Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO

GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

DISSERTAÇÃO

O FATOR HUMANO COMO ELEMENTO DA SEGURANÇA DA INFORMAÇÃO

JOÃO PAULO CORDEIRO LEAL

OUTUBRO - 2023

Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO EM
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
DISSERTAÇÃO

O FATOR HUMANO COMO ELEMENTO DA SEGURANÇA DA INFORMAÇÃO

JOÃO PAULO CORDEIRO LEAL

ORIENTAÇÃO:
PROFESSOR DOUTOR ANTÓNIO PALMA DOS REIS

OUTUBRO - 2023

Resumo

As mudanças tecnológicas impulsionadas pela Pandemia Covid-19, a utilização de equipamentos eletrónicos em que a fronteira entre o pessoal e o corporativo é muito ténue, a capacidade de aceder aos recursos e informações a partir de qualquer lugar, conjugados, criaram um panorama fértil para ser explorado por cibercriminosos.

Este trabalho procurou através de um questionário, aos colaboradores da Organização, recolher dados numa visão global sobre a temática da segurança da informação, para posterior análise e proposta de medidas e ações que resultem numa melhoria organizacional, centradas no fator humano como elemento da segurança na informação, transformando conhecimento empírico em dados.

Os resultados permitiram a identificação de aspetos e fatores comportamentais relacionados com os recursos humanos da Organização, que necessitam de ser atendados, para uma melhoria efetiva em áreas formativas que versem a pegada digital, a cibersegurança ou a segurança da informação, e na utilização dos acessos fora do ambiente protegido da Organização.

Ao nível do desempenho organizacional identificou-se a necessidade de melhorar a comunicação interna ou a adequação da função ao nível académico que alguns colaboradores detinham. Ficou igualmente patente o esforço desenvolvido em termos tecnológicos para fazer face às condicionantes decorrentes da Pandemia Covid-19, conjugado com mudança tecnológica que estava em implementação.

Palavras-chave: Fator humano, Segurança da Informação, Engenharia social, teletrabalho, trabalho remoto, trabalho híbrido

Abstract

The technological changes driven by the Covid-19 Pandemic, the usage of electronic equipment in which the boundary between the personal and the corporate is very blurred, the ability to access resources and information from anywhere, combined, have created a fertile landscape to be exploited by cybercriminals.

This work will seek, through a questionnaire, to the employees of the Organization, to collect data in a global view on the theme of information security, for subsequent analysis and proposal of measures and actions that result in an organizational improvement, focused on the human factor as an element of information security, transforming empirical knowledge into data.

The results allowed the identification of aspects and behavioural factors related to the Organization's human resources, which need to be addressed, for an effective improvement in training areas that deal with the digital footprint, cybersecurity or information security, and in the use of access outside the Organization's protected environment.

In terms of organizational performance, it was identified the need to improve internal communication or the adequacy of the function to the academic level that some employees had. The effort made in technological terms to face the constraints arising from the Covid-19 Pandemic, combined with the technological change that was being implemented, was also evident.

Keywords: Human factor, Information Security, Social engineering, teleworking, remote work, hybrid work

Agradecimentos

Eles não sabem, nem sonham,
que o sonho comanda a vida.
Que sempre que um homem sonha
o mundo pula e avança
como bola colorida
entre a mãos de uma criança." [1]

A chegada até esta minha etapa de formação académica, é o culminar de anos de adversidades e incertezas que se davam como certas ou inalcançáveis.

Agradeço por isso a todos aqueles que me ajudaram, em particular ao Carlos, ao Professor António Palma dos Reis, que foi o meu orientador neste trabalho pela sua dedicação e paciência, e aos meus colegas de trabalho e amigos que nas horas mais complicadas me incentivaram a não desistir de seguir o meu sonho.

A todos vós o meu sincero obrigado.

[1] Excerto do poema "Pedra Filosofa", de António Gedeão
(*Prof. Rómulo de Carvalho, 1906-1997*)

Índice

Acrónimos

2FA - *Two-factor authentication* (Autenticação de dois fatores)

AD - *Active Directory*

BYOD - *Bring Your Own Device*

CNCS - Centro Nacional de Cibersegurança

CNPD - Comissão Nacional de Proteção de Dados

DDoS - *Denial-of-service* (*attack*)
Ataques Distribuídos de Negação de Serviço

ENSC - Estratégia Nacional de Segurança no Ciberespaço

HSE - *Health and Safety Executive*

IA - Inteligência Artificial

IDS - *Intrusion Detection System* (Sistema de Deteção de Intrusões)

IEC - *International Electrotechnical Commission* (Comissão eletrotécnica internacional)

INE - Instituto Nacional de Estatística

IoT - Internet das Coisas (*Internet of Things)*

ISO - International Organization for Standardization (Organização internacional de normalização)

JAI - Justiça e Assuntos Internos (União Europeia)

LDAP - *Lightweight Directory Access Protocol*

MFA - *Multifactor authentication* (Autenticação multifator)

NOC - *Network Operations Center* (Centro de Operações de rede)

OMS - Organização Mundial de Saúde

P2P	-	*Peer to peer (*Par a par)
PME	-	Pequenas e Médias Empresas
PUA	-	Política de Utilização Aceitável
SARS-CoV-2	-	*Severe acute respiratória syndrome coronavirus 2 (*Coronavírus da Síndrome respiratória aguda grave 2*)*
SI	-	Sistema de Informação
SMS	-	*Short Message Service* ou *Short Messaging Service*
SOC	-	*Security Operations Center* (Centro de Operações de Segurança)
TIC	-	Tecnologias de Informação e Comunicação
VPN	-	*Virtual Private Network (*Rede Privada Virtual)
WEC	-	World Econimic Forum
Wi-fi	-	*Wireless Fidelity*

Glossário

Autenticação de dois fatores [2FA] - método de segurança de gestão de identidade e acesso que requer duas formas de identificação para aceder a recursos e dados, derivado do MFA.

[Fonte: adaptado de "*O que é a autenticação de dois fatores?*" – Microsoft (em linha)]

Autenticação multifator [MFA] - método de segurança de gestão de identidade e acesso que requer pelo menos duas formas [podem ser até quatro] de identificação para aceder a recursos e dados.

[Fonte: adaptado de "*O que é: autenticação multifator*" - Microsoft (em linha)]

Ciberataque - ataque realizado através das tecnologias de informação no ciberespaço dirigido contra um ou vários sistemas, com o objetivo de prejudicar a segurança das tecnologias de informação e da comunicação [confidencialidade, integridade e disponibilidade], em parte ou totalmente.

[Fonte: CNCS – Glossário (em linha)]

Cibersegurança - engloba as atividades necessárias para proteger as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas por ciberameaças.

[Fonte: Regulamento Cibersegurança da UE (em linha)]

Engenharia Social - ato de enganar um indivíduo no sentido de este revelar informação sensível, assim obtendo-se acesso não autorizado ou cometendo fraude, com base numa associação com este indivíduo de modo a ganhar a sua confiança.

[Fonte: traduzido de "*Digital Identity Guidelines: revision 3"* – NIST (Grassi et al., 2017, p.54]

Incidente (ou ciberincidente) - evento com um efeito adverso real na segurança das redes e dos sistemas de informação.

[Fonte: Lei n.º 46/2018, de 13 de agosto (em linha)]

Informação - dados e factos que foram organizados e comunicados de forma coerente e com significado e a partir dos quais se podem tirar conclusões.

[Fonte: APDSI – Glossário da Sociedade da Informação (em linha)]

Literacia digital - conhecimento essencial necessário para uma pessoa trabalhar com um computador de modo independente. Isto inclui a capacidade de resolver problemas, de se adaptar a situações novas, de manter a informação organizada, e de comunicar de modo eficaz com outras pessoas dotadas de literacia computacional.

[Fonte: APDSI – Glossário da Sociedade da Informação (em linha)]

Malware - programa que é introduzido num sistema, geralmente de forma encoberta, com a intenção de comprometer a confidencialidade, a integridade ou

a disponibilidade dos dados da vítima, de aplicações ou do sistema operativo, ou perturbando a vítima.

[Fonte: traduzido de "*Glossary of key information security terms"* – NIST (Paulsen & Byers, 2019), (em linha)]

Mobilidade - utilização de tecnologias sem fios para aceder a informações e aplicações na Internet a partir de dispositivos móveis, como computadores portáteis, telemóveis, dispositivos GPS e outros.

[Fonte: APDSI – Glossário da Sociedade da Informação (em linha)]

Network Operation Center **[NOC]** - responsável pela monitorização das redes de informação, equipamentos, circuitos e tráfego.

[Fonte: traduzido e adaptado de "*Organizing a Network Operation Centre on Campus*" (Oksanen, 2013)]

Pegada digital - rasto de informação que todos os utilizadores deixam na Internet enquanto navegam por sites e utilizam serviços online. Esse rasto pode incluir dados pessoais, como moradas, contactos, fotografias ou vídeos, e registos de atividade – como o tempo que o utilizador demorou num determinado site ou as vezes em que usou o cartão de crédito.

[Fonte: "*Pegada digital: como descobrir e gerir a sua identidade online*" (Duarte, 2018), (em linha)]

Ransomware – é uma estratégia de resgate suportada por um software de encriptação que bloqueia o acesso aos ficheiros ou aos computadores, até que se pague o resgate. Este software encripta os dados com uma chave secreta. [Fonte: "A Segurança da Informação - Informação ao Colaborador", (Vicente, 2017)]

Rede Privada Virtual [VPN] - rede virtual de comunicação privada que utiliza uma infraestrutura pública de telecomunicações para transmitir dados que são protegidos devido à utilização de técnicas de cifragem ou de encapsulação.
[Fonte: APDSI – Glossário da Sociedade da Informação (em linha)]

Redes Sociais - plataformas usadas para criar ligações sociais entre pessoas que partilham interesses ou atividades similares. Este sistema web providencia uma variedade de meios para que os utilizadores interajam, tais como chat, mensagem, email, vídeo, chat de voz, partilha de ficheiros, *blogging*, grupos de discussão, entre outros.
[Fonte: traduzido de "*Internet Literacy Handbook (2017) - Supporting users in the online world*", (Richardson et al., 2017 p.55)]

Risco - circunstância ou evento razoavelmente identificável, com um efeito adverso potencial na segurança das redes e dos sistemas de informação.
[Fonte: Lei n.º 46/2018, de 13 de agosto (em linha)]

Segurança da informação – processo organizado e estruturado que permite preservar a confidencialidade, integridade e a disponibilidade da informação.
[Fonte: “A Segurança da Informação - Informação ao Colaborador” (Vicente, 2017)]

Sistema de Informação - dispositivo ou grupo de dispositivos interligados ou associados, dos quais um ou mais executam, através de um programa, o tratamento automático de dados informáticos, bem como de dados informáticos armazenados, tratados, recuperados ou transmitidos por esse dispositivo ou grupo de dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção.
[Fonte: Diretiva n.º 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013 (em linha)]

Smartphone - [telefone inteligente] dispositivo com tecnologias avançadas que combina as características de um telemóvel com as de um computador tablete, e habitualmente tem câmara digital e outros funcionalidades suportadas por um sistema operativo específico para dispositivos móveis.
[Fonte: adaptado de APDSI – Glossário da Sociedade da Informação (em linha)]

***Security Operations Center* [SOC]** - responsável pela monitorização da infraestrutura de TIC de uma organização, com capacidade de deteção, resposta e prevenção de ciberameaças.

[Fonte: adaptado de "*Centro de Operações de Segurança (SOC)*" - IBM (em linha)]

Violação de dados pessoais – violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

[Fonte: Regulamento (EU) 2016/679, de 27 de abril (em linha)]

Índice das Imagens

Índice dos Gráficos

Capítulo 1 – Introdução

1.1 - Enquadramento

O rápido crescimento tecnológico recente, nomeadamente a digitalização de processos, o automatismo, a mobilidade, o surgimento da IA e dos dispositivos *IoT*, amplificado por uma mudança socialmente mais profunda, que hoje ainda está a ser escrita, tem compelido as organizações e empresas a repensar a forma de estar e agir no mercado global, onde o digital é a palavra de ordem.

