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

DESENVOLVIMENTO DE UMA METODOLOGIA PARA AVALIAÇÃO DO ESTADO DA SEGURANÇA INFORMÁTICA EM PME

BRUNO FILIPE DIOGO AZINHEIRA

Leiria, Junho de 2022

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

DESENVOLVIMENTO DE UMA METODOLOGIA PARA AVALIAÇÃO DO ESTADO DA SEGURANÇA INFORMÁTICA EM PME

BRUNO FILIPE DIOGO AZINHEIRA
Número: 2200331

Projeto realizado sob orientação do professor Doutor Mário Antunes, (mario.antunes@ipleiria.pt), da professora Doutora Marisa Maximiano, (marisa.maximiano@ipleiria.pt) e do professor Ricardo Gomes (ricardo.p.gomes@ipleiria.pt)

Leiria, Junho de 2022

AGRADECIMENTOS

No decorrer da realização deste projeto, foram celebradas várias reuniões formais de trabalho com periodicidade semanal, ou por vezes quinzenal com os professores Mário Antunes, Marisa Maximiano e Ricardo Gomes cujo contributo e acompanhamento dos mesmos foi bastante positivo, sendo até crucial para a constante motivação e empenho ao longo da sua realização até ao término efetivo do projeto. Assim sendo o meu muito obrigado aos professores pela dedicação, atenção e ajuda dispensada.

Aos meus familiares diretos, pela paciência e apoio dado durante a realização deste trabalho pois sem eles a realização deste projeto também não seria possível. Agradeço o reconhecimento por nunca duvidarem das minhas capacidades e sempre acreditarem que terminaria o projeto.

À minha entidade patronal que desde sempre estiveram ao meu lado, sem duvidar facilitando sempre que necessário a realização deste projeto, um grande bem haja.

A todos os que não estão acima referidos mas contribuíram de alguma forma para que fosse possível a realização deste projeto até ao fim, o meu muito obrigado!

RESUMO

A digitalização e a implantação dos conceitos de Indústria 4.0 são emergentes e desafiadores para as pequenas e médias empresas (PME). Os benefícios são evidentes para as empresas pois os seus processos de negócio tornam-se mais simplificados, com melhorias significativas na internacionalização, penetração nos mercados globais e confiança a novos parceiros de negócio.

No entanto, aumentam as preocupações relativas à segurança da informação e cibersegurança nas PME devendo assim serem aplicadas melhores práticas e regulamentos de conformidade. Este projeto descreve uma metodologia para o mapeamento do Roteiro de Capacidades Mínimas de Cibersegurança (RCMCS) facultado pelo Centro Nacional de Cibersegurança (CNCS), com as sugestões da norma internacional ISO 27001:2013. Este mapeamento é orientado às características das PME e permite às organizações avaliarem os seus riscos relativamente à segurança cibernética, com o intuito que sejam mitigadas as falhas identificadas.

O principal foco deste projeto é a metodologia desenvolvida que correlaciona as ações do Roteiro de Capacidades Mínimas de Cibersegurança com os controlos da norma ISO 27001:2013, justificando essas correlações as questões apresentadas às organizações em formato de questionário para levantamento de riscos cibernéticos.

Neste relatório é apresentado um caso de estudo com resultados obtidos numa amostra de 17 PME da região centro de Portugal, inquiridas através do questionário implementado, por forma a concluir se essas organizações estariam seguras.

Com esta metodologia desenvolvida é possível interligar o mundo da cibersegurança com a realidade empresarial, neste caso específico PME, concluindo assim que será uma mais valia a sua utilização para a análise do seu estado de cibersegurança.

Palavras-chave: Segurança da Informação, Roteiro de Capacidades Mínimas de Cibersegurança, Pequenas e Médias Empresas

ABSTRACT

The digitalization of companies and the implementation of Industry 4.0 concepts are emerging and challenging for small and medium-sized enterprises (SME). The benefits are evident for companies as their business processes become more simplified, with significant improvements in internationalization, global market penetration and confidence in new business partners . However, concerns about information security and cybersecurity in SME increase and therefore best practices and compliance regulations must be applied. This project describes a methodology for mapping the Minimum Cybersecurity Capabilities Roadmap (RCMCS) provided by the National Cybersecurity Center (CNCS), with the suggestions of the international standard ISO 27001:2013. This mapping is oriented to the characteristics of SMEs and allows organizations to assess their cybersecurity risks, with the aim of mitigating the identified flaws.

The main focus of this project is the methodology developed that correlates the actions of the Minimum Cybersecurity Capabilities Roadmap with the controls of the ISO 27001:2013 standard, these correlations are the basis for the creation of a questionnaire to survey cyber risks in organizations.

This report presents a case study with results obtained from a sample of 17 SME in the central region of Portugal, surveyed through the implemented questionnaire, in order to conclude whether these organizations would be safe.

With this developed methodology, it is possible to interconnect the cybersecurity world with the business reality of SME, concluding that its use for the analysis of their cybersecurity status will be an asset.

Keywords: Information Security, Roadmap of Minimum Capacities of Cybersecurity, Small and Medium Enterprises

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÓNIMOS

CERT	Computer Emergency Response Team.
CIS	Critical Security Controls.
CISO	Chief information security officer.
CNCS	Centro Nacional de Cibersegurança.
CSIRT	Computer Security Incident Response Team.
ENISA	European Union Agency for Cybersecurity.
INE	Instituto Nacional de Estatística.
IP	Internet Protocol.
IRT	Incident Response Team.
ISO	International Organization for Standardization.
LIR	Local Internet Registry.
MCSR	Mandatory cyber security controls.
NIST	National Institute of Standards and Technology.
PDCA	Plan-Do-Check-Act.
PGP	Pretty Good Privacy.
PME	Pequenas e Médias Empresas.
PUA	Política de uso aceitável.
QNRCS	Quadro Nacional de Referência para a Cibersegurança.

RCMCS	Roteiro de Capacidades Mínimas de Cibersegurança.
RGPD	Regime Geral de Proteção de Dados.
SGSI	Sistema de Gestão de Segurança da Informação.
SINP	Sistema Interno de Normas e Políticas.
SOC	Security Operations Centre.
TI	Tecnologias de Informação.
TIC	Tecnologias de Informação e Comunicação.
UE	União Europeia.
VPN	Virtual Private Network.

1

INTRODUÇÃO

A segurança da informação e a consciência da necessidade de investimento em cibersegurança numa organização aumentaram, à medida que os ataques às empresas e infraestruturas críticas aumentam à escala global [1] [2]. No entanto, a adoção de medidas eficazes como a conformidade com as melhores práticas internacionais e normas devidamente credenciadas estão longe de ser implementadas.

Nesse sentido, as características específicas das Pequenas e Médias Empresas (PME), nomeadamente o seu tamanho, âmbito regional e familiar e recursos financeiros restritos, torna-as mais vulneráveis no que se trata de segurança cibernética e segurança da informação.

Nos últimos anos, um grande número de diretrizes, *frameworks*, normas e boas práticas foram disponibilizadas por organizações de renome, nomeadamente a União Europeia (através da Agência Europeia para a Segurança das Redes e da Informação - ENISA), os consórcios de normas e *frameworks* (como ISO e NIST) e instituições governamentais nacionais. Em Portugal, o Centro Nacional de Cibersegurança (CNCS) fornece uma coletânea abrangente de conselhos e boas práticas, como roteiros e *frameworks*, direcionadas para indivíduos e empresas. Esses documentos abrangem as diretrizes Europeias e estão preparados para aplicação ao contexto económico e de negócios dos Portugueses.

A disponibilização de recursos na Internet de carácter malicioso que facilita na aprendizagem de como realizar certo tipo de ataques, muitas vezes de forma bastante simplista e sem necessidade de grandes conhecimentos, é preocupante para quem está a administrar sistemas de informação.

De igual forma o crescente interesse neste tipo de área por ser bastante proveitoso em termos monetários, quando são efetuados ataques, burlas a pessoas desprevenidas, todos os conselhos, ferramentas e metodologias com foco a proteger uma empresa de riscos de cibersegurança são bem vindas.

O desenvolvimento desta metodologia apresentada no âmbito do Projeto final do Mestrado em Cibersegurança e Informática Forense, na Escola Superior de Tecnolo-

gias e Gestão, pretende ser um bom ponto de partida para as PME que pretendem avaliar o risco em cibersegurança e melhorar algumas das falhas identificadas.

1.1 OBJETIVOS

Um Sistema de Gestão de Segurança da Informação (SGSI) tem como foco a garantia de confidencialidade, integridade e disponibilidade da informação do negócio [3], tentando assim mitigar riscos e resultados negativos, como paragens prolongadas em caso de ataques ou até colocar em causa a continuidade do negócio [4].

Pelos motivos acima descritos, complementando com a premissa de garantia de efetividade da segurança dos dados numa organização implementando um SGSI, foi desenvolvida uma metodologia. Este desenvolvimento parte com o objetivo de tentar de auxiliar e dotar as PME com os princípios e mecanismos mínimos de cibersegurança e segurança de informação, seja numa vertente humana, processos e organizacional.

Esta metodologia, tem como principal objetivo identificar os pontos de convergência entre o Roteiro de Capacidades Mínimas de Cibersegurança e a norma ISO 27001:2013, identificando a correlação entre as ações do roteiro e da norma da ISO em estudo. Essas correlações dão assim origem a questões que irão integrar o questionário para análise do estado da cibersegurança da organização, tendo em consideração o contexto das PME.

Este questionário gerado, destina-se à utilização não apenas a auditores de segurança de informação mas também pode ser utilizado por gestores, responsáveis pela informática e outros que, tenham uma visão alargada do estado da empresa relativamente ao tema em questão.

1.2 CRONOLOGIA DE DESENVOLVIMENTO DO PROJETO

A realização deste projeto consistiu numa sequência de fases como está demonstrado na Figura 1. Estas fases têm um espaço temporal associado para o alcance pretendido, a finalização do mesmo, tendo início no mês de Outubro do ano de 2021, passo a passo com trabalho constante para a efetiva realização do projeto com sucesso, terminando assim dentro do prazo inicialmente estabelecido, neste caso em Maio de 2022.

O processo de desenvolvimento do projeto (ver Figura 1) teve início com a fase de estudo do Roteiro de Capacidades Mínimas de Cibersegurança e das normas que potencialmente poderiam vir a ser consideradas no projeto, escolhendo a norma ISO 27001:2013 após levantamento de pós e contras. Seguindo a fase posterior de identificação das correlações entre ações do roteiro e controlos da norma, foi implementado o questionário e enviado para as empresas preencherem. Para finalizar foi efetuada a análise de resultados e justificados os resultados obtidos.

Relativamente ao relatório, foi sendo desenvolvido em paralelo com todas as fases, documentando para além do que foi estudado, os passos seguidos não só na criação da metodologia mas da implementação da mesma. No final, foi completado o relatório e submetido para avaliação.

Figura 1: Diagrama temporal da realização do projeto

1.3 ESTRUTURA DO DOCUMENTO

No Capítulo 2 serão apresentados alguns conceitos relevantes abordados durante o documento, tais como um resumo do Roteiro de Capacidades Mínimas de Cibersegurança [5], roteiro este desenvolvido pelo Centro Nacional de Cibersegurança (CNCS) definindo um modelo para melhoria de processos virados para a cibersegurança, acima de tudo das PME (Pequenas e Médias Empresas). De igual forma, foi efetuado um resumo relativo à norma ISO 27001:2013, norma esta utilizada também no

desenvolvimento desta metodologia criada, tais como também serão apresentados trabalhos de certa forma relacionados.

No Capítulo 3 será apresentada a metodologia desenvolvida a partir do estudo do roteiro e norma ISO 27001:2013, explicando as fases da metodologia de forma sucinta.

O Capítulo 4, irá demonstrar o processo de identificação das correlações entre as ações do roteiro, com os controlos da norma em estudo, dando assim origem ao capítulo seguinte onde se demonstra o porquê da escolha das questões do questionário, questões essas levantadas através das ações que continham correlação efetiva a algum controlo, mostrando assim a sua real importância a ser implementada na organização em análise.

O Capítulo 5 apresenta a análise dos resultados obtidos através das respostas de 17 PME maioritariamente sediadas no distrito de Leiria, aplicando-se neste caso a uma realidade portuguesa, não obstante de ser possível agilizar a metodologia a ser utilizada a organizações europeias ou até mundiais.

No término deste projeto resultou a entrega de uma metodologia consistente e ágil podendo ser utilizada qualquer outra norma que não a ISO 27001:2013, seja a norma ISO 27009:2020 [6], NIST [7], ou outra *framework*, pois o fluxo de implementar a metodologia será precisamente o mesmo.

2

CONCEITOS RELACIONADOS

Neste capítulo 2 é efetuado um enquadramento teórico dos conceitos investigados na realização do projeto, como a definição de uma PME, normas relevantes, entidades e documentos relevantes em Portugal no que toca à cibersegurança e trabalhos relacionados. Este enquadramento teórico tem como objetivo para além da justificação teórica do que foi realizado, facilitar o leitor a ter uma maior compreensão dos conceitos estudados para a validação desta metodologia desenvolvida.

2.1 DEFINIÇÃO DE PME

O Decreto-Lei n.º 372/2007, de 6 de Novembro [8], estipula o seguinte:

1 – A categoria das Micro, Pequenas e Médias Empresas (PME) é constituída por empresas que empregam menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de euros ou cujo balanço total anual não excede 43 milhões de euros.

2 – Na categoria das PME, uma pequena empresa é definida como uma empresa que emprega menos de 50 pessoas e cujo volume de negócios anual ou balanço total anual não excede 10 milhões de euros.

3 – Na categoria das PME, uma micro empresa é definida como uma empresa que emprega menos de 10 pessoas e cujo volume de negócios anual ou balanço total anual não excede 2 milhões de euros.

Em termos práticos, o Instituto Nacional de Estatística (INE)[1] como organismo oficial de Portugal responsável por produzir e divulgar informação estatística oficial de qualidade, promovendo a coordenação, o desenvolvimento e a divulgação da atividade estatística nacional considera somente a variável Número de Pessoas ao Serviço para classificar as empresas em Micro, Pequena e Média, utilizando os limiares definidos no referido Decreto-Lei.

1 INE - Instituto Nacional de Estatística: https://www.ine.pt

Ainda que as PME [9] e micro empresas representem cerca de 99,9% [10] das empresas que operam em Portugal e produzam 77% do total bruto de vendas, poucos trabalhos foram feitos para facilitar a laboração e a implementação dos regulamentos na PME, por forma a proteger as organizações de problemas adjacentes à cibersegurança [11].

2.2 GOVERNANÇA DE CIBERSEGURANÇA

No espaço Europeu, a Agência da União Europeia para a cibersegurança (ENISA)[2] dedica-se à cooperação com os Estados-Membros, instituições e agências da União Europeia a capacitar comunidades a estarem preparadas para os mais diversos ataques informáticos.

Existem estratégias e legislação Europeia que Portugal segue para combater este problema cada vez mais preocupante, conforme apresentado por investigadores em que apresentam quais as implicações para Portugal ao seguirem estas legislações e estratégias Europeias [12].

Sendo a uma preocupação partilhada entre os vários países dentro e fora da UE, esta cooperação dos Estados-Membros permite uma partilha de informação, conhecimentos e políticas, que acabam por auxiliar no reforço das capacidades de defesa dos países parceiros[13] .

Através de um estudo realizado em 2019 foi possível perceber que as preocupações com a cibercriminalidade estão em linha com a média dos cidadãos Europeus, embora a percentagem de Portugueses que tomam atitude de prevenção de combate às ameaças esteja um pouco acima da média registada pelos restantes cidadãos de países Europeus [14]. Em [15], os autores avaliam o estado em Portugal da população e entidades, quer publicas quer privadas, no que diz respeito aos comportamentos de cibersegurança.

Ainda quanto ao processo de transferência de legislação Europeia na área da cibersegurança para Portugal, na sua tese Alexandre P. analisa em detalhe a influência da União Europeia no seus estados membros em matéria de cibersegurança, olhando em particular para a legislação e papel do Centro Nacional de Cibersegurança (CNCS)[3] [16].

2 ENISA - Agência da União Europeia para a : https://www.enisa.europa.eu
3 CNCS - Centro Nacional de Cibersegurança: https://www.cncs.gov.pt

O CNCS é uma organização Portuguesa cujo principal foco é a cibersegurança. Seja relativamente a processos, tecnologias e até das pessoas no ciberespaço ao nível nacional, atua como um coordenador de operações e autoridade nacional em matéria de cibersegurança junto das entidades estatais, operadores de infraestruturas críticas, operadores de serviços essenciais, prestadores de serviços digitais.

Atua até mesmo com a sociedade em geral estando presentes nas redes sociais por forma a elucidar, aconselhar os utilizadores do que deverão ou não ter em atenção até mesmo fora do ambiente colaborativo com o fim de prevenir roubos de informação, burlas e outros.

Para atingir estes objetivos, o CNCS desenvolve várias atividades diretamente dirigidas aos cidadãos e organizações tais como:

- Treino e sensibilização para comportamentos e atitudes mais seguras e responsáveis relativamente ao uso do ciberespaço e formação especializada nos vários temas da cibersegurança;
- Produção e disseminação de avisos, alertas, orientações e boas práticas para o uso mais seguro possível da tecnologia por parte dos cidadãos e das organizações, assim como de recomendações técnicas e produção de normativos e referências dirigidas às organizações;
- Produção de conhecimento sobre o estado da cibersegurança nacional;
- Através do serviço integrante do CNCS CERT.PT[4], acreditado internacionalmente, e em estrita articulação com as demais entidades competentes, realizando a efetiva coordenação da resposta a incidentes que afetem o ciberespaço de interesse nacional;
- No âmbito Regime Jurídico de Segurança do Ciberespaço, que transpõe a diretiva europeia relativa à segurança das redes e da informação, exerce as competências de regulação e de supervisão para os diferentes setores de atividade económica.

2.3 ROTEIRO DE CAPACIDADES MÍNIMAS DE CIBERSEGURANÇA

Por forma a auxiliar as PME em território nacional a protegerem-se de ataques cibernéticos, o CNCS definiu um modelo de capacidades mínimas de cibersegurança com o objetivo de melhorar os processos e tecnologias. O roteiro está dividido

4 Serviço CERT.PT - https://www.cncs.gov.pt/pt/certpt

em cinco fases, estando cada uma delas pensada para ser implementada de forma gradual seja por meios próprios ou até mesmo recorrendo a subcontratação externa.

Este Roteiro de Capacidades Mínimas de Cibersegurança (RCMCS) está disponível para consulta no site do Centro Nacional de Cibersegurança, e pode ser acessível de forma livre e gratuita, podendo efetivamente ser bastante útil para qualquer organização que pretenda estar minimamente segura e protegida. Este é o principal objetivo do Centro Nacional de Cibersegurança com a realização deste roteiro, permitir às organizações uma capacidade mínima de proteção em Cibersegurança, para fazer face a ameaças e ataques.

Ao implementar o RCMCS numa PME, o CNCS aconselha complementar com o Quadro Nacional de Referência para a Cibersegurança [17], pois este quadro aborda também diversos pontos importantes relacionados com a segurança nas organizações, seguindo as normativas da família ISO/IEC 27000[18] ou NIST[7].

Tal como referido anteriormente, o roteiro de capacidades mínimas do CNCS está dividido em cinco fases como demonstrado na Figura 2. Essas fases serão descritas ao longo deste relatório, apresentando as ações subjacentes a cada fase e objetivos esperados no final da sua implementação.

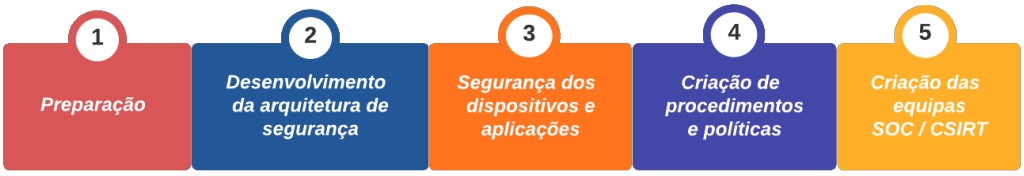


Figura 2: Fluxo das fases do RCMCS

1. A **fase um** detalhada na Tabela 1, define-se como sendo a fase preparatória em que o objetivo é o estabelecer de alicerces para uma cooperação entre uma organização (por exemplo, empresa ou uma entidade pública) e o CNCS.

   Nesta fase também é identificado o quadro de ameaças que poderá estar subjacente à organização, calculando o valor relativo aos seus ativos e graus de risco, serão definidas áreas de segurança conforme o valor dos ativos e também regras de acesso. Devem também, ser identificadas as dependências funcionais entre sistemas internos e geridos por terceiros, pois têm importância elevada para o negócio.

Ações da fase 1 Roteiro CNCS
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)
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

Tabela 1: Fase 1 - Roteiro de Capacidades Mínimas de Cibersegurança

Para que a fase um seja implementada com sucesso, na organização deverão estar implementados os objetivos apresentados na Figura 3.

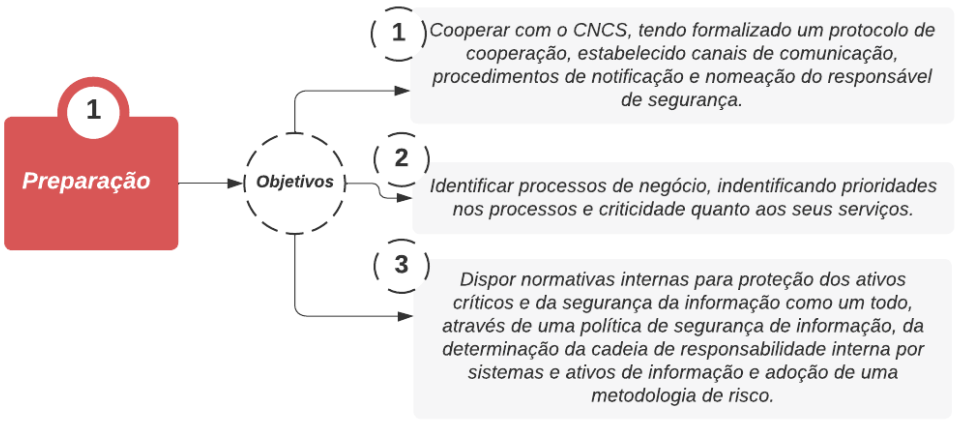


Figura 3: Fase 1 RCMCS - Objetivos esperados

2. Na **fase dois**, estando apresentadas as suas ações na Tabela 2, é a fase onde será desenvolvida a arquitetura de segurança com o foco na delimitação das várias áreas de segurança e aplicar regras de controlo de acessos. Ainda nesta fase, a organização deverá conter um repositório central por forma a correlacionar eventos de segurança detetados nos diversos elementos de segurança, seja ativa ou passiva, e agregar também a informação e metadados de comunicações e registos de sistemas e aplicações.

Ações da fase 2 Roteiro CNCS
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 *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

Tabela 2: Fase 2 - Roteiro de Capacidades Mínimas de Cibersegurança

Para que seja implementada com sucesso esta fase, a organização deverá ter implementados os objetivos apresentados na Figura 4.

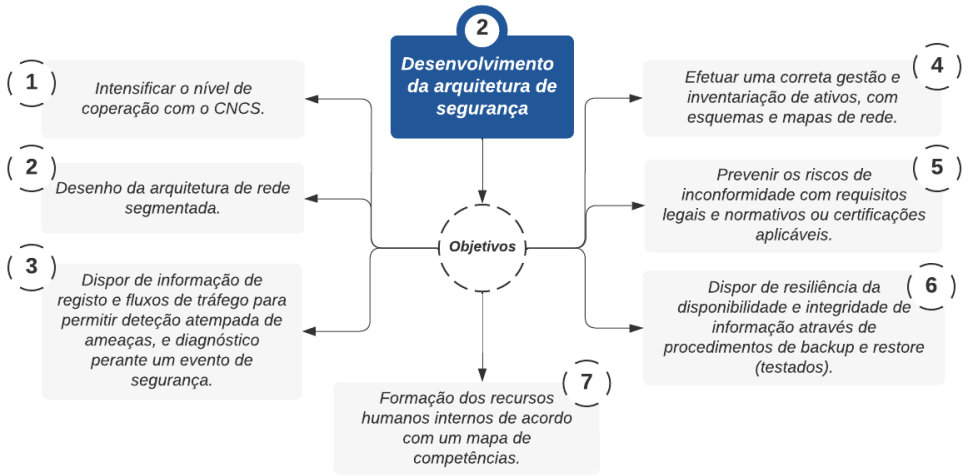


Figura 4: Fase 2 RCMCS - Objetivos esperados

3. A **fase três**, apresentadas as suas ações na Tabela 3 foca na preocupação na segurança de dispositivos e aplicações, incentivando assim implementar na organização mecanismos de deteção e prevenção de ameaças nos dispositivos que tratam os ativos mais valiosos. Nesta fase aconselha-se também que sejam definidos e implementados de mecanismos de auditoria e alerta de acessos

indevidos a bases de dados e outros ativos de elevado valor; mecanismos de alerta para falhas de desempenho e disponibilidade de serviços e mecanismos de controlo e auditoria de acessos a sites da Internet.

Ações da fase 3 Roteiro CNCS
A 3.1 - Definição de procedimentos de operação
A 3.2 - Instalação e configuração de sensores em dispositivos
A 3.3 - Auditoria de segurança a 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 SIEM
A 3.9 - Definição de planos de continuidade de negócio
A 3.10 - Aquisição de competências técnicas

Tabela 3: Fase 3 - Roteiro de Capacidades Mínimas de Cibersegurança

Para que seja implementada com sucesso esta fase, a organização deverá ter implementados os objetivos apresentados na Figura 5.

Figura 5: Fase 3 RCMCS - Objetivos esperados

4. A **fase quatro** do roteiro, apresentadas as suas ações na Tabela 4 é responsável pela criação de procedimentos e políticas que definem e melhorem as capacidades da equipa responsável pela cibersegurança interna, formalizar procedimentos para operações de cibersegurança, definir responsabilidades por essas mesmas operações e elaborar um plano de formação para todos os colaboradores envolvidos nessas ações, por forma a construir uma estrutura de cibersegurança sólida para toda a organização.

Ações da fase 4 Roteiro CNCS
A 4.1 - Cadeia de responsabilidades: formalização
A 4.2 - Definição do Sistema Interno de Normas e Políticas (SINP)
A 4.3 - Análise de risco - reavaliação
A 4.4 - Simulacro
A 4.5 - Definição de procedimentos de reação a incidentes
A 4.6 - Treino e sensibilização interna: SINP
A 4.7 - Testes de aceitação de serviços
A 4.8 - Mecanismos de engodo (*honeypots*)
A 4.9 - Gestão de mudanças e atualizações

Tabela 4: Fase 4 - Roteiro de Capacidades Mínimas de Cibersegurança

À semelhança das fases anteriores, para que seja implementada com sucesso esta fase, a organização deverá ter implementados os objetivos apresentados na Figura 6.

Figura 6: Fase 4 RCMCS - Objetivos esperados

5. Quanto à **fase cinco**, última fase estando as suas ações representadas na Tabela 5, destina-se acima de tudo a organizações em que dada a sua dimensão, criticidade ou complexidade justifique formalizar uma ou várias equipas dedicadas à deteção e resposta de incidentes com a capacidade de monitorizar e alertar incidentes de segurança - *Security Operations Centre (SOC)* e/ou *Computer Security Incident Response Team (CSIRT)*. É aconselhada também a colaboração em projetos de desenvolvimento e partilha de informação de cibersegurança com uma periodicidade regular dentro do setor de atividade e,

se for necessário, com a comunidade de cibersegurança, podendo até participar em exercícios nacionais e internacionais de cibersegurança.

Ações da fase 5 Roteiro 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 - Desenvolver 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

Tabela 5: Fase 5 - Roteiro de Capacidades Mínimas de Cibersegurança

Como referido anteriormente, esta fase depende muito das PME, pois há organizações que derivado à sua dimensão ou tipo de empresa, não há necessidade de implementar esta fase.

Para as organizações em que seja importante implementar esta fase, o sucesso da organização de estar em conformidade, depende da mesma ter implementados os objetivos apresentados na Figura 7.

Figura 7: Fase 5 RCMCS - Objetivos esperados

2.4 FAMÍLIA ISO 27000

A família ISO 27000 é constituída por uma série de normas para gestão da segurança da informação, estando demonstradas na Figura 8 alguns exemplos de normas da família ISO. Esta família evolui continuamente surgindo assim novos padrões para atender às mudanças nos requisitos de segurança de informação nos diferentes setores e ambientes [18].

