14.1.1 A.16**

13	**A.8.2.1 A.8.2.3 A.12.1.1 A.14.1.1 A.16**
14	**A.8.2.1 A.8.2.3 A.12.1.1 A.14.1 A.16**
15	**A.8.1.1 A.8.2.1 A.12.1.1 A.13.2.1 A.14.1.1**
16	**A.9 A.12.1.1 A.12.3 A.18.1.3**
17	**A.6.1 A.9 A.8.3.2 A.12.3 A.16**
18	**A.6.1.2 A.8.2.1 A.8.2.3 A.12.1.1 A.12.3 A.14.1.1 A.16 A.18.1.1**
19	**A.6.1.2 A.12.1.1 A.14.1.1 A.16**
20	**A.6.1.2 A.8.3 A.10 A.13 A.14.1.1 A.18.1.3**
21	**A.6.1.2 A.12.1.1 A.12.3 A.14.1.1 A.16**
22	**A.6.1.2 A.12.1.1 A.14.1.1 A.16**
23	**A.18.1.1**

Tabela 25: Associação dos artigos do Capítulo III do RGPD com os controlos da norma ISO/IEC 27001:2013

Capítulo IV - Responsável pelo tratamento e subcontratante

Este capítulo define as obrigações dos responsáveis de dados.

Estão definidos os responsáveis pela implementação de controlos de privacidade adequados, tendo em conta os riscos encontrados. Devem ser definidas medidas de forma que apenas sejam tratados os dados pessoais necessários para a finalidade específica de tratamento. Esta medida recomenda que seja definida a quantidade de dados pessoais recolhidos, de acordo com o tipo de tratamento, quanto tempo estarão os dados armazenados e ainda como são acedidos.

Artigo	Controlos ISO/IEC 27001:2013
24	Este artigo tem correspondência direta com quase todos os controlos da norma ISO 27001
25	Este artigo tem correspondência direta com quase todos os controlos da norma ISO 27001
26	A.15 A.18.1.4
27	A.8.1.1 A.8.2.1 A.12.1.1 A.13.2.1 A.14.1.1,
28	A.15 A.18.1.1 A.18.1.3 A.18.1.4
29	Este artigo tem correspondência direta com quase todos os controlos da norma ISO 27001
30	Sem associação
31	A.6.1.3
32	Este artigo tem correspondência direta com quase todos os controlos da norma ISO 27001
33 e 34	A.16 A.18.1.4
35 e 36	A.6.1.3 A.8.2.1
37 38 39 40 41 42 43	A.6.1.1 A.18.1.4

Tabela 26: Associação dos artigos do Capítulo IV do RGPD com os controlos da norma ISO/IEC 27001:2013

Capítulo V - Transferências de dados pessoais para países terceiros ou organizações internacionais

Este capítulo do regulamento aborda a questão da transferência de dados pessoais para outros países.

Estão descritas diversas regras que devem ser tidas em conta na transferência de dados. No caso de a transferência ser feita para outro país em que a Comissão Europeia garantiu um nível adequado de proteção para a transferência de dados, esta transferência não necessita de qualquer Autorização específica, caso contrário, será necessária autorização prévia.

Ao realizar esta transferência de dados, é necessário garantir a sua integridade.

Artigo	**Controlos ISO/IEC 27001:2013**
44 a 49	**A.18.1.4**
50	**Sem associação**

Tabela 27: Associação dos artigos do Capítulo V do RGPD com os controlos da norma ISO/IEC 27001:2013

Capítulo VI a XI - capítulos finais

Os outros capítulos que constituem este regulamento, sugerem que devem ser identificadas as entidades que controlam a aplicabilidade e auditoria deste regulamento.

São descritas as coimas aplicáveis em caso de incumprimento.

Mapeamento entre a norma ISO/IEC 27001:2013 e CIS Controls

Controlo 1 - Inventário e controlo de ativos corporativos

A intenção deste primeiro controlo é desenvolver uma gestão ativa (inventariar, rastrear e corrigir) de todos os ativos corporativos (dispositivos móveis, por exemplo,

portáteis, dispositivos móveis, dispositivos de rede, dispositivos não computacionais, Internet das Coisas e servidores), conectados fisicamente à infraestrutura, virtualmente, remotamente, e aqueles em ambientes em nuvem, com o objetivo de se saber com precisão a totalidade dos ativos que precisam de ser monitorizados e protegidos dentro da organização. Com a implementação desta gestão ativa dos ativos da organização torna-se possível identificar os ativos não autorizados e não monitorizados para os remover.

Controlo	**Controlos ISO/IEC 27001:2013**
1.1	**A.8.1.1**
1.2	**A.11.2.5 A.8.1.1**
1.3	**A.8.1.1**
1.4	**A.8.1.1**
1.5	**A.8.1.1**

Tabela 28: Associação dos cis controls 1 com os controlos da norma ISO/IEC 27001:2013

Controlo 2 - Inventário e controlo de ativos de software

O propósito da implementação deste controlo é efetuar a gestão ativa (inventariar, rastrear e corrigir) de todos os softwares (sejam eles sistemas operativos ou aplicações), na rede da organização, de maneira que apenas software autorizado seja instalado e seja executado. Assim, é expectável que o software não autorizado seja detetado atempadamente e seja impedido de ser instalado/executado.

Controlo	**Controlos ISO/IEC 27001:2013**
2.1	**A.8.1.1**
2.2	**A.12.5.1 A.12.6.2**
2.3	**A.12.5.1 A.12.6.2**
2.4	**Sem associação**
2.5	**Sem associação**
2.6	**Sem associação**
2.7	**Sem associação**

Tabela 29: Associação dos cis controls 2 com os controlos da norma ISO/IEC 27001:2013

Controlo 3 - Proteção de dados

O âmbito deste controlo consiste em desenvolver processos e controlos técnicos para identificar, clarificar, manipular com segurança, guardar e descartar dados.

Controlo	Controlos ISO/IEC 27001:2013
3.1	**Sem associação**
3.2	**A.8.1.1**
3.3	**A.8.2.2 A.9.4.1**
3.4	**Sem associação**
3.5	**Sem associação**
3.6	**A.8.3.1 A.10.1.1**
3.7	**A.8.2.2**
3.8	**Sem associação**
3.9	**A.10.1.1**
3.10	**A.10.1.1 A.13.1.1**
3.11	**A.10.1.1**
3.12	**Sem associação**
3.13	**A.12.3.1**
3.14	**A.12.4.1 A.12.4.3**

Tabela 30: Associação dos cis controls 3 com os controlos da norma ISO/IEC 27001:2013

Controlo 4 - Configuração segura de ativos físicos e software

O fundamento para este controlo consiste em definir e manter uma configuração segura de ativos físicos (por exemplo, portáteis e todo o tipo de dispositivos móveis),

dispositivos de rede, dispositivos de IoT e servidores, e ainda não menos importante, todo o software (seja sistemas operativos ou aplicações).

Controlo	Controlos ISO/IEC 27001:2013
4.1	**A.8.1.3 A.14.2.5**
4.2	**A.13.1.1**
4.3	**A.8.1.3 A.11.2.8**
4.4	**A.13.1.3**
4.5	**A.13.1.3**
4.6	**Sem associação**
4.7	**A.9.2.3**
4.8	**Sem associação**
4.9	**A.13.1.2**
4.10	**A.8.1.3 A.11.2.8**
4.11	**A.6.2.1 A.6.2.2**
4.12	**A.6.2.1 A.6.2.2**

Tabela 31: Associação dos cis controls 4 com os controlos da norma ISO/IEC 27001:2013

Controlo 5 - Gestão de contas

Neste conjunto de sub controlos é sugerido que sejam usados processos e ferramentas para atribuir e gerir as credenciais para todos os tipos de contas de utilizador.

Controlo	Controlos ISO/IEC 27001:2013
5.1	**A.8.1.1 A.9.2.1**
5.2	**A.9.2.4**
5.3	**Sem associação**
5.4	**A.9.4.1**
5.5	**A.8.1.1 A.9.2.1**
5.6	**Sem associação**

Tabela 32: Associação dos cis controls 5 com os controlos da norma ISO/IEC 27001:2013

Controlo 6 - Gestão de controlo de acesso

Nestes sub controlos aqui presentes, o seu principal objetivo é recomendar que sejam utilizados processos e ferramentas para criar, atribuir, gerir e revogar credenciais de acesso e privilégios para as contas de utilizador da organização.

Controlo	Controlos ISO/IEC 27001:2013
6.1	**A.9.2.3**
6.2	**A.9.2.6**
6.3	**A.9.4.2**
6.4	**A.9.4.2**
6.5	**A.9.4.2**
6.6	**A.8.1.1 A.9.2.1**
6.7	**Sem associação**
6.8	**A.9.2.2 A.9.4.1**

Tabela 33: Associação dos cis controls 6 com os controlos da norma ISO/IEC 27001:2013

Controlo 7 - Gestão contínua de vulnerabilidades

Neste grupo de sub controlos, o propósito é desenvolver um plano para avaliar e detetar as vulnerabilidades existentes nos ativos da organização, de maneira a antecipar as ações por parte dos atacantes. Devem ser controladas as fontes públicas e privadas para obter novas informações sobre ameaças e vulnerabilidades.

Controlo	Controlos ISO/IEC 27001:2013
7.1	**A.12.6.1**
7.2	**Sem associação**
7.3	**Sem associação**

7.4	**Sem associação**
7.5	**Sem associação**
7.6	**Sem associação**
7.7	**Sem associação**

Tabela 34: Associação dos cis controls 7 com os controlos da norma ISO/IEC 27001:2013

Controlo 8 - Gestão de registos de auditoria

Relativamente a este oitavo controlo, este recomenda que se devem recolher e efetuar a devida análise dos logs de auditoria de eventos que possam ajudar a detetar, compreender ou recuperar após um ataque.

Controlo	**Controlos ISO/IEC 27001:2013**
8.1	**Sem associação**
8.2	**A.12.4.1**
8.3	**Sem associação**
8.4	**A.12.4.4**
8.5	**Sem associação**
8.6	**Sem associação**
8.7	**Sem associação**
8.8	**Sem associação**
8.9	**Sem associação**
8.10	**Sem associação**
8.11	**A.12.4.3**
8.12	**Sem associação**

Tabela 35: Associação dos cis controls 8 com os controlos da norma ISO/IEC 27001:2013

Controlo 9 - Proteções de e-mail e Browser

Este controlo foca-se essencialmente nas proteções e deteção de ameaças no e-mail ou no browser.

Controlo	Controlos ISO/IEC 27001:2013
9.1	**A.8.1.3**
9.2	**A.13.1.1**
9.3	**A.13.1.**
9.4	**A.12.6.2**
9.5	**A.12.2.1**
9.6	**A.13.1.1**
9.7	**A.12.2.1**

Tabela 36: Associação dos cis controls 9 com os controlos da norma ISO/IEC 27001:2013

Controlo 10 - Defesas contra malware

Neste leque de controlos, a sua principal incidência é impedir e controlar a instalação, propagação e execução de aplicações, códigos ou scripts maliciosos presentes nos ativos da organização.

Controlo	Controlos ISO/IEC 27001:2013
10.1	**A.12.2.1**
10.2	**A.12.2.1**
10.3	**A.12.2.1**
10.4	**A.12.2.1**
10.5	**Sem associação**
10.6	**A.12.2.1**
10.7	**Sem associação**

Tabela 37: Associação dos cis controls 10 com os controlos da norma ISO/IEC 27001:2013

Controlo 11 - Recuperação de Dados

É essencial em qualquer organização que se estabeleça práticas de recuperação de dados suficientes para repor os ativos num estado pré-incidente e estável.

Controlo	**Controlos ISO/IEC 27001:2013**
11.1	**A.12.3.1**
11.2	**Sem associação**
11.3	**A.12.3.1**
11.4	**Sem associação**
11.5	**Sem associação**

Tabela 38: Associação dos cis controls 11 com os controlos da norma ISO/IEC 27001:2013

Controlo 12 - Gestão da infraestrutura de rede

Este controlo recomenda que todos os dispositivos de rede sejam geridos regularmente para evitar que sejam exploradas vulnerabilidades existentes nos serviços de rede e nos pontos de acesso.

Controlo	**Controlos ISO/IEC 27001:2013**
12.1	**A.13.1.1**
12.2	**A.13.1.2**
12.3	**A.13.1.1 A.13.1.2 A.13.1.3**
12.4	**Sem associação**
12.5	**Sem associação**
12.6	**Sem associação**
12.7	**Sem associação**
12.8	**Sem associação**

Tabela 39: Associação dos cis controls 12 com os controlos da norma ISO/IEC 27001:2013

Controlo 13 - Monitorização e defesa da rede

Este controlo propõe que sejam utilizados processos e ferramentas para efetuar a monitorização e defesa da rede. Assim previne-se as ameaças de segurança em toda a infraestrutura da rede.

Controlo	**Controlos ISO/IEC 27001:2013**
13.1	**Sem associação**
13.2	**Sem associação**
13.3	**A.13.1.1**
13.4	**Sem associação**
13.5	**Sem associação**
13.6	**Sem associação**
13.7	**Sem associação**
13.8	**Sem associação**
13.9	**Sem associação**
13.10	**Sem associação**
13.11	**Sem associação**

Tabela 40: Associação dos cis controls 13 com os controlos da norma ISO/IEC 27001:2013

Controlo 14 - Consciencialização sobre segurança e treino de competências

Neste grupo de subcontrolos é recomendado estabelecer um programa de consciencialização sobre esta temática da segurança para que esteja sempre presente no comportamento dos colaboradores da organização, com a finalidade de reduzir riscos básicos de segurança.

Controlo	Controlos ISO/IEC 27001:2013
14.1	**Sem associação**
14.2	**A.7.2.2**
14.3	**A.7.2.2**
14.4	**A.7.2.2**
14.5	**A.7.2.2**
14.6	**A.7.2.2**
14.7	**Sem associação**
14.8	**Sem associação**
14.9	**Sem associação**

Tabela 41: Associação dos cis controls 14 com os controlos da norma ISO/IEC 27001:2013

Controlo 15 - Gestão de fornecedores de serviços

Deve ser desenvolvido um processo para avaliar os fornecedores de serviços que mantém os dados sensíveis ou são responsáveis por plataformas e processos de TI críticos de uma empresa. Este processo garante que os fornecedores estão a proteger as plataformas e os dados da forma adequada.

Controlo	Controlos ISO/IEC 27001:2013
15.1	**Sem associação**
15.2	**Sem associação**
15.3	**Sem associação**
15.4	**Sem associação**
15.5	**Sem associação**
15.6	**Sem associação**
15.7	**Sem associação**

Tabela 42: Associação dos cis controls 15 com os controlos da norma ISO/IEC 27001:2013

Controlo 16 - Segurança das aplicações

Neste grupo de sub controlos o intuito é fazer uma gestão do ciclo de vida da segurança do software desenvolvido para prevenir, detetar e corrigir os pontos fracos de segurança que possam existir.

Controlo	Controlos ISO/IEC 27001:2013
16.1	**A.14.2.1**
16.2	**Sem associação**
16.3	**Sem associação**
16.4	**Sem associação**
16.5	**Sem associação**
16.6	**Sem associação**
16.7	**Sem associação**
16.8	**A.12.1.4**
16.9	**Sem associação**
16.10	**Sem associação**
16.11	**Sem associação**
16.12	**Sem associação**
16.13	**Sem associação**
16.14	**Sem associação**

Tabela 43: Associação dos cis controls 16 com os controlos da norma ISO/IEC 27001:2013

Controlo 17 - Gestão de Resposta a incidentes

A organização deve ter capacidade de resposta a incidentes de maneira a preparar, detetar e responder rapidamente a um ataque.

Controlo	Controlos ISO/IEC 27001:2013

17.1	**A.16.1.3**
17.2	**A.6.1.3**
17.3	**Sem associação**
17.4	**A.16.1.1**
17.5	**Sem associação**
17.6	**Sem associação**
17.7	**Sem associação**
17.8	**Sem associação**
17.9	**Sem associação**

Tabela 44: Associação dos cis controls 17 com os controlos da norma ISO/IEC 27001:2013

Controlo 18 - Testes de Penetração

Este conjunto de controlos tem como objetivo testar a força geral da defesa de uma organização (a tecnologia, os processos, e as pessoas) simulando os objetivos e ações de um atacante.

Controlo	**Controlos ISO/IEC 27001:2013**
18.1	**Sem associação**
18.2	**Sem associação**
18.3	**Sem associação**
18.4	**Sem associação**
18.5	**Sem associação**

Tabela 45: Associação dos cis controls 18 com os controlos da norma ISO/IEC 27001:2013

Mapeamento entre a norma ISO/IEC 27001:2013 e Quadro Nacional de Referência para a Cibersegurança

Medida de Segurança: Identificar

Esta medida de segurança tem como objetivo que a organização estabeleça um consenso a toda a organização sobre a gestão de risco de cibersegurança.

Categoria ID.GA - Gestão de Ativos

Nesta categoria é recomendado que a organização deve identificar os dados, colaboradores, equipamentos, sistemas e instalações são fundamentais para o desenvolvimento do seu processo de negócio.

Categoria	**Controlos ISO/IEC 27001:2013**
ID.GA-1	**A.8.1.1 A.8.1.2**
ID.GA-2	**A.8.1.1 A.8.1.2 A.12.5.1**
ID.GA-3	**A.13.2.1 A.13.2.2**
ID.GA-4	**A.11.2.6**
ID.GA-5	**A.8.2.1**

Tabela 46: Associação da categoria ID.GA com os controlos da norma ISO/IEC 27001:2013

Categoria ID.AO - Ambiente da Organização

A presente categoria sugere que a organização deve priorizar a sua missão e objetivos.

Categoria	**Controlos ISO/IEC 27001:2013**

ID.AO-1	**A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.1 A.15.2.2**
ID.AO-2	**Cláusula 4.1**
ID.AO-3	**Sem associação**
ID.AO-4	**A.11.2.2 A.11.2.3 A.12.1.3**
ID.AO-5	**A.11.1.4 A.17.1.1 A.17.1.2 A.17.2.1**

Tabela 47: Associação da categoria ID.AO com os controlos da norma ISO/IEC 27001:2013

Categoria ID.GV - Governação

A organização deve conhecer as políticas e processos para gerir e monitorizar as responsabilidades, que contribuem para a consolidação de conhecimento dos órgãos de gestão, sobre este tema.

Categoria	**Controlos ISO/IEC 27001:2013**
ID.GV-1	**A.5.1.1**
ID.GV-2	**A.18.1.1 A.18.1.2 A.18.1.3 A.18.1.4 A.18.1.5**

Tabela 48: Associação da categoria ID.GV com os controlos da norma ISO/IEC 27001:2013

Categoria ID.AR - Avaliação do Risco

A organização deve estar ciente e ser conhecedora dos riscos a que está exposta de acordo com o seu processo de negócio.

Categoria	Controlos ISO/IEC 27001:2013
ID.AR-1	A.12.6.1 A.18.2.3
ID.AR-2	A.6.1.4
ID.AR-3	Cláusula 6.1.2
ID.AR-4	A.12.6.1
ID.AR-5	Cláusula 6.1.3

Tabela 49: Associação da categoria ID.AR com os controlos da norma ISO/IEC 27001:2013

Categoria ID.GR - Estratégia de Gestão do Risco

Devem ser estabelecidas as prioridades e restrições de tolerância ao risco que são utilizados para suportar a tomada de decisão no âmbito da gestão do risco operacional.

Categoria	Controlos ISO/IEC 27001:2013
ID.GR-1	Cláusula 6.1.3 Cláusula 8.3 Cláusula 9.3
ID.GR-2	Cláusula 6.1.3 Cláusula 8.3
ID.GR-3	Cláusula 6.1.3 Cláusula 8.3

Tabela 50: Associação da categoria ID.GR com os controlos da norma ISO/IEC 27001:2013

Categoria ID.GL - Gestão do Risco da Cadeia Logística

A organização deve implementar os processos necessários para identificar e avaliar os riscos referentes à cadeira logística.

Categoria	Controlos ISO/IEC 27001:2013
ID.GL-1	A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.1 A.15.2.2
ID.GL-2	A.15.2.1 A.15.2.2
ID.GL-3	A.15.1.1 A.15.1.2 A.15.1.3
ID.GL-4	A.15.2.1 A.15.2.2
ID.GL-5	A.17.1.3

Tabela 51: Associação da categoria ID.GL com os controlos da norma ISO/IEC 27001:2013

Medida de Segurança: Proteger

O objetivo desta medida de segurança é implementar o desenvolvimento das salvaguardas necessárias para garantir a continuidade do processo de negócio da organização.

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

Nesta categoria é sugerido que o acesso aos ativos devem ser restritos apenas a quem tenha autorização para aceder a estes.

Categoria	Controlos ISO/IEC 27001:2013
PR.GA-1	A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.6 A.9.3.1 A.9.4.2 A.9.4.3

PR.GA-2	**A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.5 A.11.1.6 A.11.2.1 A.11.2.3 A.11.2.5 A.11.2.6 A.11.2.7 A.11.2.8**
PR.GA-3	**A.6.2.1 A.6.2.2 A.11.2.6 A.13.1.1 A.13.2.1**
PR.GA-4	**A.6.1.2 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5**
PR.GA-5	**A.13.1.1 A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3**
PR.GA-6	**A.7.1.1 A.9.2.1**
PR.GA-7	**A.9.2.1 A.9.2.4 A.9.3.1 A.9.4.2 A.9.4.3 A.18.1.4**

Tabela 52: Associação da categoria PR.GA com os controlos da norma ISO/IEC 27001:2013

Categoria PR.FC - Formação e Sensibilização

A organização deve disponibilizar e organizar sessões de sensibilização sobre cibersegurança a todos os seus colaboradores.

Categoria	**Controlos ISO/IEC 27001:2013**
PR.FC-1	**A.7.2.2 A.12.2.1**
PR.FC-2	**A.6.1.1 A.7.2.2**
PR.FC-3	**A.6.1.1 A.7.2.1 A.7.2.2**
PR.FC-4	**A.6.1.1 A.7.2.2**

Tabela 53: Associação da categoria PR.FC com os controlos da norma ISO/IEC 27001:2013

Categoria PR.SD - Segurança de Dados

Os dados devem estar protegidos de forma a garantir a sua integridade, confidencialidade e disponibilidade.

Categoria	Controlos ISO/IEC 27001:2013
PR.SD-1	**A.8.2.3**
PR.SD-2	**A.8.2.3 A.13.1.1 A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3**
PR.SD-3	**A.8.2.3 A.8.3.1 A.8.3.2 A.8.3.3 A.11.2.5 A.11.2.7**
PR.SD-4	**A.12.1.3 A.17.2.1**
PR.SD-5	**A.6.1.2 A.7.1.1 A.7.1.2 A.7.3.1 A.8.2.2 A.8.2.3 A.9.1.1 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5 A.10.1.1 A.11.1.4 A.11.1.5 A.11.2.1 A.13.1.1 A.13.1.3 A.13.2.1 A.13.2.3 A.13.2.4 A.14.1.2 A.14.1.3**
PR.SD-6	**A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3 A.14.2.4**
PR.SD-7	**A.12.1.4**

PR.SD-8	**A.11.2.4**

Tabela 54: Associação da categoria PR.SD com os controlos da norma ISO/IEC 27001:2013

Categoria PR.PI - Procedimentos e Processos de Proteção da Informação

As políticas de segurança devem ser utilizadas para garantir a proteção de redes e sistemas de informação.