Um dos exemplos demostrativo desta transformação, é explicado pela gestora de Recursos Humanos Marta Grilo, quando entrevistada pela jornalista do Jornal Expresso Teresa Ribeiro:

> *Os Millennials e a Geração Z estão a mudar o mercado de trabalho ao torná-lo mais digital e menos linear, já que agora o "novo normal é saltar de empresa para empresa, (…) e o "mercado está a adaptar-se ao "trabalho à distância ou com cargas de horários diferentes.*"
>
> In Ribeiro (2023)

Das medidas decretadas pela Organização Mundial da Saúde (OMS), entre março de 2020 (ONU News, 2020) e maio de 2023 (ONU News, 2023), no âmbito do combate à Pandemia Covid-19, o confinamento foi aquela de maior impacto, transversal a toda a Sociedade, tendo sido, provavelmente, a medida

mais marcante e o fator exógeno que expôs as fragilidades decorrentes de um processo transformativo que decorria, até então, a diferentes velocidades.

Contudo, havia que atender de forma imediata às condicionantes provocadas pelos confinamentos, e o teletrabalho foi a ferramenta mais utilizada.

Hoje, teletrabalho, trabalho remoto ou trabalho híbrido não são somente vocábulos que entraram no uso diário, são também uma consequência, que se transformou em necessidade, quase obrigatória, para que as empresas e organizações retenham colaboradores, sendo também apresentado como um fator diferenciador para a captação de novos colaboradores. Os períodos de confinamento, que permitiram o desfrutar dos pequenos “prazeres da vida”, antes subvalorizados, são agora difíceis de deixar de lado e retornar à mentalidade do trabalho de 8 horas diárias.

Para esta nova atitude, não é alheio o fato das mesmas ferramentas tecnológicas poderem satisfazer simultaneamente o ambiente corporativo e o ambiente familiar, a que se alia a generalização do acesso à Internet, catapultando a mobilidade para um nível até antes nunca atingido, libertando o trabalho das amarras da localização.

A imprevisibilidade do local de trabalho acarreta desafios em termos de segurança. Para as empresas ou organizações o estender do perímetro de segurança até ao colaborador remoto, até então assegurada nas redes corporativas, é um novo desafio de reorganização da infraestrutura tecnológica, e já não basta pensar, como ainda pensam muitos gestores de topo e profissionais das tecnologias de informação, que o uso de *firewalls* de perímetro*, IDSs*, ou dispositivos de autenticação sejam suficientes para que se fique imune

a ciberataques (Mitnick & Simon, 2002, p.17), a que se alia a necessidade de criar ou recriar políticas de segurança e módulos de formação, que atendam à nova realidade, garantindo que os colaboradores remotos cumprem requisitos de salvaguarda de acesso e proteção da informação.

Para os requisitos tecnológicos ou tecnologias de colaboração, o mercado tem-se adaptado e apresentado soluções que atendem a estas necessidades, contudo, na questão humana, a falta de formação em competências digitais tem-se revelado num enorme desafio, com afirmou Pedro Veiga, considerado "um dos "pais" da Internet em Portugal, na entrevista ao jornal Expresso intitulada "*Ataques informáticos: a iliteracia digital em Portugal é "muito elevada" e o teletrabalho "expôs ainda mais as vulnerabilidades*", ao "*não se qualificar as pessoas e não se tem apostado na formação dos trabalhadores mais velhos"* (Jornal Expresso, Sociedade, 2022)

As técnicas de engenharia social são atualmente uma das maiores ameaças à segurança da informação, impulsionadas com a expansão do trabalho remoto e de toda a sua envolvência, na exploração da falha humana.

As mudanças tecnológicas impulsionadas pela Pandemia Covid-19, a utilização de equipamentos eletrónicos em que a fronteira entre o pessoal e o corporativo é muito ténue, a capacidade de aceder aos recursos e informações a partir de qualquer lugar, conjugados, criaram um panorama fértil para ser explorado por cibercriminosos e pouco conhecido no seio da Organização em estudo neste trabalho, que motivou a sua realização, focado no fator humano como elemento da segurança na informação.

Esta investigação parte também da necessidade e motivação pessoal, de contribuir na criação de um ambiente seguro no seio da Organização.

É expectável que sejam identificadas algumas boas práticas no acesso, salvaguarda ou manuseio da informação, em parte devido à natureza da Organização em estudo e da cultura interna.

Através de um trabalho prático de suporte a esta investigação, questionário, procurar-se-á quantificar o conhecimento empírico em dados, que permitam a apresentação de uma visão da envolvência e do compromisso do fator humano como elemento na segurança da informação.

> *Computer users are often referred to, rather disparagingly as "the weakest link" in information security.*[2]
>
> In Renaud & Goucher (2014), p. 361.

1.2 - Domínio e Foco da Investigação

> *As developers invent continually better security technologies, making it increasingly difficult to exploit technical vulnerabilities, attackers will turn more and more to exploiting the human element. Cracking the human*

[2] Tradução livre: "*Os utilizadores de computadores são muitas vezes referidos, de forma bastante depreciativa, como "o elo mais fraco" na segurança da informação*"

firewall is often easy, requires no investment beyond the cost of a phone call, and involves minimal risk."[3]

In Mitnick & Simon (2002), p. 17.

Diversos autores têm proposto uma definição para segurança da informação, Summerss (1997) ou Feleol (2012) (cit. in. Ferreira, 2003) por exemplo, define como estando associada ao uso dos equipamentos informáticos e assenta em três vetores: confidencialidade, integridade e disponibilidade. Para Oliveira (2001, p.17), é "(…) *o processo de proteção de informações e ativos digitais armazenados em computadores e redes de processamento de dados*", ou ainda segundo Peltier (2005, p.13), expandia ainda um pouco mais esse conceito, que para além do processo físico de proteção adicionou o processo lógico, numa visão em que "*a segurança da informação direciona e apoia a empresa e organizações afiliadas na proteção de seus ativos de informação de forma intencional ou não intencional divulgação, modificação, destruição ou negação por meio de a implementação de segurança da informação adequada e políticas, procedimentos, planejamento de retomada de negócios, e diretrizes."*

Diversas visões na procura da definição de segurança da informação sem que nenhuma delas envolvesse o fator humano, embora Oliveira (2001, p.9) já fizesse alusão a essa necessidade:

[3] Tradução livre: "*À medida que os desenvolvedores inventam tecnologias de segurança cada vez melhores, tornando cada vez mais difícil a exploração de vulnerabilidades técnicas, os invasores recorrerão cada vez mais à exploração do elemento humano. Quebrar a firewall humano costuma ser fácil, não requer nenhum investimento além do custo de uma ligação telefônica e envolve riscos mínimos.*"

> *Nenhuma área da informática é tão vasta e apreciada como a segurança da informação: o ponto principal da segurança leva a um outro ponto principal, o ser humano, (…) todo o processo de segurança se inicia e tem o seu término num ser humano. Não adianta nada gastarmos fortunas em equipamentos e sistemas de segurança se não conhecermos quem utilizará os nossos sistemas, e quem pode ter acesso a eles mesmo sem autorização."*
>
> In Oliveira (2001), p. 9.

Em 2009, Barros e Costa no *paper* intitulado: "*O fator humano como pilar da Segurança da Informação: uma proposta alternativa*", apresentam o que será talvez uma das primeiras referências literárias e proposta para a mudança deste paradigma, ao sugerirem o fator humano com quarto pilar da segurança da informação (Barros & Costa, 2009).

Na norma ISO/IEC 27001:2013, o fator humano aparece associado a um dos três pilares da segurança da informação, pessoas; os outros dois são processos e tecnologias. (Alsahafi et al., 2022)

Segundo Winnefeld et al. (2015), a probabilidade de maior sucesso em ataques informáticos, recorrendo por exemplo à engenharia social, decorre da ignorância das pessoas no que respeita às práticas de segurança, isto porque são estas que interagem diariamente com os sistemas, que têm acesso à informação neles contida, que condicionam o processamento dessa mesma

informação, motivo pelo qual o pilar humano precisa de um tratamento equivalente.

1.3 - Formulação do Problema

O novo modelo de trabalho, implementado na generalidade das empresas e organizações no após Pandemia Covid-19, trouxe consigo uma nova forma de relacionalmente entre a entidade empregadora e o trabalhador.

Este modelo implica que as empresas e organizações estejam hoje mais expostas ao ambiente externo, exposição esta que aumentou a superfície de ataque.

O vasto leque de ferramentas e serviços que satisfazem as necessidades empresariais e organizacionais, e as necessidades pessoais de cada colaborador, esbatem as fronteiras entre os dois ambientes: o corporativo e o pessoal.

A conjunção destes fatores, aliado à iliteracia digital, derivada da falta de formação em conteúdos que versem a pegada digital, a segurança da informação, ou o comportamento no ambiente virtual, têm promovido o aumento bastante significativo de ataques informáticos perpetuados contra as empresas e organizações, demonstrado na diversa literatura produzida diariamente, recorrendo a técnicas de engenharia social, e os colaboradores da Organização em estudo neste trabalho não são imunes a essas técnicas.

1.4 - Objeto de Estudo

Para a realização deste trabalho na Organização em estudo, atendendo à natureza desta, a gestão da Organização impôs como condicionante a anonimização da identidade e dos dados recolhidos.

Cumprindo essa condicionante, a identidade desta será designada por "Organização". A Organização é um de dois ramos, de naturezas distintas, de uma "Entidade".

Assim como algumas palavras serão substituídas por outras representativas do conteúdo, tema ou assunto, dentro de aspas duplas e a ou as "*palavras*" em itálico. No questionário (anexo III) quanto tal não for possível, o conteúdo será substituído por *(opção omitida), (opções omitidas) ou (conteúdo omitido)*

1.4.1 - Caracterização da Organização

A Organização é parte integrante de uma Entidade, com sede comum em Lisboa, e dispõe de autonomia técnico-administrativa e financeira, sendo a sua principal função fornecer apoio técnico-administrativo ao outro ramo de atividade da Entidade.

A Entidade atua a nível global, através de 170 filiais, asseguradas pelo apoio prestado pelos 379 colaboradores internos e de *outsourcing* da Organização, a cerca de 10 milhões potenciais clientes.

As comunicações eletrónicas, de cada uma das filiais com a sede em Lisboa, são estabelecidas através de circuitos de VPN, concentrando em Lisboa

os principais ativos de rede, *backups*, segurança da informação, e facultar um único ponto de comunicação eletrónica com os parceiros de negócio.

Para que esta solução seja possível, nos últimos anos têm sido empregues investimentos, alicerçados nas melhores soluções que o mercado poderia providenciar, distribuídos por 3 vetores:

1. Hardware e serviços, com a aquisição de novos equipamentos de comunicação, o reforço tecnológico em termos de processamento, armazenamento e condições ambientais no *datacenter*, atualização do parque informático de suporte à operação técnico-administrativa, e a reformulação dos contratos de prestação de serviços de comunicação e assistência técnica, um por cada país em que existe uma filial.
2. Formação dos colaboradores, com a reformulação e reforço das ações de formação, preferencialmente *online*, de temáticas relacionadas com a Internet, redes sociais, pegada digital, e identificação de ciberameaças decorrentes de técnicas de engenharia social, perpetuadas por correio eletrónico por exemplo.
3. Por fim, no reforço preventivo na segurança contra ciberameaças, com a ativação de um *SOC* e de um *NOC*, na sede em Lisboa.

1.4.2 – População

A população em estudo circunscreveu-se aos 379 colaboradores da Organização, que desempenhavam funções na sede.

A escolha deste grupo, no universo da população da Entidade, deveu-se essencialmente a dois fatores: o primeiro advinha do tamanho e da dispersão mundial de aproximadamente 3500 colaboradores da Entidade, e o segundo, por se tratar de um grupo de colaboradores, representativo da homogeneidade de género, estratificação etária, de funções, habilitações literárias e da relação laboral/contratual, que *per* si já estavam agrupados no seio da Entidade.

Segundo Pardal & Lopes (2011) uma pequena representação do universo de investigação é o único meio de o conhecer, não da maneira plenamente segura, será pelo menos com razoável segurança, sob pena de tornar o trabalho prático de suporte a esta investigação impraticável.

Admite-se o risco de enviesamento dos resultados na extrapolação destes para o universo da Entidade, motivado, por exemplo, pelo ambiente geopolítico que cada país.

1.5 - Objetivos Específicos

- Identificar e quantificar a exposição ao ambiente virtual e *online*;
- Avaliar as práticas de proteção e autoproteção dos colaboradores no manuseamento da informação, na utilização de dispositivos eletrónicos, em contexto familiar e corporativo;
- Propor medidas de ação que atendam às necessidades identificadas no tratamento dos dados, resultantes do trabalho prático de suporte a este trabalho de investigação

1.6 - Questão de Investigação

Em que medida os colaboradores da Organização têm presente a preservação da sua identidade digital, da segurança da informação e dos equipamentos eletrónicos, e se são ações interiorizadas que se repercutem para além do ambiente corporativo.