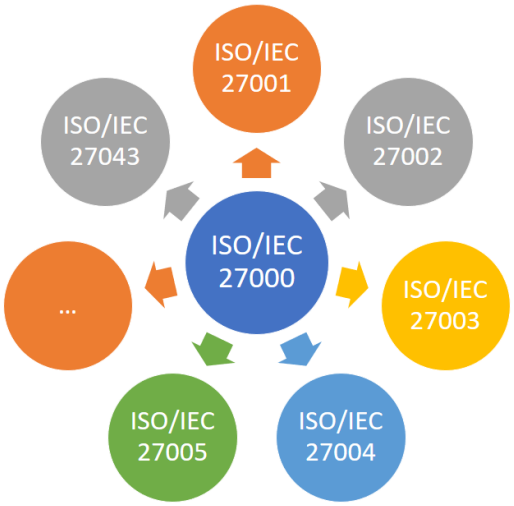


Figura 8: Exemplo de normas pertencentes à família ISO 27000 [19]

A norma ISO 27001:2013 [20] pertencente à família ISO 27000, é uma norma internacional para a gestão da Segurança da Informação com 114 controlos com bastante importância, não apenas para as empresas que procurem obter a certificação ISO mas acima de tudo para quem procure uma organização segura, pois esta especifica como deve ser implementado um Sistema de Gestão de Segurança da Informação (SGSI) em ambientes colaborativos.

Até à atualidade esta norma ISO 27001:2013 tem vindo a ser melhorada, já que esta deriva de um conjunto de normas, sendo elas a ISO 27001:2013 e a BS7799 (British Standards) [21] publicado em 1995. Este padrão, resultou numa norma conhecida por ISO/IEC 17799 [22]. Aliada à segunda parte do BS7799 na implementação de um Sistema de Gestão de Segurança da Informação que foi publicada em 1999, foi então criada a norma que hoje tão bem conhecemos, a norma ISO 27001:2013. Esta norma tem como objetivo principal a organização de um meio colaborativo, adotando um conjunto de requisitos, processos e controlos com o objetivo de diminuir os riscos na organização.

Domínios da ISO 27001:2013	**Breve descrição dos controlos do domínio**
A 5 - Políticas de segurança da informação	Definidas (e revistas) políticas de segurança da informação.
A 6 - Organização de segurança e informação	Definição das responsabilidades a atribuir. Inclui controlos para dispositivos móveis e trabalho remoto.
A 7 - Segurança na gestão de recursos humanos	Definição de procedimentos para antes, durante e término da contratação com um funcionário.
A 8 - Gestão de ativos	Controlos relacionados com inventariação de ativos e uso aceitável dos mesmos. Controlos também para classificar a informação e manuseamento de dispositivos amovíveis.
A 9 - Controlo de acesso a sistemas e aplicações	Definição dos controlos de acesso a sistemas, utilizadores e aplicações.
A 10 - Criptografia	Procedimentos para utilização de criptografia na organização.
A 11 - Segurança física e ambiental	Controlos para definição de áreas seguras, controlo de entradas, proteções contra ameaças, segurança de equipamentos, descarte seguro e zona de trabalho limpa.
A 12 - Segurança de operações	Definição de controlos relacionados com a gestão da produção de TI: gestão de mudança, de capacidade, software malicioso, cópias de segurança, registo de eventos, monitorização, instalação e vulnerabilidades.
A 13 - Segurança de comunicações	Controlos relacionados com a segurança na rede, a sua segregação das redes, os serviços de rede, transferência de informação, e-mails.
A 14 - Aquisição, desenvolvimento e manutenção de sistemas	Controlos para definir requisitos de segurança nos processos de desenvolvimento e suporte.
A 15 - Relação com fornecedores	Definição de controlos sobre o que incluir em acordos com fornecedores e como monitorizar-los.
A 16 - Gestão de incidentes de segurança da informação	Controlos para reportar eventos e vulnerabilidades que sejam detetadas, definição de responsabilidades na gestão de incidentes, procedimentos para resposta e recolha de provas.
A 17 - Aspetos de segurança da informação na gestão da continuidade do negócio	Definição de controlos, procedimentos para continuidade do negócio, revisão e redundância da TI.
A 18 - Conformidade	Controlos onde são identificadas as leis e regulamentações aplicáveis à organização, proteção da propriedade intelectual, proteção de dados pessoais e revisões à segurança da informação.

Tabela 6: Domínios da norma ISO 27001:2013 [20]

Na Tabela 6 estão demonstrados todos os domínios presentes no Anexo A da norma ISO 27001:2013, apresentando cada domínio, objetivos de controlo e por cada um destes objetivos de controlo, os seus controlos associados. A descrição apresentada, trata-se de um breve resumo do tipo de controlos que esse domínio aborda.

A norma ISO 27001:2013, como demonstra a Figura 9 adota o modelo PDCA (Plan-Do-Check-Act) [23] para descrever a estrutura de um SGSI.

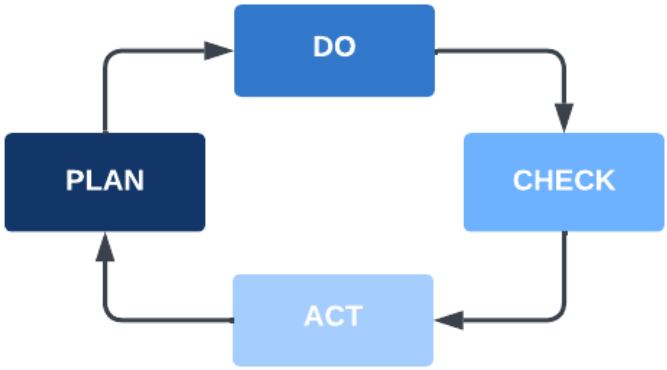


Figura 9: Modelo Plan-Do-Check-Act

1. ***Estabelecer o SGSI (PLAN)*** - É a etapa que dá vida ao SGSI. É o inicio de todo o processo, em que irão ser definidos objetivos, e limites do SGSI. Quais as metas, objetivos, ferramentas para os controlos, indicadores, cronogramas, etc.
2. ***Implementar e utilizar o SGSI (DO)*** - É nesta etapa que irá ser implementado tudo o que foi planeado na etapa anterior. Inicia-se a formação interna dos funcionários, a instalação das ferramentas e começará a rotina da empresa monitorizar o que está a ser utilizado.
3. ***Monitorizar e melhorar o SGSI (CHECK)*** - Analisar os resultados obtidos após a implementação das soluções definidas e implantadas nas fases anteriores. Vai verificar se os resultados obtidos estão de acordo com as metas estabelecidas (indicadores), e vai confirmar se está tudo em conformidade ou se é necessário melhorar.
4. ***Manter o SGSI (ACT)*** - Executar medidas de correção necessárias para melhorar o que foi verificado e que se encontra com indicador abaixo do que era esperado. Assegurar de que as melhorias atinjam os objetivos.

É importante deixar tudo documentado, o que foi planeado, o resultado obtido, os problemas encontrados e as ações que foram tomadas ou não para a melhoria. Esta documentação é importante para provar que são realizadas verificações periódicas e ações de melhorias em caso de deturpação ou fugas de dados. Estes relatórios deverão ser mostrados para defesa da organização.

Este processo é constante, e deverá ser realizado com frequência, pois a área tecnológica muda bastante rápido, assim como as ameaças são bastante dinâmicas, a organização deverá sempre estar adaptada às novas realidades para evitar possíveis problemas. Mais importante ainda é, que tudo o que estiver documentado esteja a ser implementado na prática, pois numa auditoria em caso de não estar a ser implementado na prática de nada vale estar documentado, sendo este cenário considerado como uma não conformidade

Devem ser mantidos, para fornecer provas de conformidade aos requisitos (mas protegidos e controlados) os registos de desempenho do processo, de todas as ocorrências de incidentes de segurança de informação significativos relativamente ao SGSI, por exemplo: livro de registo de visitas externas, relatórios de auditorias, quantidade de vírus detetados, etc.

A norma ISO 27001:2013 é uma norma bastante abrangente relativa a uma organização, pois trata de múltiplos temas tais como as telecomunicações, meio físico, recursos humanos, segurança das aplicações, licenciamentos, entre outros. Como tem como objetivo o estabelecimento de processos e procedimentos, e sendo os requisitos desta norma genéricos, são aplicáveis a todas as organizações independentemente do tipo, tamanho ou natureza do negócio.

De notar que, um SGSI é um processo contínuo, pois não existe uma implementação hoje que não vá necessitar de melhorias contínuas. O objetivo da norma é precisamente promover os requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI.

A seleção dos controlos a implementar podem ser definidas como ações a desempenhar para minimizar os riscos de ameaças, pelo que a seleção de quais os controlos a serem implementados dependem da decisão da organização da empresa. Alguns são controlos básicos para a segurança da informação e vão ter de existir em qualquer empresa, porém nem todos os controlos irão ser aplicados, pois poderão não fazer parte das rotinas da empresa. Pode também acontecer, os controlos existentes não serem os mais adequados ou específicos ao tipo de organização. Assim sendo poderemos aplicar mais controlos não apenas desta norma, mas sim implementar a segurança da informação da empresa com outros controlos que a possam complementar.

2.5 TRABALHOS RELACIONADOS

2.5.1 *LOG IN Innovation*

O projeto LOG IN Innovation[5] pretende "reforçar as capacidades de organização e gestão das PME com implementação de uma política de segurança na infraestrutura de tecnologias de informação (TI) e metodologias de gestão vitais para as PME", possui semelhanças quanto à metodologia desenvolvida.

A implementação do projeto "LOG IN Innovation"[24] permitiu a análise do estado e mitigação de vários riscos relacionados com segurança da informação de várias PME, seguindo a norma ISO 27001:2013. Esta análise e proposta de resolução de riscos existentes, foi dividida em dois níveis:

- **Nível 1** - Implementação da segurança da informação Standard em 30 empresas onde foram percorridos 30 pontos, em que nos pontos observados e detetados que deveriam existir medidas corretivas, foram aplicadas as mesmas nos 30 pontos, implicando por vezes na aquisição de software e/ou hardware específico. No final da intervenção, foi efetuada uma auditoria para certificar o cumprimento dos pontos selecionados.
- **Nível 2** - Implementação da segurança da informação Completa em 20 empresas, neste caso foram percorridos os 114 controlos da norma ISO 27001:2013 com objetivo de identificar riscos e as medidas que deveriam ser implementadas para a sua mitigação. Tendo em conta a complexidade do cumprimento dos 100% dos pontos, no final existiu uma auditoria para certificar se pelo menos 60% dos pontos estariam implementados.

O objetivo deste projeto LOG IN Innovation é dotar as organizações, neste caso PME, com controlos que as protejam relativamente a falhas de segurança (neste caso controlos da norma ISO 27001:2013). A semelhança com a metodologia desenvolvida neste projeto de mestrado está precisamente nesse ponto. Seguindo a metodologia, é possível efetuar melhorias na organização mitigando os pontos fracos, ou implementando os pontos não implementados por forma a melhorar a infraestrutura de segurança da informação, incluindo cibersegurança.

Na publicação [11] podemos ver em detalhe os resultados do projeto, a sua análise e as conclusões dos investigadores.

5 LOG IN Innovation: https://www.logininnovation.pt

2.5.2 *Mapeamento Mandatory Cyber Security Controls (MCSR) - ISO 27001:2013*

Como trabalho relacionado à semelhança do que mapeamento implementado no âmbito deste projeto, entre o roteiro do CNCS e norma ISO 27001:2013, em [25] os autores desenvolveram um mapeamento entre um roteiro elaborado pela autoridades Moldavas e a norma ISO 27001:2013.

Esse roteiro, utilizado em organizações públicas, é composto por controlos para proteção contra ciberataques. Este mapeamento parte pela intenção da Moldávia em querer cumprir os padrões internacionais em relação a cibersegurança até 2024.

A diferença deste mapeamento MCSR - ISO 27001:2013 apresentado no artigo acima citado e o mapeamento RCMCS - ISO 27001:2013 desenvolvido no âmbito deste projeto está na continuidade dada ao mapeamento. A partir do mapeamento RCMCS - ISO 27001:2013 gerado foi implementado um questionário para análise do estado da cibersegurança nas organizações.

3

METODOLOGIA

Neste capítulo é descrita a metodologia desenvolvida, por forma a permitir um melhor entendimento dos passos no desenvolvimento da mesma e demonstrar que se trata de uma metodologia aberta, permitindo o cruzamento não apenas com a norma ISO 27001:2013 mas com qualquer norma que pretendamos.

Para o desenvolvimento desta metodologia foi necessário um estudo sobre as normas existentes para que ao desenvolver a mesma fosse uma metodologia aberta e não fechada.

A vantagem de ser uma metodologia do tipo aberta é que esta permite não cruzar apenas uma norma com o roteiro, mas sim está preparada para que possa ser utilizada futuramente qualquer norma à escolha. Tanto podem ser cruzados com o roteiro os controlos da norma ISO 27001:2013 como os controlos da norma ISO 27009:2000, estando esta última mais voltada para controlos de cibersegurança e não da segurança de informação em geral como a ISO 27001:2013.

A metodologia desenvolvida permite, como a Figura 10 representa, ser utilizada outra norma, como por exemplo a ISO 27009:2020 [6], ou NIST [7] e até mesmo CIS Controls[26].

Na fase 1 da metodologia proposta, é efetuado um estudo dos documentos a serem utilizados, sendo um deles fixo, neste caso o roteiro de capacidade mínimas de cibersegurança, e uma norma à escolha. Após esse estudo das ações do roteiro e controlos da norma escolhida, será identificada uma correlação entre os mesmos.

Para definir essas correlações, isto na fase 2 foram atribuídos graus de correlação, neste caso heurísticas dividindo-se em três graus:

- **Ação** - (AC): Tanto o roteiro como a norma sugerem as mesmas ações ou muito semelhantes.
- **Alvo** - (AL): Tanto o roteiro como a norma têm o mesmo objetivo final, mesmo que as ações sugeridas sejam diferentes.
- **Âmbito** - (AM): Tanto o roteiro como a norma têm o mesmo âmbito mas as ações ou mesmo o objetivo final explícito são diferentes.

Após a definição dos graus de correlação é efetuada uma listagem das correlações e controlos, incluindo uma justificação teórica dessas correlações por forma a serem justificadas.

No final dessa justificação das correlações é possível efetuar mapas de correlações, ou seja o mapeamento das correlações geradas, sendo esta a fase 3. Ao ser gerado esse mapeamento gráfico das correlações, pode-se complementar o mesmo efetuando mapeamento igual mas com a classificando as relações com os graus definidos anteriormente.

Estas correlações geradas poderão assim ser aproveitadas para criar questões para um questionário, como o efetuado neste projeto. Esse questionário, aproveitando o mapeamento realizado tem justificação teórica suficiente para ser utilizado para medição de, por exemplo o estado de uma empresa, dependendo do âmbito.

Ao utilizar-se a norma ISO 27001:2013, iremos ter um complemento da cibersegurança do roteiro com a segurança da informação da ISO. Se for escolhida uma norma como a ISO 27009:2020, para além do roteiro estar mais voltado para a cibersegurança, esta norma está também voltada para esse âmbito. No caso de pretendermos uma análise efetiva do estado da cibersegurança, é também uma boa alternativa de utilização da metodologia.

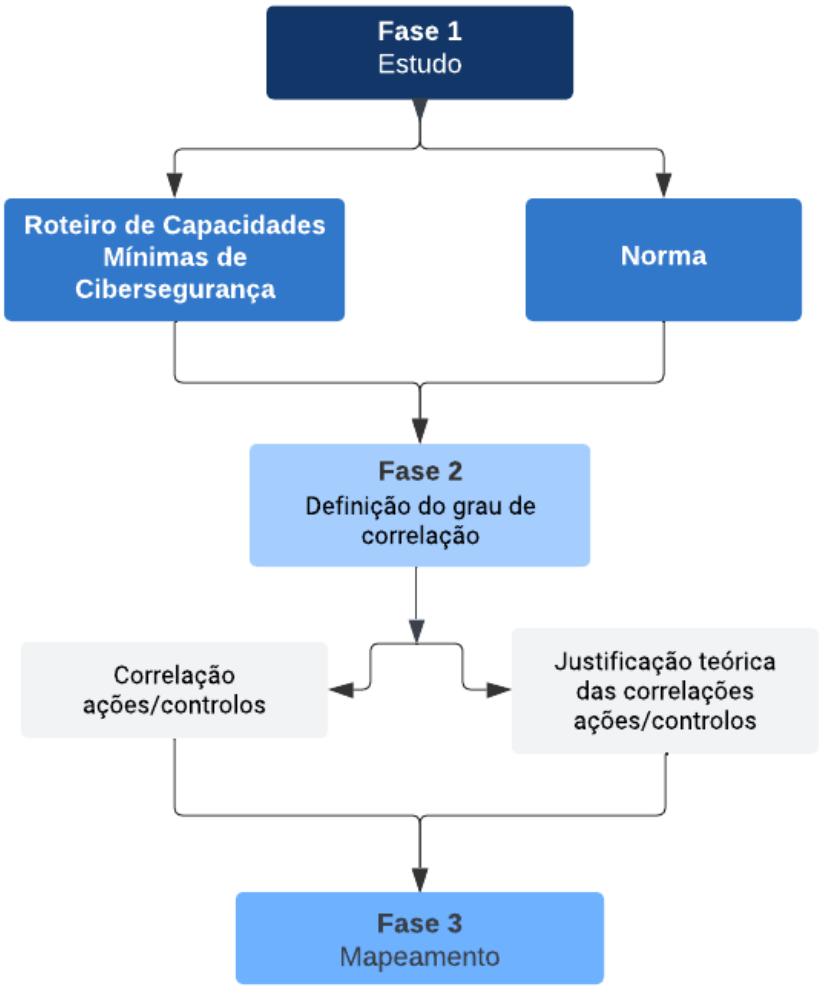


Figura 10: Descrição global da metodologia proposta

Por forma a ser desenvolvida uma metodologia mais sólida, aliando ao roteiro uma norma mais completa que tivesse controlos ligados à segurança de informação foi estudada qual a melhor norma a enquadrar.

Neste caso, na presente implementação da metodologia foi escolhida a norma ISO 27001:2013 pois é uma norma bastante completa para o desenvolvimento de um Sistema de Gestão de Segurança de Informação. Foram analisados os seus controlos por forma a identificar as correlações com as ações do roteiro, e os controlos da norma em estudo, como está demonstrado na Figura 11.

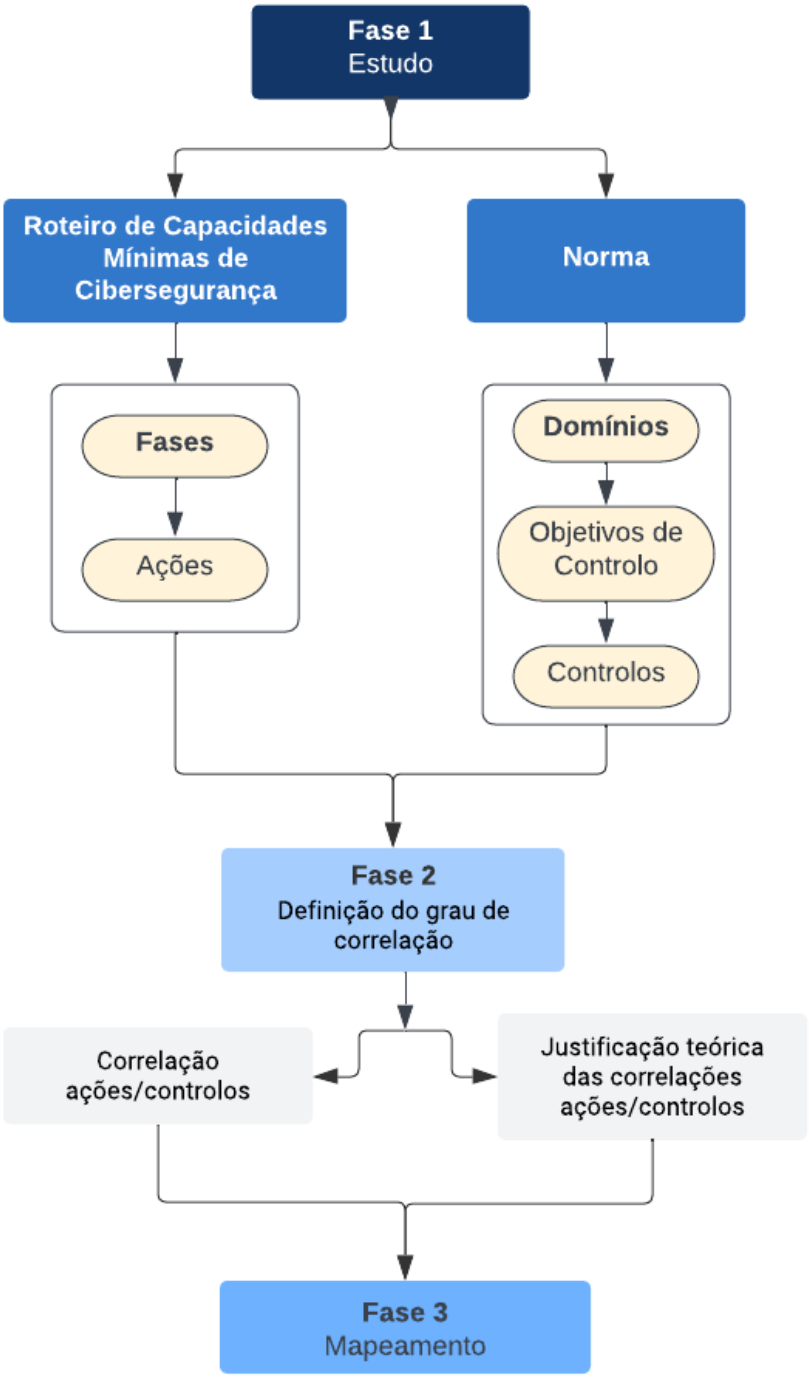


Figura 11: Diagrama da metodologia implementada

Para a realização de uma análise efetiva do estado de uma empresa em relação à cibersegurança, neste caso aplicada a PME, consistiu em várias fases utilizando como base de estudo o Roteiro de Capacidades Mínimas de Cibersegurança do Centro Nacional de Cibersegurança, e a norma internacional ISO 27001:2013.

Numa fase inicial, foi efetuado um estudo independente de cada um dos temas, sendo que, relativamente ao Roteiro de Capacidades Mínimas foram analisadas as fases fundamentais para uma PME estar em conformidade/segura em termos de cibersegurança, fases estas que se subdividem em ações que são aconselhadas a que sejam implementadas nas PME.

Quanto à norma ISO 27001:2013, foi analisada incluindo o estudo dos domínios, objetivos de controlo e por sua vez, controlos associados a esta norma que, ao ser implementada numa empresa o seu objetivo é que exista uma real segurança no armazenamento da informação de uma organização, seja utilizando mecanismos ou até mesmo procedimentos recomendados pela norma.

Após o estudo do Roteiro de Capacidades Mínimas de Cibersegurança e da norma ISO 27001:2013, foram analisadas as correlações dos controlos da norma com as ações do roteiro, tentando-se assim definir um grau de correlações existentes e justificando o porquê da relação entre os mesmos.

Numa fase seguinte, foi efetuado um mapeamento dessas mesmas correlações, dando assim origem a uma base sólida para escolha efetiva de questões a serem colocadas no questionário a ser efetuado às organizações para a análise de segurança.

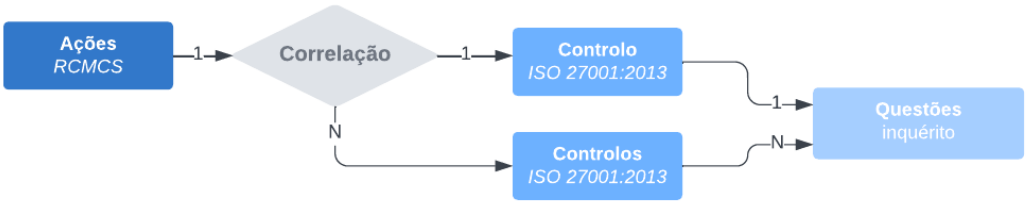


Figura 12: Resultados das correlações - Identificação das questões

Como demonstrado na Figura 12, no caso de existirem correlações cada ação com correlação a um controlo da norma irá despoletar uma questão no inquérito.

No capítulo seguinte irá ser explicado com maior detalhe a última fase desta metodologia, ou seja, o mapeamento. Esse mapeamento apresentará as correlações encontradas entre as ações do RCMCS e a norma ISO 27001:2013.

4

MAPEAMENTO

Neste capítulo é apresentado o mapeamento, que é uma das fases da metodologia, efetuado entre o Roteiro de Capacidades Mínimas de Cibersegurança e a norma ISO 27001:2013 em estudo. Descreve-se as ações do roteiro e explica-se cada ação e o porquê da correlação com determinados controlos da norma ISO 27001:2013 e de seguida um mapeamento gráfico apresentando mais sucintamente e de forma clara as correlações existentes.

4.1 FUNDAMENTAÇÃO DO MAPEAMENTO ENTRE AS AÇÕES E OS CONTROLOS

Por forma a analisar se existe uma correlação de cada ação que se encontra relatada no Roteiro de Capacidades Mínimas de Cibersegurança com as normas da ISO 27001:2013 (para além do mapeamento que se encontra no próximo sub-capítulo) foi efetuado um resumo de cada ação e de que forma se relaciona com um ou vários controlos da norma.

Esta análise teórica de identificação das ações/roteiro vs controlos/norma em estudo estará dividida pelas fases disponíveis no roteiro, onde cada ação será relacionada com um ou vários controlos da norma.

4.1.1 *Fase 1 do RCMCS - Mapeamento ações / controlos*

Ação 1.1 – Formalização de Protocolo de Colaboração e Adenda

Esta ação trata da formalização de um protocolo de colaboração entre a organização e o CNCS e dependendo dos serviços que cooperem com a organização, considerando também as respetivas adendas. O Protocolo representa a colaboração entre a organização e o CNCS, marcando o início do processo de desenvolvimento das capacidades mínimas propostas no roteiro. Fica assim definido neste protocolo o Responsável de Segurança da organização.

Relacionando este conceito, com os definidos na norma ISO 27001:2013, poderemos associar esta secção com o controlo 16.1.1 – Responsabilidades e procedimentos, domínio 16 responsável pela Gestão de incidentes de segurança de informação, objetivo de controlo em que devem de ser definidos os responsáveis pela gestão de incidentes, inclusive o responsável pela segurança da informação na organização.

Ação 1.2 - Identificação do Responsável de Segurança

Sendo o responsável pela segurança o ponto de contato da organização em termos práticos/operacionais, deverá estar preparado a responder às solicitações da equipa operacional do CNCS (CERT.PT). Este responsável deve conhecer bem a organização, não apenas em termos técnicos, mas também de negócio. Para prevenção, a organização poderá vir a definir analistas de cibersegurança para salvaguarda, no caso do responsável não estar presente/disponível.

Na norma ISO 27001:2013 à semelhança da ação anterior temos o controlo 16.1.1 – Responsabilidades e procedimentos, que define quem é o responsável de segurança, este define também procedimentos e regras a cumprir por esta entidade.

Para além deste objetivo de controlo anteriormente citado, podemos relacionar a esta ação do roteiro, o controlo da ISO em estudo 6.1.3 – Contato com autoridades competentes, do domínio 6 responsável pela organização da Segurança da Informação.

Estando relacionado com o contato às autoridades relevantes, isto incluindo o CNCS, pode ser relacionado com o controlo 6.1.4 – Contato com grupos de interesse especial, do mesmo domínio pois especifica precisamente o contato com grupos especiais, associações de profissionais especializados em segurança de informação por exemplo, por forma a trocar-se experiências sobre ataques, ameaças ou até mesmo novas proteções disponíveis no mercado.

Ação 1.3 - Identificação de funções ou atividades críticas

Para a atividade da organização, e até para ser dado o auxílio correto por parte do CNCS em caso de haver necessidade é importante que exista uma descrição dos serviços mais críticos prestados pela organização. É de igual forma importante ter registados os endereços públicos associados para que, a partir de eventos de cibersegurança recolhidos através de outras fontes, identifique rapidamente possíveis ameaças ou ataques direcionados para a organização em causa.

Interligando esta ação do roteiro aos controlos da norma ISO podemos associar para além dos serviços críticos a criticidade da informação armazenada o controlo 8.2.1 – Classificação da informação do domínio 8 de Gestão de ativos, controlo este que define que deverá ser dado um nível adequado à informação armazenada, de

acordo com a sua importância, valor, requisitos legais e sensibilidade. Esta associação faz sentido na medida que os serviços estão diretamente ligados a informação armazenada na organização. Assim definindo a criticidade da informação guardada conseguimos definir quais os serviços mais críticos ao haver fluxo/armazenamento da informação.

Ação 1.4 - Estabelecimento de canais de comunicação

Tendo em conta a sensibilidade de grande parte da informação trocada por correio eletrónico, é necessário proteger esta questão utilizando criptografia. Opcionalmente o CNCS aconselha nesta ação que cada um dos colaboradores envolvidos na troca de mensagens mais relevantes poderão até utilizar chaves PGP [27] próprias.