Categoria	**Controlos ISO/IEC 27001:2013**
PR.PI-1	**A.12.1.2 A.12.5.1 A.12.6.2 A.14.2.2 A.14.2.3 A.14.2.4**
PR.PI-2	**A.6.1.5 A.14.1.1 A.14.2.1 A.14.2.5**
PR.PI-3	**A.12.1.2 A.12.5.1 A.12.6.2 A.14.2.2 A.14.2.3 A.14.2.4**
PR.PI-4	**A.12.3.1 A.17.1.2 A.17.1.3 A.18.1.3**
PR.PI-5	**A.11.1.4 A.11.2.1 A.11.2.2 A.11.2.3**
PR.PI-6	**A.8.2.3 A.8.3.1 A.8.3.2 A.11.2.7**
PR.PI-7	**A.16.1.6 Cláusula9 Cláusula 10**
PR.PI-8	**A.16.1.6**
PR.PI-9	**A.16.1.1 A.17.1.1 A.17.1.2 A.17.1.3**
PR.PI-10	**A.17.1.3**

PR.PI-11	**A.7.1.1 A.7.1.2 A.7.2.1 A.7.2.2 A.7.2.3 A.7.3.1 A.8.1.4**
PR.PI-12	**A.12.6.1 A.14.2.3 A.16.1.3 A.18.2.2 A.18.2.3**

Tabela 55: Associação da categoria PR.PI com os controlos da norma ISO/IEC 27001:2013

Categoria PR.MA - Manutenção

As redes e sistemas de informação da organização devem ser vigiados regularmente.

Categoria	Controlos ISO/IEC 27001:2013
PR.MA-1	**A.11.1.2 A.11.2.4 A.11.2.5 A.11.2.6**
PR.MA-2	**A.11.2.4 A.15.1.1 A.15.2.1**

Tabela 56: Associação da categoria PR.MA com os controlos da norma ISO/IEC 27001:2013

Categoria PR.TP - Tecnologia de Proteção

As soluções de segurança devem ser implementadas de forma a que se garanta a confidencialidade, disponibilidade e integridade dos dados.

Categoria	Controlos ISO/IEC 27001:2013

PR.TP-1	**A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.7.1**
PR.TP-2	**A.8.2.1 A.8.2.2 A.8.2.3 A.8.3.1 A.8.3.3 A.11.2.9**
PR.TP-3	**A.9.1.2**
PR.TP-4	**A.13.1.1 A.13.2.1 A.14.1.3**
PR.TP-5	**A.17.1.2 A.17.2.1**

Tabela 57: Associação da categoria PR.TP com os controlos da norma ISO/IEC 27001:2013

Medida de Segurança: Detetar

O objetivo desta medida de segurança é implementar medidas capazes de detetar a ocorrência de eventos de cibersegurança, através da monitorização contínua das redes e sistemas de informação.

Categoria DE.AE - Anomalias e eventos

Nesta categoria é expectável que sejam detetadas atividades anómalas atempadamente, e deve ser definido qual o seu impacto para a organização.

Categoria	**Controlos ISO/IEC 27001:2013**
DE.AE-1	**A.12.1.1 A.12.1.2 A.13.1.1 A.13.1.2**
DE.AE-2	**A.12.4.1 A.16.1.1 A.16.1.4**
DE.AE-3	**A.12.4.1 A.16.1.7**
DE.AE-4	**A.16.1.4**
DE.AE-5	**A.16.1.4**

Tabela 58: Associação da categoria DE.AE com os controlos da norma ISO/IEC 27001:2013

Categoria DE.MC - Monitorização Contínua de Segurança

Nesta categoria é sugerido que as redes e sistemas de informação devem ser monitorizados, de forma a serem identificados eventos de cibersegurança.

Categoria	**Controlos ISO/IEC 27001:2013**
DE.MC-1	**Sem associação**
DE.MC-2	**A.11.1.1 A.11.1.2**
DE.MC-3	**A.12.4.1 A.12.4.3**
DE.MC-4	**A.12.2.1**
DE.MC-5	**A.12.5.1 A.12.6.2**
DE.MC-6	**A.14.2.7 A.15.2.1**
DE.MC-7	**A.12.4.1 A.14.2.7 A.15.2.1**
DE.MC-8	**A.12.6.1**

Tabela 59: Associação da categoria DE.MC com os controlos da norma ISO/IEC 27001:2013

Categoria DE.PD - Processos de Deteção

Todos os processos de deteção existentes devem ser testados para garantir o seu bom funcionamento.

Categoria	**Controlos ISO/IEC 27001:2013**
DE.PD-1	**A.6.1.1 A.7.2.2**

DE.PD-2	**A.18.1.4 A.18.2.2 A.18.2.3**
DE.PD-3	**A.14.2.8**
DE.PD-4	**A.16.1.2 A.16.1.3**
DE.PD-5	**A.16.1.6**

Tabela 60: Associação da categoria DE.PD com os controlos da norma ISO/IEC 27001:2013

Medida de Segurança: Responder

O objetivo desta medida de segurança é implementar medidas capazes de responder a um incidente de cibersegurança que tenha sido detetado na organização.

Categoria RS.PR - Planeamento de resposta

Todos os processos de resposta a incidentes de cibersegurança devem ser executados de forma contínua para garantir resposta aos incidentes.

Categoria	**Controlos ISO/IEC 27001:2013**
RS.PR-1	**A.16.1.5**

Tabela 61: Associação da categoria RS.PR com os controlos da norma ISO/IEC 27001:2013

Categoria RS.CO - Comunicações

Os eventos de cibersegurança devem ser comunicados às entidades competentes.

Categoria	**Controlos ISO/IEC 27001:2013**

RS.CO-1	**A.6.1.1 A.7.2.2 A.16.1.1**
RS.CO-2	**A.6.1.3 A.16.1.2**
RS.CO-3	**A.16.1.2 Cláusula 7.4 Cláusula 16.1.2**
RS.CO-4	**Cláusula 7.4**
RS.CO-5	**A.6.1.4**

Tabela 62: Associação da categoria RS.CO com os controlos da norma ISO/IEC 27001:2013

Categoria RS.AN - Análise

A análise de incidentes deve levar a uma resposta efetiva para apoiar as atividades de recuperação.

Categoria	**Controlos ISO/IEC 27001:2013**
RS.AN-1	**A.12.4.1 A.12.4.3 A.16.1.5**
RS.AN-2	**A.16.1.4 A.16.1.6**
RS.AN-3	**A.16.1.7**
RS.AN-4	**A.16.1.4**
RS.AN-5	**Sem associação**

Tabela 63: Associação da categoria RS.AN com os controlos da norma ISO/IEC 27001:2013

Categoria RS.MI - Mitigação

Devem ser efetuadas tarefas para conter, mitigar ou resolver um incidente.

Categoria	Controlos ISO/IEC 27001:2013
RS.MI-1	**A.12.2.1 A.16.1.5**
RS.MI-2	**A.12.2.1 A.16.1.5**
RS.MI-3	**A.12.6.1**

Tabela 64: Associação da categoria RS.MI com os controlos da norma ISO/IEC 27001:2013

Categoria RS.ME - Melhorias

Devem ser efetuadas tarefas para conter, mitigar ou resolver um incidente.

Categoria	Controlos ISO/IEC 27001:2013
RS.ME-1	**A.16.1.6 Cláusula 10**
RS.ME-2	**A.16.1.6 Cláusula 10**

Tabela 65: Associação da categoria RS.ME com os controlos da norma ISO/IEC 27001:2013

Medida de Segurança: Recuperar

O objetivo desta medida de segurança é implementar medidas capazes de manter planos de resiliência e aumentar a robustez da organização na sequência de um evento de cibersegurança.

Categoria RC.PR - Plano de recuperação

Todos os processos de recuperação de incidentes de segurança devem estar ativos para garantir a recuperação dos sistemas que tenham sido afetados pelos incidentes.

Categoria	Controlos ISO/IEC 27001:2013
RC.PR-1	A.16.1.5

Tabela 66: Associação da categoria RC.PR com os controlos da norma ISO/IEC 27001:2013

Categoria RC.ME - Melhorias

Todos os planos de recuperação devem ser alvos de melhorias contínuas através de lições aprendidas, e de incidentes passados.

Categoria	Controlos ISO/IEC 27001:2013
RC.ME-1	A.16.1.6 Cláusula 10
RC.ME-2	A.16.1.6 Cláusula 10

Tabela 67: Associação da categoria RC.ME com os controlos da norma ISO/IEC 27001:2013

Categoria RC.CO - Comunicações

Os processos de recuperação devem ser coordenados com as entidades afetadas pelo incidente.

Categoria	Controlos ISO/IEC 27001:2013
RC.CO-1	A.6.1.4 Cláusula 7.4
RC.CO-2	Cláusula 7.4

Tabela 68: Associação da categoria RC.CO com os controlos da norma ISO/IEC 27001:2013

B

APÊNDICE B - INQUÉRITO

Este apêndice corresponde à estrutura do inquérito desenvolvido com base no mapeamento entre o Roteiro das Capacidades Mínimas para a Cibersegurança e a norma ISO/IEC 27001:2013.

POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Avaliação da Maturidade em Cibersegurança do tecido industrial de Portugal

Este inquérito enquadra-se num estudo no âmbito de uma Dissertação do Mestrado de Cibersegurança e Informática Forense, realizada no Politécnico de Leiria, com o intuito de avaliar a maturidade em Cibersegurança das empresas em Portugal.
O presente estudo está a ser coordenado pelos professores **Carlos Rabadão** (carlos.rabadao@ipleiria.pt) e **Leonel Santos** (leonel.santos@ipleiria.pt).

Se a qualquer altura existir alguma dúvida em alguma questão do inquérito poderá contactar a estudante **Ana Beatriz Ribeiro** através do email: 2202642@my.ipleiria.pt

No final deste inquérito, o e-mail facultado, de forma opcional, servirá apenas para envio posterior do relatório com a análise da maturidade obtida através das respostas dadas.

Agradecemos, desde já, a sua colaboração.

Informações Gerais sobre a organização

* Qual é o setor de atividade da organização?

- ◯ Agricultura, produção animal, silvicultura e pesca
- ◯ Construção
- ◯ Cerâmica
- ◯ Moldes
- ◯ Vidro
- ◯ Plástico
- ◯ Recursos Naturais
- ◯ Outro

* Qual é o número de colaboradores da organização?

- ◯ Entre 1 a 5
- ◯ Entre 6 a 10
- ◯ Entre 11 a 19
- ◯ Entre 20 a 49
- ◯ Entre 50 a 99
- ◯ Entre 100 a 249
- ◯ Superior a 250

* Que tipo de tecnologias são utilizadas pela organização?

- ☐ Cloud Pública
- ☐ Cloud Privada
- ☐ CRM (Customer Relationship Management)

- [ ] Email Corporativo
- [ ] Dispositivos Móveis
- [ ] ERP (Enterprise Resource Planning)
- [ ] VPN (Virtual Private Network)
- [ ] Rede com fios
- [ ] Rede sem fios (wi-fi)
- [ ] Outra

* Em que região está sediada a organização?

- ◯ Norte
- ◯ Centro
- ◯ Área Metropolitana de Lisboa
- ◯ Alentejo
- ◯ Algarve
- ◯ Madeira
- ◯ Açores

Informações Gerais sobre Cibersegurança da Organização

* Qual o grau de importância da segurança a informação para a organização?

- ◯ Nada importante
- ◯ Pouco importante
- ◯ Indiferente

- ◯ Importante
- ◯ Muito importante

* A organização tem preocupação com os danos reputacionais em caso de incidente de segurança?

- ◯ Sim
- ◯ Não

* Qual é o tipo de informação processada pela organização?

- ☐ Dados bancários de colaboradores
- ☐ Dados bancários de fornecedores
- ☐ Dados empresariais de clientes
- ☐ Dados empresariais de fornecedores
- ☐ Dados Pessoais de colaboradores
- ☐ Dados Pessoais clientes
- ☐ Não sabe

Informações Gerais sobre Cibersegurança da Organização

* A sua empresa tem algum seguro contratado para cobrir incidentes de segurança?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

* A sua empresa tem colaboradores certificados na área de Cibersegurança?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

Informações Gerais sobre Cibersegurança da Organização

* Qual(is) das seguintes certificações possi(uem) os colaboradores ou a organização?

- ☐ ISO 27001
- ☐ Security+
- ☐ CCNA CyberOps
- ☐ CISSP
- ☐ Lead Auditor
- ☐ CEH
- ☐ GSEC
- ☐ SSCP
- ☐ GASP
- ☐ GCIH
- ☐ OSCP
- ☐ Outra
- ☐ Nenhuma das anteriores

* Qual o orçamento anual para investir em Cibersegurança:

- ◯ Não tem
- ◯ Menos de 3000€
- ◯ Entre 3000€ e 8000€
- ◯ Entre 8001€ e 15000€
- ◯ Mais de 20000€
- ◯ Não sabe

Fase 1 - Preparação Inicial

Esta fase avalia a colaboração entre o Centro Nacional de Cibersegurança e a organização. Tem como objetivo averiguar se existem canais de comunicação com esta entidade.

* Está definida uma forma de comunicação com o CNCS?

- ◯ Sim
- ◯ Não

Fase 1 - Preparação Inicial

Esta fase avalia a colaboração entre o Centro Nacional de Cibersegurança e a organização. Tem como objetivo averiguar se existem canais de comunicação com esta entidade.

* Quais são os canais de comunicação que estão definidos com o CNCS? (?)

- ☐ Chamada Telefónica

- [ ] Correio Eletrónico
- [ ] PGP
- [ ] Serviços de Instant Messaging (ex: Teams, Slack, Skype)
- [ ] Não sabe
- [ ] Outro

* Existe um inventário de ativos e serviços críticos da organização? (?)

- ( ) Sim
- ( ) Não
- ( ) Não sabe

Fase 1 - Preparação Inicial

Esta fase avalia a colaboração entre o Centro Nacional de Cibersegurança e a organização. Tem como objetivo averiguar se existem canais de comunicação com esta entidade.

* De que forma é feita a inventariação dos ativos? (?)

- ( ) CMDB (ex: GLPI, Solarwinds, etc)
- ( ) Manualmente (Excel, CSV, TXT, etc)
- ( ) Não sabe
- ( ) Outra

Fase 1 - Preparação Inicial

Esta fase avalia a colaboração entre o Centro Nacional de Cibersegurança e a

organização. Tem como objetivo averiguar se existem canais de comunicação com esta entidade.

* Os ativos da organização são encriptados?

- [ ] Sim
- [ ] Não

* São efetuados testes de penetração aos ativos da organização?

- [ ] Sim
- [ ] Não

Fase 2 - Arquitetura

Esta fase averigua se a organização dispõe das capacidades necessárias para defender os ativos da sua organização. Nesta fase é verificado se a organização segue os requisitos legais e normativos pertencentes ao seu processo de negócio.

* Quais das seguinte soluções de segurança estão disponíveis na organização para lidar com possíveis ameaças?

- [ ] Mecanismos de Deteção (IDS/IPS)
- [ ] Mecanismos de Prevenção (Data Loss Protection (DLP), Firewall)
- [ ] Mecanismos de Recuperação (Backups)
- [ ] Mecanismos de Deteção de Código Malicioso (Antívirus)
- [ ] Não sabe
- [ ] Outro

Fase 2 - Arquitetura

Esta fase averigua se a organização dispõe das capacidades necessárias para defender os ativos da sua organização. Nesta fase é verificado se a organização segue os requisitos legais e normativos pertencentes ao seu processo de negócio.

* As soluções de segurança indicadas na questão anterior são utilizadas nos sistemas e postos de trabalho onde é tratada informação crítica?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

* Na organização é utilizada alguma tecnologia com a capacidade de analisar tráfego malicioso?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

* Quais dos seguintes procedimentos de backup/restore estão implementados na organização? (?)

- ☐ Backups Off-site
- ☐ Definida a periodicidade e abrangência dos Backups
- ☐ Testes periódicos para garantir a integridade dos backups efetuados e da qualidade dos mecanismos de reposição
- ☐ Não sabe
- ☐ Outro

* A organização é conhecedora dos quadros legais e regulatórios a que está sujeita (nacionais e europeus)?

- Sim
- Não
- Não sabe

Fase 2 - Arquitetura

Esta fase averigua se a organização dispõe das capacidades necessárias para defender os ativos da sua organização. Nesta fase é verificado se a organização segue os requisitos legais e normativos pertencentes ao seu processo de negócio.

* Existem relatórios de auditorias que comprovem a conformidade com a legislação e regulamentação?

- Sim
- Não
- Não sabe

* É efetuado o registo de eventos como logs e atividades de utilizadores?

- Sim
- Não
- Não sabe

* Qual o número de horas de ações de formação e sensibilização de colaboradores em matéria de Cibersegurança na organização?

Cibersegurança na organização?

- ◯ Sem ações de formação
- ◯ Entre 1 a 5 horas
- ◯ Entre 6 a 10 horas
- ◯ Mais de 10 horas

* A quem se destinam estas ações de formação disponibilizadas na organização?

- ☐ Administração
- ☐ Gestores
- ☐ Todos os colaboradores (Transversais)
- ☐ Departamentos específicos
- ☐ Não sabe
- ☐ Outro

* Na organização são utilizados alguns dos seguintes lembretes relativamente a boas praticas de Cibersegurança?

- ☐ Ecrã de bloqueio com boas práticas de Cibersegurança
- ☐ Email
- ☐ Quiz
- ☐ Conteúdo Multimédia
- ☐ Não sabe
- ☐ Outro
- ☐ Nenhuma das Anteriores

Fase 3 - Segurança dos Dispositivos

Esta fase tem como finalidade determinar se estão implementadas os desenhos da arquitetura para as capacidades definidas na fase anterior. Nesta etapa averigua se são feitas auditorias de segurança e mecanismos de supervisão e gestão de eventos (SIEM).

* Com que regularidade são auditadas as configurações dos dispositivos?

- ◯ Nunca
- ◯ Raramente
- ◯ Ocasionalmente
- ◯ Frequente
- ◯ Muito Frequente

* A organização tem uma política BYOD (Gestão de Dispositivos Móveis Pessoais)?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

* De que forma é feita a gestão de eventos de segurança?

- ◯ Através de um SIEM (Security Information and Event Management)
- ◯ Não sabe
- ◯ Outra
- ◯ Nenhuma das anteriores

* Existe algum sistema de monitorização dos principais ativos de rede e sistemas que dão suporte

às atividades da organização?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

* Os colaboradores têm conhecimento de como utilizar informação crítica?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

Fase 4 - Consolidar a Cibersegurança

Esta fase apura se está definida a gestão de processos de mudança. É ainda aferido se é efetuada a formação de recursos humanos sobre este tema.

* Com que regularidade são feitas as atualizações de software?

- ◯ Nunca
- ◯ Raramente
- ◯ Ocasionalmente
- ◯ Frequente
- ◯ Muito frequente

* Quais os procedimentos de segurança que estão definidos na política de dispositivos móveis?

- ☐ Limpeza Remota

- [ ] Os colaboradores assinam um acordo reconhecendo as suas obrigações, renunciando à propriedade de dados de negócio
- [ ] Obrigatoriedade de PIN
- [ ] Criptografia de dados empresariais
- [ ] Deteção de Rootkit/Jailreak
- [ ] Não sabe
- [ ] Outro
- [ ] Nenhuma das anteriores

* Antes da entrada em produção, os sistemas e aplicações são submetidos a testes de cibersegurança?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

Fase 4 - Consolidar a Cibersegurança

Esta fase apura se está definida a gestão de processos de mudança. É ainda aferido se é efetuada a formação de recursos humanos sobre este tema.

* Por quem são efetuados os testes de cibersegurança indicados na questão anterior?

- ◯ Especialista em Cibersegurança Interno
- ◯ Especialista em Cibersegurança Externo
- ◯ Responsável de Segurança Interno
- ◯ Responsável de Segurança Externo

- ◯ Departamento de Informática Interno
- ◯ Não sabe
- ◯ Outro

* Já foi efetuado algum simulacro de Cibersegurança na organização?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

Fase 4 - Consolidar a Cibersegurança

Esta fase apura se está definida a gestão de processos de mudança. É ainda aferido se é efetuada a formação de recursos humanos sobre este tema.

* Com que frequência são efetuados estes simulacros?

- ◯ Nunca
- ◯ Raramente
- ◯ Ocasionalmente
- ◯ Frequente
- ◯ Muito frequente

* Existe uma equipa capaz de dar resposta a incidentes de cibersegurança na sua organização?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

Fase 5 - Equipa de Cibersegurança

Esta fase aplica-se a organizações cuja dimensão ou criticidade justfique a criação de um SOC (Security Operations Center trata-se do ponto de contacto único, disponível 24x7, para a monitorização e reação a incidentes de segurança) ou CSIRT (Computer Security Incident Response Team, tem como função responder a incidentes de segurança informática).

* Foi nomeado um (Responsável de Segurança de Informação) CISO na organização?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

* A organização possui algum destes serviços? (?)

- ☐ SOC
- ☐ CSIRT
- ☐ Não

* Alguma vez a organização foi alvo de um ataque informático?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

Fase 5 - Equipa de Cibersegurança

Esta fase aplica-se a organizações cuja dimensão ou criticidade justfique a criação de um SOC (Security Operations Center trata-se do ponto de contacto único, disponível 24x7, para a monitorização e reação a incidentes de segurança) ou CSIRT (Computer Security Incident Response Team, tem como função responder a incidentes de segurança informática).

* Estes ataques foram documentados?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

Fase 5 - Equipa de Cibersegurança

Esta fase aplica-se a organizações cuja dimensão ou criticidade justfique a criação de um SOC (Security Operations Center trata-se do ponto de contacto único, disponível 24x7, para a monitorização e reação a incidentes de segurança) ou CSIRT (Computer Security Incident Response Team, tem como função responder a incidentes de segurança informática).

* Que tipo(s) de ataque sofreu?

- ☐ DDoS
- ☐ Roubo de informação
- ☐ Ransomware
- ☐ Phishing
- ☐ Engenharia Social
- ☐ Não sabe
- ☐ Outro

- [ ] Nenhuma das anteriores

* Considera que qualquer colaborador sabe como atuar em caso de ataque informático?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

* Existe um processo para que todos os colaboradores possam reportar possíveis incidentes de segurança?

- ◯ Sim
- ◯ Não
- ◯ Não sabe

Relatório de Maturidade da Organização

* **O e-mail facultado será apenas utilizado para posterior envio de relatório com a análise da maturidade obtida através das respostas dadas.**
Pretende que lhe seja posteriormente enviado um relatório de maturidade da organização via e-mail?

- ◯ Sim
- ◯ Não

* Forneça por favor, o e-mail que pretende receber o relatório de maturidade de Cibersegurança:

C

APÊNDICE C - RELATÓRIO COM RESPOSTAS COMPLETAS

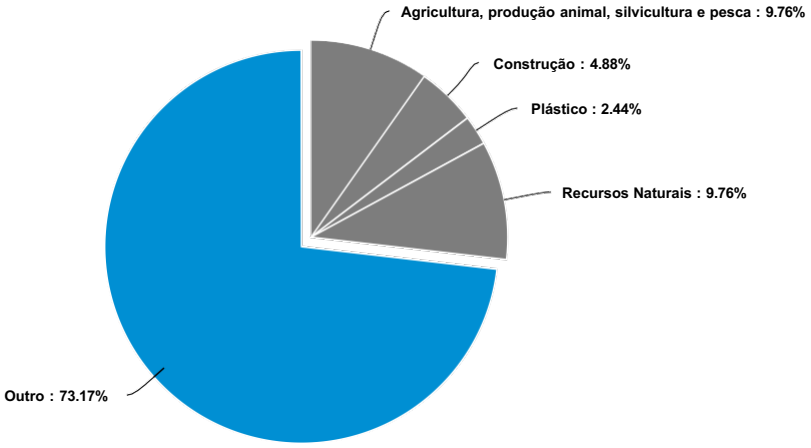
Encontra-se neste apêndice o relatório das respostas completas, em que foram baseados os dados analisados.