A questão será respondida na análise dos dados resultantes do questionário enviado à população, e que será a fonte de dados primária desta investigação

1.7 - Estrutura da Dissertação

Este trabalho de dissertação e investigação está dividido em 5 capítulos:

Capítulo 1: Introdução – que aborda o enquadramento e as temáticas que levaram à escolha e formalização do problema a que se propõe responder. Identifica o objeto em estudo, a questão de investigação e a estrutura da dissertação.

Capítulo 2: Revisão da Literatura – enquadramento da temática em investigação, através da literatura mais tradicional, complementada com literatura produzida diariamente, por se tratar de um tema de grande atualidade.

Capítulo 3: Metodologia e Dados – define os objetivos da investigação, justifica o método de pesquisa utilizado para a componente prática, e uma seção especifica onde se identificam os participantes, o design adotado, e o procedimento desenvolvido.

Capítulo 4: Análise dos dados – onde são apresentados os principais resultados do questionário, em 3 tópicos: caracterização, presença e literacia digital, e segurança da informação.

Capítulo 5: Conclusões, contributos, limitações e investigação futura - com a apresentação das conclusões, contributos, limitações e elementos para investigação futura.

Por fim é apresentada a bibliografia e os anexos.

Capítulo 2 – Revisão da Literatura

A segurança da informação, a cibersegurança e os temas relacionados com a gestão de recursos humanos numa época pós-pandemia, são temas de grande atualidade, tendo sido os principais termos de pesquisa nas consultas, nas revistas especializadas, em artigos científicos (*papers*), legislação, dissertações de mestrado e doutoramento, relatórios de entidades oficiais e na literatura de referência.

O elo comum foi o fator humano, na forma e nos resultados das suas interações com as ferramentas e serviços de âmbito tecnológico, atendendo a que a segurança da informação deixou de ser entendida apenas como um problema da área tecnológica.

Neste capítulo, serão apresentados alguns conceitos empregues neste trabalho, que permitem o enquadramento e contextualização na importância do tema.

2.1 – Informação

A definição de informação, e citando Gaivéo (2008, p.92), "(…) *é entendida como sendo dados tratados e "dotados de relevância e de um objectivo" [Drucker 1993], ou ainda como dados com um significado particular e colocados num contexto específico [Haag et al 1998, Zwass 1998, Alter 1999]*(…)".

A informação é hoje considerada um dos principais ativos das organizações e empresas, que adquiriu um "*valor central*", substituindo-se à produção de bens, do qual "*(…) o sucesso das empresas e organizações está relacionado com a eficiência e a eficácia da utilização da informação no seu dia-a-dia e com a capacidade que estas têm em armazená-la e recuperá-la.*" (Estrela, 2014, p.1), sendo por isso um fator crítico para o sucesso (Zorrinho, 1991).

2.2 – Família de normas ISO/IEC 27000

A família de normas padrão internacional denominada ISO/IEC 27000:2018 foi desenvolvida com o objetivo de ajudar as empresas e organizações a manterem seus ativos de informações protegidos, surgindo da publicação da BS 7799, pela *British Standard Institution* em 1995, através de recomendações, requisitos e orientações, que podem ser adaptados às necessidades de cada organização ou empresa (ISO/IEC, 2018)

A segurança de informação é padronizada por esta família de normas.

2.3 - Segurança da Informação

Na literatura consultada, a referência mais comum que encontramos para definição de segurança de informação, aponta para Beal (2005, p. 71) que a definiu como sendo "*o processo de proteger a informação das ameaças, para garantir a sua integridade, disponibilidade e confidencialidade*". Mais tarde Beal (2012, p.52), citado por Neto & Araújo (2019), considera que a "*autenticidade*" e o "*não-repúdio*" devem ser dois requisitos a atender, ou Coelho et al. (2014) quando citado por Neto & Araújo (2019) considera ainda a "*conformidade*" e o "*controle de acesso*", como elementos essenciais, reflexos da própria evolução tecnológica.

Todavia, a definição preconizada por Beal (2005) ou Sêmola (2014), citados por Neto & Araújo (2019), tem sido a mais amplamente defendida e todos os demais requisitos ou elementos adicionados são atendidos como derivações ou consequências resultantes da aplicação dos 3 pilares que fundamentam a segurança da informação:

- Confidencialidade - Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando limitar seu acesso e uso às pessoas a quem é destinada;
- Integridade – Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais;

- Disponibilidade – Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível quando os utilizadores necessitam dela para qualquer finalidade

In Neto & Araújo (2019), p. 28.

2.4 – Estado da cibersegurança em Portugal: 2022

É comum no primeiro semestre de cada ano a publicação de relatórios, de fontes estatais e de empresas do ramo, focados na análise das ciberameaças.

Não sendo o foco deste trabalho a apresentação exaustiva da análise desses relatórios, situação que *per si* justificava a realização de um trabalho de investigação sobre a literatura publicada, a sua leitura e acompanhamento é importante para enquadramento dos resultados e identificação de possíveis desvios.

Destes, sem desprimor pelos restantes, a 4ª edição do relatório anual publicado pelo Centro Nacional de Cibersegurança (CNCS), "Relatório de Cibersegurança em Portugal – Riscos e Conflitos" (CNCS, 2023), congrega os principais dados relativos às ciberameaças que afetaram os diversos setores de atividade em Portugal no ano de 2022.

Umas das principais conclusões apresentadas, reflete a tendência crescente dos incidentes de cibersegurança e dos cibercrimes, no território nacional. O *ransomware*, a cibersabotagem, o *phishing, smishing e vishing*, a burla *online*, o recurso à engenharia social e comprometimento de contas de acesso, foram, segundo este relatório as principais ciberameaças detetadas (CNCS, 2023, p. 7).

O ano de 2022 foi fértil na temática que envolveu as ameaças à informação ou disrupções provocadas, principalmente no primeiro trimestre, das quais se destacam, não só pela cobertura mediática, mas principalmente pela disrupção de serviços que provocou em quatro setores de atividade: na prestação de serviços de Internet e infraestruturas digitais (Vodafone), na comunicação social (Grupo Impresa), na saúde (Laboratório Germano de Sousa), e na distribuição alimentar (Sonae MC). (CNCS, 2023, p. 8)

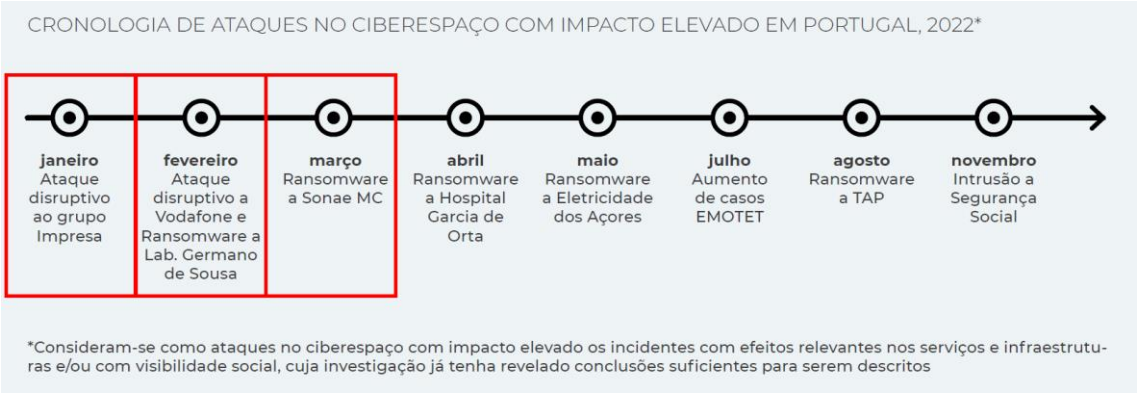


Ilustração 1: Cronologia de ataques no ciberespaço com impacto elevado em Portugal, 2022"
Fonte: CNCS (2023), p. 8.

O primeiro lugar de ameaças reportadas em Portugal, compiladas na 3.ª e na 4.ª edição do "Relatório de Cibersegurança em Portugal – Riscos e Conflitos" (CNCS, 2022; CNCS, 2023) é ocupado pelo *phishing*/*smishing* com 40% em 2001 e depois um ligeiro decréscimo em 2022 para os 37%, seguido das ameaças perpetuadas por engenharia social, e como terceira ameaça o *malware*, com 13% e 11% respetivamente (CNCS, 2022, p.10; CNCS, 2023, p.16). O número de incidentes reportado em 2021 pelo CERT.PT, que tem como missão gerir a resposta a ciberincidentes em território nacional, foram de 1781 e

em 2022 de 2023 incidentes (CNCS, 2022, p.19; CNCS, 2023, p.26), correspondendo a um aumento de 14%.

2.5 - Ameaças à Segurança da Informação

Nas mais diversas definições e interpretações do conceito de ameaça, para Teotônio (2013) "*a ameaça é algo que provoca danos na segurança de informação, prejudicando ações da empresa e a sustentação do negócio, mediante a exploração de uma vulnerabilidade (…) capaz de causar danos a um recursos, em termos de confidencialidade, integridade, e disponibilidade, etc."*, em linha com Sêmola (2014, p. 66) que a define como "*agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, e, consequentemente, causando impactos aos negócios de uma organização*". Agora numa fase pós-pandémica e com uma guerra a decorrer em solo Europeu, conseguimos encontrar sentido para cada palavra escrita por Teotônio (2013) e por Sêmola (2014).

Hoje, como relatado na 4.ª edição do "Relatório de Cibersegurança em Portugal – Riscos e Conflitos" (CNCS, 2023) estamos perante um quadro de ameaças no ciberespaço, de crescente 'profissionalização' do cibercrime, a incerteza resultante da guerra na Ucrânia, o comprometimento de sistemas por ransomware, o *DDoS* (CNCS, 2023, p.12-13), que segue a mesma tendência reportada na 18.ª edição do "*The Global Risks Report 2023*" (WEF, 2023), como o aumento da atividade maliciosa no ciberespaço, que é mais agressiva e com

ataques mais sofisticadas, tendo como vantagem uma maior superfície de ataque (WEF, 2023, p. 42).

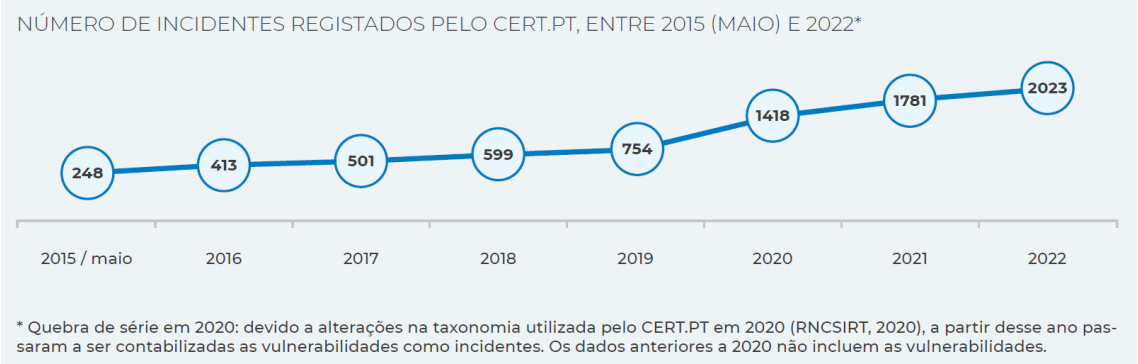


Ilustração 2: : Número de Incidentes registados pelo CERT.PT, entre 2015 (maio) e 2022
Fonte: CNCS (2023), p. 27

A nível global, as ameaças à informação e a generalização do cibercrime, são assinaladas como o oitavo risco global mais impactante, numa projeção a 2 e a 10 anos, assim como passou a figurar no top 10 dos riscos de maior gravidade (WEF, 2023, p. 6). Os primeiros riscos estão relacionados com fatores sociais e fatores ambientais.