Relativamente às correlações desta ação com controlos da norma em estudo, existe com o controlo 10.1.1 - Política para o uso de controlos criptográficos, pertencente ao domínio 10 relacionado com a Criptografia. Este aconselha que deverá ser criada uma política de criptografia de acordo com o tipo de negócio/criticidade das mensagens trocadas internamente/externamente pelos colaboradores da organização.

Para além do controlo citado anteriormente existe também correlação com o controlo 10.1.2 - Gestão de chaves, que recomenda para além do uso de chaves seja criado um processo para a gestão segura de chaves a serem utilizadas pelos colaboradores da organização.

Ação 1.5 - Registo de endereços de IP no LIR (Local Internet Registry)

Relativamente a esta ação do roteiro A 1.5 que trata do registo de endereços de IP no LIR permitindo a organização receber notificações e outra informação de cibersegurança relevante para redes e sistemas sob a sua responsabilidade, não existe correlação com nenhum controlo da norma ISO.

Ação 1.6 - Estabelecimento de metodologia de Análise de Risco

A gestão do risco é o processo contínuo de identificação, avaliação e resposta ao risco. Para uma gestão correta do risco da organização, o CNCS através do roteiro aconselha que deve ser identificado a probabilidade de um evento vir a ocorrer e qual o impacto que esse evento provocará à organização no caso de realmente acontecer.

Podemos assim associar esta ação com dois controlos da norma ISO 27001:2013 sendo uma das correlações o controlo 8.2.1 – Classificação da informação pertencendo ao domínio 8 de Gestão de ativos pois esta classificação é um processo contínuo e deverão ser definidos níveis de importância desta informação utilizada em serviços da organização. Esta ação pode também ser correlacionada ao controlo 12.6.1 - Gestão

de vulnerabilidades técnicas, em que consiste na exploração de vulnerabilidades nos ativos por forma a mitigar ou minimizar risco ou danos que poderão advir.

Relativamente a ser criada uma matriz de risco, como proposto na ação do roteiro pelo CNCS salientando a probabilidade de ocorrência vs impacto, não está definido nenhum objetivo de controlo que contemple a elaboração deste pois a norma ISO 27001:2013 está mais focada na segurança da informação.

Ação 1.7 - Cadeia de responsabilidade: Preparação

Esta ação do roteiro inicia-se com a nomeação de um órgão/equipa/pessoa responsável pela gestão de incidentes dentro da organização. De notar que pode ou não ser atribuída esta tarefa ao Responsável pela segurança da organização. Este responsável pela gestão de incidentes deverá ser conhecido por toda a organização e ser o ponto de contato para todos os assuntos relacionados com incidentes de segurança.

À semelhança das ações A 1.1 e A 1.2 esta ação tem como correlação à norma ISO 27001:2013 o controlo 16.1.1 – Responsabilidades e procedimentos, do domínio 16 de Gestão de incidentes de segurança de informação. Este controlo para além de definir quem é o responsável de segurança da informação, define também procedimentos relativamente a quem gere os incidentes de segurança na organização.

Nesta ação do roteiro serão também definidas as restantes responsabilidades, associando assim ao controlo 6.1.1 - Papéis e responsabilidades de segurança da informação, do domínio 6 focado na Organização da Segurança da Informação, definindo assim aos restantes colaboradores quais as suas responsabilidades dentro da organização.

Ação 1.8 – Definição de política de segurança de informação

Quanto à ação A 1.8 do roteiro, esta recomenda a criação de uma política de segurança de informação da organização pois será um elemento estruturante para uma efetiva proteção em termos de cibersegurança. Enquanto elemento estratégico é importante que tenha a aprovação e aceitação da gestão de topo e o envolvimento e compromisso de todos os colaboradores.

Correlacionando esta ação A 1.8 com os controlos da norma, denota-se o controlo 5.1.1 - Políticas para a segurança da informação, pertencente ao domínio 5 – Políticas de segurança de informação, citando este controlo que devem ser definidas políticas necessárias para segurança de informação, políticas estas que deverão ser aprovadas pela direção e divulgadas a todos os colaboradores da organização.

Ação 1.9 - Procedimentos de notificação de incidentes

Esta ação A 1.9 consiste na criação e obtenção da aprovação de um procedimento para notificação de incidentes de segurança de informação com impacto nas funções ou atividades críticas. O responsável deverá então selecionar os incidentes tendo em especial atenção a classificação dos mesmos, classificação essa que deverá ter em conta a sua criticidade para a organização.

Quanto à questão de notificar eventos, incidentes de segurança presentes na norma ISO podemos correlacionar vários controlos a esta ação do roteiro, nomeadamente a notificação de eventos, pontos fracos e até mesmo avaliar/classificar e decidir o que fazer relativamente a esses eventos. Esses controlos são pertencentes ao domínio 16 referentes à Gestão de incidentes de segurança de informação, e são os seguintes:

- Controlo 16.1.2 - Reportar eventos de segurança da informação que cita que os eventos de segurança devem ser comunicados através de canais próprios a todos os envolvidos, seja dentro ou fora da organização e o mais rápido possível para que cada um assuma a sua responsabilidade perante o incidente.

- Controlo 16.1.3 - Reportar os pontos fracos de segurança da informação que recomenda, como especificado no ponto acima, que os funcionários e fornecedores/prestadores de serviços que utilizam os serviços e os sistemas de informação da organização devem ser instruídos a detetar, e responsabilizados de reportar qualquer ponto fraco na segurança da informação, seja em sistemas ou serviços.

- Controlo 16.1.4 - Avaliação e decisão sobre eventos de segurança da informação salientando que os eventos de segurança devem ser avaliados e decidido com base em parâmetros definidos pela organização se são classificados efetivamente como incidentes. A prioridade e classificação de incidentes podem ajudar a identificar o impacto e a abrangência desse mesmo incidente e tomar as devidas ações.

4.1.2 *Fase 2 do RCMCS - Mapeamento ações / controlos*

Ação 2.1 - Desenho e implementação da arquitetura e segurança perimétrica

Nesta ação pretende-se que seja desenhada uma nova arquitetura de cibersegurança para a organização por forma a que sejam organizadas as várias áreas de segurança e identificadas as necessidades de deteção de eventos problemáticos com origem no exterior e entre zonas de segurança distintas.

Assim sendo para mitigar/reduzir riscos deverão existir *firewalls* na organização para controlar os acessos da/à Internet e entre diferentes zonas de segurança, com

regras que minimizem a interação entre camadas. Deverá também ser contemplado/implementado um Sistema de Deteção e Proteção de Intrusão (IDS/IPS).

Quanto à correlação com controlos da norma ISO, pode-se associar esta ação com o controlo 12.2.1 - Controlos contra código malicioso, que pertence ao domínio 12 - Segurança nas operações. Este controlo cita que é necessário criar controlos para detetar, prevenir, e recuperar em caso de danificarem alguma parte ou toda a informação. Outro controlo que pode ser relacionado a esta ação é o 13.1.3 - Segregação das redes, do domínio 13 - Segurança nas comunicações. O controlo recomenda a divisão das redes de comunicação na organização, por forma a diminuir o risco de acessos indevidos às redes.

Ação 2.2 - Implementação de sistema de recolha e armazenamento do fluxo de tráfego

Nesta ação o CNCS sugere a recolha dos metadados a ser efetuada no router/switch ou outro equipamento que controle o acesso à navegação na Internet. Esta recolha serve como prova do tráfego gerado pelos colaboradores com a navegação na Internet aproveitando também para identificar padrões de sistemas potencialmente comprometidos por forma a analisar também o tráfego considerado malicioso.

Na norma ISO 27001:2013 existe um controlo que visa precisamente a recolha de provas, incluindo tráfego, podendo até servir como provas legais (em caso de necessidade), disciplinares ou auditorias. Esse controlo é o 16.1.7 - Recolha de evidências, do domínio 16, relativo à Gestão de incidentes de segurança de informação.

Com correlação à ação A 2.2, o controlo da ISO 13.1.1 - Controlos da rede do domínio Segurança nas comunicações, recomenda que sejam considerados requisitos para garantia de segurança dos dados que fluem na rede, por exemplo utilizando software para registos de eventos e monitorizar tráfego, para que no caso de existir problemas serem devidamente identificados a tempo.

Ação 2.3 - Comunicação com o CNCS

Esta ação pressupõe a definição de procedimentos para comunicação entre a organização e o CNCS. Estes procedimentos deverão ser analisados pelo departamento jurídico e aprovado pela administração da organização.

O controlo da norma que pode ser associado a esta ação é precisamente o que está relacionado com o Contacto com grupos de interesse especial – 6.1.4 do domínio Organização da Segurança da Informação pois, este controlo como explicado

anteriormente especifica precisamente o contacto com grupos especiais, por exemplo contato com associações de profissionais e outros especializados em segurança de informação para ampliar conhecimentos, sendo este o caso do CNCS.

Ação 2.4 - Inventariação de ativos/produção de um mapa de rede

Algumas organizações já possuem uma inventariação de ativos mas tão importante como efetuar essa inventariação é a atualização periódica desse inventário de ativos e serviços efetuado no mínimo de 6 em 6 meses. Deverá também ser efetuado um diagrama de rede onde deverão constar todos os segmentos de rede, endereçamentos IP e políticas de acesso entre estes.

A norma estudada, possui um controlo que aconselha precisamente a inventariação de ativos, sendo este o controlo 8.1.1, que tal como o roteiro, recomenda que sejam inventariados todos os ativos da organização. Este controlo está associado ao domínio 8, Gestão de Ativos.

Ação 2.5 - Recolha centralizada de registos (logs)

A ação A 2.5 do roteiro recomenda que a organização possua um repositório central de *logs* com um período mínimo de 1 (um) ano pois, os *logs* produzidos pelo sistema operativo e aplicações de suporte à organização são o principal a analisar e investigar em caso de existir um incidente de cibersegurança. De igual forma, é importante que cada servidor permita armazenar os seus próprios *logs* pelo menos durante um mês. É também, imprescindível manter informação de notificações/*logging* nos planos de *backups*.

Relativamente à norma, podemos correlacionar esta ação do roteiro com controlos do domínio 12 responsável pela Segurança nas operações. Um dos controlos é o 12.4.1 - Registo de eventos, que impõe que os eventos/*logs* que aconselha que devem estar ativos *logs* em todos os sistemas/aplicações, e contendo o armazenamento de informações como: utilizador, operação que foi efetuada, data, hora, IP do posto na rede, entre outros.

Outro dos controlos, 12.4.2 - Proteção da informação registada salienta que não é apenas importante obter e conter os *logs*/registos, é importante também manter este tipo de informação segura, protegidos contra acessos não autorizados. É crucial que estes registos/*logs* se mantenham íntegros.

Ação 2.6 - Criação de instrumentos de correção ou mitigação de incidentes

Tal como a ação A 2.6 salienta, é importante que logo que identificada a origem de um incidente é necessária a aplicação de medidas corretivas e/ou de mitigação do mesmo.

Assim sendo, estes instrumentos de correção ou mitigação de incidentes deverão estar devidamente definidos e configurados na organização, para que seja dada uma resposta rápida e efetiva, associando esta ação com o objetivo de controlo 16.1.5 - Resposta a incidentes de segurança que recomenda que esses incidentes sejam mitigados/resolvidos de acordo com os procedimentos criados pela organização. Confirma-se então a importância destes procedimentos a aplicar os instrumentos de correção da problemática em causa.

Ação 2.7 - Estabelecimento de conformidade com a Legislação aplicável

Esta ação salienta que é fundamental a organização ter sempre presente os quadros legais e regulatórios que a sua atividade está sujeita a respeitar.

A norma ISO também possui um controlo que salienta precisamente esta questão, neste caso no domínio 18 de Conformidade. O controlo semelhante à ação A 2.7 é o 18.1.1 - Identificação da legislação aplicável e de requisitos contratuais salientando este que a organização tem o dever e obrigação de saber quais as legislações, regulamentações que controlam o seu tipo de negócio para que possa trabalhar respeitando a lei evitando assim problemas ou contra-ordenações por estar em não conformidade.

Ação 2.8 - Estabelecimento de conformidade com normas aplicáveis à área de atividade

Tal como no ponto anterior, a conformidade com normas ou certificações exigidas por Lei ou por força de exigências contratuais ou regulamentares impostas às atividades da organização deve então ser um fator prioritário. Caso não sejam cumpridas estas normas, certificações, pode haver perdas de reputação que poderão fazer a organização vir a perder clientes.

De igual forma, mas por forma a complementar, correlaciona nesta ação o controlo 18.1.1 - Identificação da legislação aplicável e de requisitos contratuais completando então que para além do descrito em cima, este controlo tem então como objetivo que sejam identificados todos os requisitos legislativos, regulamentares e contratuais aplicáveis à sua organização principalmente relativa à segurança de informação e RGPD.

Ação 2.9 - Criação de política de uso aceitável

De acordo com o roteiro do CNCS, a política de uso aceitável (PUA) dos recursos TIC internos é um requisito organizacional interno bastante importante. Deverão estar definidas neste documento as linhas orientadoras para a utilização dos recursos, de forma segura por todos os utilizadores.

De igual forma, relativamente a ativos, na norma em estudo existe um objetivo de controlo, do domínio Gestão de Ativos, que se define como a utilização aceitável de ativos – 8.1.3, definindo nesta política todas as regras para a utilização dos ativos da organização por parte de todos os utilizadores.

Ação 2.10 - Manutenção de infraestrutura de *Backup/Restore*

A ação A 2.10 do roteiro, relaciona-se com o controlo da norma 12.3.1 - Cópias de segurança, definindo que é fundamental a existência de mecanismos de salvaguarda da informação considerada prioritária para a organização, possibilitando a sua respetiva reposição em caso de necessidade.

Para além do hardware de armazenamento de dados de *backups* que deve ser dimensionado conforme a organização e necessidades em questão, é importante que sejam definidos esses procedimentos de *backup* e de reposição de dados.

Na maioria dos casos será importante devido à elevada importância da informação, prever o armazenamento *off-site* (fora das instalações) ou até mesmo em servidores *Cloud*. Para além da importância de serem efetuados os *backups*, é de igual forma importante testar a integridade dos mesmos, efetuando testes aos mesmos periodicamente.

Ação 2.11 - Mapa de competências e planos de formação

Relativamente a esta ação, o CNCS salienta a importância de identificar para cada colaborador a sua função e o âmbito das suas responsabilidades. Deverá ser contemplado também um plano de formação aos colaboradores para conseguirem atingir os objetivos propostos.

Interligando com a norma em estudo temos o controlo 6.1.1 - Papéis e responsabilidades de segurança da informação, em que este controlo especifica precisamente as responsabilidades e papéis a atribuir de cada um dentro da organização.

Já relativamente à formação, relacionamos com a ação o controlo 7.2.2 - Consciencialização, educação e formação em segurança da informação pertencente ao domínio Segurança nos Recursos Humanos que salienta que a formação e o treino de forma periódica, é bastante importante enquanto o colaborador está a laborar na organização.

Ação 2.12 - Treino e sensibilização interna: geral

Nesta ação o CNCS aconselha que deverão ser realizadas ações internas de sensibilização e dar a conhecer o caderno de procedimentos a todos os colaboradores pertencentes ao quadro laboral da organização. É salientado também nesta ação

que os colaboradores deverão receber formação, equiparando-se assim ao controlo da norma à semelhança da ação anterior, 7.2.2 - Consciencialização, educação e formação em segurança da informação.

Ação 2.13 - Treino e sensibilização interna: gestão

Na ação A 2.13, para além de todos os colaboradores, os elementos da gestão e outras pessoas consideradas pessoas-chave dentro da organização devem ter formação mais orientada aos principais mecanismos no que toca à política de segurança, metodologia de gestão de risco e a sua aplicação na prática.

Tal como nos dois pontos anteriores, o objetivo de controlo da norma em estudo ao qual esta ação se enquadra é o 7.2.2 - Consciencialização, educação e formação em segurança da informação.

4.1.3 *Fase 3 do RCMCS - Mapeamento ações / controlos*

Ação 3.1 - Definição de procedimentos de operação

Nesta ação aconselha-se o desenvolvimento de vários tipos de procedimentos, como procedimentos para detetar incidentes, de atualização de ativos, triagem de incidentes, controlo de fluxo de informação interno e de interação com entidades externas. Esta ação pressupõe ainda a identificação das responsabilidades e funções para os procedimentos desenvolvidos e que informação, meios e resultados são esperados de cada procedimento, quando cada procedimento deve ser utilizado.

Correlacionando esta ação com controlos da norma ISO 27001, temos dois controlos que se cruzam com a ação A 3.1, o controlo 16.1.1 - Responsabilidades e procedimentos que especifica que deverão ser definidos os responsáveis pela gestão dos incidentes e os procedimentos para a realização dos mesmos e o controlo 13.2.2 - Acordos sobre transferência de informação que tratará de como são estabelecidos acordos de transferência segura de informações do negócio entre a organização e as partes externas.

Ação 3.2 - Instalação e configuração de sensores em dispositivos

Relativamente à instalação e configuração de soluções Host-based Intrusion Detection System (HIDS) que incluem funcionalidades de verificação de integridade, conformidade a políticas, análise comportamental dos sistemas, deteção de *rootkits* e análise de tráfego de entrada e saída, entre outras funcionalidades, não está diretamente associada em nenhum dos controlos da norma ISO 27001:2013.

Ação 3.3 - Auditoria de segurança a Bases de Dados

A ação 3.3, prevê a instalação e configuração de mecanismos de registo e auditoria de acesso a bases de dados com informação crítica para salvaguarda desses dados da organização.

O controlo da norma que denota a responsabilidade não apenas na obtenção de *logs* e registos mas também manter este tipo de informação segura, protegida contra acessos não autorizados, não só para bases de dados mas para qualquer tipo de informação armazenada, é o controlo 12.4.2 - Proteção da informação registada.

Ação 3.4 - Instalação e configuração de controlo de acessos web (e.g., serviços proxy)

Um serviço de proxy irá funcionar como um intermediário entre o colaborador e o destino do seu pedido, adicionando estruturas e encapsulamento a sistemas distribuídos.

O uso deste tipo de serviço referido na ação A 3.4, encaixa no controlo 13.1.1 - Controlos da rede da norma em estudo pois este controlo especifica precisamente que deverão ser considerados requisitos para garantia de segurança dos dados que fluem na rede.

Ação 3.5 - Proteção e gestão de equipamentos

Quanto à ação 3.5 que salienta que é extremamente importante que seja instalado um antivírus, ainda que se não seja em todos os postos da organização, seja instalado nos postos com serviços críticos e nos dispositivos dos administradores de sistemas.

Já os dispositivos de comunicação deverão também ser tidos em conta pois em muitas organizações são vistos como indispensáveis para comunicação interna e externa (clientes, fornecedores). Por esse motivo deverão estar ao abrigo de políticas de segurança, da política de utilização aceitável de recursos TIC e consequentemente do Sistema Interno de Normas e Políticas.

À semelhança da ação 3.5 do roteiro, na norma ISO 27001:2013 existem controlos que denotam esse tipo de proteção organizacional, nomeadamente em termos de dispositivos móveis existe o controlo 6.2.1 – Políticas de dispositivos móveis que salienta deverão de ser definidas para utilização dos dispositivos móveis.

Podemos relacionar esta ação com o controlo da norma relativa ao Teletrabalho, controlo 6.2.2 – Teletrabalho, pois como existe um grau de criticidade/maior risco estando os equipamentos fora das instalações da empresa, desprotegidas de *firewall* on-site. Entre outros motivos, deverão ser implementadas políticas e ferramentas

como instalação de antivírus nos equipamentos, instalação de VPN para que o risco seja diminuto em termos de ataques e até mesmo perdas de informação.

Para além do controlo acima, podemos correlacionar esta ação com o controlo 12.2.1 – Controlos contra código malicioso onde salienta que deverão ser descritos procedimentos a serem implementados incluindo a instalação (e atualização) de antivírus para proteger contra ataques, *malware*, *spyware*, *rootkit* entre outros. Este controlo deverá incluir também outro tipo de procedimentos e ferramentas com intuito de proteger a informação da organização.

Ação 3.6 - Instalação e configuração de mecanismos de monitorização

Quanto à ação A 3.6 do roteiro, esta prevê que seja instalado e configurado um sistema de monitorização pelo menos dos principais ativos da rede para controlo e fácil deteção em caso de problema.

De igual forma, mas em relação a serviços de rede que pode ser considerado equivalente, pois os ativos executam serviços que fazem fluir informação na rede, a norma ISO 27001:2013 aconselha que devem ser implementados (controlo 13.1.2 – Segurança de serviços de rede) serviços de proteção e monitorização dos serviços da rede em funcionamento para o seu controlo efetivo da organização.

Ação 3.7 - *Hardening* das configurações

O *hardening* de sistemas é uma coletânea de ferramentas, técnicas e práticas recomendadas para reduzir as vulnerabilidades em *software*, sistemas ou infraestruturas.

Tal como salientado no roteiro, "este é um processo alinhado com um mapeamento das ameaças, das ações de mitigação dos riscos e com a execução das atividades corretivas com foco na infraestrutura." Muitas vezes passa pela alteração e aplicação de restrições a configurações, seja a nível de sistema operativo, quer aplicações, protegendo e assegurando que apenas se tem acesso a funcionalidades estritamente necessárias. Este processo pode também incluir a aplicação e até mesmo manutenção regular de atualizações (*firmware*, sistemas operativos e aplicações), rever permissões de acesso, segurança nos acessos entre outros.

A este tipo de medidas apresentadas na ação 3.7 do roteiro podemos relacionar com alguns controlos da norma em estudo, nomeadamente:

- Controlo 9.4.1 - Restrição de acesso à informação: O acesso às informações e ao sistema devem ser restritos e de acordo com as políticas de acesso sendo realizados de forma individual, ou seja, por utilizador.

- Controlo 12.2.1 - Controlos contra código malicioso: É necessário criar controlos para detetar, prevenir, e recuperar em caso de danificarem alguma parte ou toda a informação.

- Controlo 13.1.1 - Controlos da rede: Devem ser considerados requisitos para garantia de segurança dos dados que fluem da rede.

- Controlo 14.2.4 - Restrições sobre alterações em pacotes de software: As alterações nos pacotes de software devem ser desencorajadas, limitadas às mudanças apenas necessárias e todas as alterações deverão ser estritamente controladas.

Ação 3.8 - Instalação e configuração de um *SIEM*

De acordo com o CNCS, nesta ação com o intuito de obter uma visão holística da segurança da informação crítica da organização, esta deverá possuir um sistema de gestão e correlação de dados e eventos, conhecido como Security Information and Event Managment (SIEM). Este sistema agrega os registos (*logs*) mais relevantes produzidos pelos ativos e pelas aplicações de suporte à atividade, facilitando assim a análise em tempo real e acelerando a tomada de ações defensivas.

Relacionamos assim esta ação que contempla esta instalação e configuração de um SIEM ao controlo 13.1.1 - Controlos da rede pois este objetivo de controlo trata da garantia de segurança dos dados que fluem na rede, utilizando softwares ou serviços para monitorizar tráfego por exemplo.

Ação 3.9 - Definição de planos de continuidade de negócio

Nesta ação 3.9 é reforçada a importância da existência em qualquer organização, por questões de continuidade do negócio, de um plano de continuidade para caso seja necessário a recuperação devido a uma catástrofe, desastre ambiental, entre outros, seja possível continuar a laborar com sucesso.

Esta ação pode ser relacionada com vários controlos da norma, dentro do domínio 17 que denota os aspetos de segurança da informação na gestão da continuidade do negócio:

- Controlo 17.1.1 - Planeamento da continuidade de segurança de informação: A empresa deve determinar quais são os requisitos para a segurança da informação, tendo sempre em consideração a continuidade da informação em situações de desastre seja de que tipo for.

- Controlo 17.1.2 - Implementação da continuidade de segurança da informação: A organização deve estabelecer, documentar, implementar e manter processos,

procedimentos e controlos para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa.

- Controlo 17.1.3 - Verificar, rever e avaliar a continuidade de segurança da informação: O plano de continuidade do negócio, os planos de recuperação em caso de desastres para além de estarem estabelecidos e documentados, devem estar armazenados fora da empresa. Estes deverão ser verificados, testados em intervalos regulares para assegurar que são válidos e eficazes em situações adversas.

Ação 3.10 - Aquisição de competências técnicas

As pessoas na organização incluindo quem faz a análise de artefactos informáticos, quem faz a gestão de incidentes, quem responde a incidentes deverão ter formação periódica na área em que labora para desenvolvimento profissional, por forma a detetarem/resolverem perigos o melhor e mais rápido possível.

Esta ação, enquadra-se assim no controlo 7.2.2 - Consciencialização, educação e formação em segurança da informação tratando de formação periódica neste caso aos profissionais de cibersegurança.

4.1.4 *Fase 4 do RCMCS - Mapeamento ações / controlos*

Ação 4.1 - Cadeia de responsabilidades: formalização

Tendo a cadeia de responsabilidades sido definida na primeira fase, apenas ficará formalizada nesta quarta fase. São pressupostos nesta fase os privilégios de acesso individual aos funcionários, devendo estes ser aprovados pela administração e dado conhecimento a todos os colaboradores.

Relacionando assim esta ação com a norma em estudo, associa-se o controlo 9.4.1 – Restrição de acesso à informação, do domínio 9 - Controlo de acessos. O objetivo deste controlo é definir os acessos à informação e ao sistema, devendo estes ser restritos e estar de acordo com as políticas de acesso, sendo definidos de forma individual, por utilizador.

Ação 4.2 - Definição do Sistema Interno de Normas e Políticas (SINP)

Relativamente à ação A 4.2 do roteiro, esta consiste na regulação e normalização do funcionamento interno da organização através da criação de políticas de segurança, boas práticas e normas internas – SNIP a serem adoptadas por todos os colaboradores.

Em correlação com a norma em estudo, esta ação pode ser relacionada com o controlo 5.1.1 - Políticas para a segurança da informação onde devem ser denotadas todas as políticas de segurança de informação necessárias a serem aprovadas pela direção e divulgadas para todos os funcionários.

O controlo 9.1.1 - Política de controlo de acesso, também se relaciona com a ação A 4.2, aconselha o desenvolvimento de políticas de controlo de acesso em que para a criação destas políticas os proprietários dos ativos deverão determinar as regras apropriadas para o controlo de acesso, quais são os direitos de acesso, as restrições para o acesso aos ativos da informação que devem seguir o princípio de só ter permissão ao que efetivamente seja necessário para desempenhar as funções dentro da empresa.

Ação 4.3 - Análise de risco – reavaliação

Esta ação denota o quão é imprescindível que seja efetuada uma nova avaliação no final da implementação do Roteiro. É recomendável que este processo seja feito de forma contínua. Na norma, não existe um controlo que faça uma reavaliação ao roteiro pois, são documentos completamente independentes (roteiro/norma).

Quanto à avaliação pós implementação de procedimentos de segurança, existe o controlo da norma 17.1.3 - Verificar, rever e avaliar a continuidade de segurança da informação que tem precisamente esse propósito, ou seja garantir que é feita com regularidade e de forma contínua uma avaliação aos procedimentos que foram implementados na organização.

Ação 4.4 - Simulacro

A ação A 4.4 do roteiro aconselha que seja realizado um simulacro, seja com o auxílio do CNCS ou de forma autónoma. Este simulacro servirá para verificar a efetiva implementação do roteiro, se o que é realmente importante para a organização está devidamente implementado por forma a que a organização fique mais segura

É também aconselhado que seja efetuado um simulacro de ataques, catástrofes com uma periodicidade no mínimo anual para tentar detetar falhas na organização e analisar se o plano de continuidade está funcional.

Quanto à ISO 27001:2013, existe um controlo (o mesmo que foi apresentado na ação anterior), 17.1.3 - Verificar, rever e avaliar a continuidade de segurança da informação, que aconselha a que para além da existência de um plano de continuidade da organização, os planos de recuperação em caso de desastres devem estar estabelecidos e documentados. Aconselha também que estejam armazenados fora da empresa, devem ser verificados, testados em intervalos regulares para

assegurar que são válidos e eficazes em situações adversas, incluindo assim simulacros direcionados também aos colaboradores se estão efetivamente mais preparados para as ameaças que poderão existir.

Ação 4.5 - Definição de procedimentos de reação a incidentes

Quanto à ação A 4.5 esta tem como objetivo identificar os tipos de ataques mais comuns e criar métodos para a sua mitigação. O caderno de procedimentos resultante desta ação deverá ser aprovado pelo departamento jurídico e pela administração da empresa. Deverá também ser implementado um sistema de notificações para que um colaborador saiba como deve proceder perante um incidente.

Relativamente à norma ISO, o controlo que podemos relacionar com esta ação do roteiro é o 16.1.6 - Aprender com os incidentes de segurança da informação pois é um controlo a implementar para que haja aprendizagem com os conhecimentos obtidos da análise e resolução de incidentes para reduzir a probabilidade ou o impacto de incidentes futuros.