Inquérito Dissertação - Dashboard

226	41	41	100%	0	10 min
Visto em	Total de respostas	Concluído	Taxa de conclusão	Desistências	Tempo médio

Países	Respostas
PT	100.00%
Total	100.00%

Qual é o setor de atividade da organização?



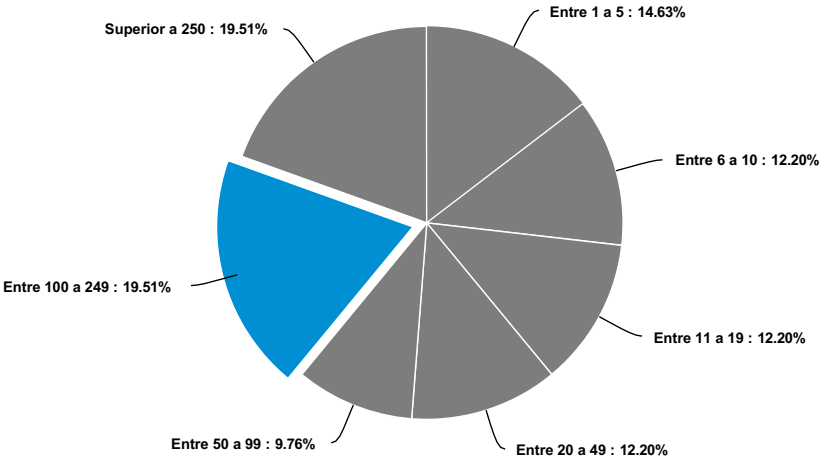
Resposta	Contagem	Percentagem
Agricultura, produção animal, silvicultura e pesca	4	9.76%
Construção	2	4.88%
Cerâmica	0	0%
Moldes	0	0%
Vidro	0	0%
Plástico	1	2.44%
Recursos Naturais	4	9.76%
Outro	30	73.17%
Total	**41**	**100 %**

Qual é o setor de atividade da organização? - Text Data for Outro

09/03/2022	83518205	Comércio
09/03/2022	83517883	Divulgação científica
09/02/2022	83433220	Gestão residuos
08/30/2022	83160535	Energias renovaveis
08/30/2022	83160094	Serviços Informaticos
08/29/2022	83038224	Financeiro
08/29/2022	83028385	Informática
08/27/2022	82930558	Consultoria
08/26/2022	82912868	Tecnologia
08/26/2022	82845561	Restauração
08/26/2022	82843394	Serviços administrativos
08/26/2022	82843211	Consultoria
08/26/2022	82841479	Software

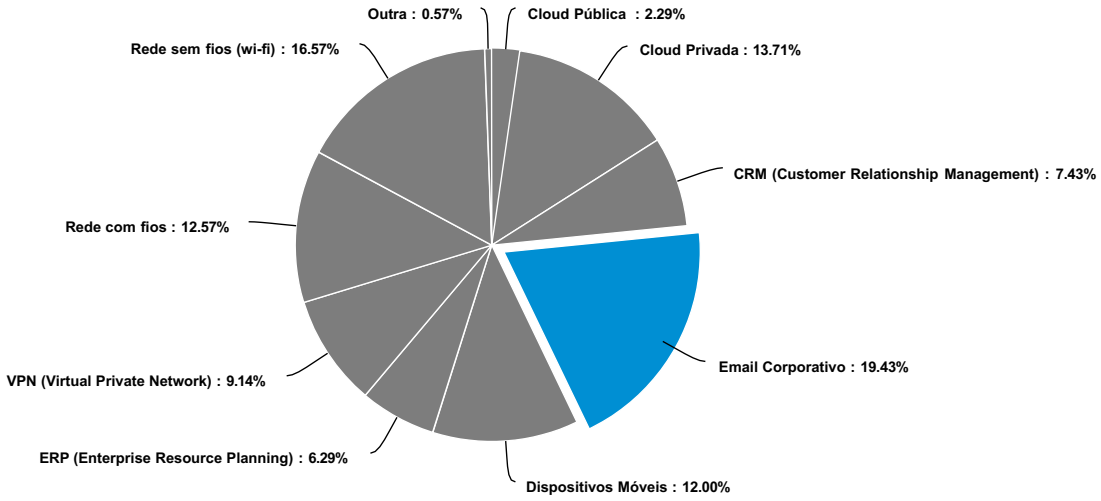
08/26/2022	82840509	Energia solar
08/25/2022	82766551	Educação
08/25/2022	82756027	Serviços
08/24/2022	82749202	Contabilidade e consultoria
08/24/2022	82747961	Banca
08/24/2022	82740853	Autarquia Local
08/24/2022	82729572	Consultoria
08/24/2022	82729271	Informática
08/24/2022	82696542	Transformação de rochas ornamentais
08/22/2022	82556464	Administrativo
08/22/2022	82545990	Curtumes
08/21/2022	82507623	Veterinária
08/20/2022	82456351	Computadores
08/19/2022	82369571	Associação Empresarial
08/19/2022	82368329	Iluminação
07/26/2022	80429807	tecnologias 4.0
07/26/2022	80397919	Metalurgica

Qual é o número de colaboradores da organização?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Entre 1 a 5	6	14.63%					
Entre 6 a 10	5	12.2%					
Entre 11 a 19	5	12.2%					
Entre 20 a 49	5	12.2%					
Entre 50 a 99	4	9.76%					
Entre 100 a 249	8	19.51%					
Superior a 250	8	19.51%					
Total	**41**	**100 %**					

Que tipo de tecnologias são utilizadas pela organização?

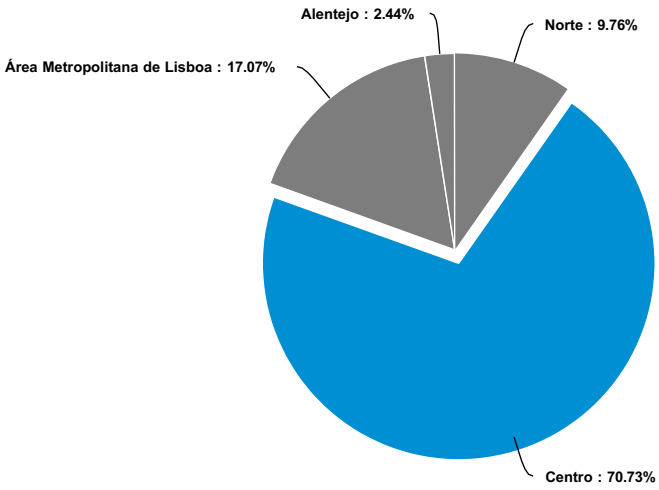


Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Cloud Pública	4	2.29%					
Cloud Privada	24	13.71%					
CRM (Customer Relationship Management)	13	7.43%					
Email Corporativo	34	19.43%					
Dispositivos Móveis	21	12%					
ERP (Enterprise Resource Planning)	11	6.29%					
VPN (Virtual Private Network)	16	9.14%					
Rede com fios	22	12.57%					
Rede sem fios (wi-fi)	29	16.57%					
Outra	1	0.57%					
Total	**175**	**100 %**					

Que tipo de tecnologias são utilizadas pela organização? - Text Data for Outra

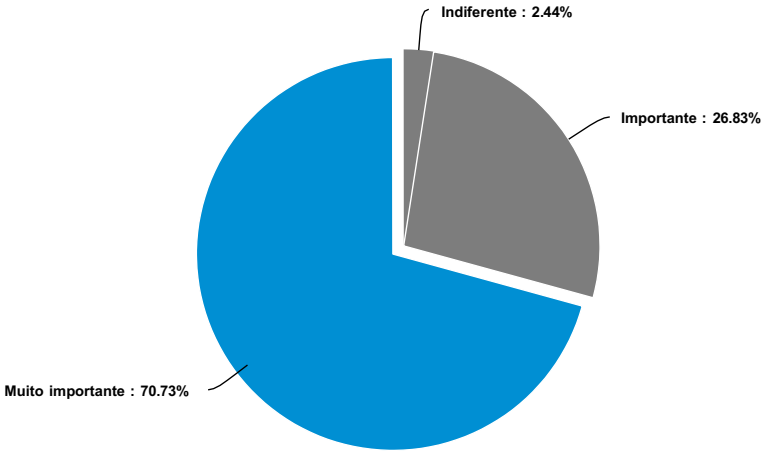
07/26/2022 80397919 Automação

Em que região está sediada a organização?



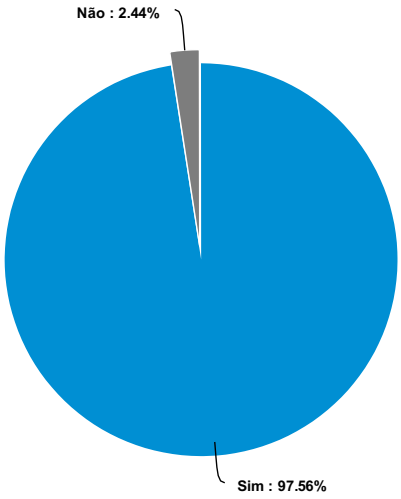
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Norte	4	9.76%					
Centro	29	70.73%					
Área Metropolitana de Lisboa	7	17.07%					
Alentejo	1	2.44%					
Algarve	0	0%					
Madeira	0	0%					
Açores	0	0%					
Total	**41**	**100 %**					

Qual o grau de importância da segurança a informação para a organização?



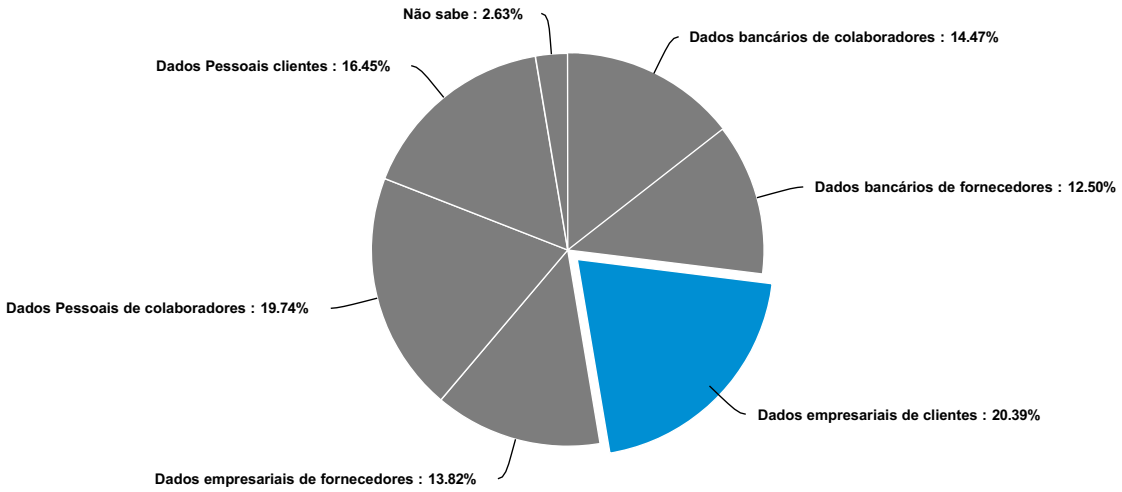
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Nada importante	0	0%					
Pouco importante	0	0%					
Indiferente	1	2.44%					
Importante	11	26.83%					
Muito importante	29	70.73%					
Total	**41**	**100 %**					

A organização tem preocupação com os danos reputacionais em caso de incidente de segurança?



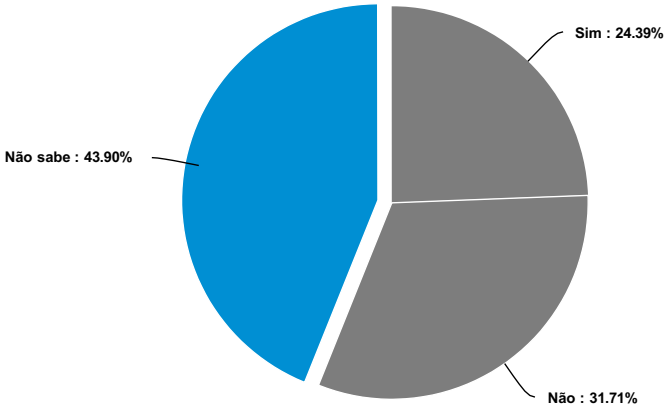
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	40	97.56%					
Não	1	2.44%					
Total	**41**	**100 %**					

Qual é o tipo de informação processada pela organização?



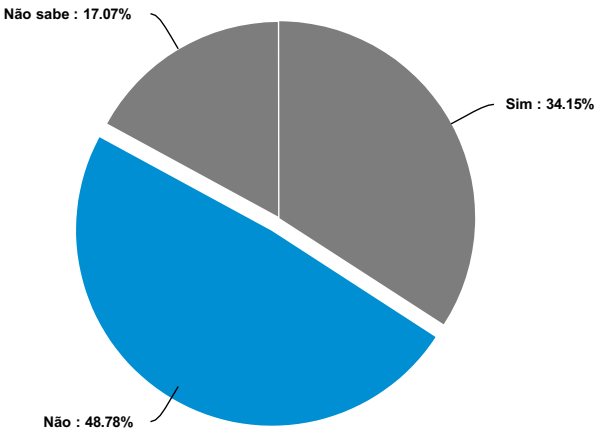
Resposta	Contagem	Percentagem
Dados bancários de colaboradores	22	14.47%
Dados bancários de fornecedores	19	12.5%
Dados empresariais de clientes	31	20.39%
Dados empresariais de fornecedores	21	13.82%
Dados Pessoais de colaboradores	30	19.74%
Dados Pessoais clientes	25	16.45%
Não sabe	4	2.63%
Total	**152**	**100 %**

A sua empresa tem algum seguro contratado para cobrir incidentes de segurança?



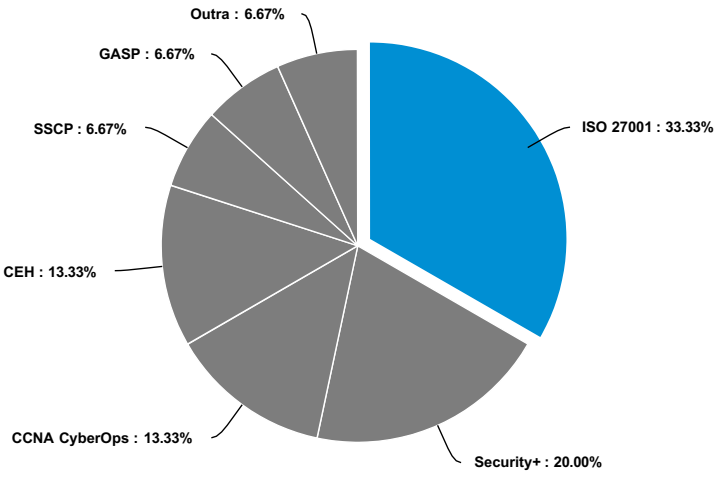
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	10	24.39%					
Não	13	31.71%					
Não sabe	18	43.9%					
Total	**41**	**100 %**					

A sua empresa tem colaboradores certificados na área de Cibersegurança?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	14	34.15%					
Não	20	48.78%					
Não sabe	7	17.07%					
Total	**41**	**100 %**					

Qual(is) das seguintes certificações possi(uem) os colaboradores ou a organização?

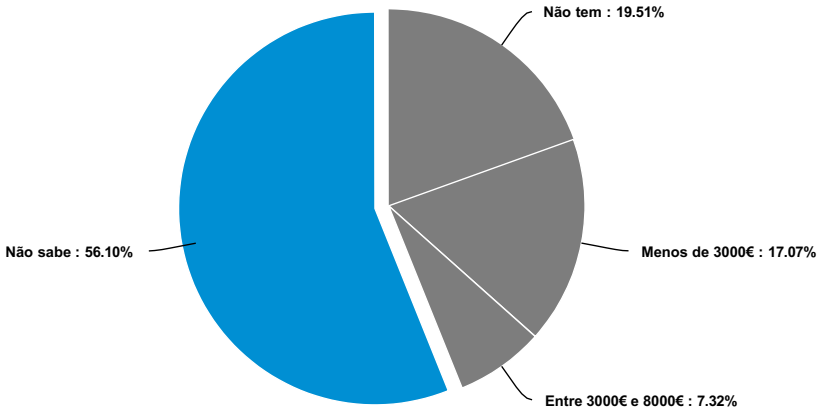


Resposta	Contagem	Percentagem
ISO 27001	5	33.33%
Security+	3	20%
CCNA CyberOps	2	13.33%
CISSP	0	0%
Lead Auditor	0	0%
CEH	2	13.33%
GSEC	0	0%
SSCP	1	6.67%
GASP	1	6.67%
GCIH	0	0%
OSCP	0	0%
Outra	1	6.67%
Total	**15**	**100 %**

Qual(is) das seguintes certificações possi(uem) os colaboradores ou a organização? - Text Data for Outra

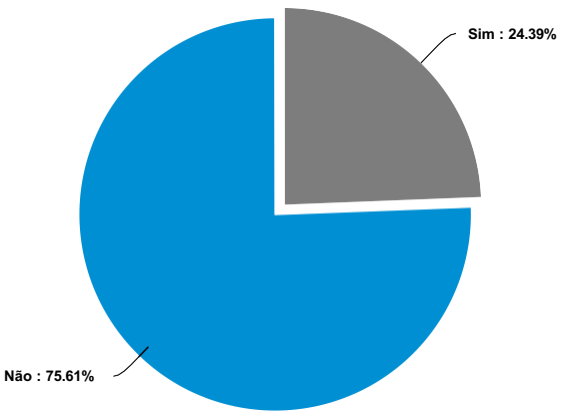
08/24/2022	82747961 Não sei

Qual o orçamento anual para investir em Cibersegurança:



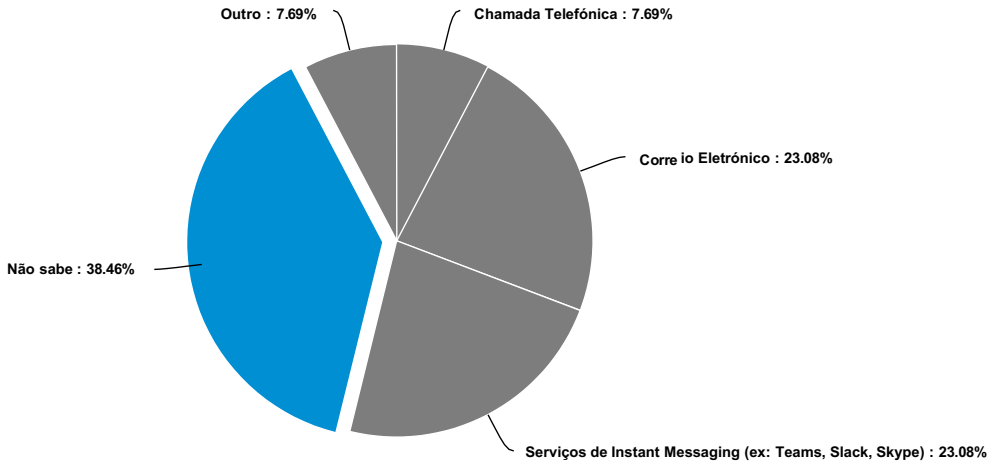
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Não tem	8	19.51%					
Menos de 3000€	7	17.07%					
Entre 3000€ e 8000€	3	7.32%					
Entre 8001€ e 15000€	0	0%					
Mais de 20000€	0	0%					
Não sabe	23	56.1%					
Total	**41**	**100 %**					

Está definida uma forma de comunicação com o CNCS?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	10	24.39%					
Não	31	75.61%					
Total	**41**	**100 %**					

Quais são os canais de comunicação que estão definidos com o CNCS?

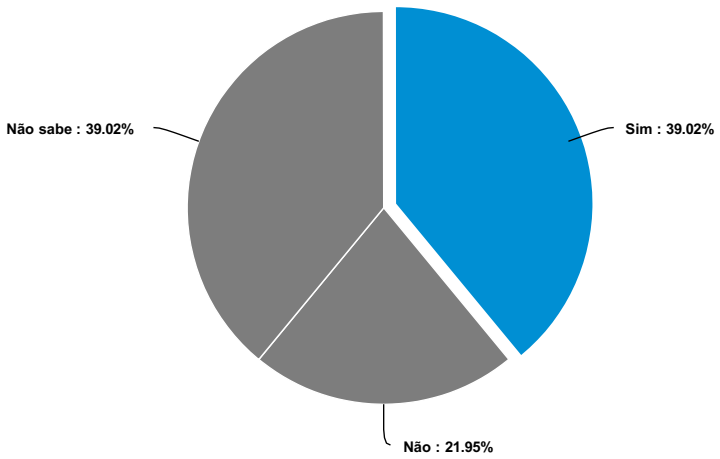


Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Chamada Telefónica	1	7.69%					
Correio Eletrónico	3	23.08%					
PGP	0	0%					
Serviços de Instant Messaging (ex: Teams, Slack, Skype)	3	23.08%					
Não sabe	5	38.46%					
Outro	1	7.69%					
Total	**13**	**100 %**					

Quais são os canais de comunicação que estão definidos com o CNCS? - Text Data for Outro

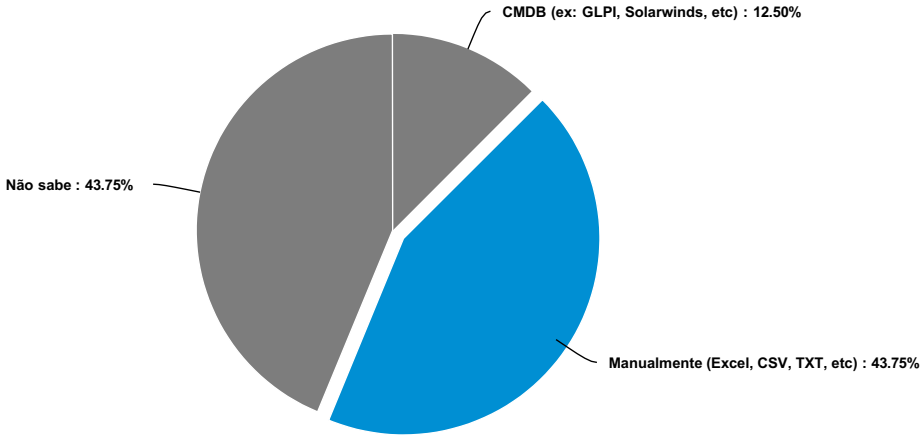
08/19/2022 82369571 O CNCS colabora regularmente com a associação

Existe um inventário de ativos e serviços críticos da organização?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	16	39.02%					
Não	9	21.95%					
Não sabe	16	39.02%					
Total	**41**	**100 %**					

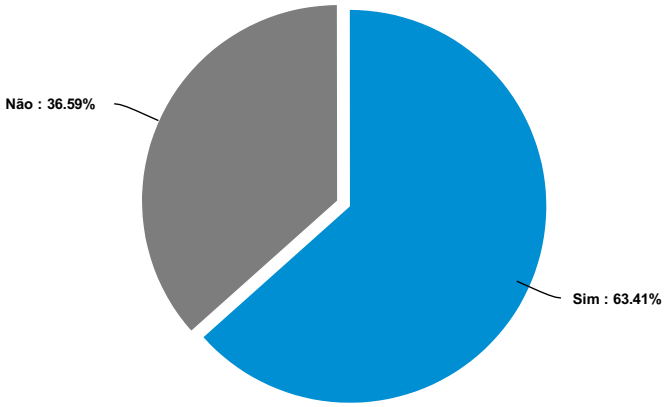
De que forma é feita a inventariação dos ativos?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
CMDB (ex: GLPI, Solarwinds, etc)	2	12.5%					
Manualmente (Excel, CSV, TXT, etc)	7	43.75%					
Não sabe	7	43.75%					
Outra	0	0%					
Total	**16**	**100 %**					

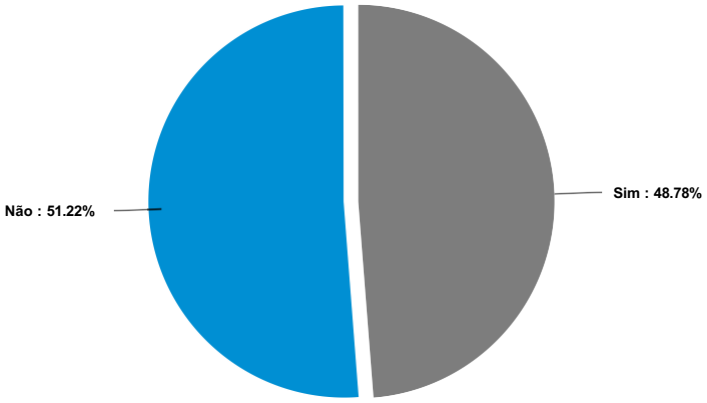
De que forma é feita a inventariação dos ativos? - Text Data for Outra

Os ativos da organização são encriptados?