2.6 - Engenharia Social

Os ataques de engenharia social visam essencialmente o elemento humano, que pode ser o objetivo ou o meio para atingir uma terceira parte. Para o sucesso dessa ação, a primeira fase "*passa na maioria das vezes pelo reconhecimento do alvo, ou seja, pela recolha de informação, o que vai possibilitar, posteriormente ao adversário definir cenários de atuação, através da modelação de métodos de ataques*" (Correia & Sousa, 2010), citados por Martins

el al (2016, p. 147), para que na fase seguinte, como defende Mitnick & Simon (2002), esta possa assumir diversas formas.

Através do uso da influência e da persuasão, irá enganar ou convencer o elemento humano a algo, para obter informações, com ou sem o uso da tecnologia, pela exploração de falhas humanas (Mitnick & Simon, 2002).

Em Portugal, de acordo com a 3.ª e 4.ª edição do "Relatório de Cibersegurança em Portugal – Riscos e Conflitos" (CNCS, 2022; CNCS, 2023), a engenharia social ocupa a segunda posição de ciberameaças com 14% em ambos os relatórios (CNCS, 2022, p.10; CNCS, 2023, p.16), que pode indiciar alguma estabilização, contudo o número reportado de incidentes para este tipo de ameaça foram de 246 em 2021 enquanto em 2022 foram de 285, ou seja, mais 39 incidentes reportados (CNCS, 2023, p. 31).

2.7 - Fator Humano

O fator humano é um conceito muito amplo e muito vasto na gestão de segurança. Segundo a *Health and Safety Executive* (HSE, 2005, p.11), os fatores humanos *"referem-se a fatores ambientais, organizativos e fatores profissionais e caraterísticas humanas e individuais, que influenciam o comportamento no local de trabalho de uma forma que pode afetar a saúde e segurança*".

Para Reason (1990), é no trabalhador que reside a possibilidade de falhar, mas não é a principal causa, ou seja, é o trabalhador que tem a capacidade de determinar o que é certo e o que é errado, porém, a forma de como os sistemas são projetados e criados podem levar a esse entendimento. Ideia também defendida Silva et al. (2003, p. 70), porque as pessoas "(…) *interagem*

diariamente com os sistemas, que têm acesso à informação neles contida, que condicionam o processamento dessa mesma informação, (…) que a gerem".

Segundo a Comissão Nacional de Proteção de Dados (CNPD), a falha humana representa 22% dos incidentes reportados (CNCS, 2023, p. 47). O *ransomware* é referenciado como a origem mais frequente reportado como incidente de violação de dados com 30% dos casos notificados, e as falhas aplicacionais representam os restantes 13%.

Talvez não seja alheia a iliteracia digital da população em geral, aliada à utilização massiva de dispositivos móveis, conjugada com a falta de recursos humanos especializados na segurança da informação, ou em cibersegurança, nas empresas e organizações.

Se atendermos que o grosso do tecido empresarial de Portugal é composto por 99.9% de PME (Pordata, 2023b), dos quais 96% corresponde a microempresas (Pordata, 2023a), que segundo o Instituto Nacional de Estatística (INE), são aquelas que empregam menos de 10 pessoas e um volume que não excede os 2 milhões de euros anuais (INE, 2023) podemos assumir que a segurança informática não será a principal preocupação destes empresários, e no seu encalce a utilização de sistema informáticos obsoletos, ferramentas de segurança limitadas, ou uso inadequado de dispositivos de rede e de armazenamento de dados.

2.8 – Crimes informáticos

As suas definições e aplicabilidade em território nacional, estão definidos na Lei n.º 109/2009, de 15 de setembro, designada como Lei do Cibercrime, transposta para a Legislação Portuguesa pela Decisão Quadro n.º 2005/222/JAI,

do Conselho da Europa, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adota o direito interno à Convenção sobre Cibercrime do Conselho da Europa, uniformizando um quadro legal a nível europeu.

Capítulo 3 – Metodologia e Dados

Neste capítulo serão apresentados os objetivos da investigação, o paradigma e metodologia da pesquisa, bem como as opções de metodologia adotadas, nas diversas etapas deste estudo.

Descreve o enquadramento da população, os procedimentos, métodos e técnicas estatísticas para a análise dos dados recolhidos.

3.1 - Objetivos da Investigação

Esta investigação pretende quantificar conhecimentos e perceções empíricas que existem no seio da Organização, capaz de gerar *insights* a serem utilizados pelos s*takeholders* da Organização, na adequação, melhoria ou reorganização de processos, numa visão global na forma de como o colaborador interage diariamente com a informação.

Para o entendimento desta visão global, era importante apurar se existe uma consciencialização intrínseca da importância da informação e se essa consciencialização decorria de normativos internos ou da autoconscientização dos colaboradores.

A análise dos dados, gerados por esta investigação, procurará identificar e propor recomendações que melhorem ou mitiguem aspetos que necessitem de uma nova abordagem, como por exemplo a adequação ou a criação de novos módulos de formação interna.

3.2 – Questionário

Depois de várias ponderações sobre qual a metodologia que melhor se adaptava aos objetivos para a recolha e análise dos dados, e de entre inquérito por questionário e o inquérito por entrevista, o inquérito por questionário apresentava-se como o mais adequado, atendendo ao número algo elevado de colaboradores e "*pela possibilidade de quantificar os dados obtidos e se proceder a inferências e a generalizações.*" (Sá et al., 2021, p. 14-15).

Quanto à natureza da pesquisa, "*a opção por uma metodologia quantitativa ou qualitativa tem de estar de acordo tanto com os objetivos da pesquisa como com os atributos dos objetos em estudo*" (Augusto, 2014, p. 2), assim como ressalta Knechtel (2014), citada por Rodrigues et al. (2021, p. 165, "*assevera que, tanto a pesquisa qualitativa quanto a quantitativa têm como foco principal o ponto de vista do indivíduo.*"

Atendendo aos objetivos deste trabalho (*ver 1.5 – Objetivos específicos*), em que "*os dados coletados estão na forma de valores numéricos e fazem sentido numa determinada escala*" (Sá et al., 2021, p. 91), e por constituir um processo sistemático de colheita de dados observáveis e quantificáveis, baseados na observação de fatos objetivos, fenómenos e acontecimentos que existem independentemente do investigador (Freixo, 2011), a quantitativa

apresentou-se como sendo aquela que melhor atingia os objetivos deste trabalho de investigação, ainda porque segundo Rodrigues et al. (2021, p. 166) citando Knechtel (2014):

> "*a pesquisa quantitativa tem como objetivo medir opiniões e informações fazendo uso dos recursos da estatística e seus elementos de demonstração de percentagem (…).Tais dados serão apresentados em forma de tabelas, gráficos ou textos*"
>
> In Rodrigues et al. (2021), p. 166.

O recurso ao questionário permite não só obter "*dados comparáveis, generalizáveis e passíveis (quando desejável) de análises quantitativas*", mas também por se destacar "*como uma das técnicas de investigação (...) apropriada para estudos de grande escala, já que pode incidir sobre atitudes, sentimentos, valores, opiniões ou informação factual*" (Coutinho, 2011; Dias, 1994; Gonçalves, 2004) citados por Sá et al. (2021, p. 17), e generalizar os resultados da amostra para a população alvo (Malhotra, 2004; cit. in Gouveia, 2012, p. 57) na procura de estabelecer tendências e regularidades da informação recolhida, assumindo assim a objetividade como a sua principal premissa (Pardal & Lopes, 2011; Coutinho, 2013) citados por Correia (2016, p. 22).

O questionário é um instrumento de medida que traduz os objetivos do estudo com variáveis mensuráveis e ajuda a organizar, normalizar e controlar os dados para que as informações possam ser escolhidas de uma maneira rigorosa (Fortin, 1999, p. 249).

Os tipos de medidas de um questionário podem ser categorizados em objetivos e subjetivos. As medidas objetivas estão relacionadas com fatos, características dos indivíduos, com os seus conhecimentos e os seus comportamentos. As medidas subjetivas referem-se a atitudes, isto é, ao que as pessoas pensam, sentem, aos julgamentos que fazem e compreendem medidas de opinião, se satisfação, de perceção, de valores e de intensões de comportamentos (Freixo, 2011).

Quanto à forma, as questões podem ser perguntas fechadas, em que as pessoas escolhem as suas respostas entre duas ou mais opções, e perguntas abertas às quais as pessoas respondem usando o seu próprio vocabulário fornecendo pormenores, comentários, permitindo assim investigações mais precisas e profundas, embora apresentem maiores dificuldades no tratamento estatístico (Freixo, 2011).

3.2.1 - Design

> *"Não acredito que haja um único design para a metodologia de uma investigação … (uma) boa metodologia para um estudo, tal como um bom design para um barco, deve ajudá-lo a atingir o destino de modo seguro e eficiente."*
>
> In Maxwell (1996), p. 26-27.

Para a realização do trabalho prático, optou-se pela pesquisa quantitativa, sob a forma de questionário.

Atendendo aos objetivos propostos, foram desenhadas 47 questões que respondessem e que traduzissem em números as diferentes perceções existentes na Organização, elaboradas da revisão literária sobre o tema e de estudos semelhantes e que resultaram das alterações ou sugestões identificadas na fase de pré-teste, que tive como finalidade assegurar que os objetivos da investigação, que a estrutura era a adequada e que as questões eram claras.

O questionário foi subdividido em 5 grupos de questões, cada um deles com uma breve descrição do assunto a abordar:

1. "I – Presença e literacia digital", grupo de 5 questões que procuravam enquadrar de forma genérica a pegada digital do respondente;
2. "II – Segurança da informação", composto por 24 questões que procuravam aferir a forma e comportamentos adotados na utilização de equipamentos eletrónicos ou no manuseio da "informação", perceção da "segurança" ou "confiança" em diferentes ambientes;
3. "III – Caracterização", com 11 questões que serviam para caracterizar o respondente;
4. IV – "*Informática*", este grupo de 6 questões era respondido unicamente por aqueles que haviam indicado no grupo anterior que desempenham funções na "*Informática*" e pretendia caracterizar de forma mais especifica o tipo de função desempenhada, formação especifica, ou tempo na função;

5. “V – Observações”, “grupo” composto por uma única questão, que ao contrário das anteriores que eram de resposta obrigatória, esta era de resposta em aberto e não obrigatória e a sua inclusão deveu-se a uma condicionante da ferramenta utilizada e derivou da necessidade demonstrada no estágio anterior, para a existência de um “campo” que pudesse ser utilizado para livre escrita do respondente, sendo por isso a última a ser apresentada.

A resposta a uma questão condicionava a apresentação da questão seguinte ou grupo de questões, desta forma o número máximo de questões apresentadas seriam de até 31, há exceção dos que haveriam de responder que desempenham funções na “*Informática*” e para esses poderia ir até 37 questões, das 47 possíveis. Convém, contudo, ressalvar que a questão do último grupo não era uma verdadeira questão, embora seja contabilizada para o número máximo de questões que poderiam ser apresentadas.

Todo o trabalho de estruturação do questionário, acompanhamento, recolha e pré-análise foi desenvolvido na *web application* “Microsoft Forms” © [*https://forms.microsoft.com*], disponibilizada pela plataforma de produtividade “Microsoft Office 365” ©, entretanto renomeada para “Microsoft 365” © [*https://www.microsoft.com/microsoft-365*], da empresa Microsoft Inc.© [*https://www.microsoft.com*].

A escolha desta *web application* aconteceu naturalmente, pelo fato de estar disponível na plataforma de produtividade e colaboração em uso na Organização, atendendo à condicionante imposta pela gestão da Organização de restinguir o acesso do questionário e dados daí resultantes unicamente ao

universo da Entidade, anónimos e restringidos a uma resposta por colaborador, não ter custos acessórios de licenciamento ou utilização, ser multiplataforma, com resultados em tempo real, pré-análise e exportação dos dados.

3.2.2 - Procedimentos

A escolhas das questões a incluir no questionário, resultaram da vasta literatura publicada sobre a temática. Procurou-se gerar questões que atendessem às particularidades da população em estudo e objetivos propostos, tendo em conta a realidade da Organização, mas que os resultados obtidos pudessem ser confrontados com dados publicados, e desse modo aferir para responder à questão em investigação (*ver 1.7 – Questão de Investigação*).

A exigência de precisão e rigor obriga a que seja necessário testar um questionário antes da sua aplicação. Para nos assegurarmos da qualidade das questões, da razoabilidade da sua ordenação e saber se as respostas correspondem à informação pretendida, torna-se necessário aplicar o questionário a uma amostra reduzida (Pardal & Lopes, 2011), que foi verificado noutra Entidade com particulares semelhanças, que resultou em algumas alterações, até ao seu formato final.