Assim sendo é importante que todos os incidentes sejam registados com todos os detalhes, numa ferramenta que nos permita consultá-los facilmente quando necessário. Estes incidentes em histórico podem também ser aproveitados para treino e consciencialização dos funcionários para tentar evitar que esses mesmos incidentes ocorram no futuro.

Em complemento ao controlo acima descrito, de forma a associar à ação 4.5 do roteiro podemos salientar a norma 16.1.3 - Reportar os pontos fracos de segurança da informação que impõe que os funcionários e fornecedores/prestadores de serviços que utilizam os serviços e os sistemas de informação da organização devem ser instruídos a detetar, e responsabilizados de reportar qualquer ponto fraco na segurança da informação.

Ação 4.6 - Treino e sensibilização interna: SINP

Estando a ação A 4.6 mais focada para o treino e sensibilização interna, e o SINP ser um sistema que deve ser transversal a todos os colaboradores da empresa, é fundamental que todos os colaboradores, principalmente os que ocupem cargos de chefia recebam formação e treino adequado para o cumprimento adequado conforme o que foi definido para cada função e até em termos de segurança de informação.

Neste aspeto, e correlacionando esta ação com um controlo da norma, o controlo 7.2.2 - Consciencialização, educação e formação em segurança da informação salienta de igual forma que a formação e o treino são bastante importantes durante o período em que o funcionário se mantenha a laborar na organização. A organização deve

manter um programa de atualização, informação e aperfeiçoamento periódico sobre segurança da informação para os seus funcionários. Por exemplo poderá ser criado um meio de comunicação periódico com dicas de segurança, informações importantes e acontecimentos. Pode até ser enviado por email ou afixado num quadro para que o funcionário possa estar sempre ciente e atualizado.

É importante a prática, o treino por exemplo semestral, anual, incluindo palestras, eventos, tudo voltado para a segurança da informação para manter o funcionário sempre ativo e consciente da necessidade de segurança da informação para que tenha atitudes seguras.

Ação 4.7 - Testes de aceitação de serviços

Na ação A 4.7 é proposto numa postura defensiva que as organizações adotem práticas que implementem o princípio da segurança na conceção e por defeito. De modo a complementar este princípio, é necessário que todos os serviços baseados em recursos TIC sejam submetidos a testes de segurança, antes de serem expostos à utilização geral.

Estes testes deverão ser efetuados por especialistas. A principal finalidade é submeter todos estes recursos a diferentes tipos de testes, de modo a prevenir possíveis problemas detetados, e aprovar o recurso quando estiver em condições aceitáveis.

O controlo 14.2.9 -Testes de aceitação de sistemas da norma ISO denota precisamente o que a ação acima salienta, que devem ser estabelecidos programas de testes de aceitação e de igual forma os respetivos critérios de aceitação para novos sistemas/serviços de informação, atualizações e novas versões.

Ação 4.8 - Mecanismos de engodo (*honeypots*)

Tal como salientado no roteiro, as proteções de perímetro são um filtro relevante para evitar/bloquear a maioria das ameaças. Porém, é necessário ter uma postura de prevenção.

Os *honeypot* são sistemas dedicados que reproduzem certas funcionalidades da organização e têm como objetivo atrair atacantes para permitir saber os seus métodos e avaliar as suas capacidades. Estes sistemas replicam o servidor de correio eletrónico, por exemplo.

Nesta fase é expectável que seja feita a instalação e configuração do *honeypot* dentro de zonas de segurança que processem ativos com informação sensível.

Esta ação, não tem diretamente correlação com qualquer controlo da norma e estudo.

Ação 4.9 - Gestão de mudança e atualizações

Quanto à ação A 4.9 do roteiro, este salienta que uma boa gestão de *patching* e atualizações de sistemas é essencial para manter um bom nível de segurança. É essencial que seja mantido o equilíbrio entre manter as aplicações o mais atualizadas possível e o facto destas atualizações trazerem consequências como incompatibilidades, pondo assim em causa o bom funcionamento dos sistemas. Os processos de mudança devem ser planeados de forma a prevenir os riscos identificados na ação A 1.6.

Relativamente a correlações com controlos da norma, esta ação encaixa com vários controlos sendo um deles o 14.2.9 - Testes de aceitação de sistemas, que aconselha que devem ser estabelecidos programas de testes de aceitação e de igual forma os respetivos critérios de aceitação para novos sistemas de informação, atualizações e novas versões como salientado na ação A 4.7 cima apresentada.

Outro controlo interligado o 12.1.4 - Separação entre ambientes de desenvolvimento, testes e de produção cujo controlo denota como boa prática a separação dos ambientes de desenvolvimento, de testes e de produção sendo que o objetivo é a redução de riscos em serviços ou sistemas em produção.

Por forma a complementar a correlação desta ação a controlos da norma, acrescenta-se o controlo 14.2.4 - Restrições sobre alterações em pacotes de software que salienta que as alterações nos pacotes de software devem ser desencorajadas, limitadas às mudanças apenas necessárias e todas as alterações deverão ser estritamente controladas.

4.1.5 *Fase 5 do RCMCS - Mapeamento ações / controlos*

Ação 5.1 – Nomear um CISO

A ação A 5.1 destina-se à nomeação de um CISO para atribuir a gestão da segurança de informação a um responsável máximo. O CISO é o topo da hierarquia relativamente à gestão da segurança da informação da organização.

Relacionando esta ação com a norma ISO em estudo, no controlo 16.1.1 – Responsabilidades e procedimentos denota precisamente o mesmo, deve ser definido quem será o responsável máximo da segurança de informação da organização e salienta

também que devem ser definidos os responsáveis pela gestão dos incidentes e os procedimentos para a realização dos mesmos, pelos analistas por exemplo.

Ação 5.2 – Estabelecer um serviço de gestão de vulnerabilidades

Este serviço é considerado indispensável no quadro de competências do SOC ou CSIRT. Este tipo de serviço engloba por norma as componentes de deteção e mitigação. Deve ser executado com a periodicidade adequada, para detetar vulnerabilidades na rede e deve utilizar ferramentas automatizadas.

O serviço de deteção também deve estar disponível como parte do portfólio de serviços para apoiar os testes de aceitação de novos serviços (ação A 4.9). Se forem detetadas vulnerabilidades, é preciso proceder à sua mitigação.

A ação A 5.2, pode ser associada ao controlo da norma 12.6.1 – Gestão de vulnerabilidades técnicas. Uma vulnerabilidade é uma falha que o ativo de informação pode conter que pode ser explorada com o objetivo de roubar ou destruir a informação. É então necessário explorar as possíveis vulnerabilidades dos ativos para eliminar ou minimizar os riscos e os danos.

Este controlo tem uma ligação para o controlo de gestão de alterações, pois dependerá de uma atualização/alteração para resolução das vulnerabilidades. Uma política e procedimentos poderão ser criados com explicativo detalhado de quem são os responsáveis pelas análises de vulnerabilidades nos ativos, qual o período de recorrência destas análises, como devem ser avaliadas essas vulnerabilidades e também criar procedimentos de como se deve agir em cada caso.

As vulnerabilidades podem ter diversos níveis, desde um nível baixo a um nível mais críticas que requerem ações mais imediatas despoletando o processo de gestão de alterações o mais imediato possível.

Ação 5.3 – Estabelecer e implementar um plano de auditorias

Esta ação tem como objetivo a definição e implementação de um plano de auditorias, tendo como objetivo avaliar e colocar à prova os controlos implementados na organização. É aconselhável que essas auditorias sejam complementadas com auditorias externas através de empresas especializadas. Essas auditorias devem ter um plano de periodicidade de pelo menos uma vez por ano.

Na norma em estudo, as atividades de auditoria também são contempladas estando presentes no controlo 12.7.1 - Controlos de auditoria nos sistemas de informação, salientando que as atividades de auditoria e os seus requisitos que envolvam verificações nestes sistemas de produção deverão para além de periódicos, ser planeados por forma a minimizar as interrupções nos processos de negócio.

Para complementar a correlação ação-controlo existe o controlo 18.2.2 - Conformidade com as políticas e normas de segurança em que os gestores devem rever regularmente a conformidade do processamento da informação e dos procedimentos dentro da sua área de responsabilidade com as políticas de segurança, normas e quaisquer outros requisitos de segurança apropriados.

Os gestores de cada setor necessitam de criar requisitos, indicadores e metas para esta revisão. Ao encontrar uma não conformidade na avaliação devem proceder com ações corretivas o mais rápido possível.

Ação 5.4 – Definir a missão, a comunidade servida e o portfólio de serviços do CSIRT

A ação A 5.4 tem como objetivo a definição da visão e da missão do CSIRT na organização. Isso consiste em definir a comunidade servida e o desenho do portfólio de serviços adequados para abranger os objetivos propostos. Neste portfólio deve constar no mínimo o tratamento de incidentes de segurança e a gestão de vulnerabilidades. Para a definição da visão é necessário contemplar a gestão de ativos, a definição de uma cadeia de responsabilidades e os processos de mitigação de incidentes.

À semelhança desta ação, a norma da ISO em estudo também potencia que sejam contemplados procedimentos relativos ao tratamento de incidentes de segurança e também relativamente à gestão de vulnerabilidades.

Quanto à gestão de vulnerabilidades, o controlo 12.6.1 – Gestão de vulnerabilidades técnicas à semelhança da ação A 5.2, tratará precisamente da gestão e mitigação das vulnerabilidades.

Ação 5.5 – Elaborar e fazer aprovar o plano e o orçamento para o CSIRT

Tal como está presente no roteiro do CNCS na ação A 5.5, "um SOC ou CSIRT deve ter uma estrutura capaz e sustentável. Para esse efeito é necessária a aprovação, por parte da direção da organização, de um plano de ação e orçamento para montar e operar a equipa. O sucesso do SOC ou CSIRT depende da objetividade da sua missão e da adequação dos meios e dos instrumentos para atingir os seus objetivos."

Tendo em conta o acima descrito, não existe nenhum controlo da norma em estudo que possamos associar a esta ação.

Ação 5.6 – Implementar e anunciar o CSIRT

Quanto à ação A 5.6, normalmente um CSIRT precisa de um sistema de registo de ocorrências e comunicações, canais de comunicação (telefone, correio eletrónico

ou portais web), mecanismos de encriptação e de ferramentas de suporte à análise forense de artefactos.

Esta ação prevê a aquisição e montagem das infraestruturas técnicas e operacionais bem como a afetação, requalificação ou contratação dos recursos humanos necessários. As capacidades exigidas dos colaboradores que façam parte do CSIRT são: procedimentos de tratamento de incidentes, análise técnica de tráfego, análise técnica de artefactos e análise técnica de *malware*.

O CSIRT deve igualmente solicitar ao prestador de serviços de comunicações eletrónicas a publicação de um objeto IRT junto do LIR.

Tal como na ação anterior, não existe correlação prática, direta ou até mesmo indireta com qualquer controlo da norma em estudo.

Ação 5.7 – Estabelecer um sistema de gestão de Crise

Na ação A 5.7 é demonstrado o quão é importante um sistema de gestão de crise para lidar com grandes incidentes de segurança que coloquem em causa a continuidade laboral da organização.

À semelhança do roteiro, a norma ISO em estudo também contempla um controlo responsável por implementar procedimentos que em caso de existir uma grande catástrofe seja possível a continuidade laboral da organização. Este controlo é o 17.1.2 - Implementação da continuidade de segurança da informação e salienta que a organização deve estabelecer, documentar, implementar e manter processos, procedimentos e controlos para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa. Deve assegurar uma estrutura de gestão adequada por forma a mitigar e responder a um evento de interrupção, designar pessoas com autoridade e competências para resposta aos incidentes existentes.

É crucial que os planos estejam documentados com procedimentos de recuperação e as respostas estejam devidamente aprovadas pela administração. Estes planos deverão ser detalhados por exemplo, como se irá desenrolar um evento de interrupção. Esses planos ditarão as regras do que fazer, e como fazer caso haja um incidente. É importante manter esses documentos fora da empresa, pois dependendo do tipo de desastre, poderá existir perda também desses mesmos planos.

Ação 5.8 – Afiliação nas comunidades nacionais e internacionais de CSIRT

Esta ação indica que "O sucesso de um CSIRT depende da sua boa integração nas várias comunidades de cibersegurança e das relações de confiança que aí são criadas."

É então aconselhado que o CSIRT deverá "afiliar-se e participar ativamente nos programas de trabalhos das comunidades nacionais de CSIRT, tais como a Rede Nacional de CSIRT e, se adequado, do Task-Force for CSIRTs in Europe (TF-CSIRT) ou Forum of Incident Response and Security Teams (FIRST)".

Esta ação, na norma em estudo não se relaciona com nenhum dos controlos.

Ação 5.9 – Participação num exercício nacional de cibersegurança

Os exercícios de cibersegurança salientados nesta ação têm dois objetivos importantes: um deles é o testar as capacidades do que foi implementado, mas principalmente testar os procedimentos para responder aos incidentes por forma a melhorar a articulação interna e externa com as partes interessadas.

Este tipo de exercícios acima descritos podem ser equiparados aos exercícios a serem efetuados com a implementação do controlo da norma em estudo 17.1.3 - Verificar, rever e avaliar a continuidade de segurança da informação. O objetivo é precisamente avaliar se os procedimentos de segurança de informação estão efetivamente bem implementados, a serem seguidos pelos utilizadores, testados em intervalos regulares por forma a que o plano de continuidade do negócio esteja válido e pronto a ser colocado em prática em situações adversas.

Em relação à participação num exercício de cibersegurança pelo menos uma vez por ano, seja o mesmo de âmbito nacional ou internacional, não existe correlação na norma em estudo com este ponto de vista do roteiro pois, na norma apenas é salientado que deverá existir exercícios, testes, garantindo a continuidade do negócio, e não impõe que seja um exercício nacional/internacional.

4.2 MAPEAMENTO GRÁFICO DAS AÇÕES - CONTROLOS

Numa perspetiva de facilitar a análise de correlações entre as ações do roteiro e controlos da norma ISO 27001:2013, esses relacionamentos foram ilustrados graficamente através de uma tabela com dois eixos. O eixo apresentado na horizontal indica as ações do RCMCS, apresentadas a verde quando existe uma correlação e a vermelho quando não existiu correlação encontrada. Quanto ao eixo na vertical, estão apresentados os controlos da norma ISO 27001:2013 em estudo.

Este mapeamento apresentado em forma de tabela é o resultado dos mapeamentos teóricos analisados anteriormente, cujas correlações estão apresentadas na tabela através do caracter X, a cor verde. As células a vermelho na horizontal que demarcadas a vermelho são controlos da norma sem encaixe nas ações do roteiro (exemplo

AC	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
CTR																																																			
A 5.1.1								X																								X																	
A 5.1.2																																																			
A 6.1.1							X													X																															
A 6.1.2																																																			
A 6.1.3		X																																																
A 6.1.4		X										X																																						
A 6.1.5																																																			
A 6.2.1																											X																								
A 6.2.2																											X																								
A 7.1.1																																																			
A 7.1.2																																																			
A 7.2.1																																																			
A 7.2.2																				X	X	X										X						X												
A 7.3.1																																																			
A 8.1.1													X																																						
A 8.1.2																																																			
A 8.1.3																		X																																	
A 8.1.4																																																			
A 8.2.1			X			X																																												
A 8.2.2																																																			
A 8.2.3																																																			
A 8.3.1																																																			
A 8.3.2																																																			
A 8.3.3																																																			
A 9.1.1																																		X																	
A 9.1.2																																																			
A 9.2.1																																																			
A 9.2.2																																																			
A 9.2.3																																																			
A 9.2.4																																																			
A 9.2.5																																																			
A 9.2.6																																																			
A 9.3.1																																																			
A 9.4.1																													X				X																	
A 9.4.2																																																			
A 9.4.3																																																			
A 9.4.4																																																			
A 9.4.5																																																			
A 10.1.1				X																																														
A 10.1.2				X																																														
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 11.2.2																																																			
A 11.2.3																																																			
A 11.2.4																																																			
A 11.2.5																																																			
A 11.2.6																																																			
A 11.2.7																																																			
A 11.2.8																																																			
A 11.2.9																																																			
A 12.1.1																																																			
A 12.1.2																																																			

Figura 13: Tabela de mapeamento entre ações/controlos - Parte 1

AC	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
A 12.1.3																																																			
A 12.1.4																																									X										
A 12.2.1										X																	X		X																					
A 12.3.1																			X																																
A 12.4.1														X																																					
A 12.4.2														X											X																									
A 12.4.3																																																		
A 12.4.4																																																		
A 12.5.1																																																		
A 12.6.1						X																																					X		X				
A 12.6.2																																																		
A 12.7.1																																													X					
A 13.1.1											X															X			X	X																			
A 13.1.2																												X																						
A 13.1.3										X																																								
A 13.2.1																																																		
A 13.2.2																							X																											
A 13.2.3																																																		
A 13.2.4																																																		
A 14.1.1																																																		
A 14.1.2																																																		
A 14.1.3																																																		
A 14.2.1																																																		
A 14.2.2																																																		
A 14.2.3																																																		
A 14.2.4																													X													X								
A 14.2.5																																																		
A 14.2.6																																																		
A 14.2.7																																																		
A 14.2.8																																																		
A 14.2.9																																										X		X						
A 14.3.1																																																		
A 15.2.1																																																		
A 15.2.2																																																		
A 16.1.1	X	X					X																X																				X						
A 16.1.2									X																																									
A 16.1.3									X																																				X					
A 16.1.4									X																																								
A 16.1.5														X																																				
A 16.1.6																																													X					
A 16.1.7											X																																							
A 17.1.1																																																			
A 17.1.2																																																			
A 17.1.3																																																			
A 17.2.1																																																			
A 18.1.1																X	X																																		
A 18.1.2																																																		
A 18.1.3																																																		
A 18.1.4																																																		
A 18.1.5																																																		
A 18.2.1																																																		
A 18.2.2																																															X			
A 18.2.3																																																	

Figura 14: Tabela de mapeamento entre ações/controlos - Parte 2

- A 5.1.2; A 6.1.2), à semelhança das células a vermelho na vertical que demonstram as ações sem correlação com controlos da ISO (exemplo - A 1.5; A 3.2).

Dando continuidade ao mapeamento gráfico demonstrado nas Figuras 13 e 14, e por forma a complementar o mesmo, foi gerado um novo mapa de mapeamento.

Este novo mapa, desta vez simplificado apresentando à esquerda apenas os controlos da norma que estão de alguma forma correlacionados com alguma ação do roteiro em estudo, complementando assim as correlações encontradas com uma classificação utilizando heurísticas divididas em três graus:

- **Ação** - (AC): são definidas estas correlações no caso da ação do roteiro e o controlo da norma em estudo, serem iguais ou muito semelhantes em termos de âmbito ou objetivo ao serem aplicados.
- **Alvo** - (AL): no caso de uma correlação tipo "alvo", esta corresponde a que tanto o roteiro como a norma têm o mesmo objetivo final, mesmo que as ações sugeridas sejam diferentes.
- **Âmbito** - (AM): já a correlação tipo "âmbito", neste caso tanto o roteiro como a norma têm o mesmo âmbito mas as ações ou mesmo o objetivo final explícito são diferentes.

Um exemplo de correlação entre uma ação do RCMCS e um controlo da norma ISO 27001 temos:

- RCMCS (Ação 2.10) - Manutenção de infraestrutura de cópias de segurança e reposição (Backup/Restore): é importante possuir equipamentos e aplicações que permitam a salvaguarda da informação considerada fulcral para a organização, por forma a ser reposta em caso de necessidade. Para verificar a integridade dessas cópias de segurança, devem ser efetuados a testes periódicos de reposição.

- ISO 27001:2013 (Controlo 12.3.1) - Para além de ser realizadas cópias de segurança, deverão ser testadas periodicamente estas cópias de segurança efetuadas para assegurar o seu bom estado.

A correlação apresentada acima demonstra uma correlação do tipo AC "ação", pois os propósitos e objetivos da ação e do controlo são os mesmos.

Na Figura 15 apresenta-se uma tabela com o mapeamento das correlações classificadas com as heurísticas definidas para todas as correlações encontradas entre o roteiro e a norma.

AC	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
CTR																																																			
A 5.1.1								AL																									AL																		
A 6.1.1							AL													AC																																
A 6.1.3		AL																																																	
A 6.1.4		AL										AM																																							
A 6.2.1																											AL																								
A 6.2.2																											AL																								
A 7.2.2																				AL	AM	AM										AL							AM													
A 8.1.1													AL																																						
A 8.1.3																		AC																																		
A 8.2.1			AC			AM																																													
A 9.1.1																																		AL																
A 9.4.1																													AM				AC																
A 10.1.1				AM																																														
A 10.1.2				AM																																														
A 12.1.4																																										AL								
A 12.2.1										AC																	AL		AM																			
A 12.3.1																			Ac																																
A 12.4.1														AC																																				
A 12.4.2														AC											AL																								
A 12.6.1						AM																																					AC		AM				
A 12.7.1																																												AC					
A 13.1.1											AC															AL			AM	AM																	
A 13.1.2																												AC																				
A 13.1.3										AM																																						
A 13.2.2																							AM																										
A 14.2.4																													AM												AL						
A 14.2.9																																								AC		AL						
A 16.1.1	AL	AL					AL																AM																			AC						
A 16.1.2									AC																																							
A 16.1.3									AC																																							
A 16.1.4									AC																																							
A 16.1.5															AL																																		
A 16.1.6																																							AL									
A 16.1.7											AC																																					
A 17.1.1																															AC																	
A 17.1.2																															AC													AM			
A 17.1.3																															AC				AM	AL									AM	
A 18.1.1																AC	Ac																															
A 18.2.2																																													AL				

Legenda - *Heuristicas*

AC	**Ação:** Tanto o roteiro como a norma sugerem as mesmas ações ou muito semelhantes.
AL	**Alvo:** Tanto o roteiro como a norma têm o mesmo objetivo final, mesmo que as ações sugeridas sejam diferentes.
AM	**Âmbito:** Tanto o roteiro como a norma têm o mesmo âmbito mas as ações ou mesmo o objetivo final explícito são diferentes.

Figura 15: Tabela de mapeamento com classificação - Heurísticas

5

CASO DE ESTUDO - APLICAÇÃO EM PME

Este capítulo apresenta detalhes sobre a implementação do caso de estudo, descrevendo na prática o pós mapeamento, ou seja, desde a escolha das questões para o questionário através das correlações existentes, até à obtenção das respostas através da disponibilização do questionário a 17 empresas PME localizadas na região de Leiria.

5.1 VISÃO TÉCNICA ANTES DA REALIZAÇÃO DO QUESTIONÁRIO

Antes da realização do questionário às empresas escolhidas para preenchimento, tendo em conta que existe o conhecimento técnico amplo do que está presente ou implementado na área das TIC destas empresas, foi efetuado um levantamento ponderado em escala de uma interpretação técnica do estado de cibersegurança destas.

Este levantamento embora subjetivo é um parecer com base numa perceção relativa ao estado da cibersegurança na organização pois conhecendo a empresa através de serviços técnicos efetuados na mesma, conhecendo serviços, tipo de informação armazenada, cópias de segurança efetuadas, procedimentos de organização, é possível classificar a empresa se está ou não segura ainda que numa base percepcional.

Esta perceção foi enquadrada, dentro de uma escala de 1 a 4 (não satisfaz a muito bom), demonstrada no capítulo seguinte para que fosse possível uma comparação pós realização do questionário se o que tecnicamente é conhecido, é de alguma forma concordante com os resultados obtidos num levantamento efetivo e justificado, do questionário gerado através da correlação entre as ações do roteiro e controlos da norma.

5.2 PLATAFORMA PARA REALIZAÇÃO DO QUESTIONÁRIO

Foram consideradas diversas plataformas para a operacionalização de implementação do questionário como por exemplo a aplicação Survey Monkey[1], porém os vários testes efetuados não preencheram os requisitos pretendidos, um deles a simplicidade no preenchimento por parte do utilizador.

A plataforma escolhida após a realização de testes noutras plataformas, tem de seu nome Question Pro[2], sendo uma aplicação bastante intuitiva e efetiva na realização do que se pretendia apurar pois, para além de uma personalização completa do questionário, permitiu também a existência de lógica avançada para que, ao escolher determinada questão aparecessem ou não questões de resposta condicionada.

Na Figura 16 está apresentada a página inicial do questionário, utilizando a aplicação Question Pro acima mencionada.

Figura 16: Questionário - Ecrã inicial

Para além de uma interface intuitiva para o utilizador que responde ao questionário, esta plataforma possui um *backoffice* bastante completo, sendo assim possível uma análise de resultados mais completa, com gráficos, tabelas e dados bastante relevantes.

1 Survey Monkey - https://pt.surveymonkey.com
2 QuestionPro - https://www.questionpro.com

Em termos de condicionalismos das questões presentes no questionário, esta aplicação permitiu uma configuração bastante simplificada, e bastante simples no âmbito do utilizador. Estas condições configuradas na aplicação permitiram em algumas questões se respondidas de forma negativa as perguntas relacionadas com essa questão "mãe"não eram apresentadas.

Na Figura 17 é visível um exemplo de uma questão condicional.

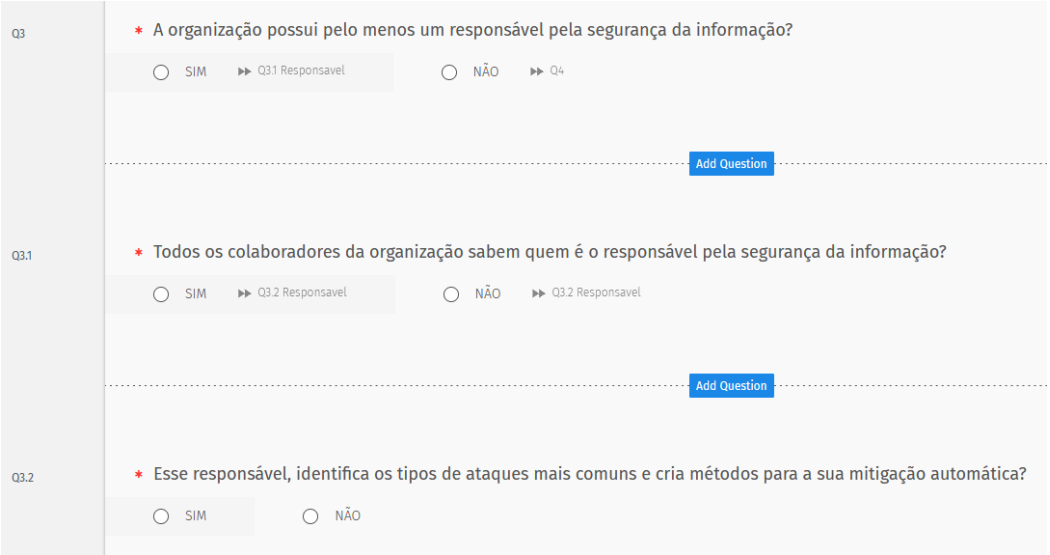


Figura 17: Implementação do questionário - Exemplo de uma questão condicional

Neste exemplo apresentado, no caso da questão três (3) for respondida de forma positiva (opção "sim"), o utilizador irá entrar nas duas questões condicionais a ela associada neste caso 3.1, relativamente a um responsável da informação. Caso seja respondido à questão 3 "não", significa que não existe um responsável de informação não fazendo sentido apresentar as questões relativas ao mesmo. Neste caso ao ser respondido negativamente (opção "não") à pergunta três (3), a questão seguinte será a questão quatro (4).

No Anexo A encontra-se para consulta o questionário final, tal como este foi disponibilizado às organizações implementado utilizando a plataforma anteriormente citada.

5.3 IMPLEMENTAÇÃO DO CASO DE ESTUDO

Na implementação do caso de estudo apresentado neste relatório, como demonstrado na Figura 18, foram delineadas 5 fases a seguir, as quais se encontram descritas de

seguida. O processo descreve as tarefas realizadas desde a construção do questionário até à análise dos resultados obtidos pelo mesmo.

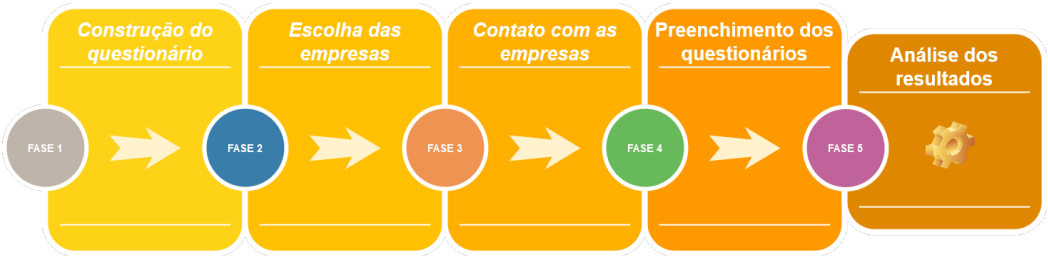


Figura 18: Processo de desenvolvimento e implementação do questionário

5.3.1 *Construção do questionário*

Para que fosse possível um levantamento de questões a serem apresentadas no questionário, após o estudo e mapeamento anteriormente apresentado, foi efetuada uma lista de ações do roteiro que continham uma correlação com um controlo da norma ISO 27001:2013.