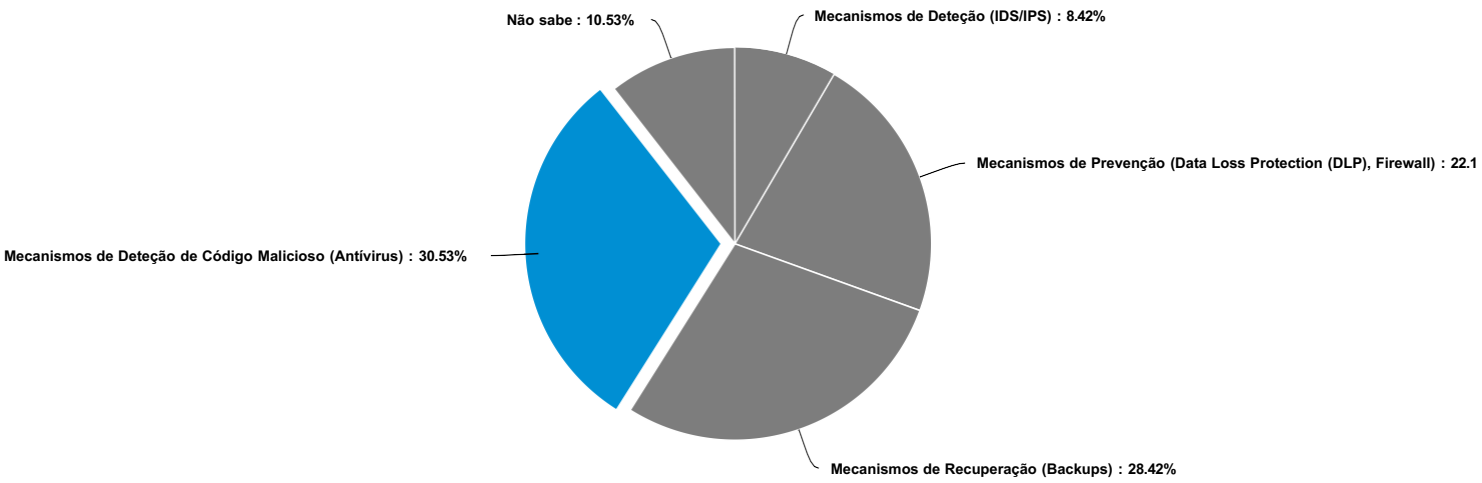
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	26	63.41%					
Não	15	36.59%					
Total	**41**	**100 %**					

São efetuados testes de penetração aos ativos da organização?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	20	48.78%					
Não	21	51.22%					
Total	**41**	**100 %**					

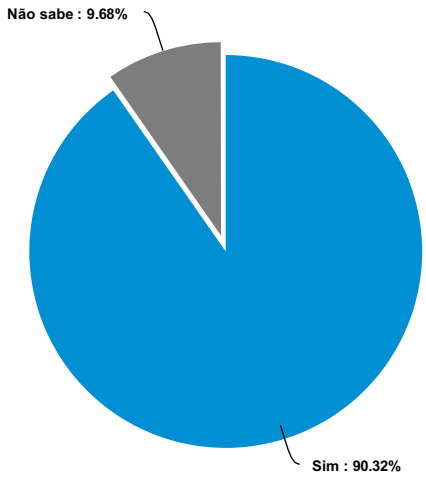
Quais das seguinte soluções de segurança estão disponíveis na organização para lidar com possíveis ameaças?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Mecanismos de Deteção (IDS/IPS)	8	8.42%					
Mecanismos de Prevenção (Data Loss Protection (DLP), Firewall)	21	22.11%					
Mecanismos de Recuperação (Backups)	27	28.42%					
Mecanismos de Deteção de Código Malicioso (Antívirus)	29	30.53%					
Não sabe	10	10.53%					
Outro	0	0%					
Total	**95**	**100 %**					

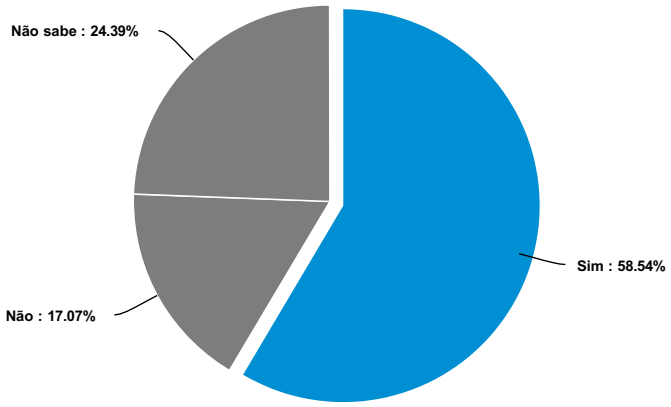
Quais das seguinte soluções de segurança estão disponíveis na organização para lidar com possíveis ameaças? - Text Data for Outro

As soluções de segurança indicadas na questão anterior são utilizadas nos sistemas e postos de trabalho onde é tratada informação crítica?



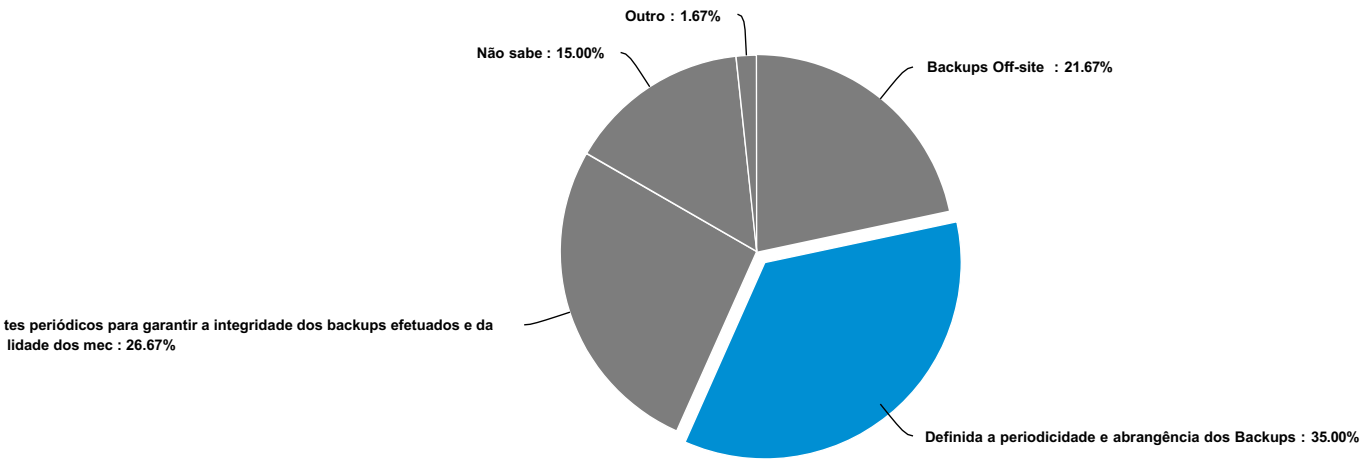
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	28	90.32%					
Não	0	0%					
Não sabe	3	9.68%					
Total	**31**	**100 %**					

Na organização é utilizada alguma tecnologia com a capacidade de analisar tráfego malicioso?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	24	58.54%					
Não	7	17.07%					
Não sabe	10	24.39%					
Total	**41**	**100 %**					

Quais dos seguintes procedimentos de backup/restore estão implementados na organização?

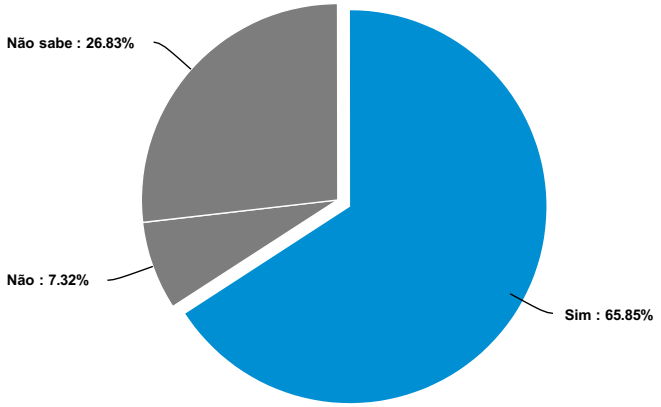


Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Backups Off-site	13	21.67%					
Definida a periodicidade e abrangência dos Backups	21	35%					
Testes periódicos para garantir a integridade dos backups efetuados e da qualidade dos mecanismos de reposição	16	26.67%					
Não sabe	9	15%					
Outro	1	1.67%					
Total	**60**	**100 %**					

Quais dos seguintes procedimentos de backup/restore estão implementados na organização? - Text Data for Outro

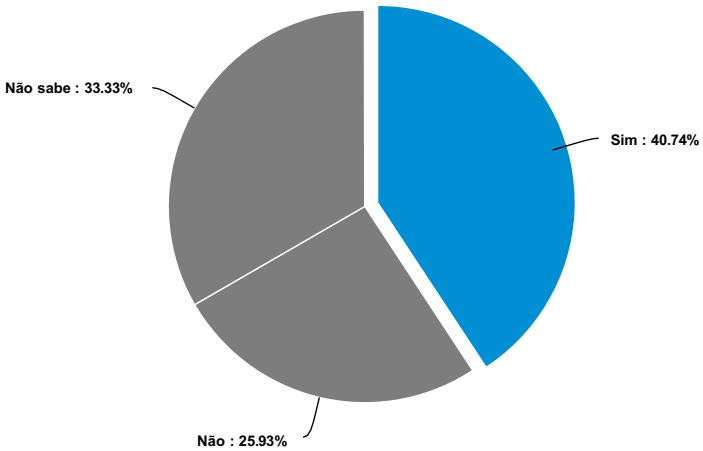
09/15/2022 85511986 Antivírus

A organização é conhecedora dos quadros legais e regulatórios a que está sujeita (nacionais e europeus)?



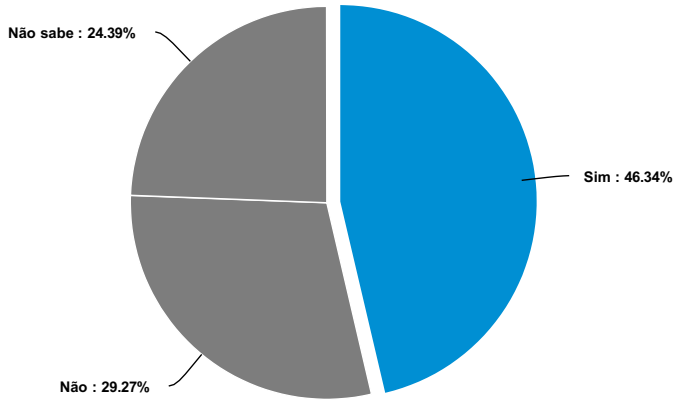
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	27	65.85%					
Não	3	7.32%					
Não sabe	11	26.83%					
Total	**41**	**100 %**					

Existem relatórios de auditorias que comprovem a conformidade com a legislação e regulamentação?



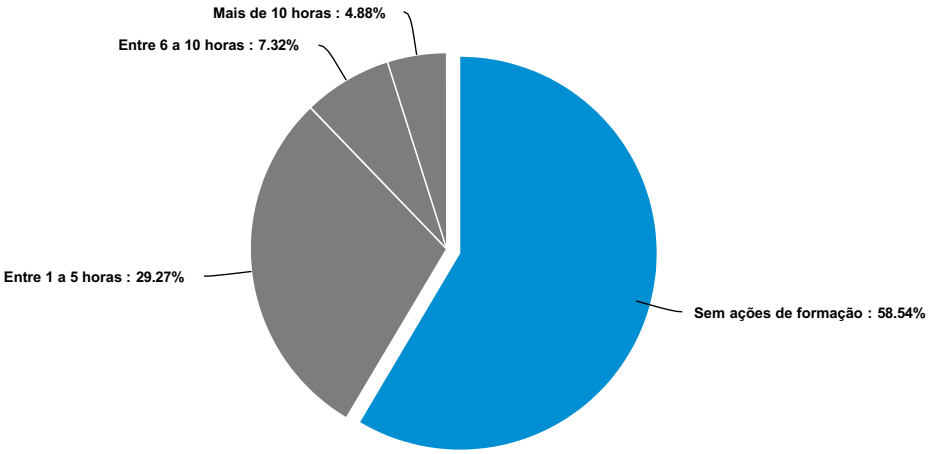
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	11	40.74%					
Não	7	25.93%					
Não sabe	9	33.33%					
Total	**27**	**100 %**					

É efetuado o registo de eventos como logs e atividades de utilizadores?



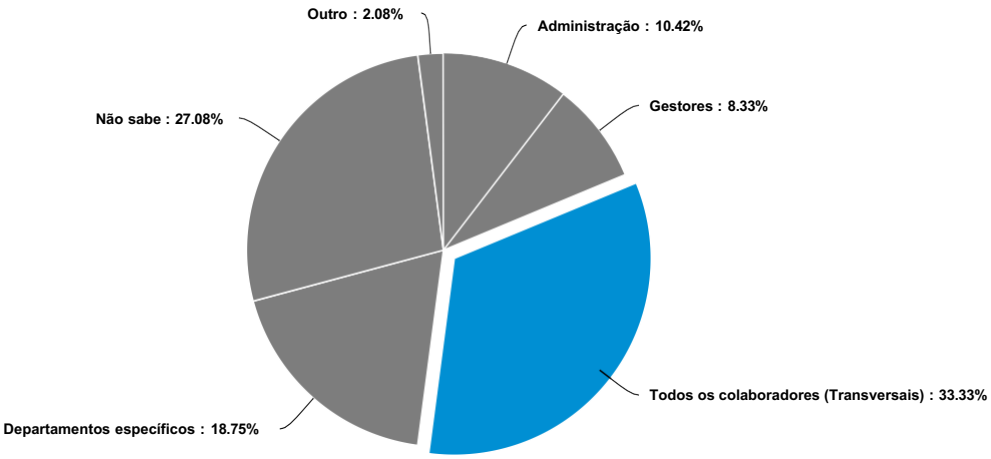
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	19	46.34%					
Não	12	29.27%					
Não sabe	10	24.39%					
Total	**41**	**100 %**					

Qual o número de horas de ações de formação e sensibilização de colaboradores em matéria de Cibersegurança na organização?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sem ações de formação	24	58.54%					
Entre 1 a 5 horas	12	29.27%					
Entre 6 a 10 horas	3	7.32%					
Mais de 10 horas	2	4.88%					
Total	**41**	**100 %**					

A quem se destinam estas ações de formação disponibilizadas na organização?

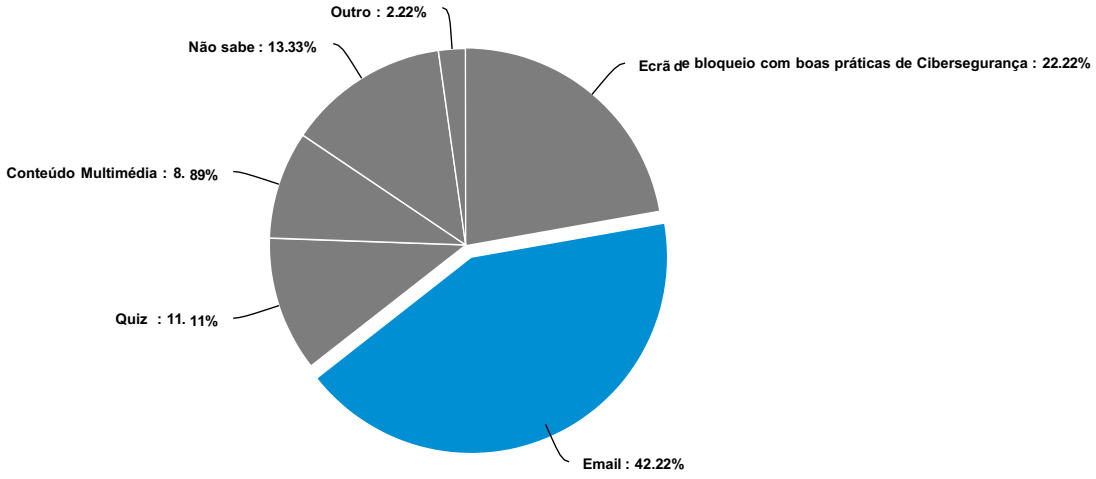


Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Administração	5	10.42%					
Gestores	4	8.33%					
Todos os colaboradores (Transversais)	16	33.33%					
Departamentos específicos	9	18.75%					
Não sabe	13	27.08%					
Outro	1	2.08%					
Total	**48**	**100 %**					

A quem se destinam estas ações de formação disponibilizadas na organização? - Text Data for Outro

08/24/2022	82696542	Ninguém

Na organização são utilizados alguns dos seguintes lembretes relativamente a boas praticas de Cibersegurança?

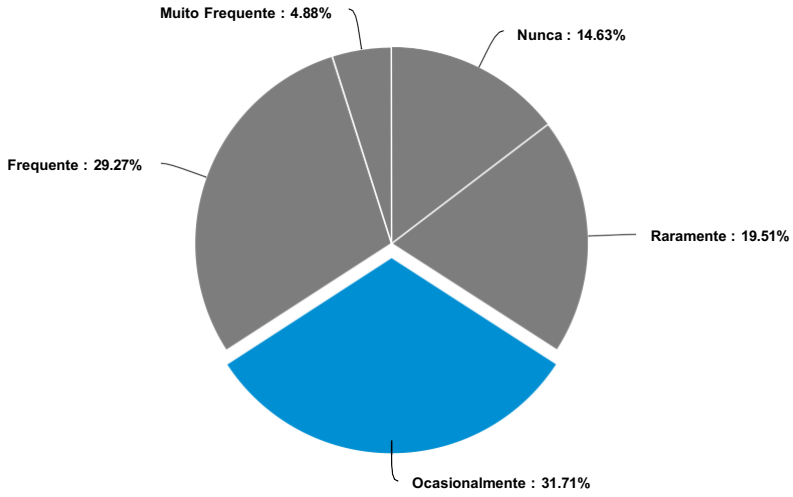


Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Ecrã de bloqueio com boas práticas de Cibersegurança	10	22.22%					
Email	19	42.22%					
Quiz	5	11.11%					
Conteúdo Multimédia	4	8.89%					
Não sabe	6	13.33%					
Outro	1	2.22%					
Total	**45**	**100 %**					

Na organização são utilizados alguns dos seguintes lembretes relativamente a boas praticas de Cibersegurança? - Text Data for Outro

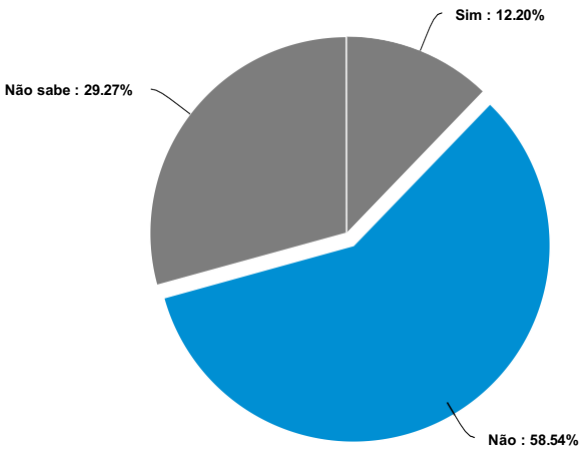
08/29/2022	83028385	envio de m-email de phising interno para testes

Com que regularidade são auditadas as configurações dos dispositivos?



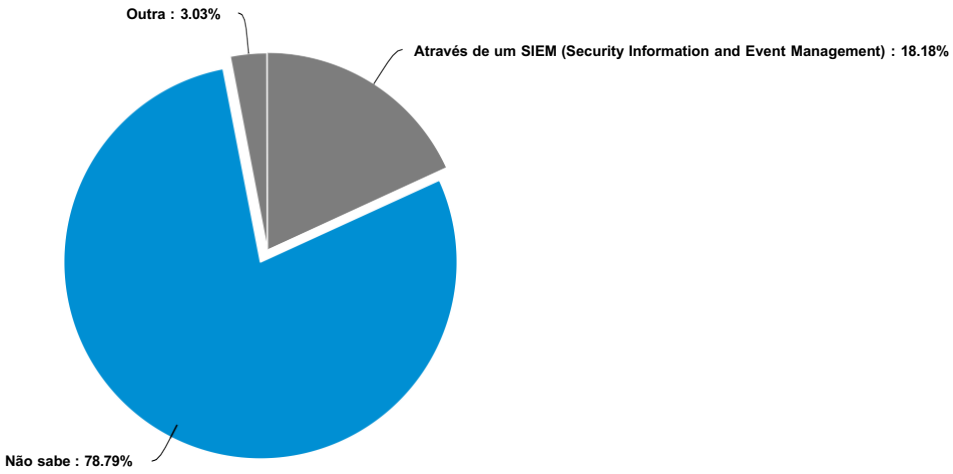
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Nunca	6	14.63%					
Raramente	8	19.51%					
Ocasionalmente	13	31.71%					
Frequente	12	29.27%					
Muito Frequente	2	4.88%					
Total	**41**	**100 %**					

A organização tem uma política BYOD (Gestão de Dispositivos Móveis Pessoais)?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	5	12.2%					
Não	24	58.54%					
Não sabe	12	29.27%					
Total	**41**	**100 %**					

De que forma é feita a gestão de eventos de segurança?