A nível interno, na Organização, foi criado na *Active Directory* (AD) um grupo de segurança, com a finalidade de segregar os colaboradores da Organização daqueles que compõem o universo da Entidade (*ver 1.5.1 - Caracterização da Organização*), a que se associou uma lista de distribuição, com um endereço de correio eletrónico criado e que atendia exclusivamente a este trabalho. Esta metodologia permitia atender às condicionantes impostas

pela Organização (*ver 1.5 - Objeto de Estudo*) e aos requisitos (*ver 3.5.2 – Design*).

Na semana anterior ao envio, o elemento da Direção da Organização que acompanhava a realização deste trabalho e parte interessada nos resultados, informou os restantes colegas, diretores departamentais, sobre a proximidade do envio do questionário para as caixas de correio eletrónico dos colaboradores, apelando à participação de todos.

Na data estipulada, foi enviada uma mensagem de correio eletrónico a todos os colaboradores inscritos na lista de distribuição, com uma explicação dos objetivos, identificação e forma de contato com o investigador deste trabalho, bem como o *link* eletrónico de acesso ao questionário, que ficou disponível por 12 dias.

No dia anterior ao término, foi enviada uma nova mensagem de correio eletrónico a todos, reforçando o pedido de participação e agradecendo aos que eventualmente já o haviam preenchido e finalizado

Capítulo 4 – Análise dos Dados

Os dados que fundamentam este capítulo, resultam das respostas obtidas do questionário enviado por correio eletrónico aos 379 colaboradores da Organização, a população em estudo. Esteve disponível para participação entre o dia 22 de setembro de 2022 e o dia 4 de outubro de 2022.

4.1 - Procedimento para a recolha dos resultados

A recolha e pré-análise dos resultados foram realizadas através das funcionalidades nativas da *web application* de suporte à componente prática deste trabalho de investigação. (*ver 3.5.2 – Design*).

As submissões e resultados puderam ser acompanhados em tempo real, e embora houvesse entusiasmo para a participação, os níveis estavam abaixo do expectável, motivo pelo qual, dois dias antes do término, foi enviada uma nova mensagem de correio eletrónico, agradecendo aos que já haviam preenchido e reforçando o pedido de participação.

4.2 – Análise dos principais resultados

Foram concluídos 68 questionários, que se traduziu num nível de participação de 18%, dos quais 55,58% do sexo feminino e os restantes 44,12% do sexo masculino. Em média cada colaborador necessitou de 14 minutos para o preenchimento. O grupo etário com maior percentagem de respostas foi dos colaboradores com idades compreendidas entre os 45 e os 54 anos, com 44,12%, logo seguido do grupo com idades compreendidas entre os 55 e os 64 anos, com 19,12%.

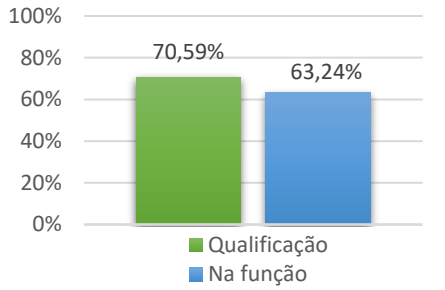


Gráfico 1 - Qualificação QNQ 6 + 7 vs Na função

Os níveis de ensino 6 e 7, Bacharelato e Licenciatura do 1.º Ciclo de Bolonha com 30,88%, e Licenciatura pré-Bolonha e Mestrado com 39,71%, respetivamente, somados correspondem a 70,59% do total de respostas obtidas, foram as qualificações académicas mais assinaladas. Seria expectável observar o mesmo valor quando questionados sobre a caracterização da carreira ou função exercida, contudo esta hipótese não se revelou ser verdadeira.

Depois de analisados os dados, na procura da diferença entre 70,59% e os 63.24% que assinalaram executar funções correspondentes com as de técnico superior, foi possível identificar colaboradores a executar funções em categoria profissional inferior à sua qualificação académica. A justificação para esta razão não foi abordada no questionário.

Um fator importante a assinalar são os 79,41% respeitantes à modalidade do vínculo de trabalho ou relação com a Organização, que indica que aproximadamente 4/5 dos colaboradores da Organização têm um vínculo de trabalho

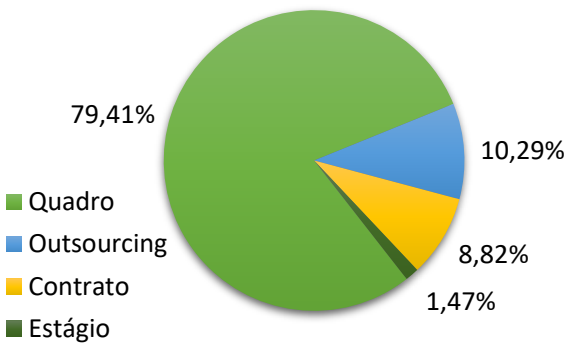


Gráfico 2 - Relação jurídica com a Organização

estável.

Na abordagem à temática sobre a presença no ciberespaço e da literacia digital, 97,06% respondeu que contactou diariamente com plataformas de serviços *online* e redes sociais.

Para estes foi solicitado que de entre um grupo de empresas, para as quais se associaram as plataformas e serviços que disponibilizam, e de entre um grupo de setores de atividades, que assinalassem a principal forma de identificação utilizada para *login*.

No global, a utilização do endereço de correio eletrónico pessoal ou do número de telemóvel pessoal são as principais formas de identificação. A utilização do endereço eletrónico pessoal corporativo ou do número de telemóvel foram assinaladas de forma muito residual, em empresas ou setores de atividade com alguma relação laboral.

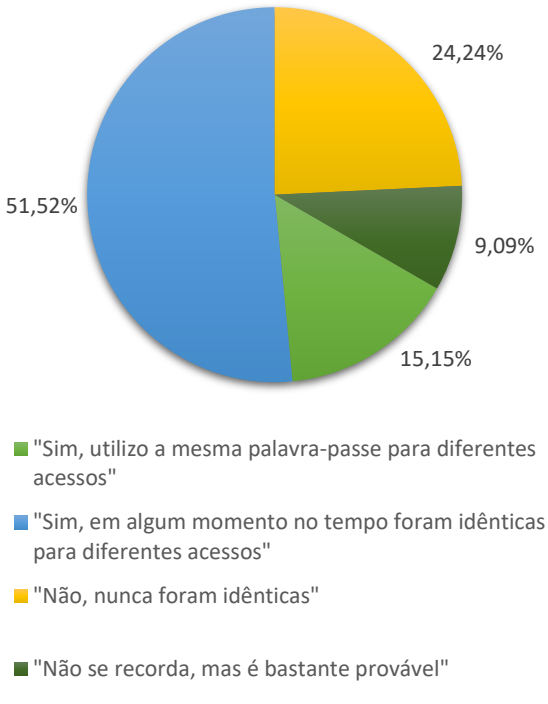


Gráfico 3 - Utilização da palavra-passe

Na maioria das plataformas o *login* efetua-se por um par de chave, pelo que faria sentido perceber da importância dada à utilização da palavra-passe, e desta questão, 51,52% que responderam "*Sim, em algum momento no tempo foram idênticas para diferentes acessos*", associados aos 15,15% que

indicaram utilizar a mesma palavra-passe, e aos 9,09% que não se recorda, mas que é bastante provável, obtém-se um panorama preocupante a necessitar de reflexão.

Principalmente nos últimos anos, a maioria destas plataformas têm vindo a implementar mecanismos adicionais de segurança, como por exemplo a Autenticação de dois fatores (2FA) ou a Autenticação multifator (MFA), para acesso aos seus serviços.

Não foi colocada nenhuma questão se este mecanismo era ou não conhecido, pelo fato da Organização ter identificado a necessidade de implementar este mecanismo de segurança, de forma faseada, a todos os colaboradores numa fase inicial da Pandemia Covid-19, contudo era interessante entender se este mecanismo de segurança, que está disponível nas principais plataformas de correio eletrónico de uso pessoal, era utilizado:

- 42,42% respondeu que utilizava;
- 46,97% respondeu que não;
- 10,61% indicou que não sabia responder.

Numa primeira análise, não deixa de ser preocupante o fato de 57,58%, ou seja, pouco mais de metade ter respondido "*Não*" ou "*Não sabiam responder*". De salientar que a utilização do 2FA ou MFA na Organização é uma imposição, contudo, atendendo à natureza da Organização, a possibilidade para utilização, nestas plataformas deste tipo de mecanismo, deveria ser entendida como uma camada extra à segurança e desse modo aplicar igual peso à segurança da informação do seu correio eletrónico pessoal como aquele que é aplicado no correio eletrónico pessoal corporativo.

Ainda sobre este tema, foi solicitado uma autoavaliação aos conhecimentos que detinham na área de TIC. Eram apresentados 5 perfis, devendo selecionar aquele em que melhor se avaliava:

1. utilizador com fracos conhecimentos informáticos, motivo que condiciona o acesso e compreensão do e ao meio digital, tornando-o dependente da ajuda de terceiros;
2. utilizador com alguns conhecimentos que lhe permitia uma autonomia muito básica, mas ainda assim não o capacitava para a resolução de novas situações;
3. conhecimentos na ótica do utilizador, com formações, que lhe permite ser autónomo na utilização da Internet e das redes sociais, mas ainda havia situações sobre as quais necessitava da ajuda de terceiros;
4. utilizador uma autonomia acima da média, facilidade na utilização do meio digital e das ferramentas a ele associado;
5. utilizador com conhecimentos especializados.

Os 70.59% da soma do perfil 3 e 4 era expetável ou muito aproximado, tendo em conta que 70,59% do questionário foi respondido por colaboradores com formação académica de nível universitário, não causando por isso surpresa.

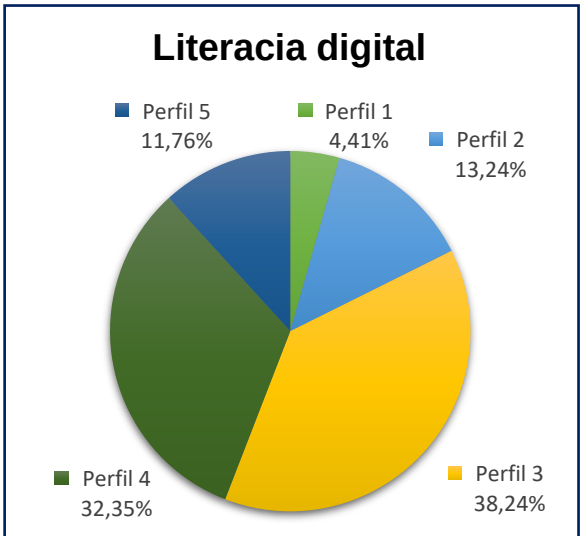


Gráfico 4 - Autoavaliação: Literacia digital

Atendendo à nova realidade gerada com o teletrabalho ou trabalho híbrido, tornava-se evidente e natural, atendendo inclusive à época em que este trabalho de investigação foi realizado, que indicasse, de entre 3 possibilidades de escolha, se o considerava uma ameaça à informação:

- 61,76% indicou que “não”;
- 14,71% indicou que “sim”;
- 23,53% não tinha opinião formada.

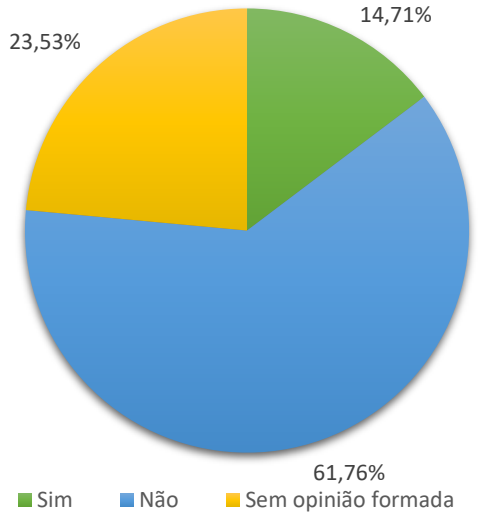


Gráfico 5 -Teletrabalho ou trabalho híbrido: uma ameaça?

Para que este modelo de trabalho consiga atingir a sua plenitude, é necessário atender à mobilidade e providenciar acesso até ao ambiente corporativo.

Desta forma procurou-se saber se o acesso aos dados na Organização, se efetuava por recurso a equipamentos eletrónicos de uso privado, e aqui entenda-se que o proprietário do equipamento era o colaborador, ou se a Organização os havia facultado.