Relativamente às condições de aceitação por parte de quem preenche o questionário para prosseguir para as questões seguintes, mais técnicas estão presentas na Figura 19.

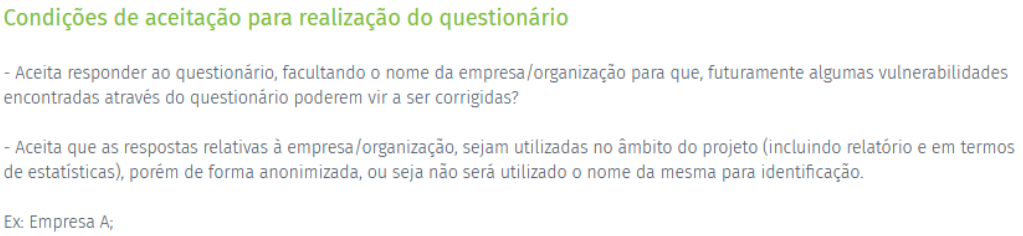


Figura 19: Condições de aceitação - Questionário

Ainda que anonimizados os resultados foi solicitado o nome da organização para que pudessem ser implementados alguns controlos numa fase futura. Para o desenvolvimento deste projeto, foi atribuído um identificador utilizando uma letra (A, B, C, ...) a cada empresa e todo o tratamento e apresentação de resultados foi através dessa identificação atribuída.

Por forma a complementar as questões, foram acrescentadas duas perguntas relevantes no âmbito da metodologia implementada, nomeadamente se a empresa

possuía infraestruturas críticas dentro das instalações da empresa, por exemplo, servidores. Outra questão apresentada é se a empresa inquirida seria efetivamente uma PME, elucidando o utilizador quais são as condições para uma empresa ter estatuto de PME.

- *Questão 0:*

A organização em estudo no questionário, é uma PME* (Pequena ou Média Empresa)?

- *Questão 1:*

A organização possui infraestruturas informáticas críticas nas instalações da empresa? Ex: Servidores, etc.

De notar que abaixo não serão apresentadas ações sem correlação com os controlos, pois estas não geraram questões a serem efetuadas ao utilizador.

Quanto às questões geradas através do relacionamento entre as ações do roteiro de capacidades mínimas e os controlos da norma ISO 27001:2013, questões estas agrupadas pelas ações do roteiro apresenta-se,

Ação 1.1 & Ação 1.2 & Ação 5.1:

- *Questão 2:*

  A organização possui pelo menos um responsável pela segurança da informação?

- *Questão 3:*

  Em relação a incidentes de segurança que aconteçam, a organização possui um elemento responsável pela gestão desses incidentes?

Ação 1.3:

- *Questão 4:*

  Na organização estão definidos quais os serviços/funções e atividades críticas, atividades estas que limitem a produção laboral?

- *Questão 5:*

  A informação que está armazenada na organização, tem definida classificação relativamente à sua importância, valor e sensibilidade?

Ação 1.4:

- *Questão 6:*

  Aquando existe troca de informação critica seja com entidades internas ou externas são utilizados controlos criptográficos para salvaguarda da informação em trânsito?

Ação 1.6:

- *Questão 7:*

  Existe uma análise/gestão de riscos definida na organização, onde estão identificados os mais prováveis riscos que poderão advir, avaliados e também como deverão ser respondidos em caso de se tornarem uma realidade?

Ação 1.7:

- *Questão 2.1:* (Se resposta à questão 2 for positiva)

  Todos os colaboradores da organização sabem quem é o responsável pela segurança da informação?

- *Questão 8:*

  Todos os colaboradores da organização têm pleno conhecimento de quais as suas responsabilidades, direitos e papéis a desempenhar na organização?

Ação 1.8:

- *Questão 9:*

  A organização tem definidas políticas de segurança da informação, políticas estas aprovadas pela administração e divulgadas aos restantes colaboradores?

Ação 1.9 & Ação 3.1:

- *Questão 10:*

  Existem procedimentos internos definidos para notificação de incidentes de cibersegurança por parte dos colaboradores?

- *Questão 10.1:* (Se resposta à questão 10 for positiva)

  Esses incidentes, são classificados conforme a sua criticidade para que haja uma triagem/prioridade na resolução dos incidentes?

Ação 2.1:

- *Questão 11:*

  Estão definidas áreas/zonas críticas de acesso à organização quer em termos físicos quer em termos lógicos (através dos sistemas)?

- *Questão 12:*

  A arquitetura de rede & segurança da informação estão desenhadas?

- *Questão 13:*

  A organização tem implementados sistemas de deteção/prevenção de intrusão como uma Firewall/IDS?

Ação 2.2:

- *Questão 14:*

  A organização tem implementado um sistema de recolha de metadados do tráfego que flui na rede?

Ação 2.3:

- *Questão 15:*

  A organização comunica com algum grupo de profissionais, seja o CNCS (Centro Nacional de Cibersegurança), seja outro especializado em segurança de informação com objetivo de ampliar conhecimentos?

Ação 2.4:

- *Questão 16:*

  Na sua organização é efetuada uma inventariação de ativos e serviços?

- *Questão 16.1:* (Se resposta à questão 16 for positiva)

  Essa inventariação de ativos e serviços, é atualizada pelo menos de 6 em 6 meses?

Ação 2.5:

- *Questão 17:*

  Relativamente à recolha centralizada de registos (Logs), que devem ser preservados pelo menos um ano, a sua organização efetua essa recolha de registos e por sua vez o seu armazenamento seguro?

- *Questão 20.2:* (Se resposta à questão 20 for positiva)

  As notificações de cópias de segurança (backups), estão configuradas para notificar em caso de falha?

Ação 2.6:

- *Questão 10.2:* (Se resposta à questão 10 for positiva)

  A organização possui configurados mecanismos de correção ou mitigação de incidentes de segurança de informação?

Ação 2.7 & Ação 2.8:

- *Questão 18:*

  A organização tem presentes e são periodicamente atualizados, os quadros legais e regulatórios que a sua atividade está sujeita a respeitar?

Ação 2.9:

- *Questão 19:*

  Está definida a política de uso aceitável (PUA) na organização, política esta

que contém as linhas orientadoras para a utilização dos recursos, de forma segura por todos os colaboradores?

Ação 2.10:

- *Questão 20:*

  Em relação a cópias de segurança, a organização tem implementados mecanismos de salvaguarda de informação (backups), pelo menos da informação considerada prioritária?

- *Questão 20.1:* (Se resposta à questão 10 for positiva)

  As cópias de segurança efetuadas são periodicamente testadas com o fim de se confirmar que não estão corrompidas?

- *Questão 20.3:* (Se resposta à questão 10 for positiva)

  As cópias de segurança efetuadas, (existindo) estão a ser replicadas para o exterior?

Ação 2.11:

- *Questão 21:*

  Está contemplado na organização um plano de formação para os colaboradores?

Ação 2.12:

- *Questão 22:*

  A organização efetua ações de sensibilização e treino interno para consciencialização dos colaboradores?

Ação 2.13:

- *Questão 23:*

  As pessoas chave da organização (administração, chefias) têm formação mais orientada aos principais mecanismos no que toca à política de segurança, metodologia de gestão de risco e sua aplicação na prática?

Ação 3.3:

- *Questão 24:*

  A organização tem configurados mecanismos de registo e auditoria de acesso a bases de dados com informação crítica?

Ação 3.4:

- *Questão 25:*

  Estão configurados mecanismos de controlo de acessos web (proxy por exemplo)?

Ação 3.5:

- *Questão 26:*

  A organização possuí um antivírus fidedigno configurado nos ativos mais críticos da organização?

- *Questão 27:*

  Existem procedimentos definidos para utilização dos dispositivos de comunicação e/ou dispositivos móveis? (Telemóveis, portáteis, tablets)

Ação 3.6:

- *Questão 28:*

  A organização tem configurado um sistema de monitorização de pelo menos os principais ativos da rede?

Ação 3.8:

- *Questão 29:*

  A organização tem implementado um SIEM, que agrega os registos (logs) mais relevantes produzidos pelos ativos e pelas aplicações de suporte à atividade?

Ação 3.9:

- *Questão 30:*

  Está definido um plano de continuidade da organização, para que em caso de catástrofe seja possível continuar com o negócio?

Ação 3.10:

- *Questão 31:*

  O staff de quem faz parte do departamento de segurança de informação, TIC, possuí formação periódica na área para que seja devidamente atualizado em termos de perigos existentes, vulnerabilidades, etc.

Ação 4.1:

- *Questão 32:*

  Os privilégios de acesso individual à informação, foram devidamente aprovados pela administração e revistos com frequência?

Ação 4.2:

- *Questão 33:*

  A organização procedeu a criação de políticas de segurança, boas práticas e normas internas a serem adotadas por todos os colaboradores?

Ação 4.3:

- *Questão 34:*

  Existe uma reavaliação continua de acessos, privilégios, procedimentos implementados na empresa em relação à segurança de informação?

Ação 4.4:

- *Questão 35:*

  A organização efetua um simulacro periodicamente por forma a encontrar vulnerabilidades no que foi implementado para a segurança de informação?

Ação 4.5:

- *Questão 10.3:* (Se resposta à questão 10 for positiva)

  Todos os colaboradores da organização sabem como devem notificar um incidente?

- *Questão 2.2:* (Se resposta à questão 2 for positiva)

  Esse responsável, identifica os tipos de ataques mais comuns e cria métodos para a sua mitigação automática?

Ação 4.6:

- *Questão 36:*

  Os colaboradores, principalmente os que ocupam cargos de chefia recebem formação e treino adequado para o cumprimento adequado conforme o que foi definido para cada função e até em termos de segurança de informação?

Ação 4.7 & Ação 4.9:

- *Questão 37:*

  São efetuados testes de segurança a novos serviços/aplicações antes de serem expostos à utilização por todos os utilizadores?

- *Questão 38:*

  Em caso de atualização de aplicações/serviços, são efetuados testes por forma a garantir que não é colocado em causa o bom funcionamento atual?

Ação 5.3:

- *Questão 39:*

  Está implementado um plano de auditorias, com periodicidade de pelo menos um ano?

Ação 5.5 & Ação 5.6:

- *Questão 40:*

  Está contemplado um plano de ação e orçamento aprovados para montar e operar a equipa CSIRT ou SOC?

Ação 5.7:

- *Questão 41:*

  A organização possui um sistema de gestão de crise, capaz de lidar com grandes incidentes de segurança?

5.3.2 *Caracterização das empresas*

Para a obtenção de respostas ao questionário por forma a fazer levantamento de requisitos implementados ou não nas PME escolhidas, foi enviado um convite para os responsáveis pelos parques informáticos ao qual presto assistência técnica de informática. Para além do convite enviado por email às organizações foi reforçado esse convite via chamada telefónica e de modo presencial.

Em termos de caracterização das empresas em estudo, são empresas sediadas na zona centro com um número de funcionários entre os 10 e 100 colaboradores. As áreas de foco das organizações divergem, sendo algumas da área das energias renováveis, climatização, fabricação e comércio de móveis, prestação de serviços de contabilidade, entre outros.

5.3.3 *Preenchimento dos questionários*

Por forma a reforçar o convite apresentado às empresas para o preenchimento do questionário telefonicamente e email, existiu na maior parte dos casos uma visita técnica para resolução de problemas técnicos de informática aproveitando assim para ser efetuado um explicativo do âmbito do mesmo.

Após a concordância em colaborar com o estudo a ser realizado via telefone ou presencial nos casos que não tenham recebido o email, o questionário foi enviado *link* para o seu preenchimento por parte da entidade mais preparada para responder ao mesmo.

Em grande parte das empresas e até por forma a serem os mais fidedignos possíveis os resultados obtidos, ainda que na maior parte dos casos o preenchimento ser efetuado por pessoas com conhecimentos técnicos de segurança de informação e

informática em geral, existiu um acompanhamento no preenchimento dos mesmos presencialmente ou via telefónica com o fim de retirar duvidas que pudessem advir.

6

ANÁLISE DE RESULTADOS

Neste capítulo após terem sido analisados os questionários, serão apresentados os resultados obtidos/tratados nos questionários considerados no caso de estudo a 17 PME da zona de Leiria, de diversos setores como energias renováveis, climatização, contabilidade, entre outros. Por forma a anonimizar as organizações inquiridas, foi atribuído um identificador a cada uma das empresas, correspondendo a uma letra de A a Q.

6.1 RESULTADOS DA AVALIAÇÃO DO ESTADO DA CIBERSEGURANÇA NUMA VISÃO TÉCNICA

Tal como salientado na seção 5.1, tendo em conta que as empresas inquiridas fazem parte do parque informático a ser seguido em termos técnicos relativamente a informática pela pessoa que desenvolveu este caso de estudo, foi efetuada uma avaliação quantitativa com o que se conhecia implementado, seja em termos de processos ou mecanismos implementados cujo intervalo de valores a avaliar a organização foi de 1 a 4 como demonstrado na Tabela 7:

Valor	Definição
1	Não satisfaz
2	Satisfaz
3	Bom
4	Muito bom

Tabela 7: Intervalo quantitativo de estados - Cibersegurança

Esta avaliação permite-nos obter um ponto de comparação num parecer de opinião técnica de alguém com conhecimentos sobre a organização e, a realidade do estado da organização em relação à cibersegurança.

Na Figura 20 são apresentados os resultados obtidos na avaliação técnica de estado de cibersegurança efetuada antes da realização dos questionários às PME's envolvidas no caso de estudo.

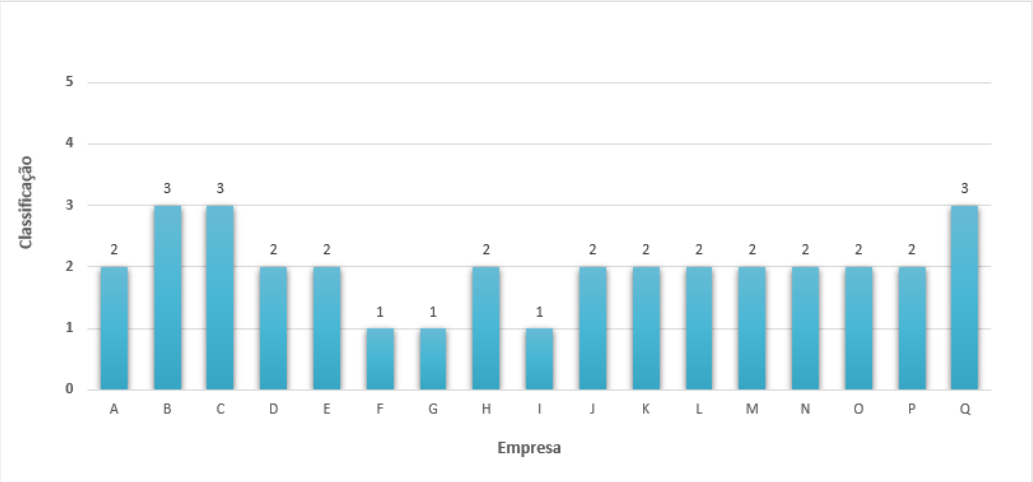


Figura 20: Resultados da visão técnica do estado cibersegurança

Em termos médios, o resultado obtido é de valor **2** (dois) na visão técnica levantada às empresas inquiridas. Este valor obtido em termos de visão técnica permite-nos visualizar que em termos técnicos, através da perceção do que está ou falta implementar em termos de cibersegurança nas organizações inquiridas, que o nível de cibersegurança em termos médios estará abaixo do ideal.

Neste levantamento técnico, apenas 3 das 17 empresas (18 %) teve classificação 3 (Bom) e o 11 das 17 empresas (65 %) teve classificação 2 (Satisfaz), isto indica que nesta visão técnica a maioria das empresas se encontra no mesmo estado do ponto de vista de cibersegurança, empresas a fazerem esforços para melhorarem a sua posição defensiva pois já existem mecanismos de proteção implementados. Um exemplo de preocupação constante nas empresas são as cópias de segurança, ainda que muitas vezes a replicação para o exterior e testes para garantir o seu bom estado, não são contemplados.

Por forma a confirmar este cenário através dos resultados obtidos através do preenchimento efetivo dos questionários, com uma escala igual com as mesmas percentagens, irá haver um cruzamento que será o comprovativo refutação do resultado menos positivo da visão técnica, em termos de cibersegurança.

6.2 RESULTADOS DOS QUESTIONÁRIOS PREENCHIDOS PELAS PME

Como salientado anteriormente, foram utilizadas para o caso de estudo 17 PME do distrito de Leiria, solicitando aos responsáveis ou alguém com conhecimentos técnicos/informáticos que respondessem ao questionário, tendo havido em grande parte dos casos um acompanhamento no preenchimento para evitar respostas ambíguas ou enganos.

Algumas questões disponibilizadas no questionário gerado através das correlações ações - controlos, são de resposta condicionada. Esse condicionalismo denota que dependendo da resposta do utilizador irá ou não aparecer as questões com condicionalismo associado.

Nas questões com condicionalismos em que é escolhida a opção "não", as questões associadas a esse condicionalismo são consideradas negativas, pois as questões subjacentes à questão principal que tem o condicionalismo com resposta negativa são na realidade ações não implementadas na PME avaliada.

No capítulo anterior que descreve a construção do questionário, está demonstrado na Figura 17 um exemplo de uma questão que tem associada condicionalismos.

As respostas positivas no questionário efetuado, revelam um âmbito positivo na PME, ou seja, que um parâmetro está implementado na empresa avaliada (em 98% das questões, na primeira questão se existe infraestruturas físicas como servidor, etc, o haver infraestruturas físicas ou em *cloud*. A resposta sim ou o não, implicam no resultado positivo ou negativo no questionário mas sim a forma como essa infraestrutura está ou não protegida).

Nas Figuras 21, 22 e 23, são visíveis os resultados globais, quantitativos por questão, associado a cada empresa. A cor verde, está representada uma questão com resposta positiva, a cor vermelha uma questão com resposta negativa e, a cor de laranja está apresentada uma resposta negativa por condicionalismo. Esta resposta cor de laranja, significa o que foi explicado anteriormente que ao responder negativamente à questão principal, as questões associadas a essa serão negativas.

Ao terminarem a resposta às questões todos os utilizadores responderam se necessitaram de auxílio ao preencher o questionário, sendo que as respostas positivas tiveram efetivamente acompanhamento presencial ao responder ao mesmo.

Por forma a facilitar a compreensão das imagens, na parte superior da imagem está presente uma legenda explicativa do que se tratam as cores das células da tabela de resultados obtidos.

No final desta tabela estão apresentados os resultados obtidos com o preenchimento dos questionários, não só em termos quantitativos mas também percentuais.

LEGENDA:

SIM NÃO NÃO Por condição

	Identificativo empresa:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Nº	*Questão:*																	
1	A organização possui infraestruturas informáticas criticas nas instalações da empresa? Ex: Servidores, etc.																	
2	A organização possui pelo menos um responsável pela segurança da informação?																	
2.1	Todos os colaboradores da organização sabem quem é o responsável pela segurança da informação?																	
2.2	Esse responsável, identifica os tipos de ataques mais comuns e cria métodos para a sua mitigação automática?																	
3	Em relação a incidentes de segurança que aconteçam, a organização possui um elemento responsável pela gestão desses incidentes?																	
4	Na organização estão definidos quais os serviços/funções e atividades críticas, atividades estas que limitem a produção em pelo da produção laboral?																	
5	A informação que está armazenada na organização, tem definida classificação relativamente à sua importância, valor e sensibilidade?																	
6	Aquando existe troca de informação critica seja com entidades internas ou externas são utilizados controlos criptográficos para salvaguarda da informação em trânsito?																	
7	Existe uma análise/gestão de riscos definida na organização, onde estão identificados os mais prováveis riscos que poderão advir, avaliados e também como deverão ser respondidos em caso de se tornarem uma realidade?																	
8	Todos os colaboradores da organização têm pleno conhecimento de quais as suas responsabilidades direitos e papéis a desempenhar na organização?																	
9	A organização tem definidas políticas de segurança da informação, políticas estas aprovadas pela administração e divulgadas aos restantes colaboradores?																	
10	Existem procedimentos internos definidos para notificação de incidentes de Cibersegurança por parte dos colaboradores?																	
10.1	Esses incidentes, são classificados conforme a sua criticidade para que haja uma triagem/prioridade na resolução dos incidentes?																	
10.2	A organização possui configurados mecanismos de correção ou mitigação de incidentes de segurança de informação?																	
10.3	Todos os colaboradores da organização sabem como devem notificar um incidente?																	
11	Estão definidas áreas/zonas críticas de acesso à organização quer em termos físicos quer em termos lógicos (através dos sistemas)?																	

Figura 21: Resultados das questões por empresas - parte 1

	Identificativo empresa:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Nº	*Questão:*																	
12	A arquitetura de rede & segurança da informação estão desenhadas?																	
13	A organização tem implementados sistemas de deteção/prevenção de intrusão como uma Firewall/IDS?																	
14	A organização tem implementado um sistema de recolha de metadados do tráfego que fluem na rede?																	
15	A organização comunica com algum grupo de profissionais, seja o CNCS (Centro Nacional de Cibersegurança), seja outro especializado em segurança de informação com objetivo de ampliar conhecimentos?																	
16	Na sua organização é efetuada uma inventariação de ativos e serviços?																	
16,1	Essa inventariação de ativos e serviços, é atualizada pelo menos de 6 em 6 meses?																	
17	Relativamente à recolha centralizada de registos (Logs), que devem ser preservados pelo menos um ano, a sua organização efetua essa recolha de registos e por sua vez o seu armazenamento seguro?																	
18	A organização tem presentes e são periodicamente atualizados, os quadros legais e regulatórios que a sua atividade está sujeita a respeitar?																	
19	Está definida a política de uso aceitável (PUA) na organização, política esta que contém as linhas orientadoras para a utilização dos recursos, de forma segura por todos os colaboradores?																	
20	Em relação a cópias de segurança, a organização tem implementados mecanismos de salvaguarda de informação (backups), pelo menos da informação considerada prioritária?																	
20.1	As cópias de segurança efetuadas são periodicamente testadas com o fim de se confirmar que não estão corrompidas?																	
20.2	As notificações de cópias de segurança (backups), estão configuradas para notificar em caso de falha?																	
20.3	As cópias de segurança efetuadas, (existindo) estão a ser replicadas para o exterior?																	
21	Está contemplado na organização um plano de formação para os colaboradores?																	
22	A organização efetua ações de sensibilização e treino interno para consciencialização dos colaboradores?																	
23	As pessoas chave da organização (administração, chefias) têm formação mais orientada aos principais mecanismos no que toca à política de segurança, metodologia de gestão de risco e sua aplicação na prática?																	
24	A organização tem configurados mecanismos de registo e auditoria de acesso a bases de dados com informação crítica?																	
25	Estão configurados mecanismos de controlo de acessos web (proxy por exemplo)?																	
26	A organização possuí um antivírus fidedigno configurado nos ativos mais críticos da organização?																	

Figura 22: Resultados das questões por empresas - parte 2

	Identificativo empresa:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Nº	Questão:																	
27	Existem procedimentos definidos para utilização dos dispositivos de comunicação e/ou dispositivos móveis? (Telemóveis, portáteis, tablets)																	
28	A organização tem configurado um sistema de monitorização de pelo menos os principais ativos da rede?																	
29	A organização tem implementado um SIEM, que agrega os registos (logs) mais relevantes produzidos pelos ativos e pelas aplicações de suporte à atividade?																	
30	Está definido um plano de continuidade da organização, para que em caso de catástrofe seja possível continuar com o negócio?																	
31	O staff de quem faz parte do departamento de segurança de informação, TIC, possuí formação periódica na área para que seja devidamente atualizado em termos de perigos existentes, vulnerabilidades, etc																	
32	Os privilégios de acesso individual à informação, foram devidamente aprovados pela administração e revistos com frequência?																	
33	A organização procedeu a criação de políticas de segurança, boas práticas e normas internas a serem adotadas por todos os colaboradores?																	
34	Existe uma reavaliação continua de acessos, privilégios, procedimentos implementados na empresa em relação à segurança de informação?																	
35	A organização efetua um simulacro periodicamente por forma a encontrar vulnerabilidades no que foi implementado para a segurança de informação?																	
36	Os colaboradores, principalmente os que ocupam cargos de chefia recebem formação e treino adequado para o cumprimento adequado conforme o que foi definido para cada função e até em termos de segurança de informação?																	
37	São efetuados testes de segurança a novos serviços/aplicações antes de serem expostos à utilização por todos os utilizadores?																	
38	Em caso de atualização de aplicações/serviços, são efetuados testes por forma a garantir que não é colocado em causa o bom funcionamento atual?																	
39	Está implementado um plano de auditorias, com periodicidade de pelo menos um ano?																	
40	Está contemplado um plano de ação e orçamento aprovados para montar e operar a equipa CSIRT ou SOC?																	
41	A organização possui um sistema de gestão de crise, capaz de lidar com grandes incidentes de segurança?																	
	Ao preencher este questionário, sentiu necessidade de acompanhamento técnico para o correto e conciso preenchimento	SIM	NÃO	SIM	SIM	NÃO	SIM	NÃO	SIM	SIM	SIM	SIM	SIM	SIM	NÃO	SIM	NÃO	NÃO
	Número de respostas SIM	17	34	25	16	26	19	6	30	15	10	16	12	16	22	10	15	24
	Número de respostas NÃO	33	16	25	34	24	31	44	20	35	40	34	38	34	28	40	35	26
	Percentagem de respostas SIM (%)	34,0	68,0	50,0	32,0	52,0	38,0	12,0	60,0	30,0	20,0	32,0	24,0	32,0	44,0	20,0	30,0	48,0
	Percentagem de respostas NÃO (%)	66,0	32,0	50,0	68,0	48,0	62,0	88,0	40,0	70,0	80,0	68,0	76,0	68,0	56,0	80,0	70,0	52,0

Figura 23: Resultados das questões por empresas - parte 3

Relativamente aos dados obtidos, observando uma grande mancha vermelha na tabela temos logo a perceção que existe muito a implementar e melhorar nas organizações para que estejam efetivamente seguras.

Analisando os valores percentuais das respostas obtidas, temos apenas 3 (três) organizações com resultados superior a 50% de respostas positivas, perfazendo apenas 18% das organizações inquiridas.

Seguidamente, serão apresentados graficamente os resultados obtidos nos questionários efetuados às 17 organizações, apresentados por percentagem de respostas positivas e negativas. Também são apresentadas o número de respostas positivas e negativas dadas por cada entidade inquirida.

Serão também apresentadas as questões, com detalhe de quantas respostas foram obtidas positivas e negativas, visíveis na Figura 25, percentuais das resposta visíveis na Figura 24. Observando essas imagens, temos de igual forma a perceção que existem empresas que estão com um número de respostas negativas bastante elevado, o que faz com que possamos afirmar que são organizações pouco preparadas, seguras relativamente a cibersegurança.

Nas Figuras 26 e 27, são apresentados os resultados detalhadamente por questão, incluindo a média de respostas e desvio padrão das respostas obtidas.