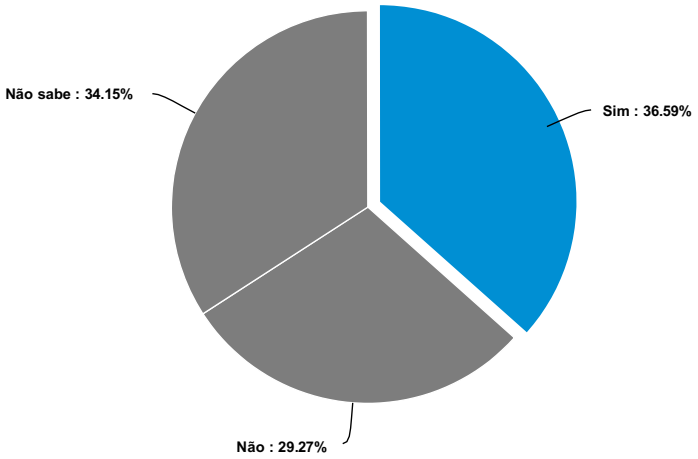


Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Através de um SIEM (Security Information and Event Management)	6	18.18%					
Não sabe	26	78.79%					
Outra	1	3.03%					
Total	**33**	**100 %**					

De que forma é feita a gestão de eventos de segurança? - Text Data for Outra

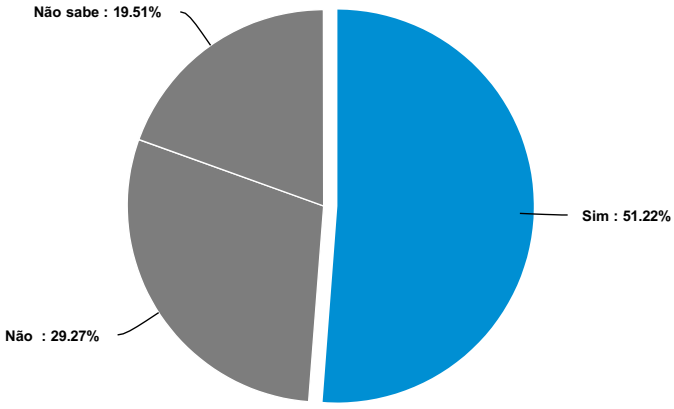
09/15/2022 85511986 Empresa de informática

Existe algum sistema de monitorização dos principais ativos de rede e sistemas que dão suporte às atividades da organização?



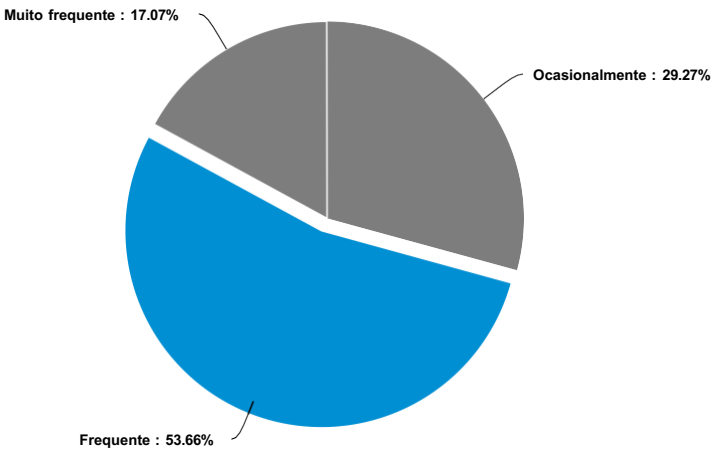
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	15	36.59%					
Não	12	29.27%					
Não sabe	14	34.15%					
Total	**41**	**100 %**					

Os colaboradores têm conhecimento de como utilizar informação crítica?



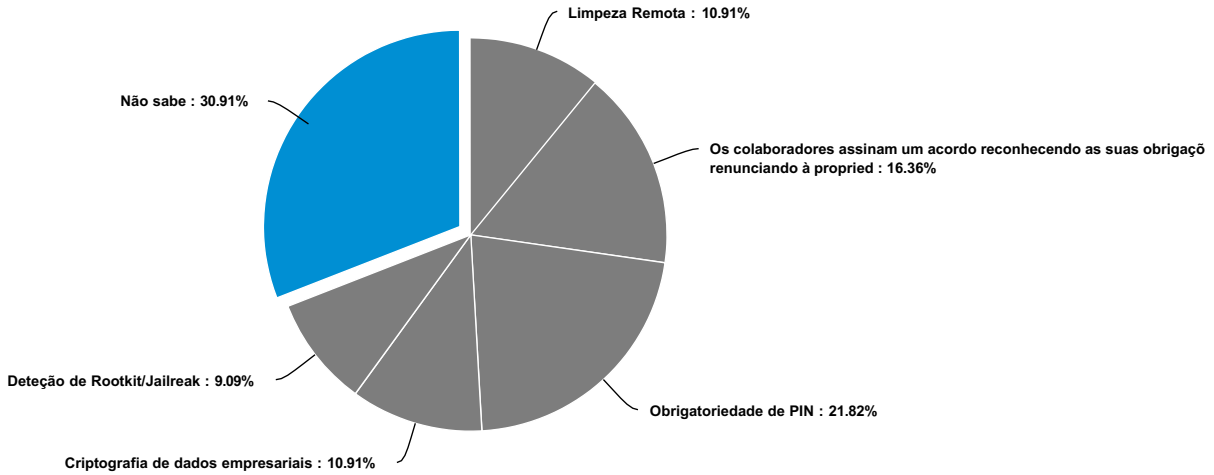
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	21	51.22%					
Não	12	29.27%					
Não sabe	8	19.51%					
Total	**41**	**100 %**					

Com que regularidade são feitas as atualizações de software?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Nunca	0	0%					
Raramente	0	0%					
Ocasionalmente	12	29.27%					
Frequente	22	53.66%					
Muito frequente	7	17.07%					
Total	**41**	**100 %**					

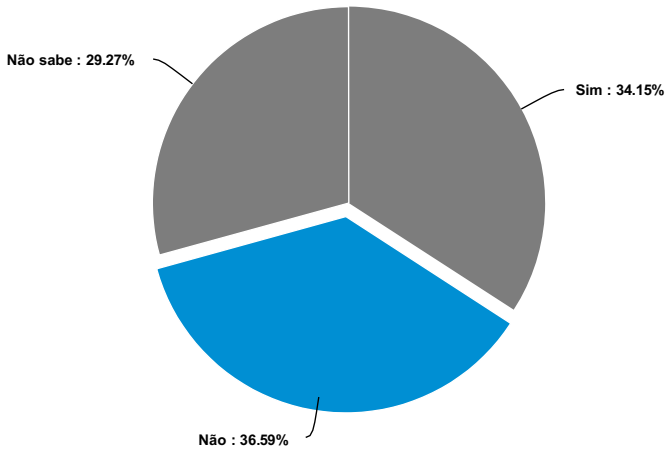
Quais os procedimentos de segurança que estão definidos na política de dispositivos móveis?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Limpeza Remota	6	10.91%					
Os colaboradores assinam um acordo reconhecendo as suas obrigações, renunciando à propriedade de dados de negócio	9	16.36%					
Obrigatoriedade de PIN	12	21.82%					
Criptografia de dados empresariais	6	10.91%					
Deteção de Rootkit/Jailreak	5	9.09%					
Não sabe	17	30.91%					
Outro	0	0%					
Total	**55**	**100 %**					

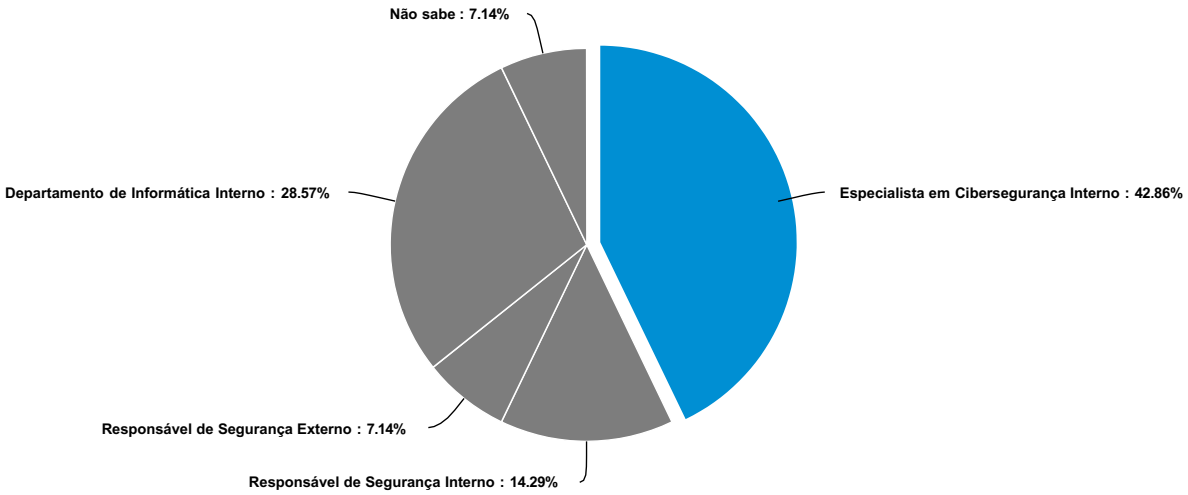
Quais os procedimentos de segurança que estão definidos na política de dispositivos móveis? - Text Data for Outro

Antes da entrada em produção, os sistemas e aplicações são submetidos a testes de cibersegurança?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	14	34.15%					
Não	15	36.59%					
Não sabe	12	29.27%					
Total	**41**	**100 %**					

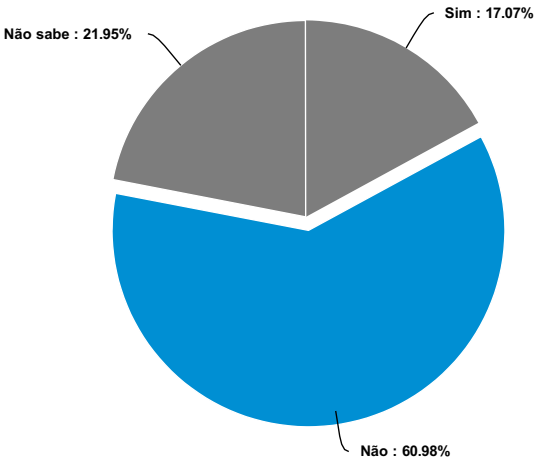
Por quem são efetuados os testes de cibersegurança indicados na questão anterior?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Especialista em Cibersegurança Interno	6	42.86%					
Especialista em Cibersegurança Externo	0	0%					
Responsável de Segurança Interno	2	14.29%					
Responsável de Segurança Externo	1	7.14%					
Departamento de Informática Interno	4	28.57%					
Não sabe	1	7.14%					
Outro	0	0%					
Total	**14**	**100 %**					

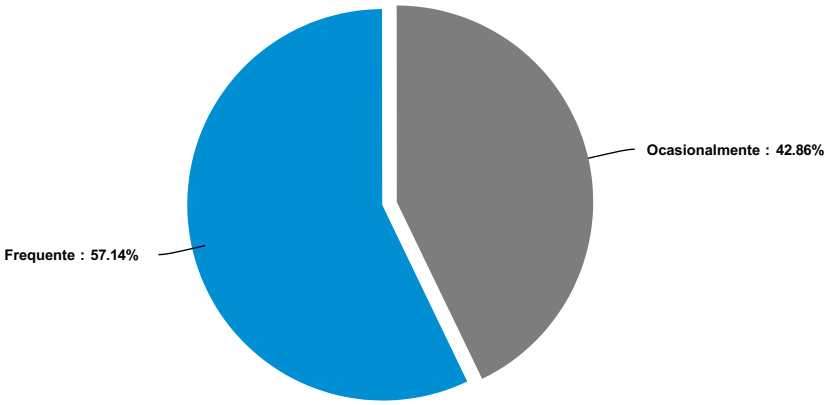
Por quem são efetuados os testes de cibersegurança indicados na questão anterior? - Text Data for Outro

Já foi efetuado algum simulacro de Cibersegurança na organização?



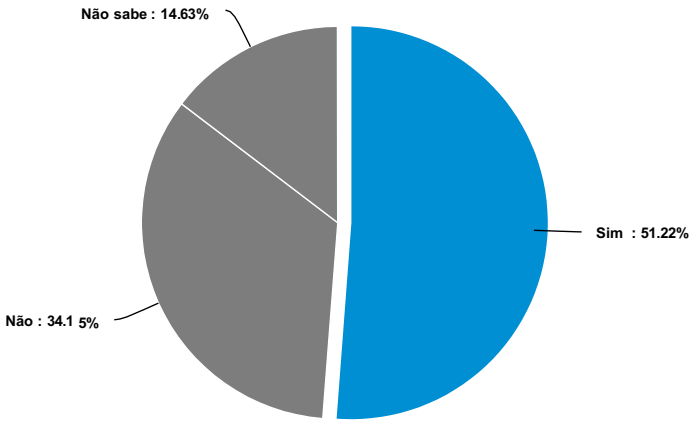
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	7	17.07%					
Não	25	60.98%					
Não sabe	9	21.95%					
Total	**41**	**100 %**					

Com que frequência são efetuados estes simulacros?



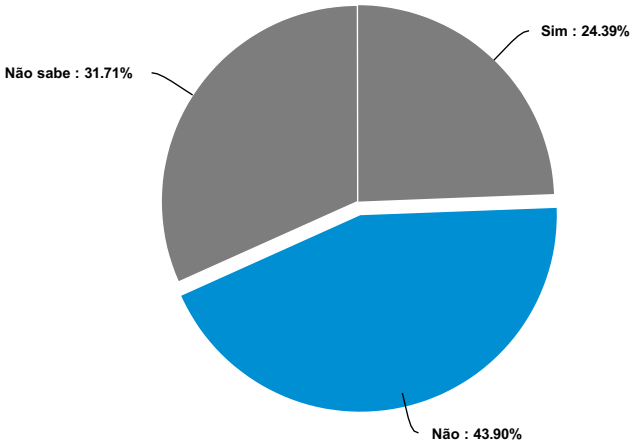
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Nunca	0	0%					
Raramente	0	0%					
Ocasionalmente	3	42.86%					
Frequente	4	57.14%					
Muito frequente	0	0%					
Total	**7**	**100 %**					

Existe uma equipa capaz de dar resposta a incidentes de cibersegurança na sua organização?



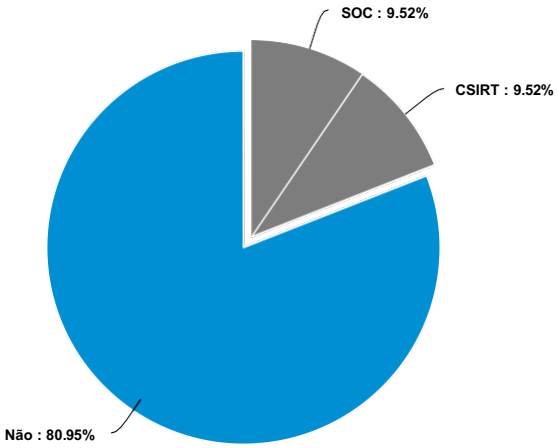
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	21	51.22%					
Não	14	34.15%					
Não sabe	6	14.63%					
Total	**41**	**100 %**					

Foi nomeado um (Responsável de Segurança de Informação) CISO na organização?



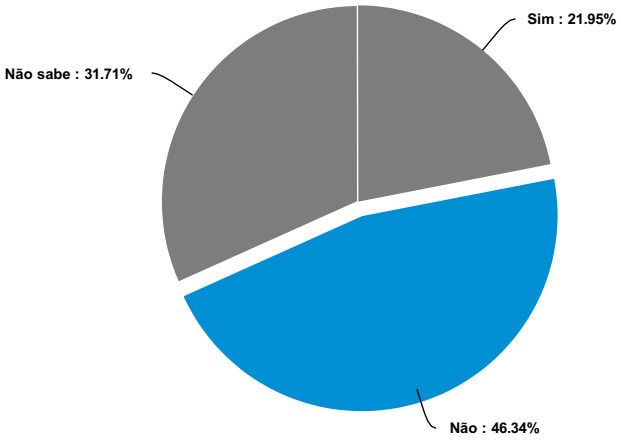
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	10	24.39%					
Não	18	43.9%					
Não sabe	13	31.71%					
Total	**41**	**100 %**					

A organização possui algum destes serviços?



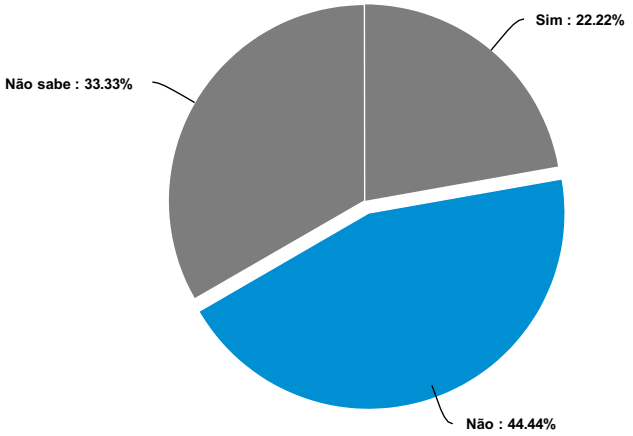
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
SOC	4	9.52%					
CSIRT	4	9.52%					
Não	34	80.95%					
Total	**42**	**100 %**					

Alguma vez a organização foi alvo de um ataque informático?



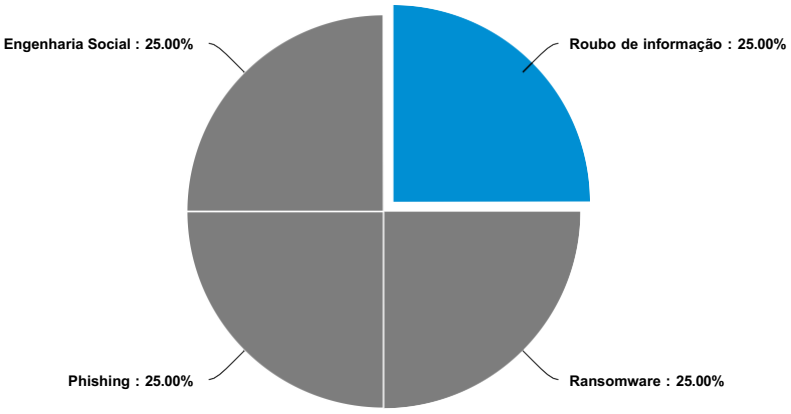
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	9	21.95%					
Não	19	46.34%					
Não sabe	13	31.71%					
Total	**41**	**100 %**					

Estes ataques foram documentados?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	2	22.22%					
Não	4	44.44%					
Não sabe	3	33.33%					
Total	**9**	**100 %**					

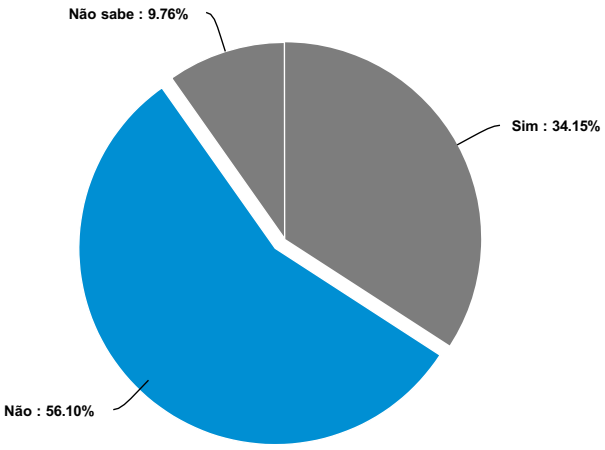
Que tipo(s) de ataque sofreu?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
DDoS	0	0%					
Roubo de informação	1	25%					
Ransomware	1	25%					
Phishing	1	25%					
Engenharia Social	1	25%					
Não sabe	0	0%					
Outro	0	0%					
Total	4	100 %					

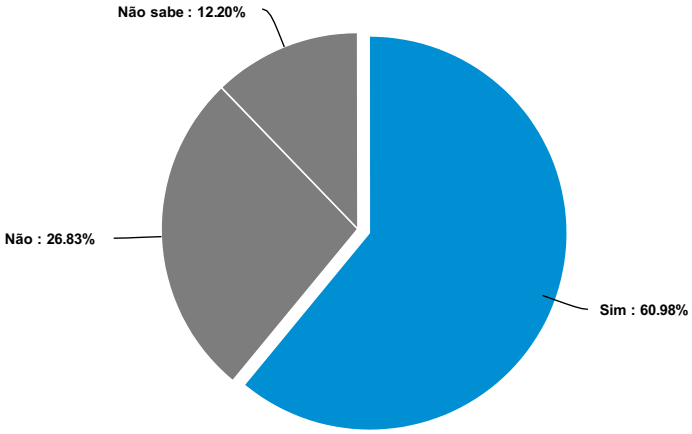
Que tipo(s) de ataque sofreu? - Text Data for Outro

Considera que qualquer colaborador sabe como atuar em caso de ataque informático?



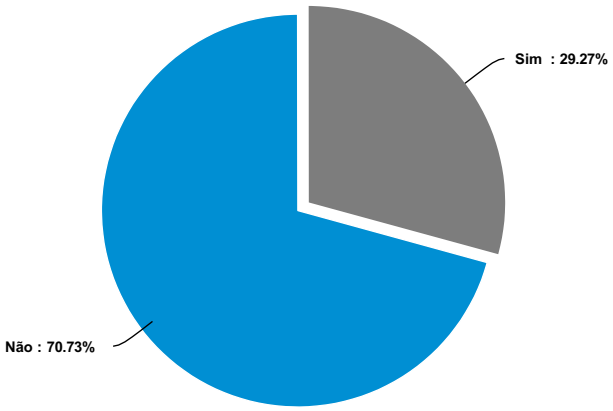
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	14	34.15%					
Não	23	56.1%					
Não sabe	4	9.76%					
Total	**41**	**100 %**					

Existe um processo para que todos os colaboradores possam reportar possíveis incidentes de segurança?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	25	60.98%					
Não	11	26.83%					
Não sabe	5	12.2%					
Total	**41**	**100 %**					

O e-mail facultado será apenas utilizado para posterior envio de relatório com a análise da maturidade obtida através das respostas dadas. Pretende que lhe seja posteriormente enviado um relatório de maturidade da organização via e-mail?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	12	29.27%					
Não	29	70.73%					
Total	**41**	**100 %**					

Forneça por favor, o e-mail que pretende receber o relatório de maturidade de Cibersegurança:

D

APÊNDICE D - RELATÓRIO COM RESPOSTAS INCOMPLETAS

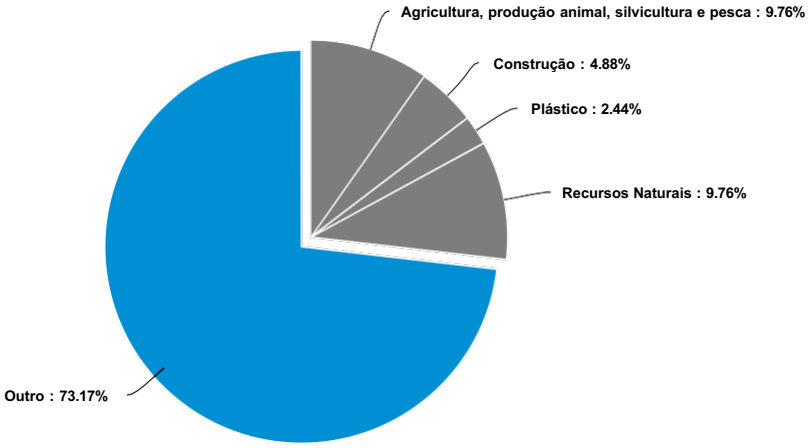
Encontra-se neste apêndice o relatório das respostas incompletas, onde se pode constatar o número de desistências.