Das respostas obtidas, 64,71% indicou que utilizava equipamento eletrónico de uso pessoal em contexto de teletrabalho. Deste grupo de respostas, o telemóvel (*smartphone*) de uso pessoal foi identificado em mais de metade das respostas obtidas, 58.52%

Quando questionados se a Organização havia facultado equipamento eletrónico para utilização em contexto de teletrabalho, 75% respondeu que sim, ou seja, a ¾ dos colaboradores a Organização havia facultado equipamento, tendo sido o computador portátil (*laptop*), com 87,27%, o equipamento mais assinalado.

A explicação para que destas duas questões aparentarem ser conflituantes, advém de a Entidade disponibilizar o acesso em equipamento pessoal, por exemplo, ao correio eletrónio corporativo ou trabalho colaborativo através da plataforma Microsoft Teams © [*https://www.microsoft.com/microsoft-teams*] ou da extensão telefónica interna, permitindo que o colaborador recriasse um ambiente típico de escritório, composto por um equipamento de computação e outro de comunicação (voz).

A segurança e a forma para a utilização destes equipamentos, para acesso ao ambiente corporativo, foi-se desenvolvendo e alargando, à medida que se ia tornando evidente com os constrangimentos provocados pela Pandemia Covid-19 iriam perdurar por mais tempo do que aquele que inicialmente se antevia. Esse esforço é demonstrado quando 89.71% dos colaboradores indicou a utilização de mecanismo de duplo fator de autenticação no acesso ao correio eletrónico corporativo ou no acesso à plataforma colaborativa.

Aquando do desenho da infraestrutura e definição dos processos, entendeu-se que os equipamentos que se iriam conectar à rede corporativa não deveriam conter dados ou aplicativos associados ao negócio da Organização, que em caso de furto não comprometia os dados ou a sua utilização. Deveriam

comportar-se como veículos para estabelecimento da comunicação até ao perímetro externo de segurança, e só depois de passar esta primeira barreira de segurança, seriam redirecionadas para outros equipamentos internos com permissões de acesso aos dados.

Desta forma era possível facultar o acesso em equipamentos não pertencentes à Organização, que se revelou de crucial importância, principalmente nas fases iniciais da Pandemia Covid-19, ao possibilitar o teletrabalho a um maior número de colaboradores. A utilização de VPN foi o mecanismo, assinalado em 80,88% das respostas, para o estabelecimento da ligação remota ao ambiente de trabalho corporativo. Este valor não atingiu os 100% ou algo mais próximo, pelo fato de se ter identificado colaboradores em que a necessidade de acesso a dados da Organização poderia ser atendida unicamente pela utilização do telemóvel (*smartphone*).

O estender do perímetro de segurança da Organização até ao ambiente familiar implicaria, numa outra situação e numa normal abordagem, o aumento dos recursos humanos especializados em TIC, capazes de atender aos pedidos e à necessidade imediata de transmitir regras básicas de segurança.

Apesar das dificuldades sentidas, é reconhecido por 61,82% dos colaboradores que houve transmissão destas regras. Destes, 1 em cada 10 necessitou de recorrer à ajuda de elementos externos à Organização para a resolução de algum problema ou situação inerente à utilização do estabelecimento de acesso remoto, por VPN, à Organização.

Nas questões que abordavam o comportamento humano em situações como por exemplo, o bloqueio do ambiente de trabalho, a salvaguarda de

documentos impressos fora de olhares curiosos, ou a aplicação do conceito de “secretária limpa”, a escolha da opção “sempre” ou “sim” é predominante, com valores superiores a 70%.

“Não” ou “nunca” são as escolhas assinaladas, com valores nunca inferiores 80%, quando se pretendeu saber, por exemplo, se já haviam enviado documentação de trabalho para o seu correio eletrónico pessoal, ou dado a conhecer a sua palavra-passe a algum(a) colega, ou ainda se a guardavam em algum equipamento de uso pessoal.

Até agora a análise das questões, que haviam sido colocadas, tiveram como enfoque o ambiente corporativo e na proteção que este fornece, faltando compreender o comportamento fora deste ambiente, nomeadamente sobre o comportamento que assumem para a salvaguarda física do computador portátil, seja o pessoal ou da Organização, numa deslocação: 70,59% indicou que o transportam sempre consigo, nunca o perdendo de vista.

Também é interessante a resposta obtida de 79,41% dos colaboradores, quando assinalam que em ambientes públicos ou em reuniões, têm o cuidado de proteger o conteúdo da visão ou leitura de terceiros, independentemente do tipo de equipamento eletrónico em uso.

Ainda na senda do entendimento do comportamento adotado, a forma de acesso à informação corporativa esta intrinsecamente ligada à forma de como é estabelecida a comunicação remota.

Se no ambiente corporativo o acesso aos dados pela utilização da rede cabeada ou por *Wi-fi* retira muita da carga de alerta e vigilância, procurou-se saber qual seria o comportamento fora desse ambiente protegido, recorrendo a um acesso *Wi-fi* aberto, como por exemplo num espaço comercial: 55,88% assinalou que utilizaria, dos quais 13,24% desses utilizaria mesmo tendo dados móveis, contra os 44,12% que indicou "não".

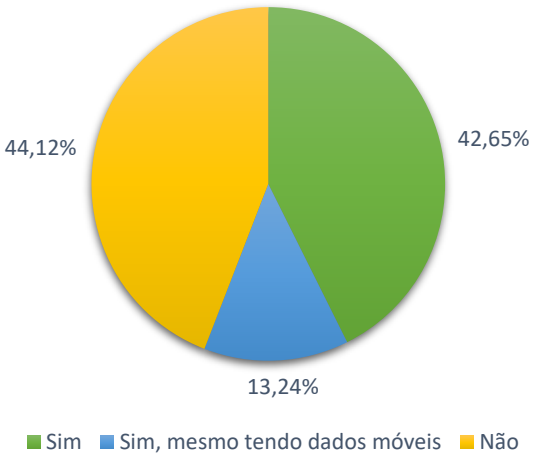


Gráfico 6 – Utilização de *Wi-fi* aberta em estabelecimento comercial ou similar

Quando questionados se a consideravam seguro o acesso à Internet por uma rede *Wi-fi* aberta (sem utilização de palavra-passe), 70,59% considerou que "não", contra 7,35% que entende que são seguras e os 22,06% que não tem opinião formada. Numa análise mais pormenorizada a estes dados, procurou-se entender se para o universo dos que respondem "sim" ou que "não tinham opinião formada", que totaliza 29.41% das respostas, a formação académica seria um fator de influência para este resultado, e foi com alguma surpresa que 55% desse universo de colaboradores, ou seja, mais de metade, têm formação académica superior.

Ainda na abordagem à utilização de redes *Wi-fi*, foi colocada uma questão que procurava entender se o comportamento se alterava quando o acesso dependia da digitação de uma palavra-passe, que poderia estar colada em local

visível, ser fornecida a pedido ou por pré-registo numa plataforma, para a qual 22,06% indicou que não tinha opinião formada, em linha quando questionados se consideravam segura a sua utilização sem palavra-passe.

E efetivamente há uma mudança na perceção provocada pela utilização de uma palavra-passe, nas condições indicadas, em que 23.53% daqueles que consideram que não era segura a utilização de uma rede *Wi-fi* aberta, mudaram de opinião com a adição deste fator.

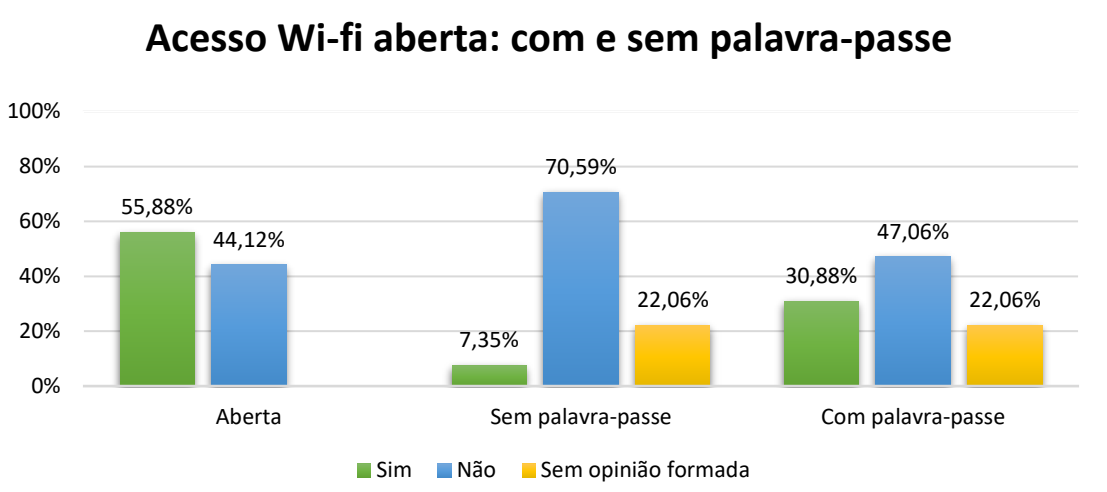


Gráfico 7 - Rede *Wi-fi* aberta: fator palavra-passe

A Política de Utilização Aceitável (PUA) é um documento comum em muitas organizações e empresas, que regulamenta através de uma política a forma e uso adequados dos equipamentos e dos sistemas, revelou ser desconhecido de 73.53% dos colaboradores.

Na última década temos assistido ao incremento de campanhas maliciosas e fraudulentas, recorrendo, por exemplo, à engenharia social ou focadas nos processos e protocolos utilizados para o acesso remoto que permitem o teletrabalho ou trabalho híbrido.

Este fato é patente quando 60,29% respondeu que já havia sido alvo de campanhas de engenharia social, envolvendo *phishing*, *smishing* ou *vishinhg*.

Não deixa de ser curioso e ao mesmo tempo preocupante, que obriga a uma reflexão mais aprofundada, quando 25% assinalou que "não" e 14, 71% assinalou que não sabia responder.

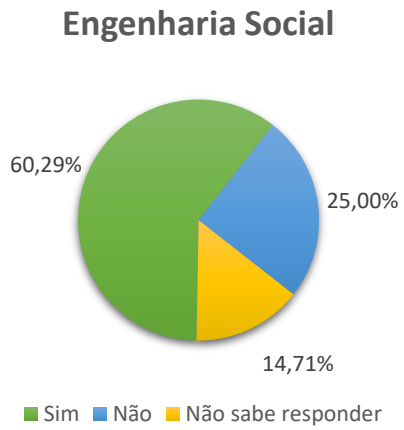


Gráfico 8 - Alvo de engenharia social?

Se até agora a maioria das questões procuraram quantificar comportamentos e fatores dos colaboradores fora da esfera do ambiente corporativo, o desenvolvimento seguinte resulta da tradução da perceção pessoal no ambiente corporativo, como por exemplo, quando questionados se consideravam segura a utilização dos seus dados pessoais na rede corporativa, em que 51,47% respondeu que "sim" e os restantes indicaram que "não" ou "sem opinião formada".

Gráfico 9 - Uso de dados pessoais na rede corporativa

Para a compreensão destes resultados, haveriam de contribuir os resultados conjugados da perceção da segurança informática da rede corporativa com os "resultados" dessa perceção. De certo modo, as perceções seguem par a par, embora com tendência ligeiramente inferior nos "resultados",

o que poderá indicar que nem todo o potencial percecionado na segurança da informação na rede corporativa esteja a ser explorado. No entanto é de salientar os 16 pontos percentuais que separam no parâmetro da necessidade de melhorias, a perceção dos mecanismos de cibersegurança com os resultados percecionados desses mecanismos, podendo querer evidenciar que se está a conseguir tirar bom proveito de todo o potencial instalado.