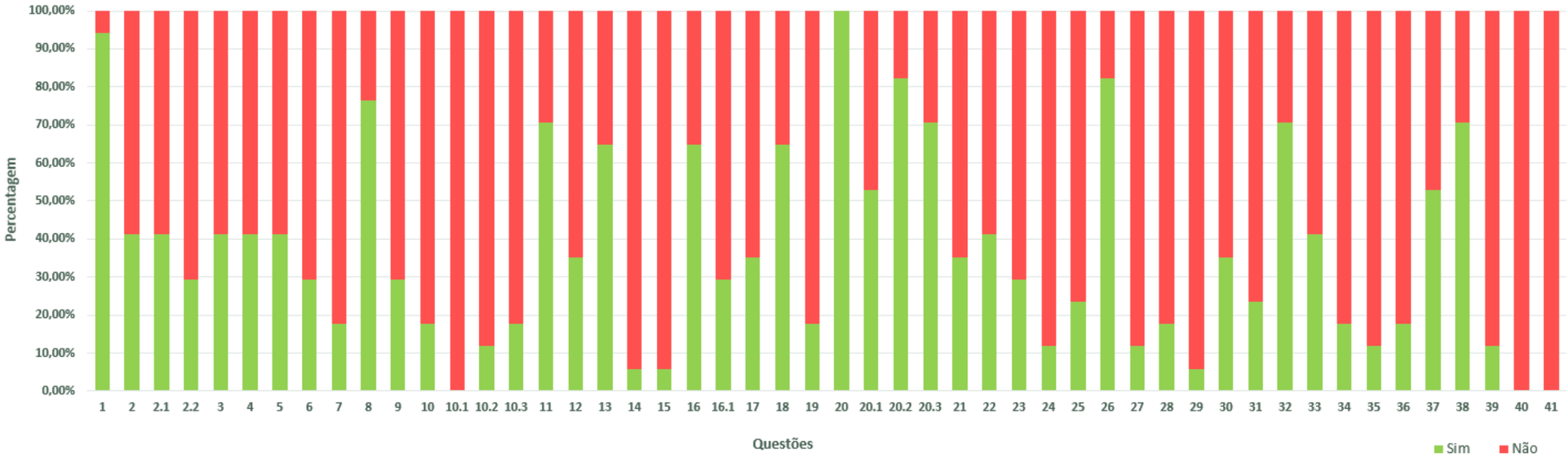


Figura 24: Resultados por questão - Percentagens

Figura 25: Resultados por questão - Número de empresas

Nº	Questão:	SIM	NÃO	N/A	NÃO + N/A	% SIM	% NÃO	Desvio Padrão
1	A organização possui infraestruturas informáticas criticas nas instalações da empresa? Ex: Servidores, etc.	16	1	0	1	94,12%	5,88%	10,61
2	A organização possui pelo menos um responsável pela segurança da informação?	7	10	0	10	41,18%	58,82%	2,12
2.1	Todos os colaboradores da organização sabem quem é o responsável pela segurança da informação?	7	0	10	10	41,18%	58,82%	2,12
2.2	Esse responsável, identifica os tipos de ataques mais comuns e cria métodos para a sua mitigação automática?	5	2	10	12	29,41%	70,59%	4,95
3	Em relação a incidentes de segurança que aconteçam, a organização possui um elemento responsável pela gestão desses incidentes?	7	10	0	10	41,18%	58,82%	2,12
4	Na organização estão definidos quais os serviços/funções e atividades críticas, atividades estas que limitem a produção em pelo da produção laboral?	7	10	0	10	41,18%	58,82%	2,12
5	A informação que está armazenada na organização, tem definida classificação relativamente à sua importância, valor e sensibilidade?	7	10	0	10	41,18%	58,82%	2,12
6	Aquando existe troca de informação critica seja com entidades internas ou externas são utilizados controlos criptográficos para salvaguarda da informação em trânsito?	5	12	0	12	29,41%	70,59%	4,95
7	Existe uma análise/gestão de riscos definida na organização, onde estão identificados os mais prováveis riscos que poderão advir, avaliados e também como deverão ser respondidos em caso de se tornarem uma realidade?	3	14	0	14	17,65%	82,35%	7,78
8	Todos os colaboradores da organização têm pleno conhecimento de quais as suas responsabilidades direitos e papéis a desempenhar na organização?	13	4	0	4	76,47%	23,53%	6,36
9	A organização tem definidas políticas de segurança da informação, políticas estas aprovadas pela administração e divulgadas aos restantes colaboradores?	5	12	0	12	29,41%	70,59%	4,95
10	Existem procedimentos internos definidos para notificação de incidentes de Cibersegurança por parte dos colaboradores?	3	14	0	14	17,65%	82,35%	7,78
10.1	Esses incidentes, são classificados conforme a sua criticidade para que haja uma triagem/prioridade na resolução dos incidentes?	0	3	14	17	0,00%	100,00%	12,02
10.2	A organização possui configurados mecanismos de correção ou mitigação de incidentes de segurança de informação?	2	1	14	15	11,76%	88,24%	9,19
10.3	Todos os colaboradores da organização sabem como devem notificar um incidente?	3	0	14	14	17,65%	82,35%	7,78
11	Estão definidas áreas/zonas críticas de acesso à organização quer em termos físicos quer em termos lógicos (através dos sistemas)?	12	5	0	5	70,59%	29,41%	4,95
12	A arquitetura de rede & segurança da informação estão desenhadas?	6	11	0	11	35,29%	64,71%	3,54
13	A organização tem implementados sistemas de deteção/prevenção de intrusão como uma Firewall/IDS?	11	6	0	6	64,71%	35,29%	3,54
14	A organização tem implementado um sistema de recolha de metadados do tráfego que fluem na rede?	1	16	0	16	5,88%	94,12%	10,61
15	A organização comunica com algum grupo de profissionais, seja o CNCS (Centro Nacional de Cibersegurança), seja outro especializado em segurança de informação com objetivo de ampliar conhecimentos?	1	16	0	16	5,88%	94,12%	10,61
16	Na sua organização é efetuada uma inventariação de ativos e serviços?	11	7	0	7	64,71%	41,18%	2,83
16.1	Essa inventariação de ativos e serviços, é atualizada pelo menos de 6 em 6 meses?	5	6	6	12	29,41%	70,59%	4,95
17	Relativamente à recolha centralizada de registos (Logs), que devem ser preservados pelo menos um ano, a sua organização efetua essa recolha de registos e por sua vez o seu armazenamento seguro?	6	11	0	11	35,29%	64,71%	3,54
18	A organização tem presentes e são periodicamente atualizados, os quadros legais e regulatórios que a sua atividade está sujeita a respeitar?	11	6	0	6	64,71%	35,29%	3,54
19	Está definida a política de uso aceitável (PUA) na organização, política esta que contém as linhas orientadoras para a utilização dos recursos, de forma segura por todos os colaboradores?	3	14	0	14	17,65%	82,35%	7,78
20	Em relação a cópias de segurança, a organização tem implementados mecanismos de salvaguarda de informação (backups), pelo menos da informação considerada prioritária?	17	0	0	0	100,00%	0,00%	12,02
20.1	As cópias de segurança efetuadas são periodicamente testadas com o fim de se confirmar que não estão corrompidas?	9	8	0	8	52,94%	47,06%	0,71

Figura 26: Resultados por questão - por empresa parte 1

Nº	Questão:	SIM	NÃO	N/A	NÃO + N/A	% SIM	% NÃO	Desvio Padrão
20.2	As notificações de cópias de segurança (backups), estão configuradas para notificar em caso de falha?	14	3	0	3	82,35%	17,65%	7,78
20.3	As cópias de segurança efetuadas, (existindo) estão a ser replicadas para o exterior?	12	5	0	5	70,59%	29,41%	4,95
21	Está contemplado na organização um plano de formação para os colaboradores?	6	11	0	11	35,29%	64,71%	3,54
22	A organização efetua ações de sensibilização e treino interno para consciencialização dos colaboradores?	7	10	0	10	41,18%	58,82%	2,12
23	As pessoas chave da organização (administração, chefias) têm formação mais orientada aos principais mecanismos no que toca à política de segurança, metodologia de gestão de risco e sua aplicação na prática?	5	12	0	12	29,41%	70,59%	4,95
24	A organização tem configurados mecanismos de registo e auditoria de acesso a bases de dados com informação crítica?	2	15	0	15	11,76%	88,24%	9,19
25	Estão configurados mecanismos de controlo de acessos web (proxy por exemplo)?	4	13	0	13	23,53%	76,47%	6,36
26	A organização possuí um antivírus fidedigno configurado nos ativos mais críticos da organização?	14	3	0	3	82,35%	17,65%	7,78
27	Existem procedimentos definidos para utilização dos dispositivos de comunicação e/ou dispositivos móveis? (Telemóveis, portáteis, tablets)	2	15	0	15	11,76%	88,24%	9,19
28	A organização tem configurado um sistema de monitorização de pelo menos os principais ativos da rede?	3	14	0	14	17,65%	82,35%	7,78
29	A organização tem implementado um SIEM, que agrega os registos (logs) mais relevantes produzidos pelos ativos e pelas aplicações de suporte à atividade?	1	16	0	16	5,88%	94,12%	10,61
30	Está definido um plano de continuidade da organização, para que em caso de catástrofe seja possível continuar com o negócio?	6	11	0	11	35,29%	64,71%	3,54
31	O staff de quem faz parte do departamento de segurança de informação, TIC, possuí formação periódica na área para que seja devidamente atualizado em termos de perigos existentes, vulnerabilidades, etc	4	13	0	13	23,53%	76,47%	6,36
32	Os privilégios de acesso individual à informação, foram devidamente aprovados pela administração e revistos com frequência?	12	5	0	5	70,59%	29,41%	4,95
33	A organização procedeu a criação de políticas de segurança, boas práticas e normas internas a serem adotadas por todos os colaboradores?	7	10	0	10	41,18%	58,82%	2,12
34	Existe uma reavaliação continua de acessos, privilégios, procedimentos implementados na empresa em relação à segurança de informação?	3	14	0	14	17,65%	82,35%	7,78
35	A organização efetua um simulacro periodicamente por forma a encontrar vulnerabilidades no que foi implementado para a segurança de informação?	2	15	0	15	11,76%	88,24%	9,19
36	Os colaboradores, principalmente os que ocupam cargos de chefia recebem formação e treino adequado para o cumprimento adequado conforme o que foi definido para cada função e até em termos de segurança de informação?	3	14	0	14	17,65%	82,35%	7,78
37	São efetuados testes de segurança a novos serviços/aplicações antes de serem expostos à utilização por todos os utilizadores?	9	8	0	8	52,94%	47,06%	0,71
38	Em caso de atualização de aplicações/serviços, são efetuados testes por forma a garantir que não é colocado em causa o bom funcionamento atual?	12	5	0	5	70,59%	29,41%	4,95
39	Está implementado um plano de auditorias, com periodicidade de pelo menos um ano?	2	15	0	15	11,76%	88,24%	9,19
40	Está contemplado um plano de ação e orçamento aprovados para montar e operar a equipa CSIRT ou SOC?	0	17	0	17	0,00%	100,00%	12,02
41	A organização possui um sistema de gestão de crise, capaz de lidar com grandes incidentes de segurança?	0	17	0	17	0,00%	100,00%	12,02

Figura 27: Resultados por questão - por empresa parte 2

Para completar a análise dos dados obtidos para obtenção de um estado da cibersegurança efetiva nas empresas em estudo, utilizou-se o método quantitativo acima com escala de 1 a 4, com diferenciação percentual para cada valor em escala, à semelhança da visão técnica como demonstrado na Tabela 8.

Valor	Definição	Intervalo
1	Não satisfaz	0 a 24,99%
2	Satisfaz	25 a 49,99%
3	Bom	50 a 74,99%
4	Muito bom	75 a 100%

Tabela 8: Intervalo quantitativo de estados com variação percentual - Cibersegurança

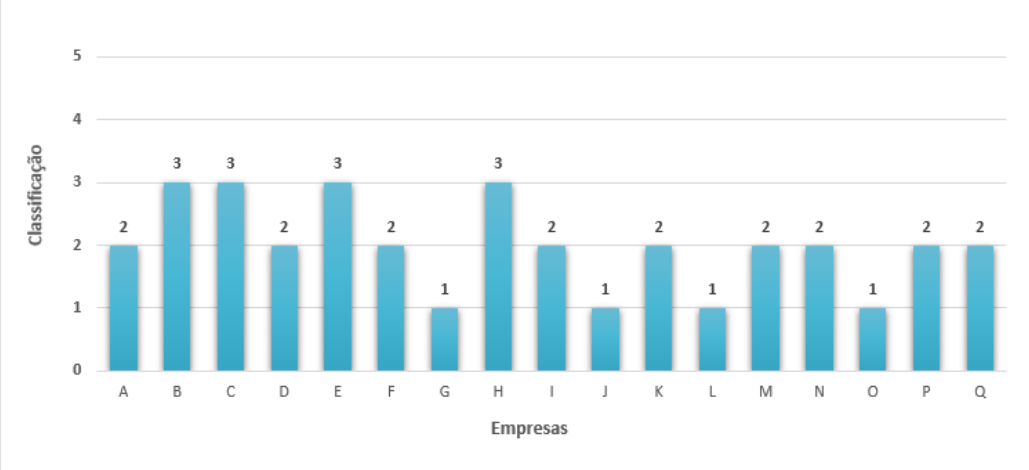


Figura 28: Resultados dos questionários

Em termos médios como demonstrado na Figura 28, o resultado médio obtido com o resultado dos questionários efetuados às organizações inquiridas é de valor **2** (dois). Este valor permite-nos de forma justificada afirmar que as organizações em termos gerais não estão devidamente preparadas, protegidas para problemas que poderão advir em termos de cibersegurança.

Quanto aos resultados obtidos, podemos observar que existem pelo menos três questões com desvio padrão acima de 10 valores, nomeadamente relativamente a mecanismos SIEM implementados na organização, equipas CSIRT e SOC e também se a organização ou empresa tem um sistema de gestão de crise. Esta análise permite-nos salientar que são controlos que não estão implementados nas empresas em estudo, pressupondo-se que por falta de recursos para implementação.

No preenchimento do questionário, a seção do roteiro CNCS com mais respostas negativas, é a seção 5 (cinco). Uma explicação possível para este resultado para além da falta de recursos para implementação como referido anteriormente, é que estas empresas não têm uma estrutura organizacional onde se encaixem as sugestões presentes nessa secção.

6.3 COMPARAÇÃO ENTRE A AVALIAÇÃO TÉCNICA E OS RESULTADOS OBTIDOS

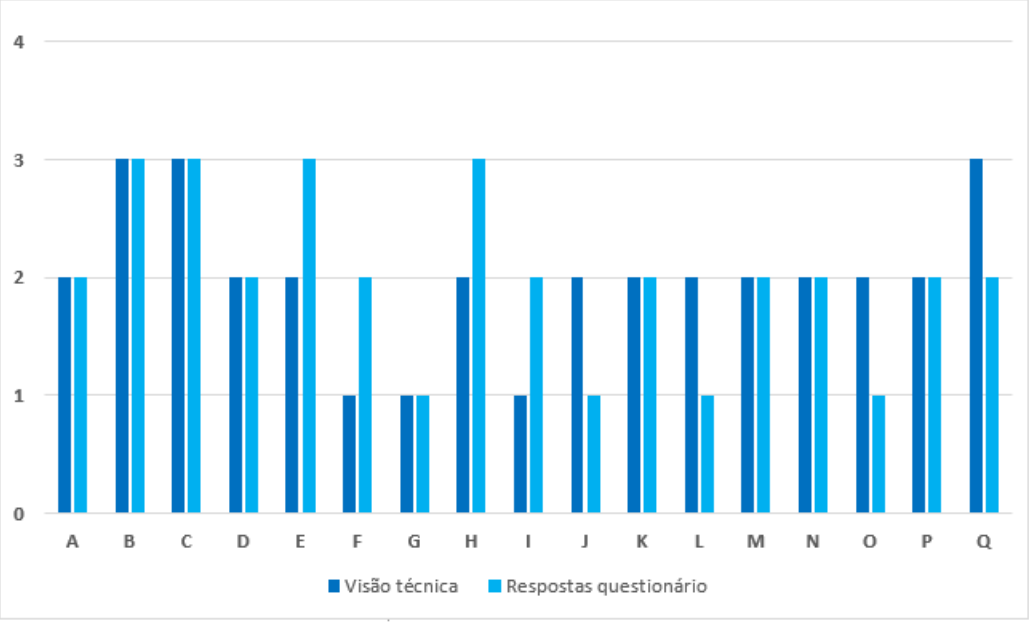


Figura 29: Comparação entre a avaliação técnica e os resultados obtidos

Como demonstrado na Figura 29, aliando graficamente os resultados do levantamento da visão técnica e dos resultados efetivos resultantes da elaboração dos questionários às organizações, em termos médios o valor obtido é de **2** (dois), satisfaz. Porém, em algumas das organizações a visão técnica e a realidade do estado da organização, não

são coincidentes sendo o valor obtido resultante do preenchimento dos questionários diferente da visão técnica efetuada inicialmente.

Assim sendo poderemos afirmar que, ferramentas como o questionário permitem melhorar a análise técnica. A existência de vários pontos de análise da organização, mesmo sendo efetuado por técnicos, não é possível saber o real estado de uma organização mas sim apenas ter uma ideia se estará ou não segura. Nesse sentido, o uso de uma metodologia sustentada e fidedigna, é a melhor forma da obtenção do estado real da organização, permitindo assim uma ideia mais real do que poderia ser implementado.

No Anexo B estão disponíveis os resultados em bruto exportados através da aplicação Question Pro.

7

CONCLUSÕES

Tendo em conta que cada vez mais as organizações e empresas estão a optar pela utilização massiva da computação e armazenamento digital e que os dados são essenciais seja para que tipo de negócio ou organização for, as equipas de TI deverão estar incumbidas de garantir que a indisponibilidade de sistemas é minimizada, devendo os dados estarem devidamente protegidos.

A sensibilização dos responsáveis de topo de uma organização para investir nesta área, é uma missão um pouco trabalhosa pois o investimento na cibersegurança acaba por ser visto como um custo, pois para um administrador ou responsável apenas trará rentabilidade no caso de existir incidentes graves de segurança, mesmo sabendo que esses incidentes são cada vez mais comuns.

Por este motivo, qualquer ferramenta ou metodologia com o fim de verificar o estado de segurança de uma organização, se for com validade provada, como por exemplo este projeto desenvolvido com cruzamento de ações do Roteiro de Capacidades Mínimas de Cibersegurança do Centro Nacional de Cibersegurança e controlos de uma norma internacional ISO 27001:2013, voltada para a segurança, demonstrará ao gestor a necessidade de investimento nesta área de cibersegurança.

O estudo de documentação complexa como normas, roteiro permitiu aumentar os conhecimentos no campo da cibersegurança, sendo esta uma área que me interessa bastante.

Para além do objetivo do projeto fundamentado acima, a elaboração deste projeto visou também auxiliar no campo profissional, permitindo-me um nível de enriquecimento e de preparação como consultor de sistemas e redes a propor soluções, procedimentos à organizações ao qual estou responsável pelo funcionamento dos seus sistemas em produção.

Um dos aspetos que marcou o desenvolvimento deste projeto foi o preenchimento do questionário das empresas ao qual a responsabilidade do parque informático está entregue ao meu parecer técnico, podendo assim colmatar falhas presentes que, sem ter os resultados obtidos e apresentados aos responsáveis de topo, não iria ser fácil de colocar em prática.

Por forma complementar a metodologia, seria importante aumentar a amplitude do caso de estudo para que fossem analisadas as respostas obtidas. Se continuarem a existir questões baixa relevância, uma grande percentagem de respostas negativas, reavaliar essas questões para saber se valeria a pena estarem presentes no questionário.

Para ser comprovada a eficácia utilizando outra norma por exemplo como ISO 27009:2020 estando esta focada mais para a tecnologia e cibersegurança, auxiliando na criação de padrões e dispondo também conselhos para as organizações estarem protegidas num ambiente cibernético.

Outra norma que seria interessante integrar na metodologia desenvolvida, seria a ISO/IEC 27002:2022 [28]. Esta é uma norma recente que está orientada para a segurança da informação, segurança cibernética e proteção da privacidade, sendo assim adequado atualizar a metodologia com os inputs desta nova versão.

O mundo da cibersegurança está em constante expansão, e a realidade empresarial, e mesmo individual, faz com que essas entidades tenham uma grande dificuldade em saber qual é o melhor uso dos seus recursos. Este trabalho é uma ferramenta que permite precisamente interligar estes dois mundos.

BIBLIOGRAFIA

[1] *Sophos 2022 Threat Report - Interrelated threats target an interdependent world*, visitado em 07-02-2022. URL: https://www.sophos.com/en-us/labs/security-threat-report.

[2] *Cyber Security Report 2022*, visitado em 07-02-2022. URL: https://resources.checkpoint.com/cyber-security-resources/check-point-softwares-2022-security-report.

[3] D. Makupi, «An iso 27001 based model to determine university information security maturity under uncertainty», 2021. URL: http://ir.kabarak.ac.ke/handle/123456789/827.

[4] P. Vladimir e F. Franklin, *A Contingency Plan Framework for Cyber-Attacks - Journal of Information Systems Engineering & Management*. 2019. URL: https://doi.org/10.29333/jisem/5898.

[5] CNCS, *Roteiro de capacidades mínimas de Cibersegurança*. 2019, visitado em 27-11-2021. URL: https://www.cncs.gov.pt/docs/cncs-%20roteiro-capacidades-minimas-ciberseguranca.pdf.

[6] ISO, *ISO/IEC 27009:2020 - Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements*, visitado em 11-12-2021. URL: https://www.iso.org/standard/73907.html.

[7] N. C. FRAMEWORK, *Framework for Improving Critical Infrastructure Cybersecurity. NIST*. 2018, visitado em 10-12-2021. URL: https://doi.org/10.6028/NIST.CSWP.04162018.

[8] M. da Economia e da Inovação, *Diário da República n.º 213/2007, Série I de 2007-11-06, páginas 8080 - 8084*, Website, visitado em 01-12-2021, 2007. URL: https://dre.pt/dre/detalhe/decreto-lei/372-2007-629439.

[9] L. Cacciolatti e S. Hee Lee, «The Nature of the Small and Medium-Sized Enterprise. Entrepreneurial Marketing for SMEs, 6–27», 2015.

[10] *Pequenas e médias empresas em % do total de empresas: total e por dimensão*, visitado em 01-02-2022. URL: https://www.pordata.pt/Portugal/

Pequenas+e+m%5C%c3%5C%a9dias+empresas+em+percentagem+do+total+de+empresas+total+e+por+dimens%5C%c3%5C%a3o-2859.

[11] M. Antunes, M. Maximiano, R. Gomes e D. Pinto, «Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal», *Journal of Cybersecurity and Privacy*, vol. 1, n.º 2, pp. 219–238, 2021, ISSN: 2624-800X. DOI: 10.3390/jcp1020012. URL: https://www.mdpi.com/2624-800X/1/2/12.

[12] J. V. Carvalho, S. Carvalho e Á. Rocha, «European strategy and legislation for cybersecurity: implications for Portugal», 2020. URL: https://doi.org/10.1007/s10586-020-03052-y.

[13] A. Issah, «Achieving cyber peace through an effective Cybersecurity Governance», 2021. URL: https://trepo.tuni.fi/handle/10024/135607.

[14] J. V. Carvalho e A. Victor, «Portuguese Concerns and Impact on Behaviour About Cybersecurity: A Comparison with the European Average», 2022. URL: https://doi.org/10.1007/978-981-16-4884-7_2.

[15] P. Costa, R. Montenegro, T. Pereira e P. Pinto, «The Security Challenges Emerging from the Technological Developments», 2019. URL: https://doi.org/10.1007/s11036-018-01208-0.

[16] P. M. Alexandre, *Europeanization processes regarding matters of cybersecurity: The case of Portugal*, visitado em 17-12-2021. URL: http://hdl.handle.net/10071/21643.

[17] CNCS, *Quadro Nacional de Referência para a Cibersegurança*. 2019, visitado em 03-11-2021. URL: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf.

[18] S. Quality, *Família ISO 27000*, visitado em 07-12-2021, 2019. URL: https://smartqualityglobal.com/blog/familia-iso-27000.

[19] A. P. Sothanon, *ISO/IEC 27000 Family*, visitado em 02-12-2021. URL: https://itsannex.wordpress.com/2017/04/23/isoiec-27000-family/.

[20] ISO, *ISO-ISO/IEC 27001:2013—Information Technology—Security Techniques—Information Security Management Systems—Requirements*, visitado em 28-11-2021. URL: https://www.iso.org/standard/54534.html.

[21] R. von Solms, «Information security management (3): the Code of Practice for Information Security Management (BS 7799)», 1998. URL: https://doi.org/10.1108/09685229810240158.

[22] T. Wiander, «Implementing the ISO/IEC 17799 standard in practice - findings from small and medium sized software organisations», 2007. URL: https://ieeexplore.ieee.org/document/4629320.

[23] E. Ramos, E. A. Lopes Cordeiro, G. Cristina Martins, N. Souza Silva e E. Mataruco Duarte, «Orientações para implementação do Sistema de Gestão de Segurança da Informação com base na ISO 27001 e o Ciclo PDCA», *FatecSeg - Congresso de Segurança da Informação*, vol. 1, out. de 2021. URL: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/34.

[24] NERLEI, *O projeto "LOG IN INNOVATION"*, visitado em 01-12-2021. URL: https://www.logininnovation.pt/projeto.

[25] A. Alexei, «A Contingency Plan Framework for Cyber-Attacks - Journal of Information Systems Engineering & Management», 2021. URL: http://repository.utm.md/handle/5014/14062.

[26] C. for Internet Security, *CIS Critical Security Controls®*, visitado em 15-12-2021. URL: https://learn.cisecurity.org/cis-controls-download.

[27] *CHAVE PGP - CERT@CERT.PT*, visitado em 17-12-2021. URL: https://www.cncs.gov.pt/pt/certpt/chave-pgp/.

[28] *ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls*, visitado em 01-12-2021. URL: https://www.iso.org/standard/75652.html.

ANEXOS

A

ANEXO A - ESTRUTURA DO QUESTIONÁRIO

Este anexo corresponde ao questionário disponibilizado às organizações com o objetivo de obtenção de respostas, questionário este realizado na plataforma online QuestionPro como salientado no relatório.

POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Questionário para avaliação de maturidade de Cibersegurança de PME

*Questionário efetuado no âmbito de projeto do **Mestrado em Cibersegurança e Informática Forense** com objetivo de analisar se a PME (Pequena ou Média Empresa) em estudo cumpre os requisitos de proteção internos para que, em caso de um ataque informático/tentativo acesso indevido de informação, seja possível a normal laboração sem perturbações e continuidade da empresa.*

* Termos de aceitação para realização do questionário no âmbito escolar

Consulte as condições aqui

◯ Eu compreendo e aceito as condições descritas

* Nome da organização/empresa em estudo (Denominação social)

* A organização em estudo no questionário, é uma PME* (Pequena ou Média Empresa)?

Como sei se uma empresa é PME?

◯ SIM ◯ NÃO

* A organização possui infraestruturas informáticas criticas nas instalações da empresa? Ex: Servidores, etc.

SIM NÃO

* A organização possui pelo menos um responsável pela segurança da informação?

SIM NÃO

* Todos os colaboradores da organização sabem quem é o responsável pela segurança da informação?

SIM NÃO

* Esse responsável, identifica os tipos de ataques mais comuns e cria métodos para a sua mitigação automática?

SIM NÃO

* Em relação a incidentes de segurança que aconteçam, a organização possui um elemento responsável pela gestão desses incidentes?

SIM NÃO

* Na organização estão definidos quais os serviços/funções e atividades críticas, atividades estas que limitem a produção laboral?

SIM NÃO

* A informação que está armazenada na organização, tem definida classificação relativamente à sua importância, valor e sensibilidade?

SIM NÃO

* Aquando existe troca de informação critica seja com entidades internas ou externas são utilizados controlos criptográficos para salvaguarda da informação em trânsito?

SIM NÃO

* Existe uma análise/gestão de riscos definida na organização, onde estão identificados os mais prováveis riscos que poderão advir, avaliados e também como deverão ser respondidos em caso de se tornarem uma realidade?

SIM NÃO

* Todos os colaboradores da organização têm pleno conhecimento de quais as suas responsabilidades, direitos e papéis a desempenhar na organização?

SIM NÃO

* A organização tem definidas políticas de segurança da informação, políticas estas aprovadas pela administração e divulgadas aos restantes colaboradores?

SIM NÃO

* Existem procedimentos internos definidos para notificação de incidentes de Cibersegurança por parte dos colaboradores?

SIM NÃO

* Esses incidentes, são classificados conforme a sua criticidade para que haja uma triagem/prioridade na resolução dos incidentes?

SIM NÃO

* A organização possui configurados mecanismos de correção ou mitigação de incidentes de segurança de informação?

SIM NÃO

* Todos os colaboradores da organização sabem como devem notificar um incidente?

SIM NÃO

* Estão definidas áreas/zonas críticas de acesso à organização quer em termos físicos quer em termos lógicos (através dos sistemas)?

SIM NÃO

* A arquitetura de rede & segurança da informação estão desenhadas?

SIM NÃO

* A organização tem implementados sistemas de deteção/prevenção de intrusão como uma Firewall/IDS?

SIM NÃO

* A organização tem implementado um sistema de recolha de metadados do tráfego que fluem na rede?

SIM NÃO

* A organização comunica com algum grupo de profissionais, seja o CNCS (Centro Nacional de Cibersegurança), seja outro especializado em segurança de informação com objetivo de ampliar conhecimentos?

SIM NÃO

* Na sua organização é efetuada uma inventariação de ativos e serviços?

SIM NÃO

* Essa inventariação de ativos e serviços, é atualizada pelo menos de 6 em 6 meses?

SIM NÃO

* Relativamente à recolha centralizada de registos (Logs), que devem ser preservados pelo menos um ano, a sua organização efetua essa recolha de registos e por sua vez o seu armazenamento seguro?

SIM NÃO

* A organização tem presentes e são periodicamente atualizados, os quadros legais e regulatórios que a sua atividade está sujeita a respeitar?