Inquérito Dissertação - Dashboard

226	41	41	100%	0	10 min
Visto em	Total de respostas	Concluído	Taxa de conclusão	Desistências	Tempo médio

Países	Respostas
PT	100.00%
Total	100.00%

Qual é o setor de atividade da organização?



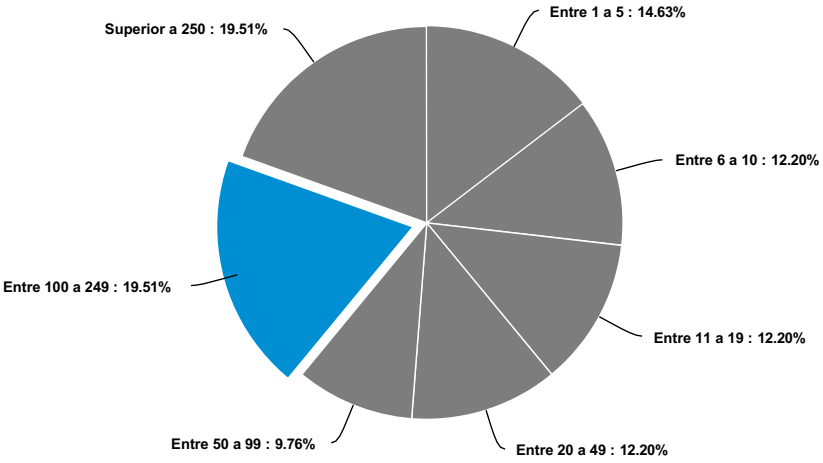
Resposta	Contagem	Percentagem
Agricultura, produção animal, silvicultura e pesca	4	9.76%
Construção	2	4.88%
Cerâmica	0	0%
Moldes	0	0%
Vidro	0	0%
Plástico	1	2.44%
Recursos Naturais	4	9.76%
Outro	30	73.17%
Total	**41**	**100 %**

Qual é o setor de atividade da organização? - Text Data for Outro

09/03/2022	83518205	Comércio
09/03/2022	83517883	Divulgação científica
09/02/2022	83433220	Gestão residuos
08/30/2022	83160535	Energias renovaveis
08/30/2022	83160094	Serviços Informaticos
08/29/2022	83038224	Financeiro
08/29/2022	83028385	Informática
08/27/2022	82930558	Consultoria
08/26/2022	82912868	Tecnologia
08/26/2022	82845561	Restauração
08/26/2022	82843394	Serviços administrativos
08/26/2022	82843211	Consultoria
08/26/2022	82841479	Software

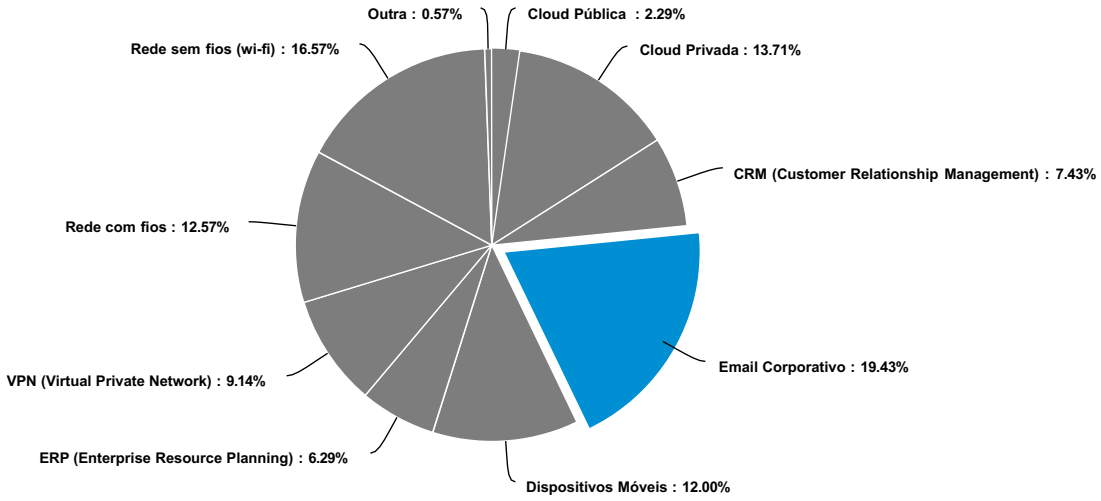
08/26/2022	82840509	Energia solar
08/25/2022	82766551	Educação
08/25/2022	82756027	Serviços
08/24/2022	82749202	Contabilidade e consultoria
08/24/2022	82747961	Banca
08/24/2022	82740853	Autarquia Local
08/24/2022	82729572	Consultoria
08/24/2022	82729271	Informática
08/24/2022	82696542	Transformação de rochas ornamentais
08/22/2022	82556464	Administrativo
08/22/2022	82545990	Curtumes
08/21/2022	82507623	Veterinária
08/20/2022	82456351	Computadores
08/19/2022	82369571	Associação Empresarial
08/19/2022	82368329	Iluminação
07/26/2022	80429807	tecnologias 4.0
07/26/2022	80397919	Metalurgica

Qual é o número de colaboradores da organização?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Entre 1 a 5	6	14.63%					
Entre 6 a 10	5	12.2%					
Entre 11 a 19	5	12.2%					
Entre 20 a 49	5	12.2%					
Entre 50 a 99	4	9.76%					
Entre 100 a 249	8	19.51%					
Superior a 250	8	19.51%					
Total	**41**	**100 %**					

Que tipo de tecnologias são utilizadas pela organização?

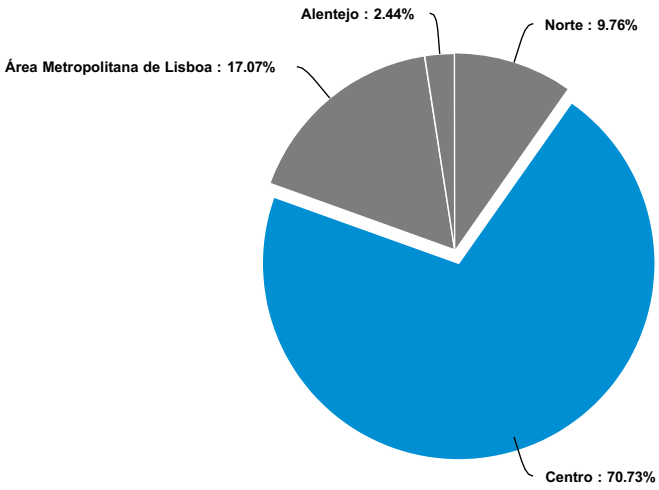


Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Cloud Pública	4	2.29%					
Cloud Privada	24	13.71%					
CRM (Customer Relationship Management)	13	7.43%					
Email Corporativo	34	19.43%					
Dispositivos Móveis	21	12%					
ERP (Enterprise Resource Planning)	11	6.29%					
VPN (Virtual Private Network)	16	9.14%					
Rede com fios	22	12.57%					
Rede sem fios (wi-fi)	29	16.57%					
Outra	1	0.57%					
Total	**175**	**100 %**					

Que tipo de tecnologias são utilizadas pela organização? - Text Data for Outra

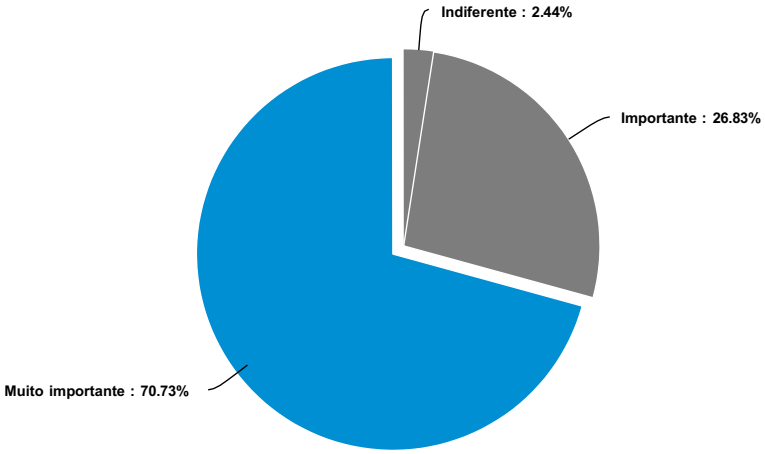
07/26/2022 80397919 Automação

Em que região está sediada a organização?



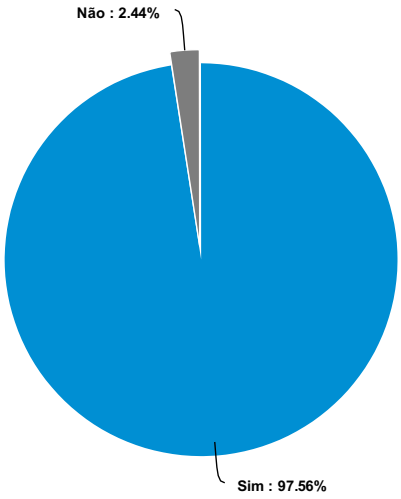
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Norte	4	9.76%					
Centro	29	70.73%					
Área Metropolitana de Lisboa	7	17.07%					
Alentejo	1	2.44%					
Algarve	0	0%					
Madeira	0	0%					
Açores	0	0%					
Total	**41**	**100 %**					

Qual o grau de importância da segurança a informação para a organização?



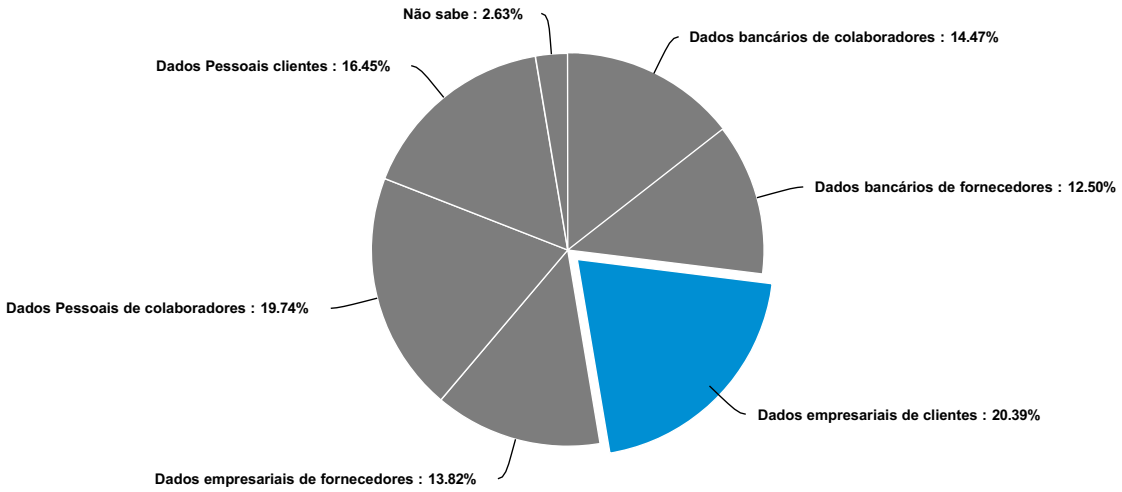
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Nada importante	0	0%					
Pouco importante	0	0%					
Indiferente	1	2.44%					
Importante	11	26.83%					
Muito importante	29	70.73%					
Total	**41**	**100 %**					

A organização tem preocupação com os danos reputacionais em caso de incidente de segurança?



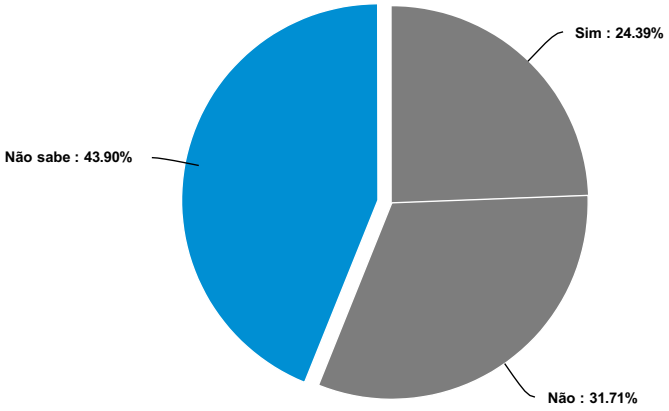
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	40	97.56%					
Não	1	2.44%					
Total	**41**	**100 %**					

Qual é o tipo de informação processada pela organização?



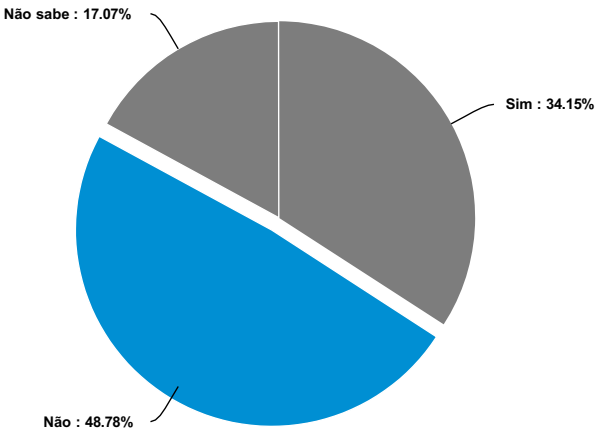
Resposta	Contagem	Percentagem
Dados bancários de colaboradores	22	14.47%
Dados bancários de fornecedores	19	12.5%
Dados empresariais de clientes	31	20.39%
Dados empresariais de fornecedores	21	13.82%
Dados Pessoais de colaboradores	30	19.74%
Dados Pessoais clientes	25	16.45%
Não sabe	4	2.63%
Total	**152**	**100 %**

A sua empresa tem algum seguro contratado para cobrir incidentes de segurança?



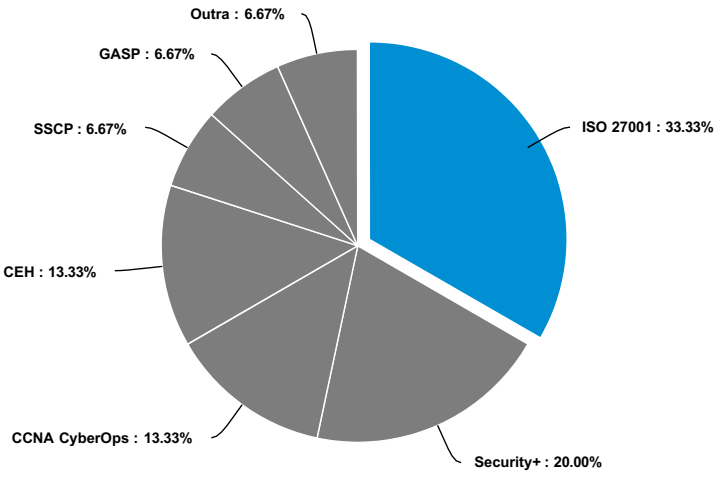
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	10	24.39%					
Não	13	31.71%					
Não sabe	18	43.9%					
Total	**41**	**100 %**					

A sua empresa tem colaboradores certificados na área de Cibersegurança?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	14	34.15%					
Não	20	48.78%					
Não sabe	7	17.07%					
Total	**41**	**100 %**					

Qual(is) das seguintes certificações possi(uem) os colaboradores ou a organização?

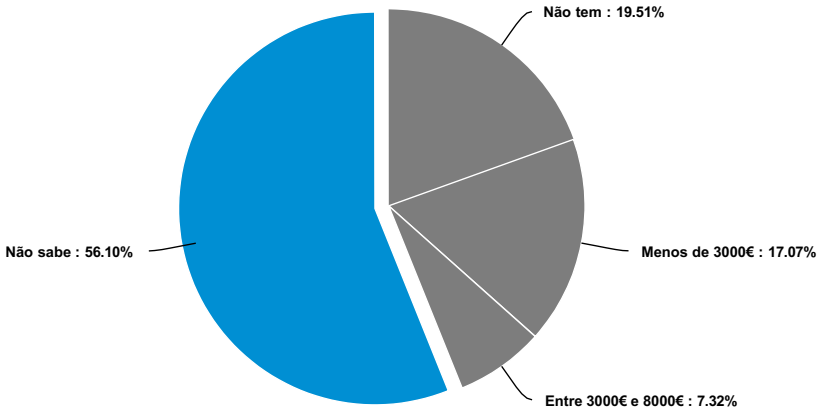


Resposta	Contagem	Percentagem
ISO 27001	5	33.33%
Security+	3	20%
CCNA CyberOps	2	13.33%
CISSP	0	0%
Lead Auditor	0	0%
CEH	2	13.33%
GSEC	0	0%
SSCP	1	6.67%
GASP	1	6.67%
GCIH	0	0%
OSCP	0	0%
Outra	1	6.67%
Total	**15**	**100 %**

Qual(is) das seguintes certificações possi(uem) os colaboradores ou a organização? - Text Data for Outra

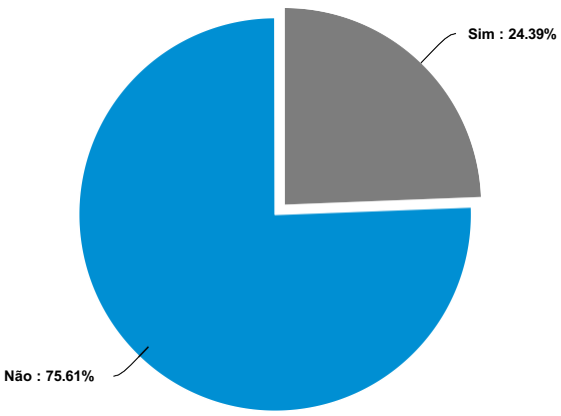
08/24/2022	82747961 Não sei

Qual o orçamento anual para investir em Cibersegurança:



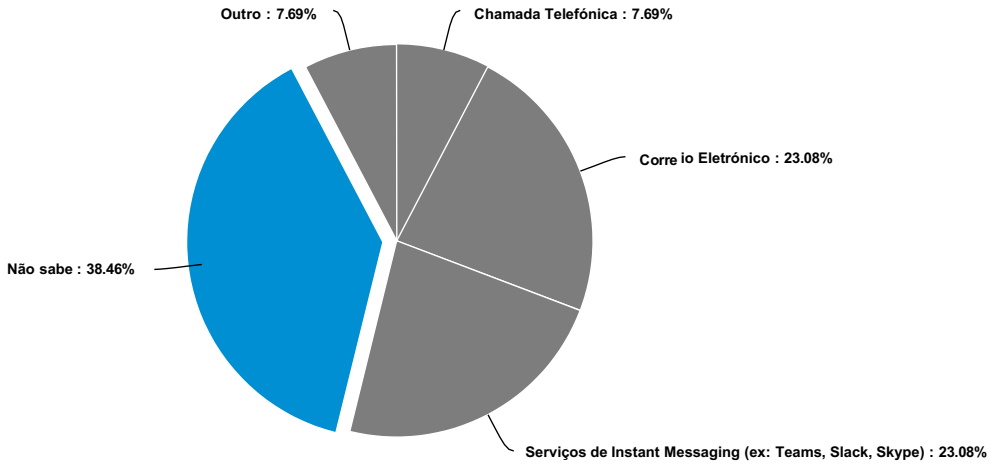
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Não tem	8	19.51%					
Menos de 3000€	7	17.07%					
Entre 3000€ e 8000€	3	7.32%					
Entre 8001€ e 15000€	0	0%					
Mais de 20000€	0	0%					
Não sabe	23	56.1%					
Total	**41**	**100 %**					

Está definida uma forma de comunicação com o CNCS?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	10	24.39%					
Não	31	75.61%					
Total	**41**	**100 %**					

Quais são os canais de comunicação que estão definidos com o CNCS?

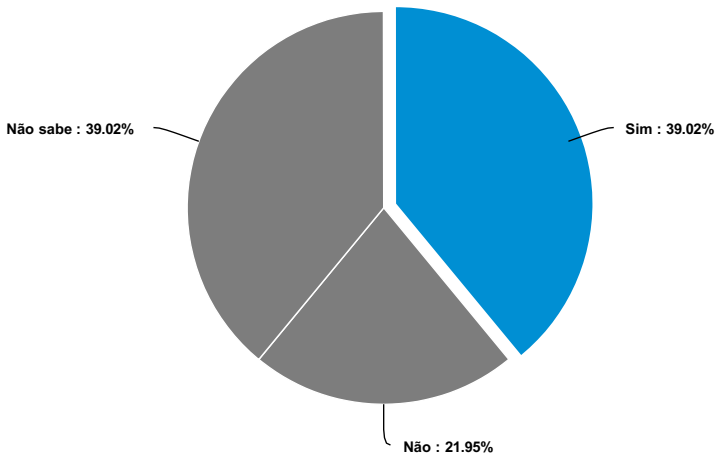


Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Chamada Telefónica	1	7.69%					
Correio Eletrónico	3	23.08%					
PGP	0	0%					
Serviços de Instant Messaging (ex: Teams, Slack, Skype)	3	23.08%					
Não sabe	5	38.46%					
Outro	1	7.69%					
Total	**13**	**100 %**					

Quais são os canais de comunicação que estão definidos com o CNCS? - Text Data for Outro

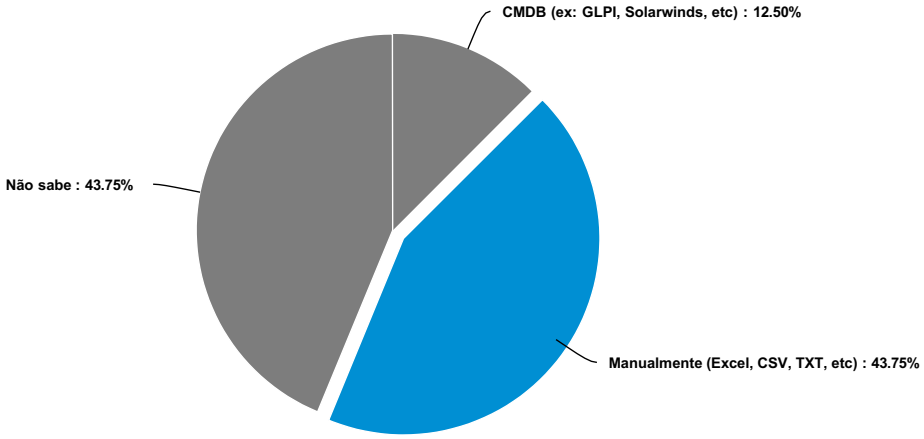
08/19/2022 82369571 O CNCS colabora regularmente com a associação

Existe um inventário de ativos e serviços críticos da organização?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	16	39.02%					
Não	9	21.95%					
Não sabe	16	39.02%					
Total	**41**	**100 %**					

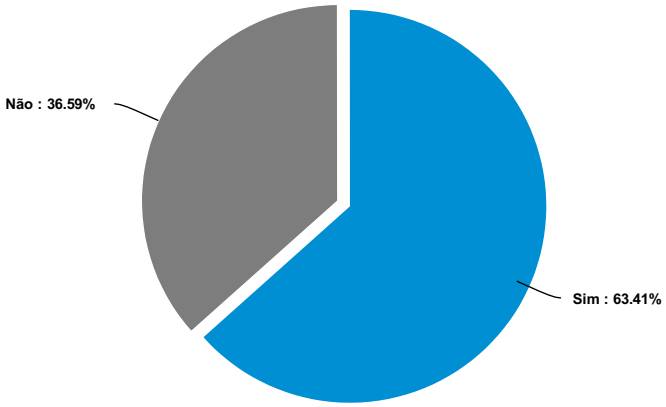
De que forma é feita a inventariação dos ativos?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
CMDB (ex: GLPI, Solarwinds, etc)	2	12.5%					
Manualmente (Excel, CSV, TXT, etc)	7	43.75%					
Não sabe	7	43.75%					
Outra	0	0%					
Total	**16**	**100 %**					

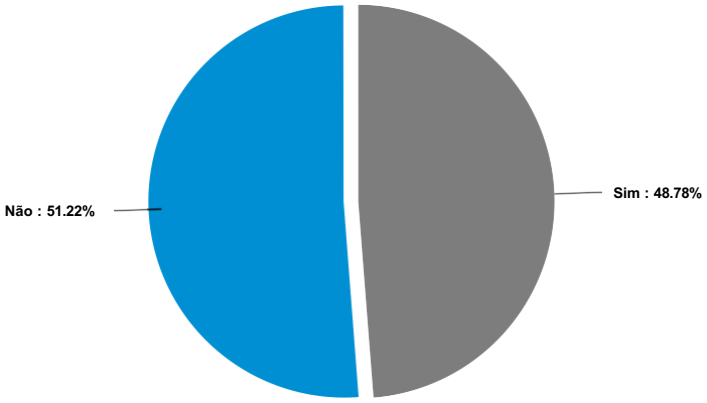
De que forma é feita a inventariação dos ativos? - Text Data for Outra

Os ativos da organização são encriptados?