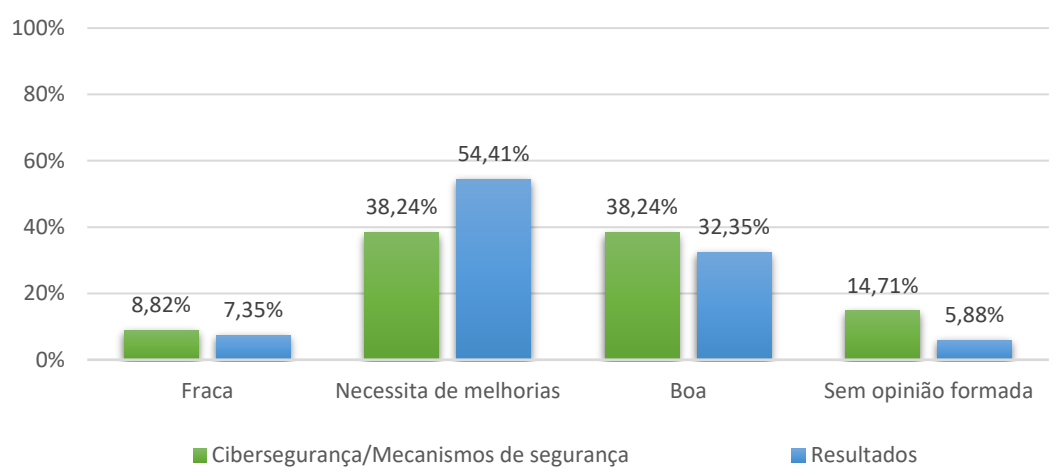


Gráfico 10 - Perceção da segurança informática vs perceção dos resultados

Ainda dentro deste âmbito, quando solicitada a opinião se a Organização dispunha dos meios técnicos e humanos de proteção e segurança contra ciberataques:

- 38,24% considera que “sim”
- 26,47% entende “não”
- 35.29% não tem opinião formada

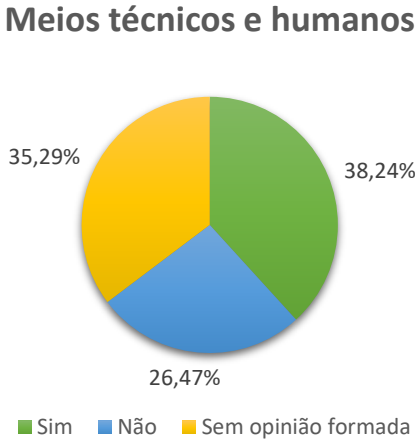


Gráfico 11 - Perceção dos meios técnicos e humanos

Por fim, foi apresentado um grupo de questões que abordavam o tema da formação.

Quando questionados se haviam participado em alguma formação que abordasse pelo menos um dos temas ou que o tema tivesse sido abordado numa outra temática, metade respondeu que sim, e deste destacam-se os resultados para as formações em Segurança da Informação e em Cibersegurança, que somadas correspondem a 55,56% de toda a formação ministrada. De salientar

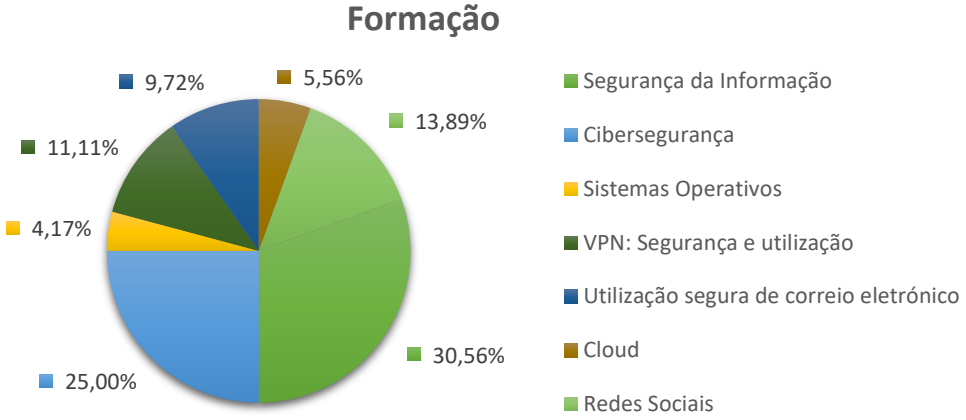


Gráfico 12 - Distribuição das formações por temas

ainda que 53,66% assinalou que a Organização havia sido a responsável, direta ou por subsidiação, por essa formação.

Chama particular atenção, o fato de 50% ter respondido que nos últimos 5 anos não ter participado em nenhuma formação que abordasse as temáticas indicadas, que em parte se consegue justificar com as condicionantes impostas pela Pandemia Covid-19.

Seria de supor que a maioria, senão mesmo a maioria destes colaboradores, não tivessem formação superior, o que de certo modo justificaria a necessidade

de uma aposta maior neste grupo, contudo os dados revelaram que o grupo dos colaboradores com formação superior é o grupo dominante com 64,71%.

Capítulo 5 - Conclusões, contributos, limitações e investigação futura

O fator humano continua a ser, como sempre foi, um desafio na gestão de riscos e prevenção de acidentes e incidentes.

O rápido crescimento tecnológico recente amplificado por uma mudança socialmente mais profunda, tem compelindo as organizações e empresas a repensar a forma de estar e agir no mercado global, onde o digital é a palavra de ordem.

As ciberameaças continuam a representar em Portugal quase metade das tentativas de burla, apesar de ser uma das principias preocupações da gestão de topo, cada mais sensibilizada para a importância de educar e formar os colaboradores, criando uma cultura em ciber-resiliência.

Os novos regulamentos de conformidade, com medidas cada vez mais severas de governança em TIC, e o levantamento dos riscos associados ao negócio, são três pilares que os gestores procuram cumprir e implementar nas suas empresas e organizações, onde praticamente todo o negócio passou a ser digitalizado.

A Pandemia Covid-19 pós a nu as fragilidades de um processo tecnológico que decorria a diferentes velocidades e que necessitou de um ímpeto

para atender aos confinamentos, que numa fase mais imediata, pelo menos na Organização aqui em estudo, foi atendido com a utilização de equipamentos tecnológicos pessoais.

Se no aspeto tecnológico, de uma forma mais ou menos consciente, o processo de alargar o perímetro seguro de uma rede corporativa até ao seio familiar do colaborador foi-se construindo e adaptando as circunstâncias, no horizonte já se vislumbravam alterações que trariam, como se comprovou, uma nova forma de encarrar o trabalho, que agora se quer mais flexível e móvel.

Contudo, esta nova forma de atender ao trabalho trouxe consigo preocupações para a segurança da informação das empresas e organizações, e que tem obrigado à reformulação da arquitetura de TIC, não só pela imprevisibilidade do local remoto de trabalho, em que cada um representa uma nova possibilidade de ataque e compromisso da infraestrutura corporativa, mas também pela necessidade de consciencializar os colaboradores que estes são também um elemento ativo nessa proteção.

Na Organização em estudo neste trabalho de investigação, todos estes fatores se fizeram e fazem sentir na gestão diária da segurança da informação. Contudo, a não existência de dados que corroborem o conhecimento empírico deste tema na Organização, foi o principal mote que levou à realização deste trabalho.

5.1 - Principais Conclusões da Investigação

Das principais conclusões que se retiram, a primeira de todas e que salta logo à vista, está relacionada com o fraco conhecimento demostrado em temas

relacionados com a cibersegurança e na abordagem comportamental, acesso e uso das ferramentas tecnológicas, principalmente em contexto pessoal ou familiar, ficando demostrada a necessidade de desenvolver atividades e ações internas que melhor expliquem a necessidade de transpor medidas e mecanismo de segurança aplicados no ambiente corporativo, para o ambiente pessoal ou familiar.

Em termos de formação, ficou patente a necessidade de aumentar de forma substancial a quantidade de formandos em temas relacionados com segurança da informação, pegada digital ou engenharia social. Esta será uma das possibilidades a que a Organização poderá recorrer para que estes temas não sejam entendidos como unicamente algo da esfera tecnológica e do ambiente corporativo, mas que têm repercussões na vida diária de cada um dos colaboradores.

Não será alheio para este entendimento o fato, também encontrado da análise dos dados, a necessidade de a Organização melhorar a comunicação interna com os colaboradores e criar canais que permitam a comunicação nos dois sentidos. Esta será, por exemplo, uma forma de envolver os colaboradores, acolhendo a atendendo às sugestões que poderão apresentar e ai sim, estaremos perante ser um esforço conjunto de proteger a informação e os ativos da Organização.

Outro aspeto que necessita de ser atendido é a existência de colaboradores a executarem funções de um nível inferior à sua qualificação académica.

5.2 – Contributos

Um dos primeiros contributos que resulta deste trabalho, prende-se com a necessidade de implementar uma política efetiva de comunicação interna, focada em assegurar que a informação chega ao destinatário, é assimilada e sujeita a critica, e que dessa forma faça parte da memória coletiva da Organização.

Um outro contributo, não menos importante e que se reveste de uma amplitude mais vasta, prende-se com a necessidade generalizada de aumentar o nível de conhecimento quanto ao uso de redes externas, cibersegurança, ou na utilização de equipamento tecnológico em uso pessoal. Esta medida pode, por exemplo, ser promovida com o apoio e a orientação do Centro Nacional de Cibersegurança (CNCS), que já providencia algumas no âmbito das suas campanhas de sensibilização, e que podem ser adaptadas para as especificidades dos colaboradores e natureza da Organização.

O plano de formação deve atender à necessidade de alargar os temas relacionados com a segurança da informação ou a ela conexa, e a um número maior de colaboradores, espelhando e adaptando-se às mutações decorrente da evolução tecnológica ou social.

Estes contributos não se fecham na sua elaboração e aplicação, devem ser objeto de critica constante para que se mantém atuais e com sentido prático na Organização.

5.3 - Limitações da Investigação

O fato da coleta dos dados decorrentes do trabalho prático ter decorrido quando ainda se faziam sentir as medidas decretadas no âmbito da Pandemia Covid-19, poderá apresentar desvios quando comparados com outros trabalhos realizados anteriormente, com um ambiente social e laboral totalmente diferente. Contudo e é um fato, a Pandemia Covid-19 veio acelerar um processo transformativo que já estava a ocorrer, e o os resultados aqui obtidos não poderiam ficar inumes a essa transformação.

Outra limitação que acabou por alongar por mais um ano esta realização, mas de âmbito pessoal, adveio do fato de quando este trabalho estava a ser realizado, pelo menos até à coleta dos dados do questionário, a Organização estava a ser alvo de constantes ciberataques, o que provocou muitas horas de sono acumuladas, e cansado mental e físico, a que se juntou a ansiedade decorrente para as leituras, pesquisas e demais necessidades para a recolha de informação, que teve como consequência ter sofrido um *burnout*, que após aconselhamento médico e familiar, expos e agradeço mais uma vez ao Professor Doutor António Palma dos Reis pela sua compreensão, a necessidade de o adiar.

5.4 - Sugestões para investigação futura

As validações destes dados ganharão uma outra força, se a metodologia aplicada neste trabalho pudesse ser executada noutra Organização da mesma tipologia, e embora o seu conteúdo seja agnóstico, tem como vantagem poder ser transposta para qualquer organização. Será evidente que poderá haver

fatores que poderão enviesar esses resultados, dependendo por exemplo da maturidade e da natureza da organização, no entanto que não deverá ser entendido como um motivo dissuasor para a realização.

Replicar a metodologia aqui utilizada, nesta mesma Organização, numa data adiante no tempo, com por exemplo dentro de 9 anos, e confrontar os dados aí obtidos com estes, na procura de desvios ou alterações significativas que evidenciam por exemplo, que os contributos apresentados foram atendidos e há uma mudança em sentido positivo na Organização.

Bibliografia

Alsahafi, T., Halboob, W. & Almuhtadi, J. (2022). Compliance with Saudi NCA - ECC based on ISO/IEC 27001. *Tehnicki Vjesnik*. [Em linha]. 29 (6). Disponível em: https://hrcak.srce.hr/file/412478. [Acesso em: 17 março 2023].

Anon (2022). Ataques informáticos: a iliteracia digital em Portugal é “muito elevada” e o teletrabalho “expôs ainda mais as vulnerabilidades”. [Em linha]. Disponível em: https://expresso.pt/sociedade/2022-02-11-ataques-informaticos-a-iliteracia-digital-em-portugal-e-muito-elevada-e-o-teletrabalho-expos-ainda-mais-as-vulnerabilidades. [Acesso em: 24 augusto 2022].

Anon (n.d.). *Glossário*. [Em linha]. Centro Nacional de Cibersegurança (CNCS). Disponível em: https://www.cncs.gov.pt/pt/glossario/. [Acesso em: 4 abril 2023a].

Anon (n.d.). *Glossário da Sociedade da Informação*. [Em linha]. APDSI – Associação para a Promoção e Desenvolvimento da Sociedade da Informação. Disponível em: https://apdsi.pt/glossario/. [Acesso em: 3 augusto 2023b].