SIM NÃO

* Está definida a política de uso aceitável (PUA) na organização, política esta que contém as linhas orientadoras para a utilização dos recursos, de forma segura por todos os colaboradores?

SIM NÃO

* Em relação a cópias de segurança, a organização tem implementados mecanismos de salvaguarda de informação (backups), pelo menos da informação considerada prioritária?

SIM NÃO

* As cópias de segurança efetuadas são periodicamente testadas com o fim de se confirmar que não estão corrompidas?

SIM NÃO

* As notificações de cópias de segurança (backups), estão configuradas para notificar em caso de falha?

SIM NÃO

* As cópias de segurança efetuadas, (existindo) estão a ser replicadas para o exterior?

SIM NÃO

* Está contemplado na organização um plano de formação para os colaboradores?

SIM NÃO

* A organização efetua ações de sensibilização e treino interno para consciencialização dos colaboradores?

SIM NÃO

* As pessoas chave da organização (administração, chefias) têm formação mais orientada aos principais mecanismos no que toca à política de segurança, metodologia de gestão de risco e sua aplicação na prática?

SIM NÃO

* A organização tem configurados mecanismos de registo e auditoria de acesso a bases de dados com informação crítica?

SIM NÃO

* Estão configurados mecanismos de controlo de acessos web (proxy por exemplo)?

SIM NÃO

* A organização possuí um antivírus fidedigno configurado nos ativos mais críticos da organização?

SIM NÃO

* Existem procedimentos definidos para utilização dos dispositivos de comunicação e/ou dispositivos móveis? (Telemóveis, portáteis, tablets)

SIM NÃO

* A organização tem configurado um sistema de monitorização de pelo menos os principais ativos da rede?

SIM NÃO

* A organização tem implementado um SIEM, que agrega os registos (logs) mais relevantes produzidos pelos ativos e pelas aplicações de suporte à atividade?

SIM NÃO

* Está definido um plano de continuidade da organização, para que em caso de catástrofe seja possível continuar com o negócio?

SIM NÃO

* O staff de quem faz parte do departamento de segurança de informação, TIC, possuí formação periódica na área para que seja devidamente atualizado em termos de perigos existentes, vulnerabilidades, etc

SIM NÃO

* Os privilégios de acesso individual à informação, foram devidamente aprovados pela administração e revistos com frequência?

SIM NÃO

* A organização procedeu a criação de políticas de segurança, boas práticas e normas internas a serem adotadas por todos os colaboradores?

SIM NÃO

* Existe uma reavaliação continua de acessos, privilégios, procedimentos implementados na empresa em relação à segurança de informação?

SIM NÃO

* A organização efetua um simulacro periodicamente por forma a encontrar vulnerabilidades no que foi implementado para a segurança de informação?

SIM NÃO

* Os colaboradores, principalmente os que ocupam cargos de chefia recebem formação e treino adequado para o cumprimento adequado conforme o que foi definido para cada função e até em termos de segurança de informação?

SIM NÃO

* São efetuados testes de segurança a novos serviços/aplicações antes de serem expostos à utilização por todos os utilizadores?

SIM NÃO

* Em caso de atualização de aplicações/serviços, são efetuados testes por forma a garantir que não é colocado em causa o bom funcionamento atual?

SIM NÃO

* Está implementado um plano de auditorias, com periodicidade de pelo menos um ano?

SIM NÃO

* Está contemplado um plano de ação e orçamento aprovados para montar e operar a equipa CSIRT ou SOC?

O que é CSIRT e SOC?

SIM NÃO

* A organização possui um sistema de gestão de crise, capaz de lidar com grandes incidentes de segurança?

SIM NÃO

* Ao preencher este questionário, sentiu necessidade de acompanhamento técnico para o correto e conciso preenchimento

SIM NÃO

Engenheiro Informático - Bruno Filipe Diogo Azinheira
Mestrado em Cibersegurança e Informática Forense - 2021/2022

B

ANEXO B - RELATÓRIO DE RESPOSTAS OBTIDAS NO QUESTIONÁRIO

Este anexo abaixo demonstra um Dashboard que agrega as respostas obtidas dos questionários respondidos pelas organizações inquiridas para comprovativo dos resultados apresentados no relatório.

De notar que, neste Dashboard apresentado, as organizações em questão estão anonimizadas.

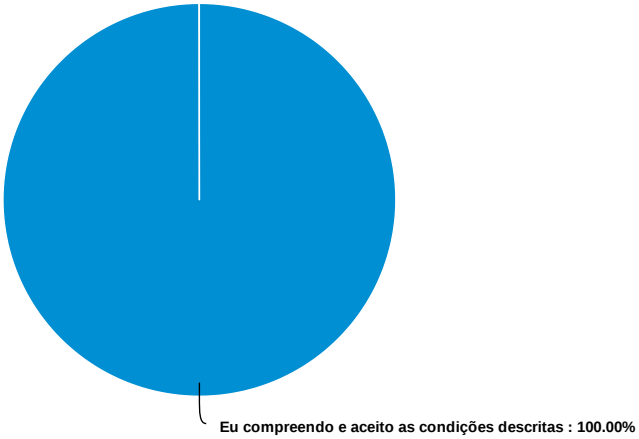
POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Mestrado MCIF - Dashboard

Resultados obtidos

79	17	17	100%	0	26 mins
Viewed	Total Responses	Completed	Completion Rate	Dropouts	Average Time

Termos de aceitação para realização do questionário no âmbito escolar

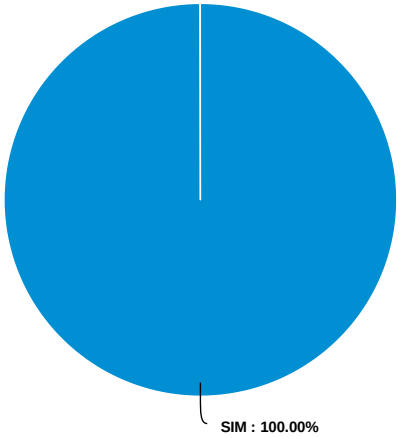


Answer	Count	Percent	20%	40%	60%	80%	100%
Eu compreendo e aceito as condições descritas	17	100%					
Total	**17**	**100%**					

Nome da organização/empresa em estudo (Denominação social)

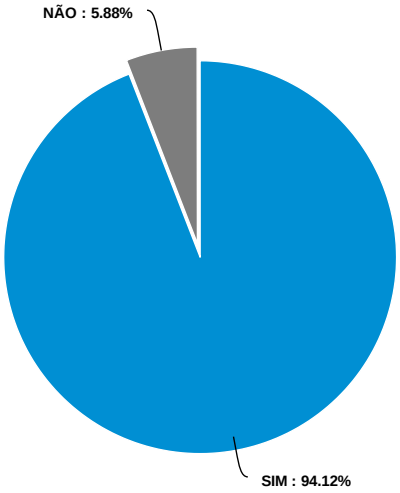
03/03/2022	67286432	Empresa Q
03/03/2022	67269380	Empresa P
03/03/2022	67250204	Empresa O
03/02/2022	67201753	Empresa N
03/02/2022	67190901	Empresa M
03/02/2022	67175262	Empresa L
03/02/2022	67171536	Empresa K
03/02/2022	67152510	Empresa J
02/28/2022	67057897	Empresa I
02/28/2022	67037481	Empresa H
02/24/2022	66845998	Empresa G
02/24/2022	66829449	Empresa F
02/24/2022	66828856	Empresa E
02/23/2022	66744957	Empresa D
02/22/2022	66686308	Empresa C
02/21/2022	66645052	Empresa B
02/21/2022	66625855	Empresa A

A organização em estudo no questionário, é uma PME* (Pequena ou Média Empresa)?



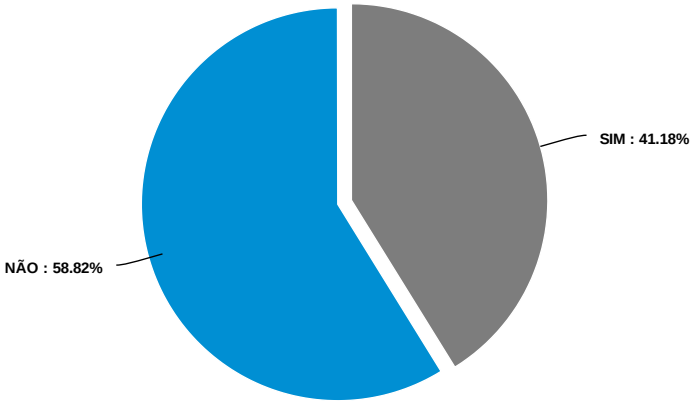
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	17	100%					
NÃO	0	0%					
Total	**17**	**100%**					

A organização possui infraestruturas informáticas criticas nas instalações da empresa? Ex: Servidores, etc.



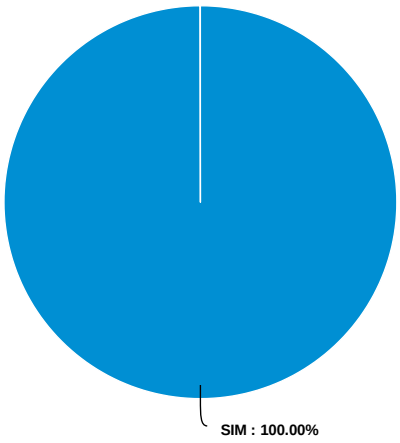
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	16	94.12%					
NÃO	1	5.88%					
Total	**17**	**100%**					

A organização possui pelo menos um responsável pela segurança da informação?



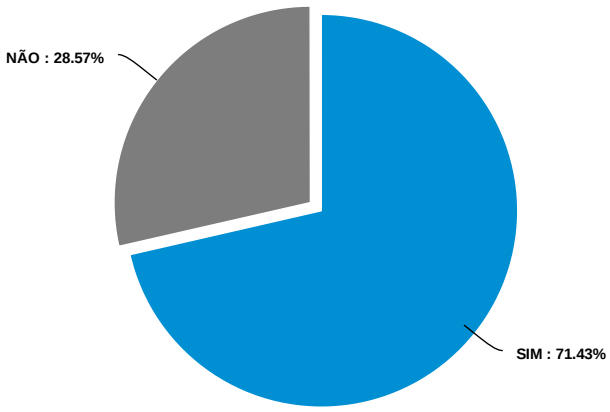
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	7	41.18%					
NÃO	10	58.82%					
Total	**17**	**100%**					

Todos os colaboradores da organização sabem quem é o responsável pela segurança da informação?



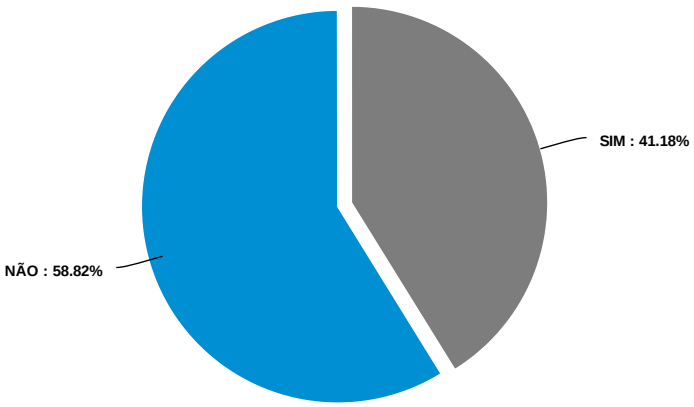
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	7	100%					
NÃO	0	0%					
Total	**7**	**100%**					

Esse responsável, identifica os tipos de ataques mais comuns e cria métodos para a sua mitigação automática?



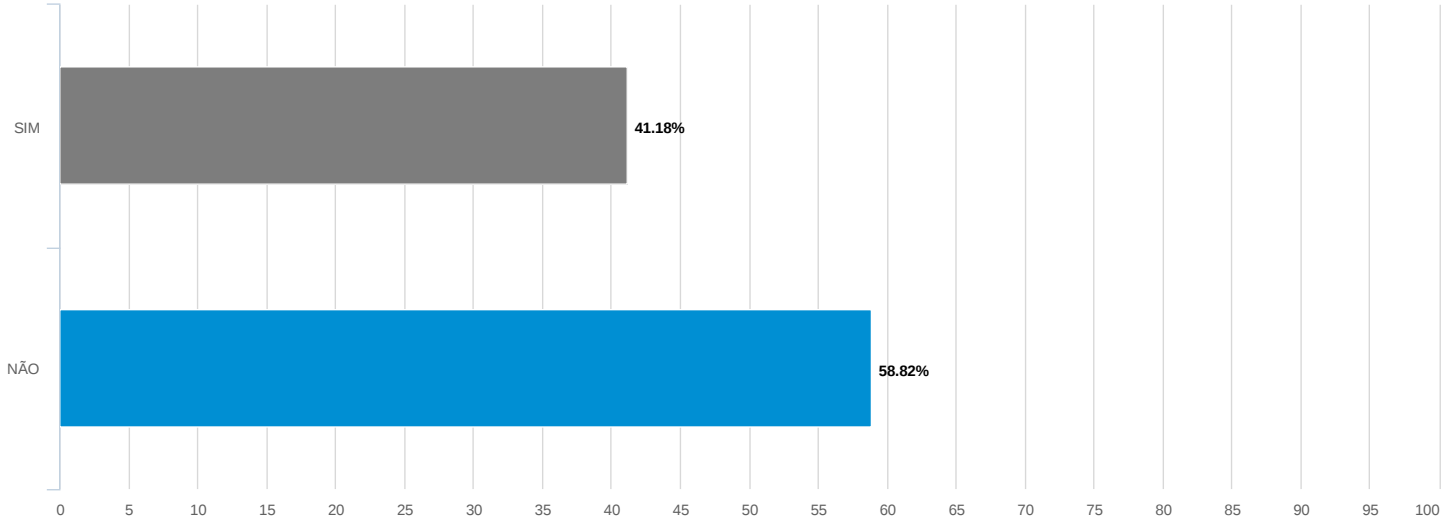
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	5	71.43%					
NÃO	2	28.57%					
Total	**7**	**100%**					

Em relação a incidentes de segurança que aconteçam, a organização possui um elemento responsável pela gestão desses incidentes?



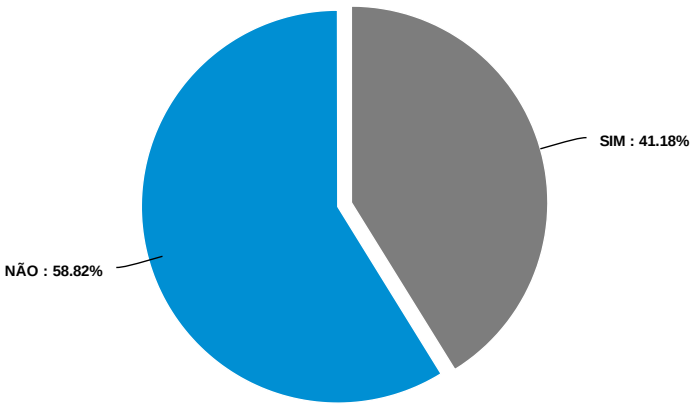
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	7	41.18%					
NÃO	10	58.82%					
Total	**17**	**100%**					

Na organização estão denidos quais os serviços/funções e atividades críticas, atividades estas que limitem a produção laboral?



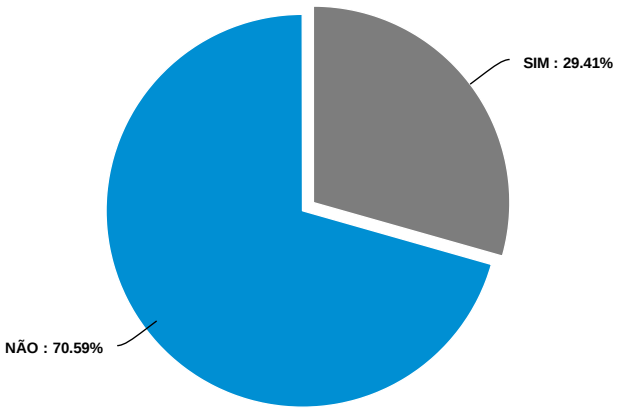
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	7	41.18%					
NÃO	10	58.82%					
Total	**17**	**100%**					

A informação que está armazenada na organização, tem definida classificação relativamente à sua importância, valor e sensibilidade?



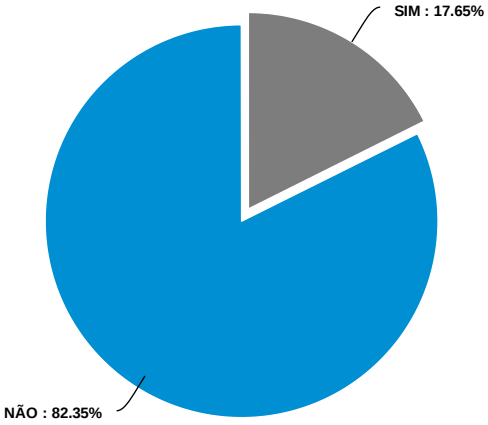
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	7	41.18%					
NÃO	10	58.82%					
Total	**17**	**100%**					

Aquando existe troca de informação critica seja com entidades internas ou externas são utilizados controlos criptográficos para salvaguarda da informação em trânsito?



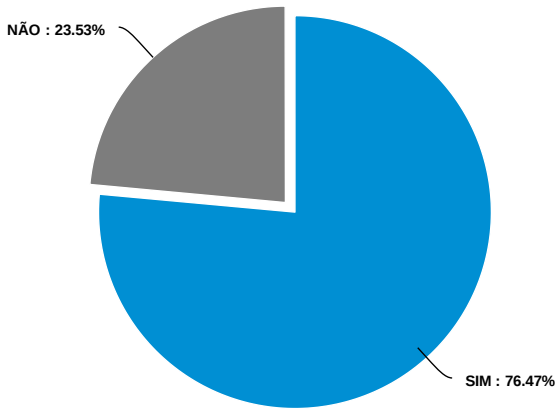
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	5	29.41%					
NÃO	12	70.59%					
Total	**17**	**100%**					

Existe uma análise/gestão de riscos definida na organização, onde estão identificados os mais prováveis riscos que poderão advir, avaliados e também como deverão ser respondidos em caso de se tornarem uma realidade?



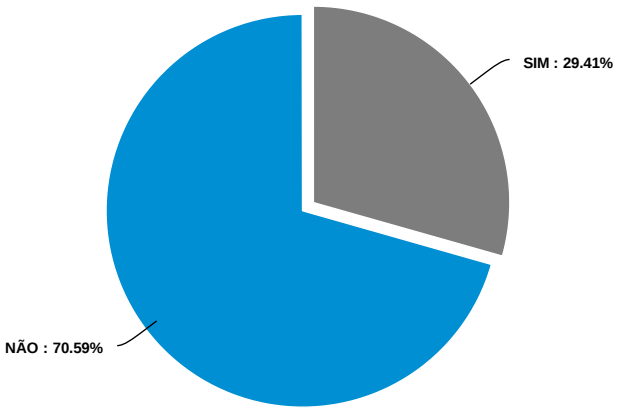
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	3	17.65%					
NÃO	14	82.35%					
Total	**17**	**100%**					

Todos os colaboradores da organização têm pleno conhecimento de quais as suas responsabilidades direitos e papéis a desempenhar na organização?



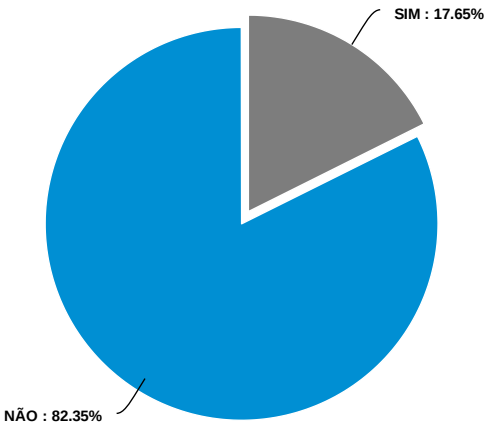
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	13	76.47%					
NÃO	4	23.53%					
Total	**17**	**100%**					

A organização tem definidas políticas de segurança da informação, políticas estas aprovadas pela administração e divulgadas aos restantes colaboradores?



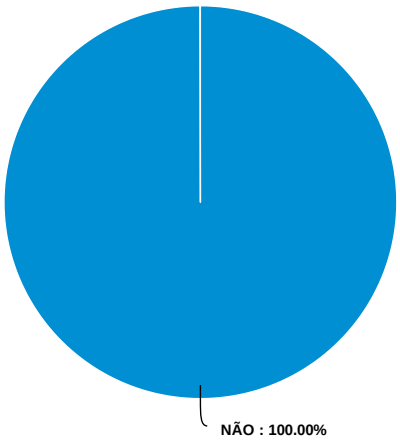
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	5	29.41%					
NÃO	12	70.59%					
Total	**17**	**100%**					

Existem procedimentos internos definidos para notificação de incidentes de Cibersegurança por parte dos colaboradores?



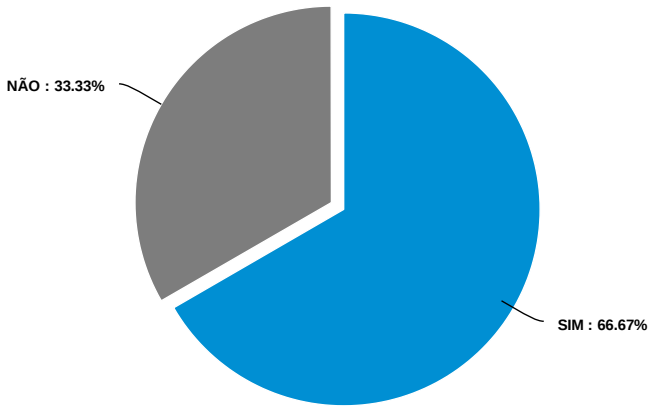
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	3	17.65%					
NÃO	14	82.35%					
Total	**17**	**100%**					

Esses incidentes, são classificados conforme a sua criticidade para que haja uma triagem/prioridade na resolução dos incidentes?



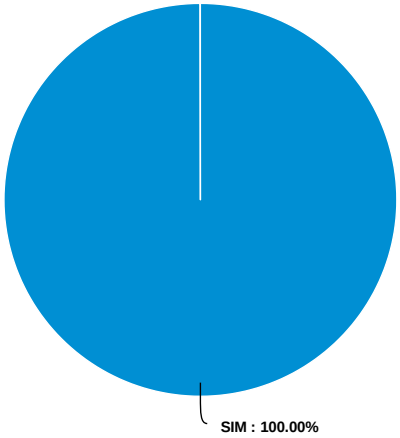
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	0	0%					
NÃO	3	100%					
Total	**3**	**100%**					

A organização possui configurados mecanismos de correção ou mitigação de incidentes de segurança de informação?



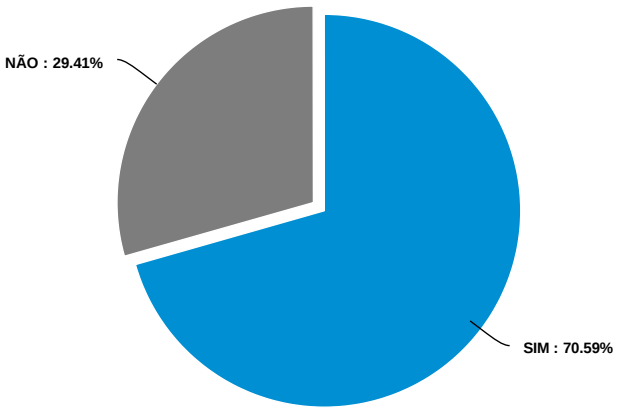
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	2	66.67%					
NÃO	1	33.33%					
Total	**3**	**100%**					

Todos os colaboradores da organização sabem como devem notificar um incidente?



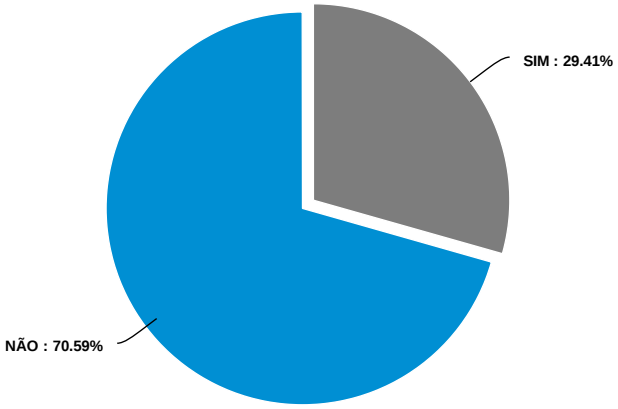
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	3	100%					
NÃO	0	0%					
Total	**3**	**100%**					

Estão definidas áreas/zonas críticas de acesso à organização quer em termos físicos quer em termos lógicos (através dos sistemas)?



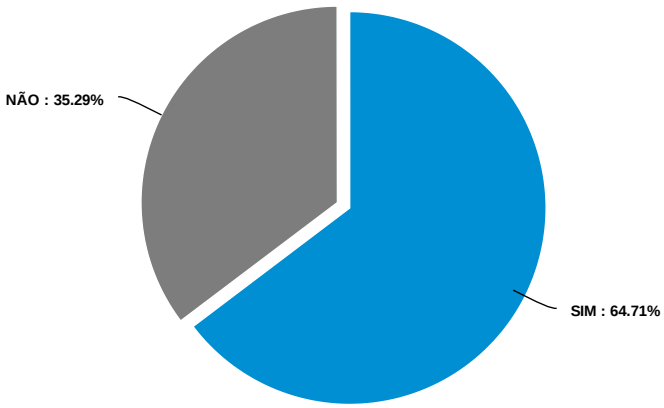
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	12	70.59%					
NÃO	5	29.41%					
Total	**17**	**100%**					

A arquitetura de rede & segurança da informação estão desenhadas?



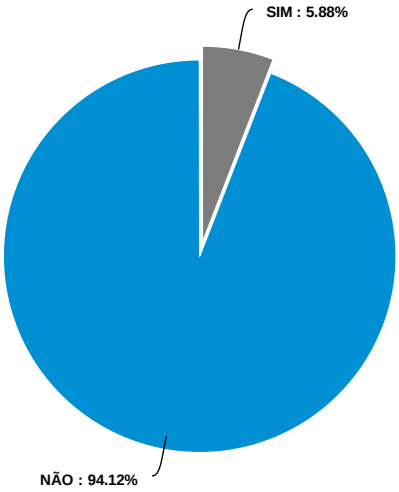
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	5	29.41%					
NÃO	12	70.59%					
Total	**17**	**100%**					

A organização tem implementados sistemas de deteção/prevenção de intrusão como uma Firewall/IDS?



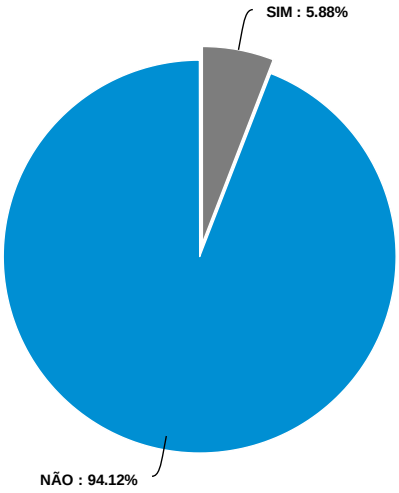
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	11	64.71%					
NÃO	6	35.29%					
Total	**17**	**100%**					

A organização tem implementado um sistema de recolha de metadados do tráfego que fluem na rede?



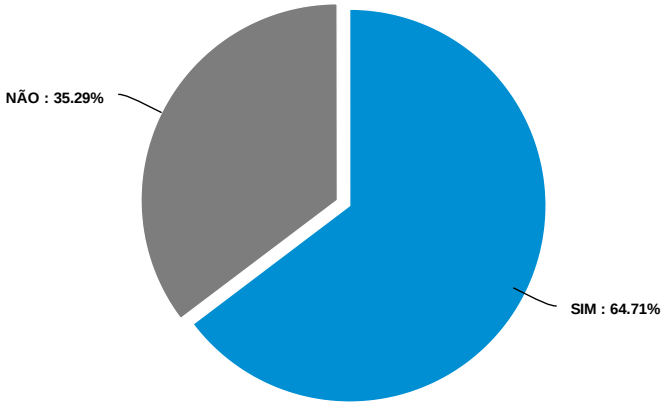
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	1	5.88%					
NÃO	16	94.12%					
Total	**17**	**100%**					

A organização comunica com algum grupo de profissionais, seja o CNCS (Centro Nacional de Cibersegurança), seja outro especializado em segurança de informação com objetivo de ampliar conhecimentos?



Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	1	5.88%					
NÃO	16	94.12%					
Total	**17**	**100%**					

Na sua organização é efetuada uma inventariação de ativos e serviços?