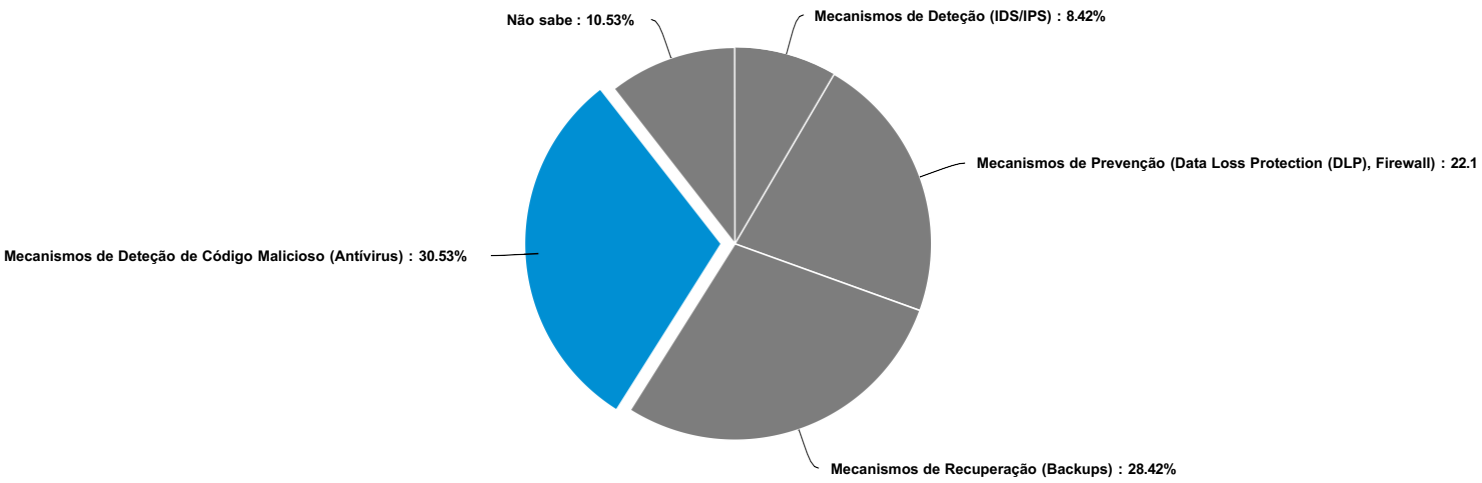
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	26	63.41%					
Não	15	36.59%					
Total	**41**	**100 %**					

São efetuados testes de penetração aos ativos da organização?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	20	48.78%					
Não	21	51.22%					
Total	**41**	**100 %**					

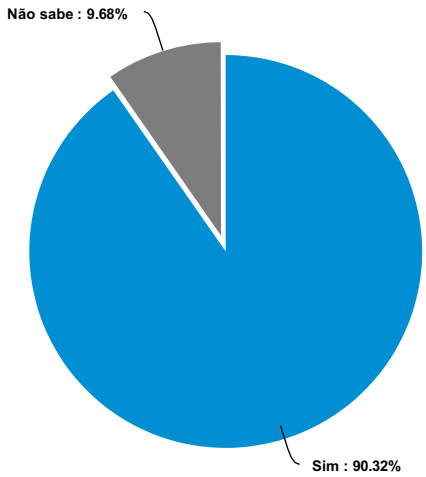
Quais das seguinte soluções de segurança estão disponíveis na organização para lidar com possíveis ameaças?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Mecanismos de Deteção (IDS/IPS)	8	8.42%					
Mecanismos de Prevenção (Data Loss Protection (DLP), Firewall)	21	22.11%					
Mecanismos de Recuperação (Backups)	27	28.42%					
Mecanismos de Deteção de Código Malicioso (Antívirus)	29	30.53%					
Não sabe	10	10.53%					
Outro	0	0%					
Total	**95**	**100 %**					

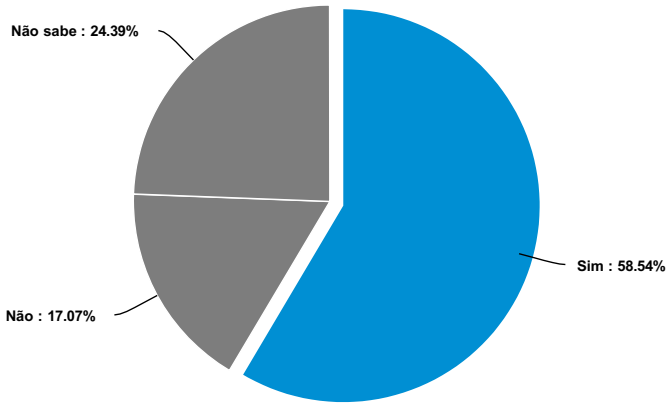
Quais das seguinte soluções de segurança estão disponíveis na organização para lidar com possíveis ameaças? - Text Data for Outro

As soluções de segurança indicadas na questão anterior são utilizadas nos sistemas e postos de trabalho onde é tratada informação crítica?



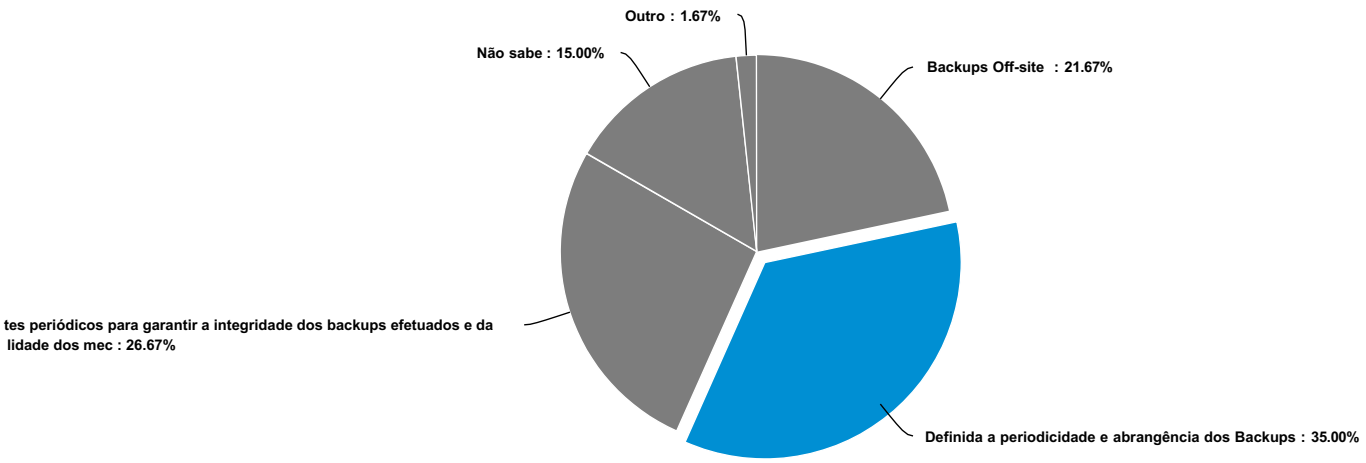
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	28	90.32%					
Não	0	0%					
Não sabe	3	9.68%					
Total	**31**	**100 %**					

Na organização é utilizada alguma tecnologia com a capacidade de analisar tráfego malicioso?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	24	58.54%					
Não	7	17.07%					
Não sabe	10	24.39%					
Total	**41**	**100 %**					

Quais dos seguintes procedimentos de backup/restore estão implementados na organização?

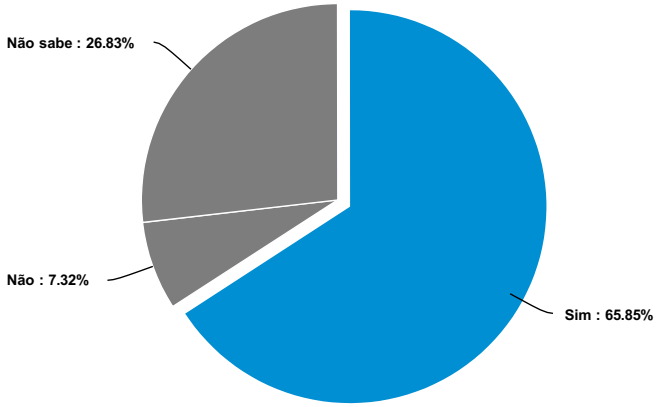


Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Backups Off-site	13	21.67%					
Definida a periodicidade e abrangência dos Backups	21	35%					
Testes periódicos para garantir a integridade dos backups efetuados e da qualidade dos mecanismos de reposição	16	26.67%					
Não sabe	9	15%					
Outro	1	1.67%					
Total	**60**	**100 %**					

Quais dos seguintes procedimentos de backup/restore estão implementados na organização? - Text Data for Outro

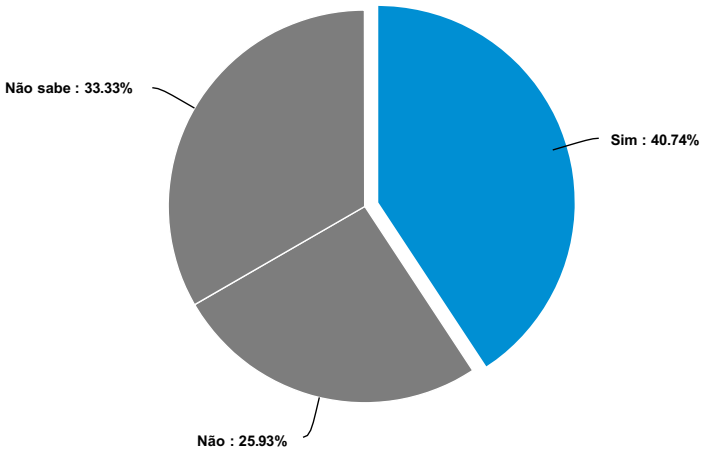
09/15/2022 85511986 Antivírus

A organização é conhecedora dos quadros legais e regulatórios a que está sujeita (nacionais e europeus)?



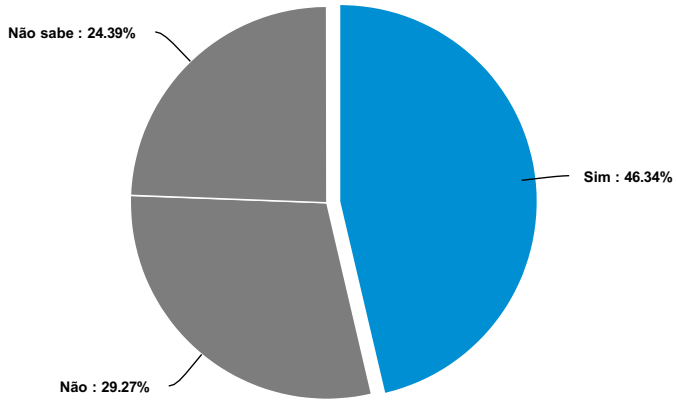
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	27	65.85%					
Não	3	7.32%					
Não sabe	11	26.83%					
Total	**41**	**100 %**					

Existem relatórios de auditorias que comprovem a conformidade com a legislação e regulamentação?



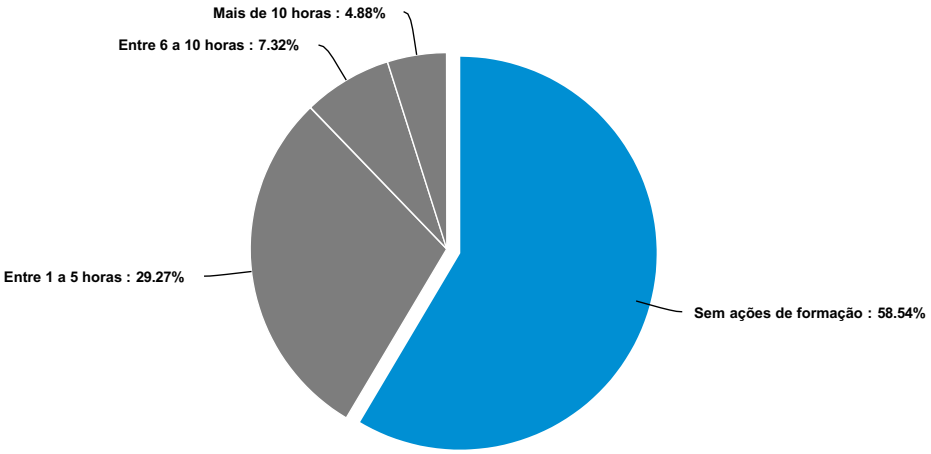
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	11	40.74%					
Não	7	25.93%					
Não sabe	9	33.33%					
Total	**27**	**100 %**					

É efetuado o registo de eventos como logs e atividades de utilizadores?



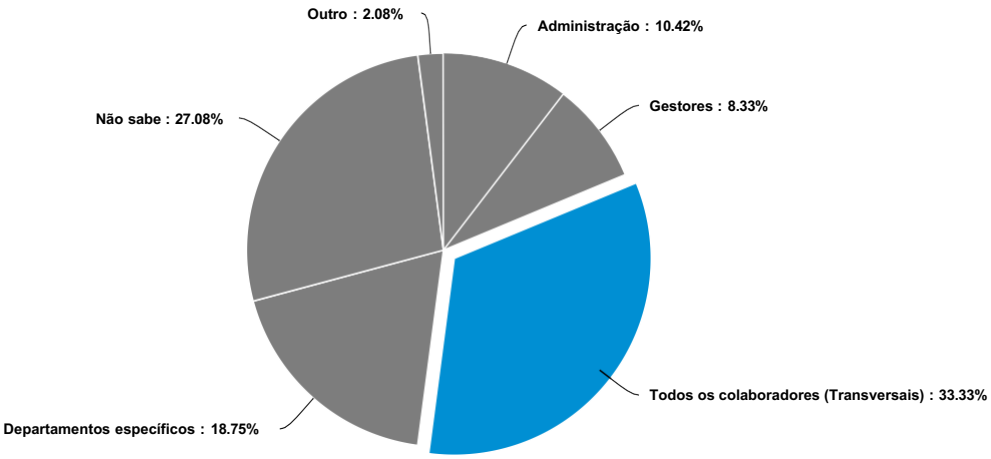
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	19	46.34%					
Não	12	29.27%					
Não sabe	10	24.39%					
Total	**41**	**100 %**					

Qual o número de horas de ações de formação e sensibilização de colaboradores em matéria de Cibersegurança na organização?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sem ações de formação	24	58.54%					
Entre 1 a 5 horas	12	29.27%					
Entre 6 a 10 horas	3	7.32%					
Mais de 10 horas	2	4.88%					
Total	**41**	**100 %**					

A quem se destinam estas ações de formação disponibilizadas na organização?

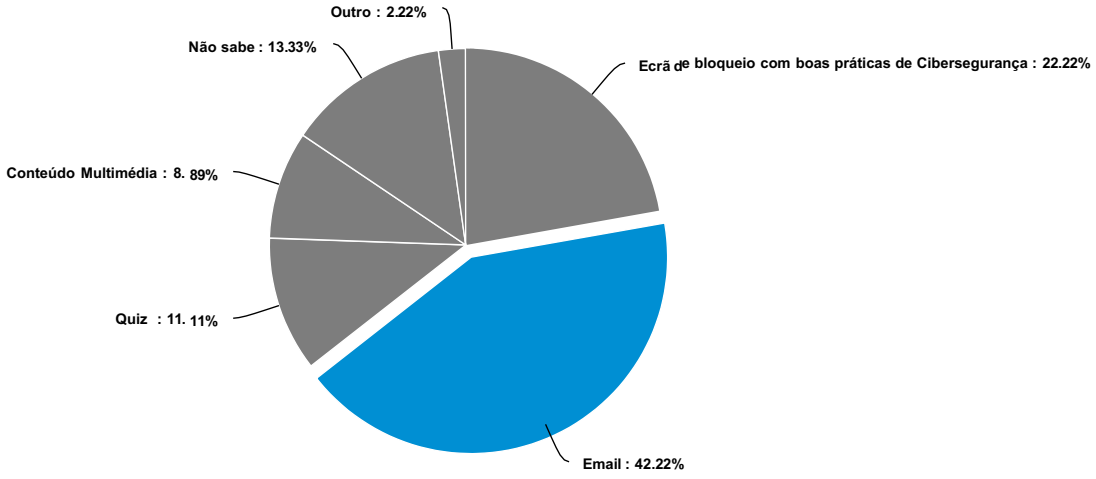


Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Administração	5	10.42%					
Gestores	4	8.33%					
Todos os colaboradores (Transversais)	16	33.33%					
Departamentos específicos	9	18.75%					
Não sabe	13	27.08%					
Outro	1	2.08%					
Total	**48**	**100 %**					

A quem se destinam estas ações de formação disponibilizadas na organização? - Text Data for Outro

08/24/2022	82696542	Ninguém

Na organização são utilizados alguns dos seguintes lembretes relativamente a boas praticas de Cibersegurança?

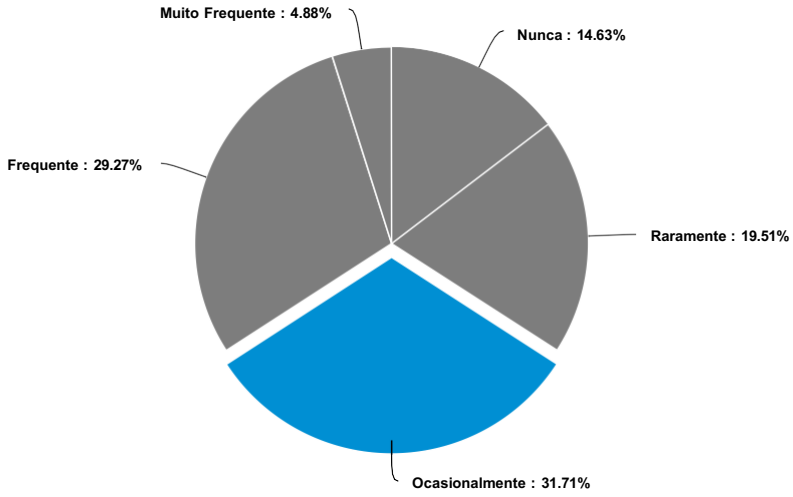


Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Ecrã de bloqueio com boas práticas de Cibersegurança	10	22.22%					
Email	19	42.22%					
Quiz	5	11.11%					
Conteúdo Multimédia	4	8.89%					
Não sabe	6	13.33%					
Outro	1	2.22%					
Total	**45**	**100 %**					

Na organização são utilizados alguns dos seguintes lembretes relativamente a boas praticas de Cibersegurança? - Text Data for Outro

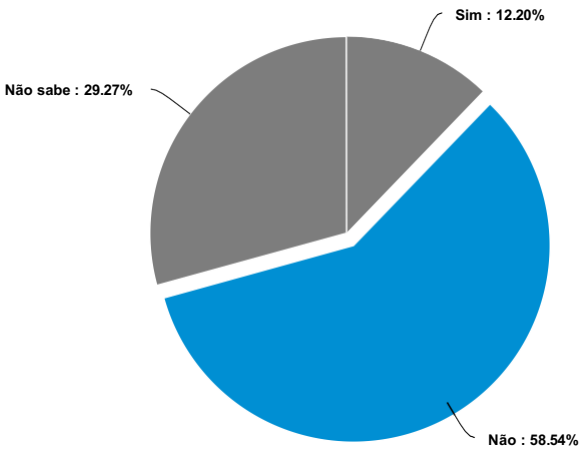
08/29/2022	83028385	envio de m-email de phising interno para testes

Com que regularidade são auditadas as configurações dos dispositivos?



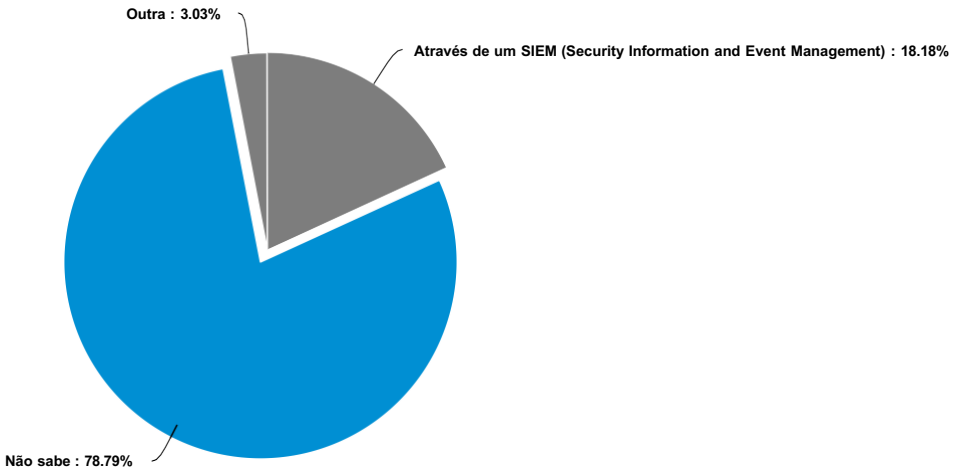
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Nunca	6	14.63%					
Raramente	8	19.51%					
Ocasionalmente	13	31.71%					
Frequente	12	29.27%					
Muito Frequente	2	4.88%					
Total	**41**	**100 %**					

A organização tem uma política BYOD (Gestão de Dispositivos Móveis Pessoais)?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	5	12.2%					
Não	24	58.54%					
Não sabe	12	29.27%					
Total	**41**	**100 %**					

De que forma é feita a gestão de eventos de segurança?

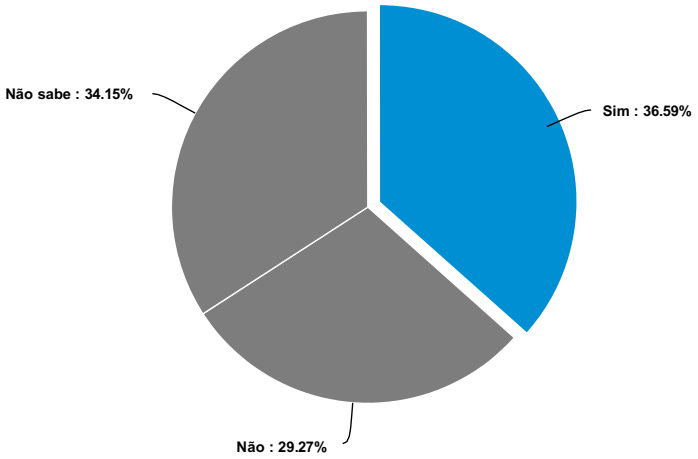


Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Através de um SIEM (Security Information and Event Management)	6	18.18%					
Não sabe	26	78.79%					
Outra	1	3.03%					
Total	**33**	**100 %**					

De que forma é feita a gestão de eventos de segurança? - Text Data for Outra

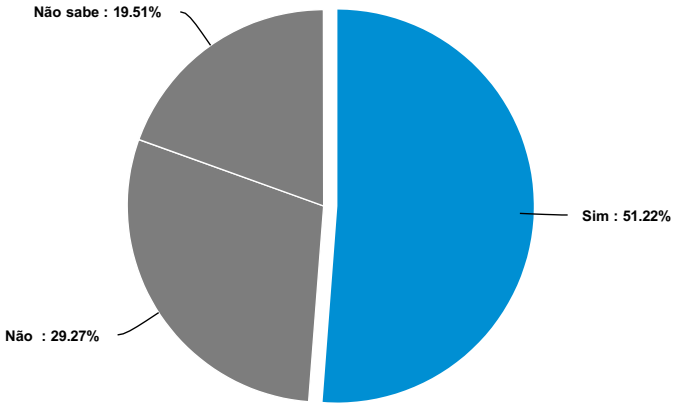
09/15/2022 85511986 Empresa de informática

Existe algum sistema de monitorização dos principais ativos de rede e sistemas que dão suporte às atividades da organização?



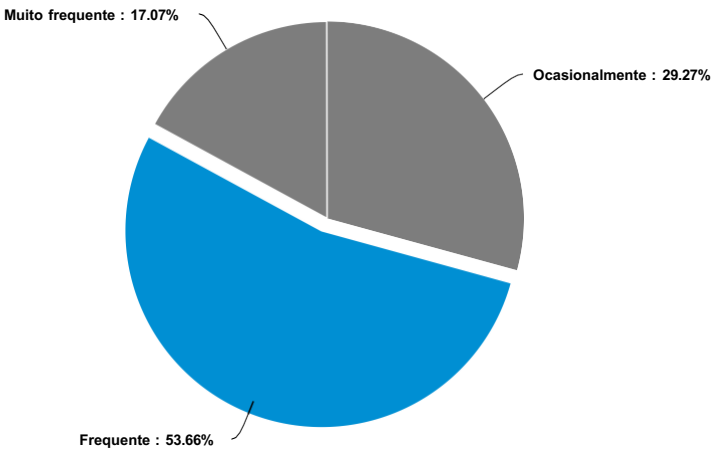
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	15	36.59%					
Não	12	29.27%					
Não sabe	14	34.15%					
Total	**41**	**100 %**					

Os colaboradores têm conhecimento de como utilizar informação crítica?



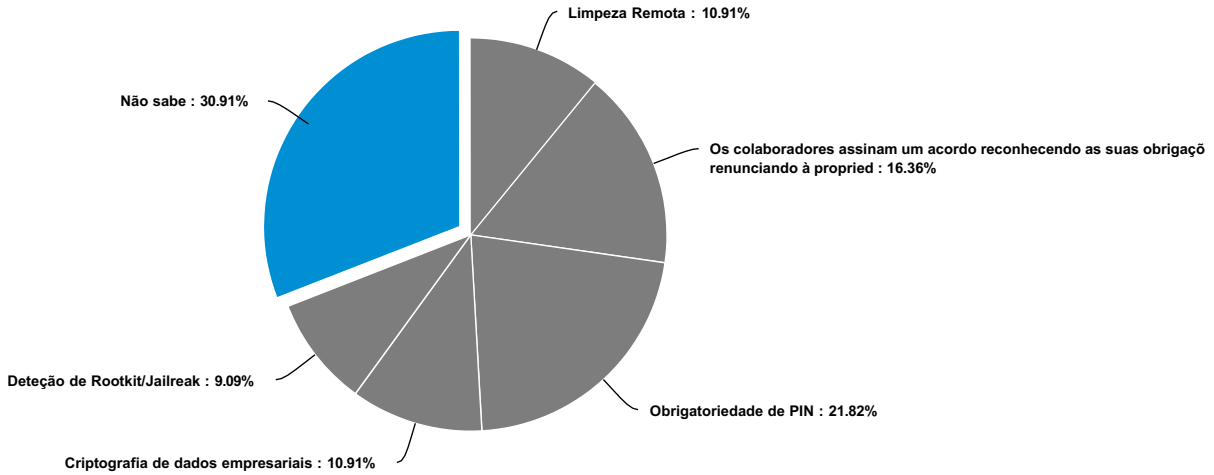
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	21	51.22%					
Não	12	29.27%					
Não sabe	8	19.51%					
Total	**41**	**100 %**					

Com que regularidade são feitas as atualizações de software?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Nunca	0	0%					
Raramente	0	0%					
Ocasionalmente	12	29.27%					
Frequente	22	53.66%					
Muito frequente	7	17.07%					
Total	**41**	**100 %**					

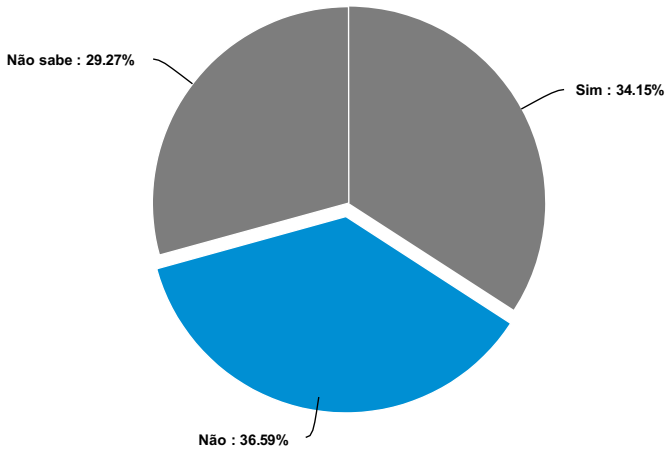
Quais os procedimentos de segurança que estão definidos na política de dispositivos móveis?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Limpeza Remota	6	10.91%					
Os colaboradores assinam um acordo reconhecendo as suas obrigações, renunciando à propriedade de dados de negócio	9	16.36%					
Obrigatoriedade de PIN	12	21.82%					
Criptografia de dados empresariais	6	10.91%					
Deteção de Rootkit/Jailreak	5	9.09%					
Não sabe	17	30.91%					
Outro	0	0%					
Total	**55**	**100 %**					

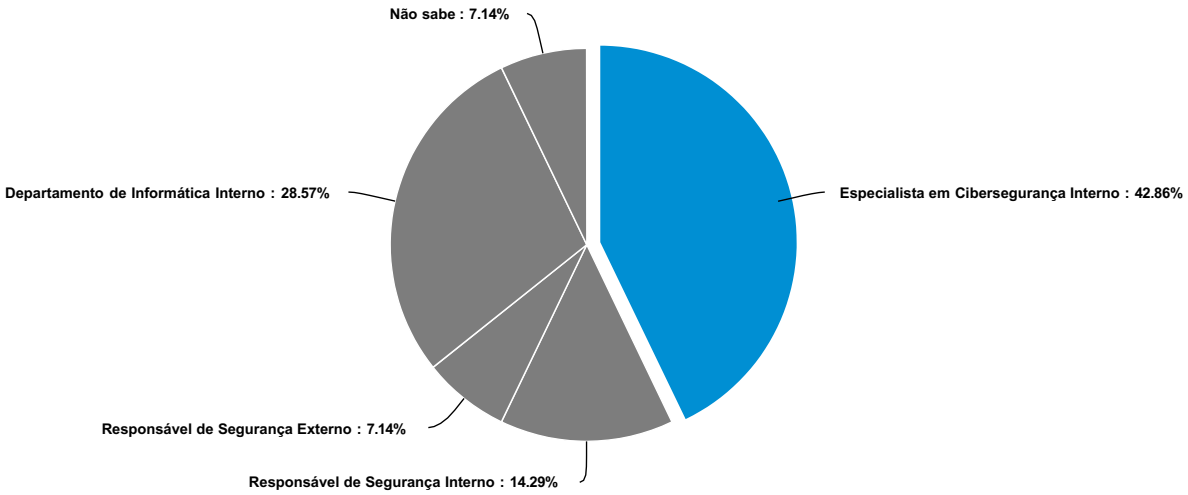
Quais os procedimentos de segurança que estão definidos na política de dispositivos móveis? - Text Data for Outro

Antes da entrada em produção, os sistemas e aplicações são submetidos a testes de cibersegurança?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	14	34.15%					
Não	15	36.59%					
Não sabe	12	29.27%					
Total	**41**	**100 %**					

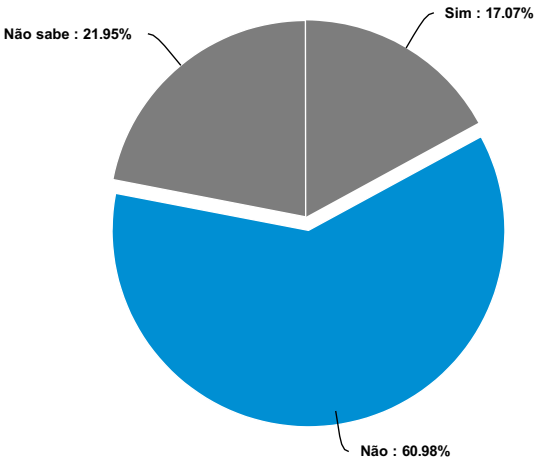
Por quem são efetuados os testes de cibersegurança indicados na questão anterior?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Especialista em Cibersegurança Interno	6	42.86%					
Especialista em Cibersegurança Externo	0	0%					
Responsável de Segurança Interno	2	14.29%					
Responsável de Segurança Externo	1	7.14%					
Departamento de Informática Interno	4	28.57%					
Não sabe	1	7.14%					
Outro	0	0%					
Total	**14**	**100 %**					

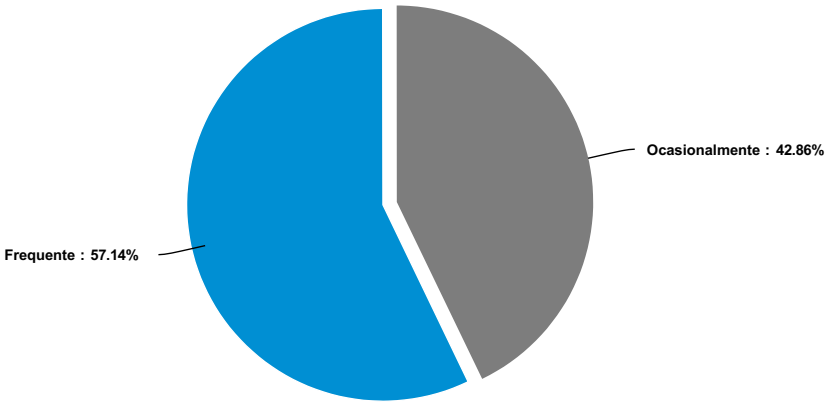
Por quem são efetuados os testes de cibersegurança indicados na questão anterior? - Text Data for Outro

Já foi efetuado algum simulacro de Cibersegurança na organização?



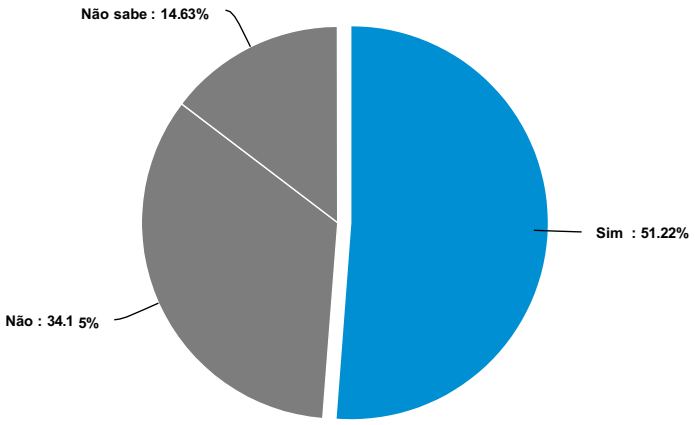
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	7	17.07%					
Não	25	60.98%					
Não sabe	9	21.95%					
Total	**41**	**100 %**					

Com que frequência são efetuados estes simulacros?



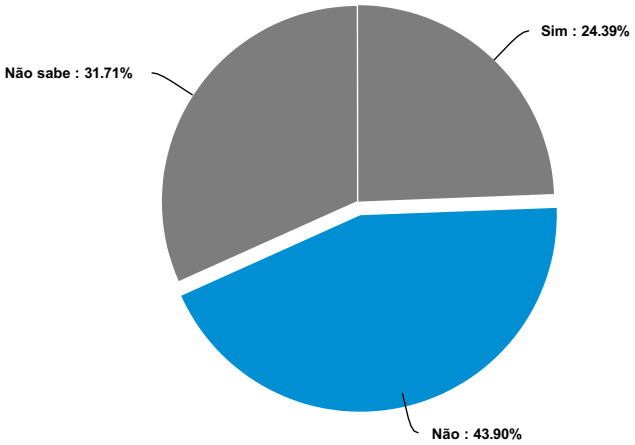
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Nunca	0	0%					
Raramente	0	0%					
Ocasionalmente	3	42.86%					
Frequente	4	57.14%					
Muito frequente	0	0%					
Total	**7**	**100 %**					

Existe uma equipa capaz de dar resposta a incidentes de cibersegurança na sua organização?



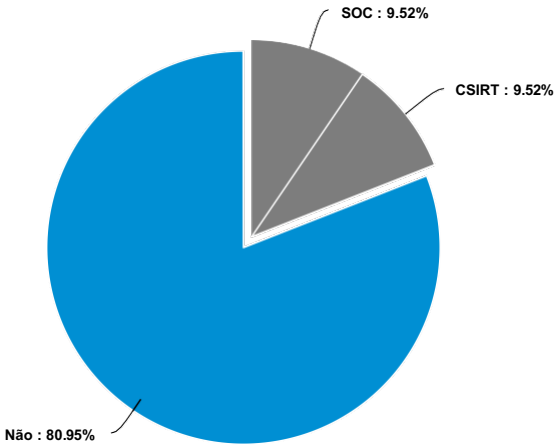
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	21	51.22%					
Não	14	34.15%					
Não sabe	6	14.63%					
Total	**41**	**100 %**					

Foi nomeado um (Responsável de Segurança de Informação) CISO na organização?



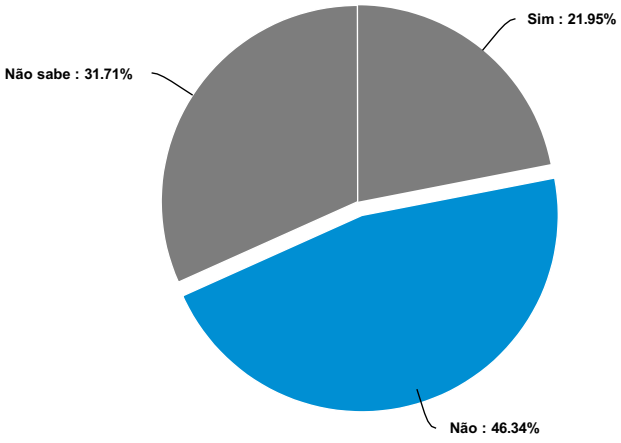
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	10	24.39%					
Não	18	43.9%					
Não sabe	13	31.71%					
Total	**41**	**100 %**					

A organização possui algum destes serviços?



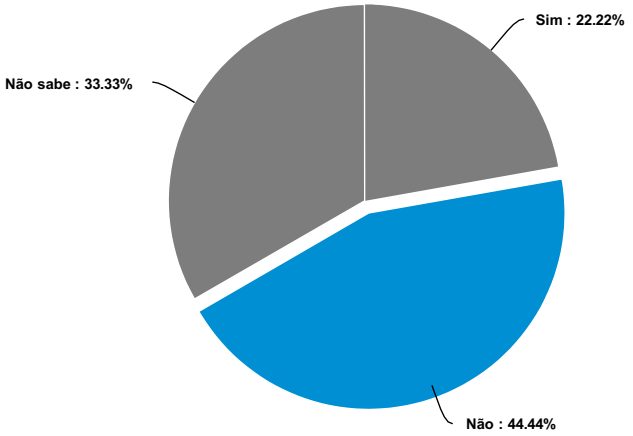
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
SOC	4	9.52%					
CSIRT	4	9.52%					
Não	34	80.95%					
Total	**42**	**100 %**					

Alguma vez a organização foi alvo de um ataque informático?



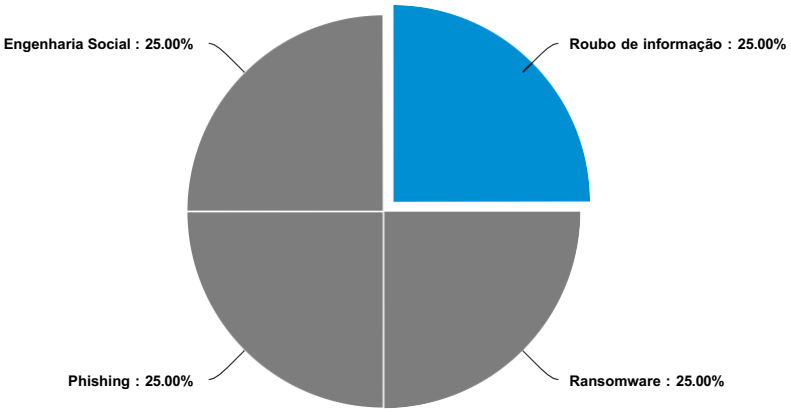
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	9	21.95%					
Não	19	46.34%					
Não sabe	13	31.71%					
Total	**41**	**100 %**					

Estes ataques foram documentados?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	2	22.22%					
Não	4	44.44%					
Não sabe	3	33.33%					
Total	**9**	**100 %**					

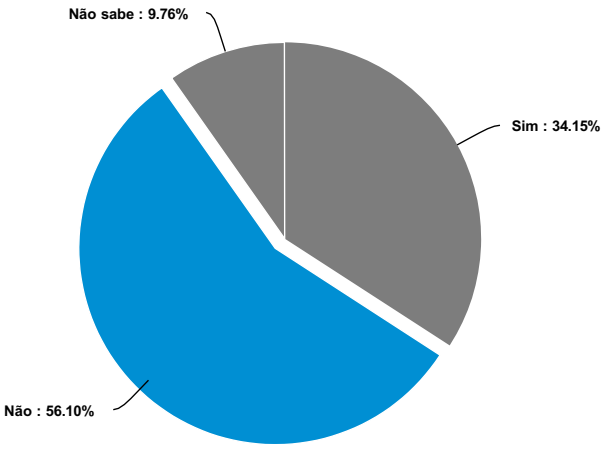
Que tipo(s) de ataque sofreu?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
DDoS	0	0%					
Roubo de informação	1	25%					
Ransomware	1	25%					
Phishing	1	25%					
Engenharia Social	1	25%					
Não sabe	0	0%					
Outro	0	0%					
Total	4	100 %					

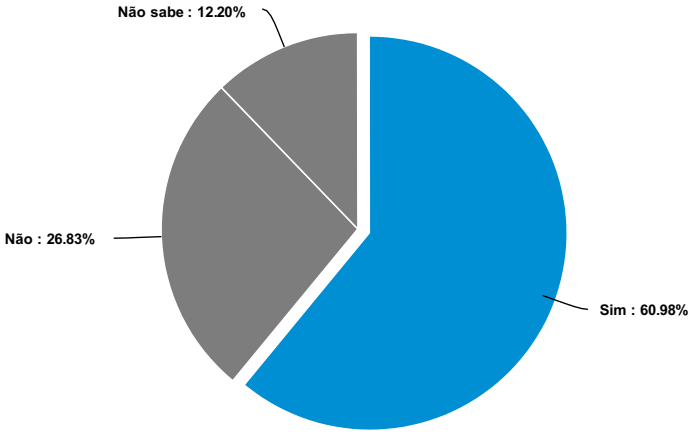
Que tipo(s) de ataque sofreu? - Text Data for Outro

Considera que qualquer colaborador sabe como atuar em caso de ataque informático?



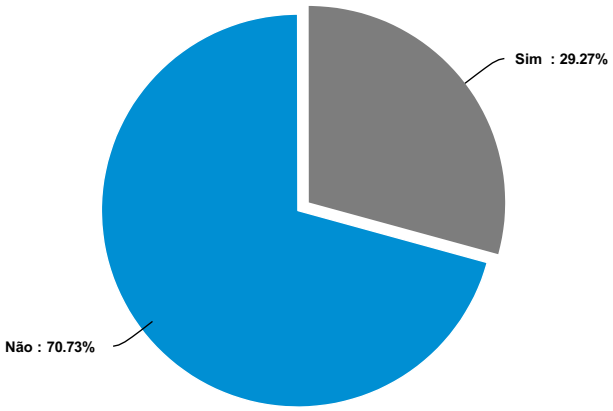
Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	14	34.15%					
Não	23	56.1%					
Não sabe	4	9.76%					
Total	**41**	**100 %**					

Existe um processo para que todos os colaboradores possam reportar possíveis incidentes de segurança?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	25	60.98%					
Não	11	26.83%					
Não sabe	5	12.2%					
Total	**41**	**100 %**					

O e-mail facultado será apenas utilizado para posterior envio de relatório com a análise da maturidade obtida através das respostas dadas. Pretende que lhe seja posteriormente enviado um relatório de maturidade da organização via e-mail?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
Sim	12	29.27%					
Não	29	70.73%					
Total	**41**	**100 %**					

Forneça por favor, o e-mail que pretende receber o relatório de maturidade de Cibersegurança:

D E C L A R A Ç Ã O

Declaro, sob compromisso de honra, que o trabalho apresentado nesta dissertação, com o título *"AVALIAÇÃO DA MATURIDADE EM CIBERSEGURANÇA DO TECIDO INDUSTRIAL PORTUGUÊS"*, é original e foi realizado por Ana Beatriz Nunes Ribeiro (2202642) sob orientação de Professor Doutor Carlos Manuel da Silva Rabadão (carlos.rabadao@ipleiria.pt) e Professor Doutor Leonel Filipe Simões Santos (leonel.santos@ipleiria.pt).

Assinado por: **ANA BEATRIZ NUNES RIBEIRO**
Num. de Identificação: 14843656
Data: 2023.06.13 09:26:57+01'00'

Leiria, Março de 2023

Ana Beatriz Nunes Ribeiro