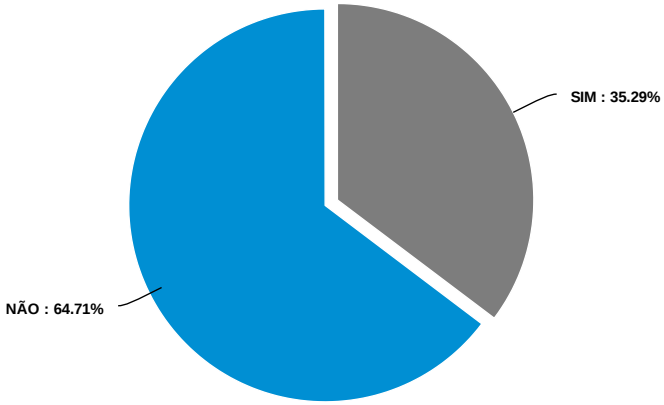


Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	11	64.71%					
NÃO	6	35.29%					
Total	**17**	**100%**					

Essa inventariação de ativos e serviços, é atualizada pelo menos de 6 em 6 meses?

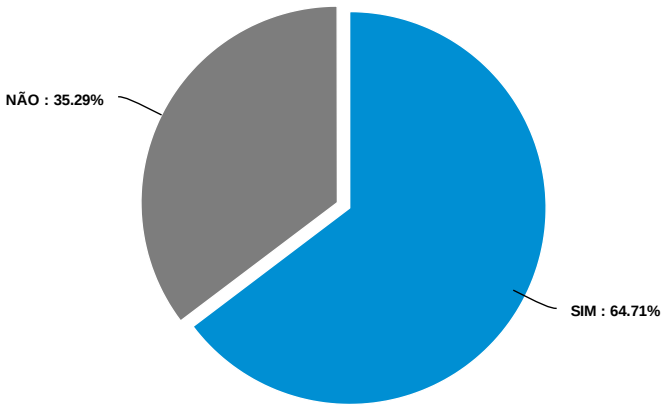
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	5	45.45%					
NÃO	6	54.55%					
Total	**11**	**100%**					

Relativamente à recolha centralizada de registos (Logs), que devem ser preservados pelo menos um ano, a sua organização efetua essa recolha de registos e por sua vez o seu armazenamento seguro?



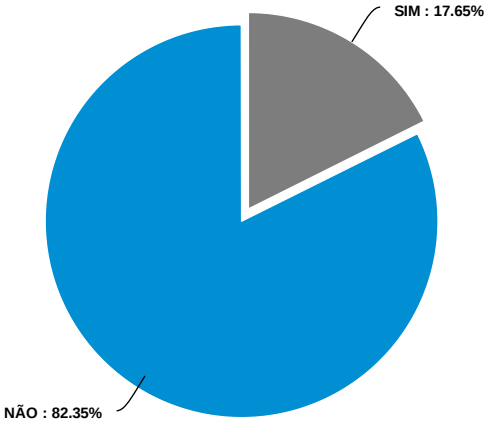
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	6	35.29%					
NÃO	11	64.71%					
Total	**17**	**100%**					

A organização tem presentes e são periodicamente atualizados, os quadros legais e regulatórios que a sua atividade está sujeita a respeitar?



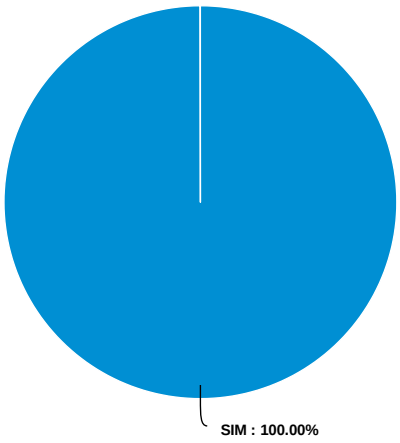
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	11	64.71%					
NÃO	6	35.29%					
Total	**17**	**100%**					

Está definida a política de uso aceitável (PUA) na organização, política esta que contém as linhas orientadoras para a utilização dos recursos, de forma segura por todos os colaboradores?



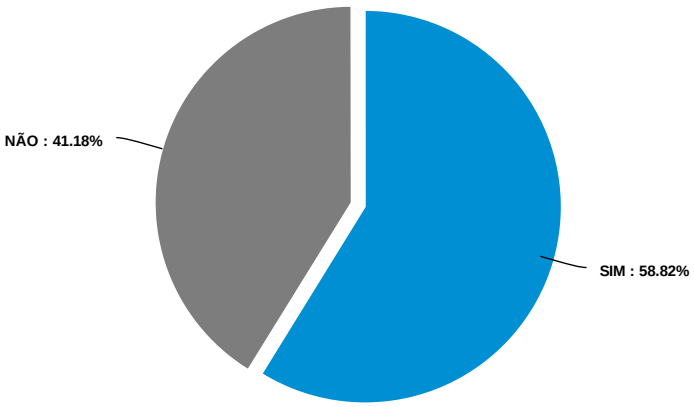
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	3	17.65%					
NÃO	14	82.35%					
Total	**17**	**100%**					

Em relação a cópias de segurança, a organização tem implementados mecanismos de salvaguarda de informação (backups), pelo menos da informação considerada prioritária?



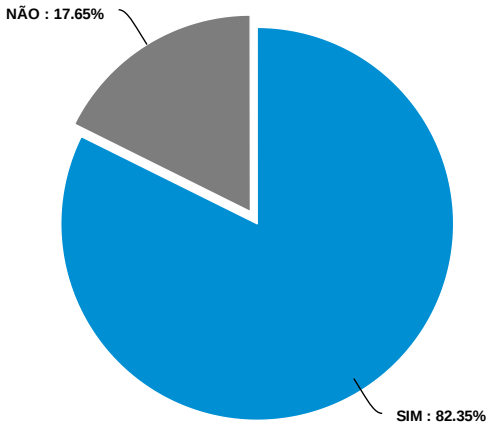
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	17	100%					
NÃO	0	0%					
Total	**17**	**100%**					

As cópias de segurança efetuadas são periodicamente testadas com o fim de se confirmar que não estão corrompidas?



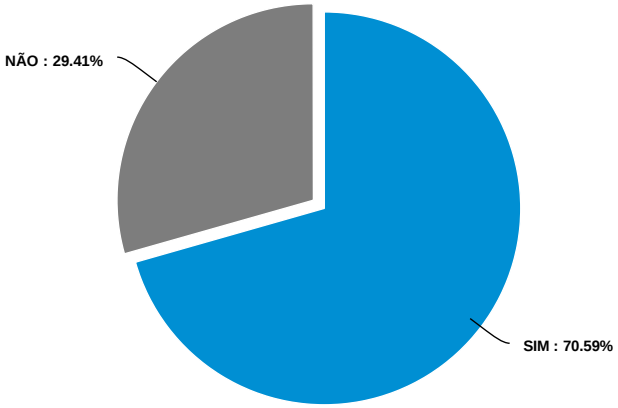
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	10	58.82%					
NÃO	7	41.18%					
Total	**17**	**100%**					

As notificações de cópias de segurança (backups), estão configuradas para notificar em caso de falha?



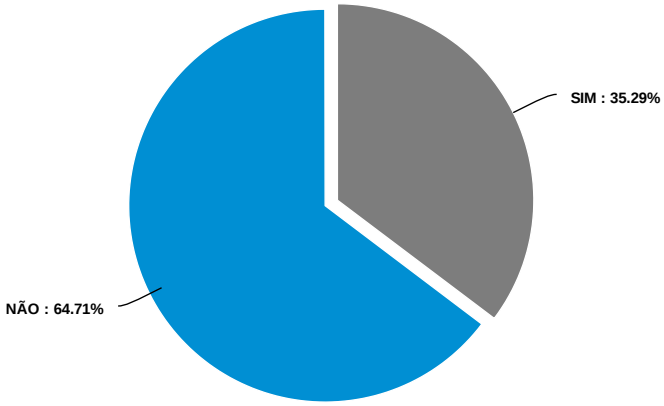
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	14	82.35%					
NÃO	3	17.65%					
Total	**17**	**100%**					

As cópias de segurança efetuadas, (existindo) estão a ser replicadas para o exterior?



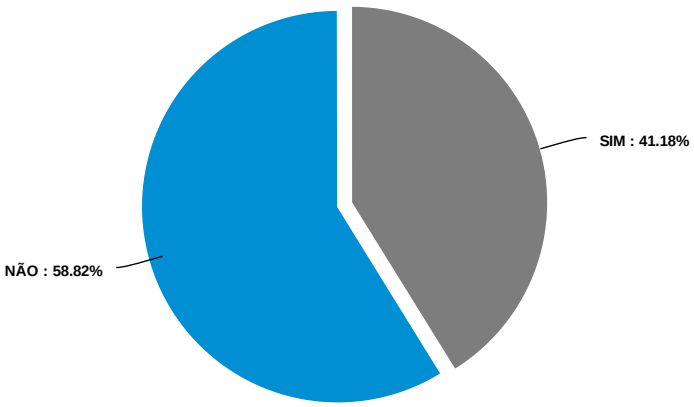
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	12	70.59%					
NÃO	5	29.41%					
Total	**17**	**100%**					

Está contemplado na organização um plano de formação para os colaboradores?



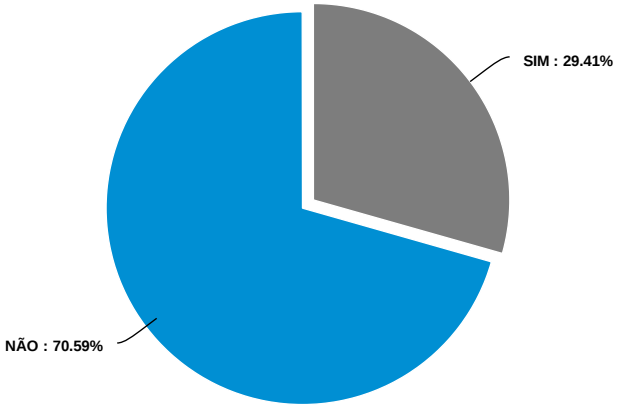
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	6	35.29%					
NÃO	11	64.71%					
Total	**17**	**100%**					

A organização efetua ações de sensibilização e treino interno para consciencialização dos colaboradores?



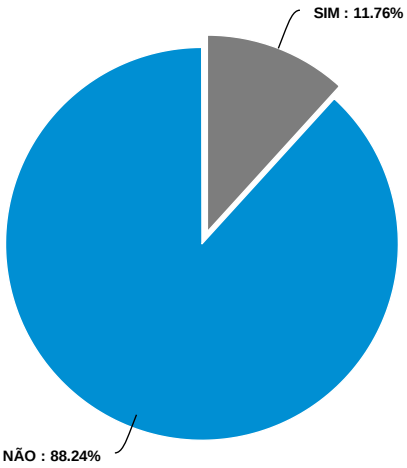
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	7	41.18%					
NÃO	10	58.82%					
Total	**17**	**100%**					

As pessoas chave da organização (administração, chefias) têm formação mais orientada aos principais mecanismos no que toca à política de segurança, metodologia de gestão de risco e sua aplicação na prática?



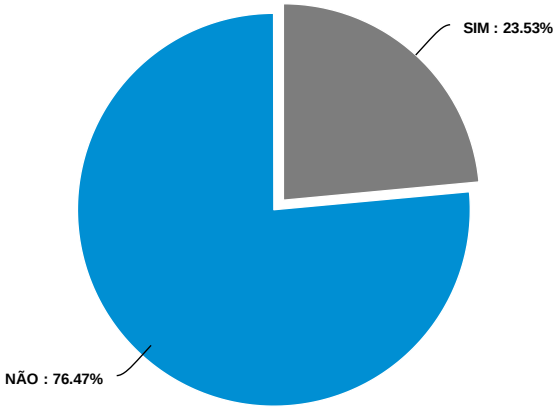
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	5	29.41%					
NÃO	12	70.59%					
Total	**17**	**100%**					

A organização tem configurados mecanismos de registo e auditoria de acesso a bases de dados com informação crítica?



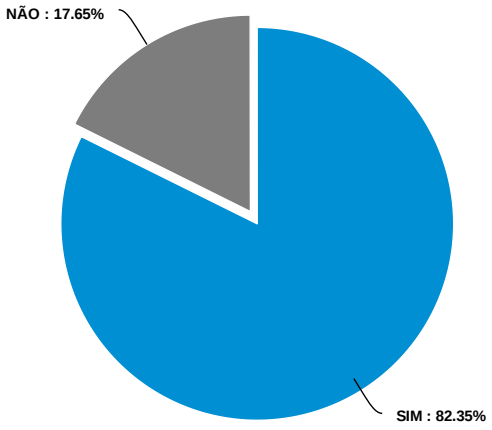
Answer	Count	Percent
SIM	2	11.76%
NÃO	15	88.24%
Total	**17**	**100%**

Estão configurados mecanismos de controlo de acessos web (proxy por exemplo)?



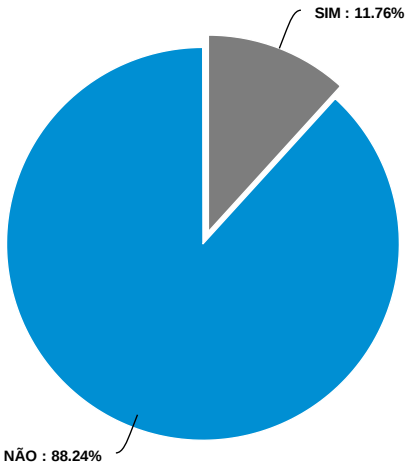
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	4	23.53%					
NÃO	13	76.47%					
Total	**17**	**100%**					

A organização possuí um antivírus fidedigno configurado nos ativos mais críticos da organização?



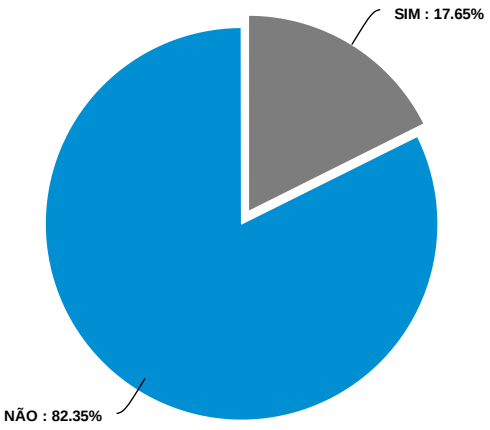
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	14	82.35%					
NÃO	3	17.65%					
Total	**17**	**100%**					

Existem procedimentos definidos para utilização dos dispositivos de comunicação e/ou dispositivos móveis? (Telemóveis, portáteis, tablets)



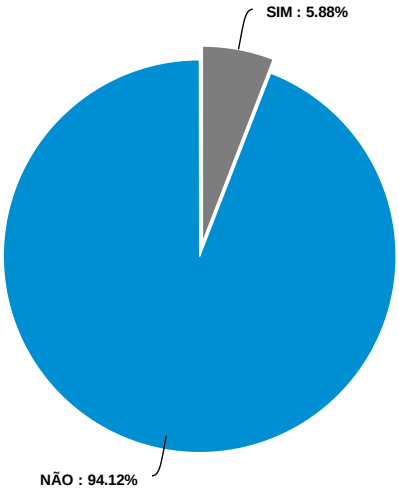
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	2	11.76%					
NÃO	15	88.24%					
Total	**17**	**100%**					

A organização tem configurado um sistema de monitorização de pelo menos os principais ativos da rede?



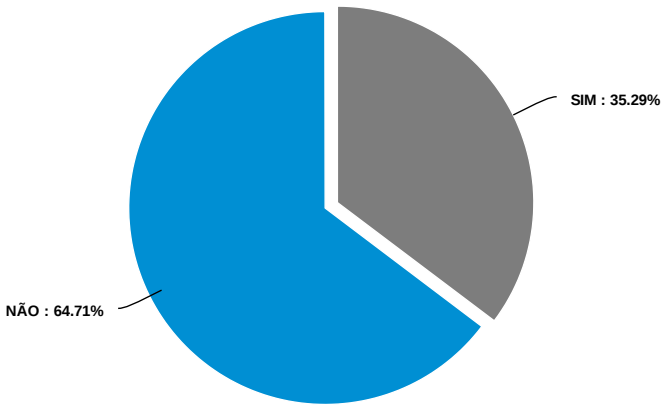
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	3	17.65%					
NÃO	14	82.35%					
Total	**17**	**100%**					

A organização tem implementado um SIEM, que agrega os registos (logs) mais relevantes produzidos pelos ativos e pelas aplicações de suporte à atividade?



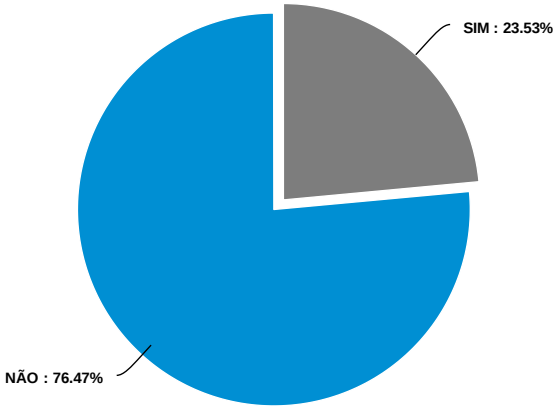
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	1	5.88%					
NÃO	16	94.12%					
Total	**17**	**100%**					

Está definido um plano de continuidade da organização, para que em caso de catástrofe seja possível continuar com o negócio?



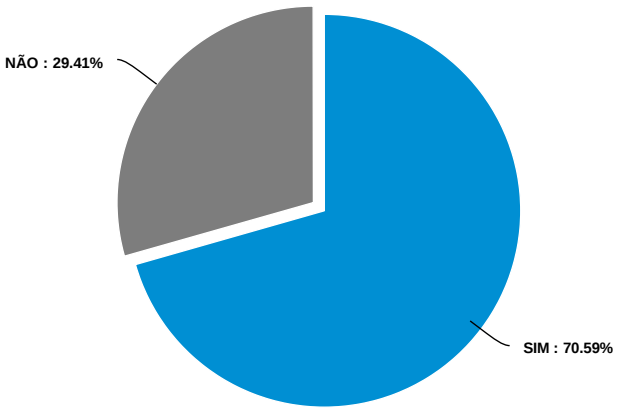
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	6	35.29%					
NÃO	11	64.71%					
Total	**17**	**100%**					

O staff de quem faz parte do departamento de segurança de informação, TIC, possuí formação periódica na área para que seja devidamente atualizado em termos de perigos existentes, vulnerabilidades, etc



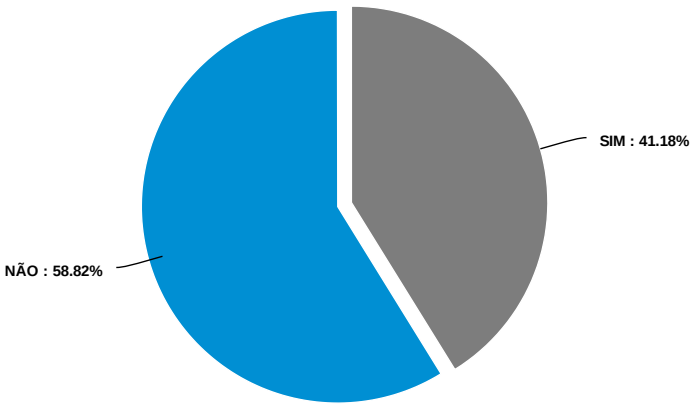
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	4	23.53%					
NÃO	13	76.47%					
Total	**17**	**100%**					

Os privilégios de acesso individual à informação, foram devidamente aprovados pela administração e revistos com frequência?



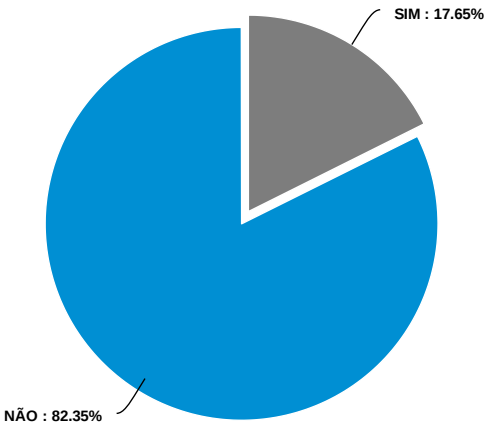
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	12	70.59%					
NÃO	5	29.41%					
Total	**17**	**100%**					

A organização procedeu a criação de políticas de segurança, boas práticas e normas internas a serem adotadas por todos os colaboradores?



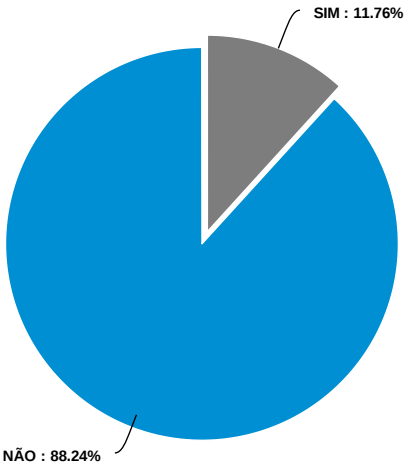
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	7	41.18%					
NÃO	10	58.82%					
Total	**17**	**100%**					

Existe uma reavaliação continua de acessos, privilégios, procedimentos implementados na empresa em relação à segurança de informação?



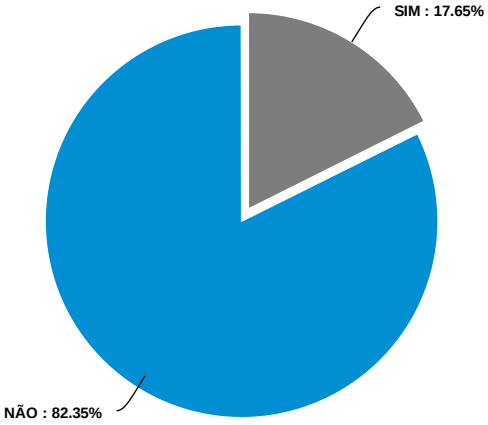
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	3	17.65%					
NÃO	14	82.35%					
Total	**17**	**100%**					

A organização efetua um simulacro periodicamente por forma a encontrar vulnerabilidades no que foi implementado para a segurança de informação?



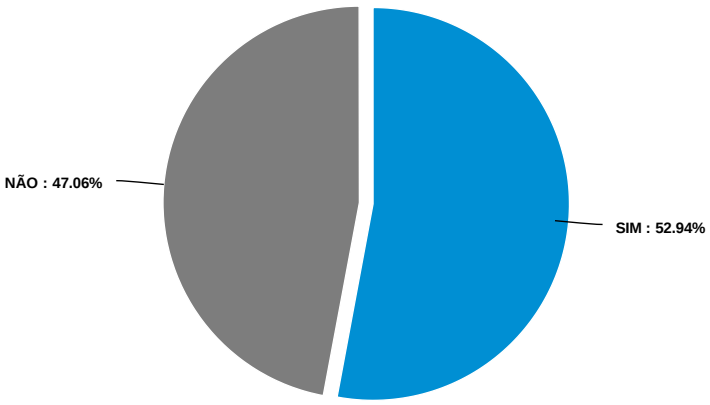
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	2	11.76%					
NÃO	15	88.24%					
Total	**17**	**100%**					

Os colaboradores, principalmente os que ocupam cargos de chefia recebem formação e treino adequado para o cumprimento adequado conforme o que foi definido para cada função e até em termos de segurança de informação?



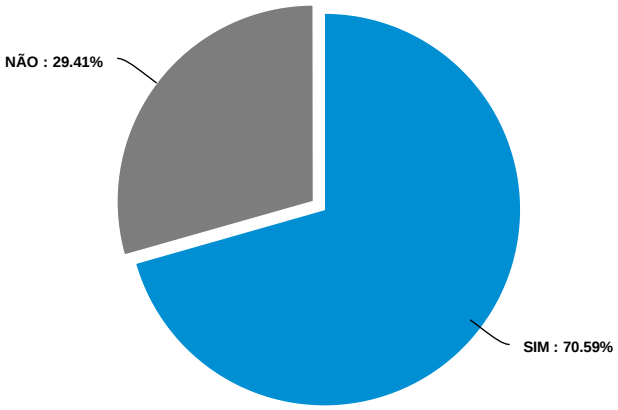
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	3	17.65%					
NÃO	14	82.35%					
Total	**17**	**100%**					

São efetuados testes de segurança a novos serviços/aplicações antes de serem expostos à utilização por todos os utilizadores?



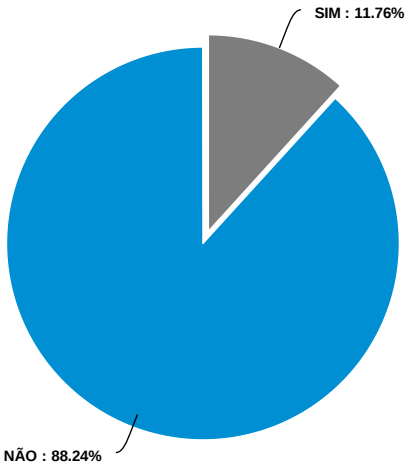
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	9	52.94%					
NÃO	8	47.06%					
Total	**17**	**100%**					

Em caso de atualização de aplicações/serviços, são efetuados testes por forma a garantir que não é colocado em causa o bom funcionamento atual?



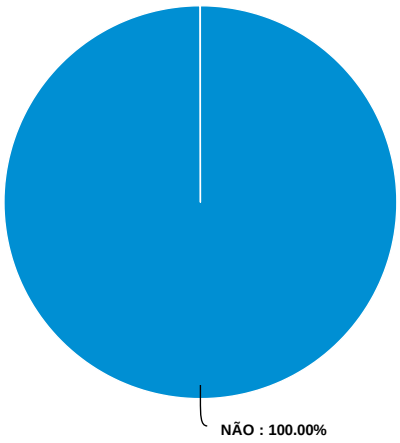
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	12	70.59%					
NÃO	5	29.41%					
Total	**17**	**100%**					

Está implementado um plano de auditorias, com periodicidade de pelo menos um ano?



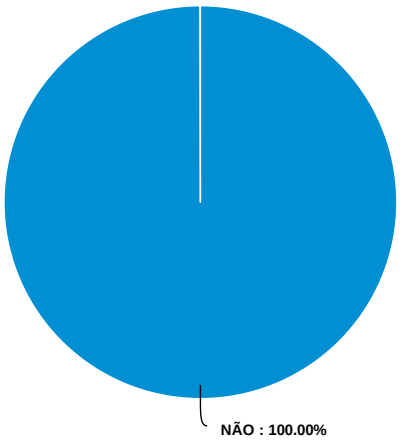
Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	2	11.76%					
NÃO	15	88.24%					
Total	**17**	**100%**					

Está contemplado um plano de ação e orçamento aprovados para montar e operar a equipa CSIRT ou SOC?



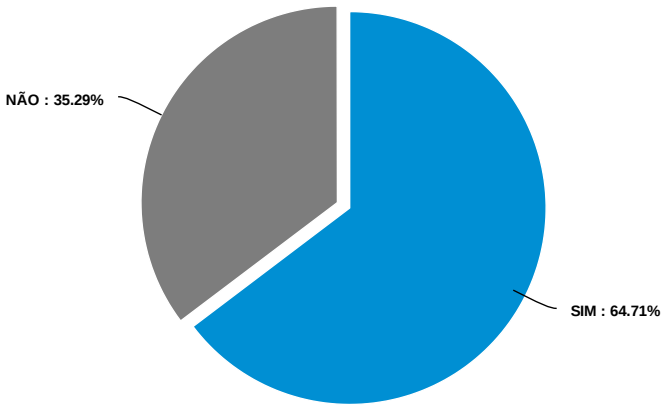
Answer	Count	Percent
SIM	0	0%
NÃO	17	100%
Total	**17**	**100%**

A organização possui um sistema de gestão de crise, capaz de lidar com grandes incidentes de segurança?



Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	0	0%					
NÃO	17	100%					
Total	**17**	**100%**					

Ao preencher este questionário, sentiu necessidade de acompanhamento técnico para o correto e conciso preenchimento



Answer	Count	Percent	20%	40%	60%	80%	100%
SIM	11	64.71%					
NÃO	6	35.29%					
Total	**17**	**100%**					

DECLARAÇÃO

Declaro, sob compromisso de honra, que o trabalho apresentado nesta dissertação, com o título *"Desenvolvimento de uma metodologia para avaliação do estado da Segurança Informática em PME"*, é original e foi realizado por Bruno Filipe Diogo Azinheira (2200331) sob orientação de do professor Doutor Mário Antunes, (mario.antunes@ipleiria.pt), da professora Doutora Marisa Maximiano, (marisa.maximiano@ipleiria.pt) e e do professor Ricardo Gomes (ricardo.p.gomes@ipleiria.pt).

Assinado por: **BRUNO FILIPE DIOGO AZINHEIRA**
Num. de Identificação: 13816051
Data: 2022.07.27 16:08:35+01'00'

Leiria, Junho de 2022

Bruno Filipe Diogo Azinheira