Anon (n.d.). *O que é a autenticação de dois fatores?* [Em linha]. Microsoft Security (Em linha). Disponível em: https://www.microsoft.com/pt-pt/security/business/security-101/what-is-two-factor-authentication-2fa. [Acesso em: 28 setembro 2023c].

Anon (n.d.). *O que é: Autenticação Multifator*. [Em linha]. Microsoft Security. [Em linha]. Disponível em: https://support.microsoft.com/pt-pt/topic/o-que-%C3%A9-autentica%C3%A7%C3%A3o-multifator-e5e39437-121c-be60-d123-eda06bddf661. [Acesso em: 14 setembro 2023d].

Anon (n.d.). *O que é um Security Operations Center (SOC)*. [Em linha]. IBM. Disponível em: https://www.ibm.com/br-pt/topics/security-operations-center. [Acesso em: 5 maio 2023e].

Anon (n.d.). *O que se considera uma PME (micro, pequena e média empresa)?* [Em linha]. Instituto Nacional de Estatísticas (INE). Disponível em: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_faqs&FAQSfaq_boui=64092016&FAQSmodo=1&xlang=pt. [Acesso em: 7 julho 2023f].

Anon (2023b). *OMS declara que Covid-19 não é mais uma Emergência Global de Saúde*. [Em linha]. 5 Maio 2023. ONU News. Disponível em: https://news.un.org/pt/story/2023/05/1813942. [Acesso em: 3 junho 2023].

Anon (2020). *Organização Mundial da Saúde declara novo coronavírus uma pandemia*. [Em linha]. 11 Março 2020. ONU News. Disponível em: https://news.un.org/pt/story/2020/03/1706881. [Acesso em: 3 junho 2023].

Anon (2023c). *PORDATA - Estatísticas sobre Portugal e Europa (indicador: Micro)*. [Em linha]. 28 Fevereiro 2023. Fundação Francisco Manuel dos Santos. Disponível em: https://www.pordata.pt/portugal/pequenas+e+medias+empresas+em+percentagem+do+total+de+empresas+total+e+por+dimensao-2859-248025. [Acesso em: 7 julho 2023].

Anon (2023d). *PORDATA - Estatísticas sobre Portugal e Europa (Indicador: Total PME)*. [Em linha]. 28 fevereiro 2023. Fundação Francisco Manuel dos Santos. Disponível em: https://www.pordata.pt/portugal/pequenas+e+medias+empresas+em+percenta

gem+do+total+de+empresas+total+e+por+dimensao-2859. [Acesso em: 7 julho 2023].

Anon (2023e). *The Global Risks Report 2023 (18.ª)*. [Em linha]. Disponível em: https://www.weforum.org/reports/global-risks-report-2023. [Acesso em: 22 setembro 2023].

Augusto, A. (2014). Metodologias quantitativas/metodologias qualitativas: mais do que uma questão de preferência. *Forum Sociológico [Online]*. [Em linha]. Série II (24). p.pp. 73–77. Disponível em: http://journals.openedition.org/sociologico/1073; DOI: [Acesso em: 12 setembro 2022].

Barros, M. & Costa, V. (2009). *O fator humano como pilar da Segurança da Informação: uma proposta alternativa*. In: [Em linha]. 1 janeiro 2009. Disponível em: https://www.researchgate.net/publication/325273412_O_fator_humano_como_pilar_da_Seguranca_da_Informacao_uma_proposta_alternativa/link/5b0321c10f7e9be94bdabefc/download. [Acesso em: 3 fevereiro 2022].

Beal, A. (2012). *Gestão estratégica da informação: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações*. Atlas.

Beal, A. (2005). *Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações*. 1ª edição. São Paulo: Atlas.

CNCS (2022). *Relatório Cibersegurança em Portugal - Riscos e Conflitos (3.ª edição)*. [Em linha]. Lisboa. Disponível em: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf. [Acesso em: 29 junho 2023].

CNCS (2023). *Relatório Cibersegurança em Portugal - Riscos e Conflitos (4.ª edição)*. [Em linha]. Disponível em: https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf. [Acesso em: 29 junho 2023].

Correia, J.M. (2016). *Planificar a Aprendizagem: A Construção de uma Aprendizagem Autodirigida na temática Magmatismo, Rochas Magmáticas*. [Em linha]. Universidade do Minho - Instituto de educação. Disponível em: https://repositorium.sdum.uminho.pt/bitstream/1822/43895/1/Jo%C3%A3o%20Miguel%20Correia.pdf. [Acesso em: 17 maio 2022].

Coutinho, C.P. (2011). *Metodologias de Investigação em Ciências Humanas: teoria e prática*. Coimbra: Almedina.

Decisão-Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação. (2005). [Em linha]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222. [Acesso em: 1 augusto 2022].

Dias, I.C.D. (1994). *O inquérito por questionário: problemas teóricos e metodológicos gerais*. [Em linha]. Porto. Disponível em: https://hdl.handle.net/10216/104265. [Acesso em: 8 fevereiro 2022].

Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho. (2013). [Em linha]. Disponível em:

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32013L0040. [Acesso em: 13 abril 2022].

Duarte, A. (2018). Pegada digital: como descobrir e gerir a sua identidade Em linha. *Ekonomista*. [Em linha]. Disponível em: https://www.e-konomista.pt/pegada-digital/. [Acesso em: 4 fevereiro 2022].

Estrela, S.C.L. (2014). *A Gestão da Informação na Tomada de Decisão das PME da Região Centro um estudo exploratório e de multicasos no âmbito da Ciência da Informação*. Tese de doutoramento. [Em linha]. Coimbra: Universidade de Coimbra. Disponível em: http://hdl.handle.net/10316/25956. [Acesso em: 15 fevereiro 2022].

Feleol, A. (2012). *Os três pilares da segurança da informação*. [Em linha]. 23 junho 2012. Disponível em: https://feleol.com.br/2012/06/23/os-tres-pilares-da-seguranca-da-informacao/. [Acesso em: 7 outubro 2022].

Fortin, M.-F. (1999). *O processo de investigação: da concepção à realização*. 5th Ed. Loures: Lusociência.

Freixo, M.J.V. (2011). *Metodologia Científica: Fundamentos, Métodos e Técnicas*. 3.ª. Lisboa: Instituto Piaget.

Gaivéo, J.M. (2008). *As pessoas nos sistemas de gestão da segurança da informação*. Tese de doutoramento. [Em linha]. Lisboa: Universidade Aberta. Disponível em: http://hdl.handle.net/10400.2/1272. [Acesso em: 2 junho 2021].

Gouveia, H.M.M. (2012). *Dissertação de Mestrado: Das Beiras para o Centro*. Tese de mestrado. [Em linha]. Escola Superior de Aveiro. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/6787/1/Hermano%20Gouveia%20protegido.pdf. [Acesso em: 14 maio 2022].

Grassi, P.A., Garcia, M.E. & Fenton, J.L. (2017). *Digital identity guidelines: revision 3*. NIST Special Publication. [Em linha]. Gaithersburg, MD. Disponível em: https://doi.org/10.6028/NIST.SP.800-63-3. [Acesso em: 22 julho 2022].

HSE (2005). *Portuguese - Human-Factors*. [Em linha]. Disponível em: https://www.hse.gov.uk/humanfactors//topics/toolkit-introduction-portugese.pdf. [Acesso em: 30 junho 2022].

ISO/IEC (2018). *ISO/IEC 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary*. 5.ª. [Em linha]. Disponível em: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip. [Acesso em: 10 fevereiro 2023].

Lei n.º 46/2018, de 13 de Agosto - Regime jurídico da segurança do ciberespaço. *Diário da República*. (2018). [Em linha]. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2930&tabela=leis&nversao=. [Acesso em: 5 junho 2023].

Lei n.º 109/2009, de 15 de Setembro- Lei do Cibercrime. *Diário da República*. (109/2009, 15 de setembro). [Em linha]. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis. [Acesso em: 10 maio 2023].

Martins, J., Silva, J., Pimentel, C., Galindro, A., Rocha, J. & Custódio, M. (2016). *Revista Científica da Academia Militar, Série X, n.º 10 (2016)*. [Em linha]. Lisboa. Disponível em: https://academiamilitar.pt/images/site_images/Revista_Proelium/Proelium_2016_10.pdf. [Acesso em: 11 fevereiro 2023].

Maxwell, J.A. (1996). *Qualitative Research Design: An Interactive Approach*. 3rd Ed. London: SAGE Publications, Ltd.

Mitnick, K. & Simon, W. (2002). *A Arte de Enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação*. São Paulo: Pearson Makron Books.

Neto, P.T.M. & Araújo, W.J. (2019). *Segurança da Informação: Uma visão sistêmica para implantação em organizações*. 1st Ed. [Em linha]. Editora da UFPB. Disponível em: https://www.researchgate.net/publication/339107559_SEGURANCA_DA_INFORMACAO_Uma_visao_sistemica_para_implantacao_em_organizacoes. [Acesso em: 14 julho 2022].

Oksanen, J. (2013). *Organizing a Network Operation Centre on Campus Best Practice Document*. [Em linha]. Disponível em: https://archive.geant.org/projects/gn3/geant/services/cbp/Documents/gn3-na3-t4-organizing-noc.pdf. [Acesso em: 11 augusto 2023].

Oliveira, W. (2001). *Segurança da Informação – Técnicas e Soluções*. 1.ª. Vila Nova de Famalicão: Centro Atlântico.

Pardal, L. & Lopes, E.S. (2011). *Métodos e Técnicas de Investigação Social*. [Em linha]. Porto: Areal Editores. Disponível em: http://id.bnportugal.gov.pt/bib/bibnacional/1825944. [Acesso em: 11 setembro 2022].

Paulsen, C. & Byers, R. (2019). *Glossary of key information security terms*. [Em linha]. Gaithersburg, MD. Disponível em:

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf. [Acesso em: 4 junho 2023].

Peltier, T.R. (2005). *Information security risk analysis*. 2.ª. Boca Raton: CRC Press.

Reason, J. (1990). *Human error*. [Em linha]. Cambridge [England] ; New York : Cambridge University Press. Disponível em: https://archive.org/details/humanerror0000reas/page/n3/mode/2up. [Acesso em: 25 março 2020].

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). (2016). [Em linha]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. [Acesso em: 26 abril 2023].

Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril - Lei da Cibersegurança da UE. *Jornal Oficial da União Europeia*. (2019/881). [Em linha]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0881&qid=1697016417752. [Acesso em: 21 maio 2023].

Renaud, K. & Goucher, W. (2014). The Curious Incidence of Security Breaches by Knowledgeable Employees and the Pivotal Role a of Security Culture. In: T. Tryfonas & I. Askoxylakis (eds.). *Human Aspects of Information Security, Privacy, and Trust*. [Em linha]. Junho 2014, Cham: Springer International Publishing, pp. 361–372. Disponível em: https://www.researchgate.net/publication/289754089_The_Curious_Incidence_

of_Security_Breaches_by_Knowledgeable_Employees_and_the_Pivotal_Role_a_of_Security_Culture. [Acesso em: 5 julho 2023].

Ribeiro, T.A. (2023). Millenials e Geração Z recusam viver só para trabalhar: eis o que querem (e algumas dicas para manter equilíbrio entre lazer e trabalho). *Expresso*. [Em linha]. Economia (Online). Disponível em: https://expresso.pt/economia/2023-01-12-Millenials-e-Geracao-Z-recusam-viver-so-para-trabalhar-eis-o-que-querem--e-algumas-dicas-para-manter-equilibrio-entre-lazer-e-trabalho--51256e68. [Acesso em: 15 julho 2023].

Richardson, J., Milovidov, E. & Schmalzried, M. (2017). *Internet Literacy Handbook (2017) - Supporting users in the Em linha world*. 10th Ed. [Em linha]. Strasbourg: Council of Europe. Disponível em: https://edoc.coe.int/en/internet/7515-internet-literacy-handbook.html. [Acesso em: 2 augusto 2023].

Rodrigues, T.D. de F.F., Oliveira, G.S. de & Santos, J.A. dos (2021). As pesquisas qualitativas e quantitativas na educação. *Revista Prisma*. [Em linha]. 2 (1). p.pp. 154–174. Disponível em: https://revistaprisma.emnuvens.com.br/prisma/article/view/49. [Acesso em: 12 setembro 2022].

Sá, P. (Org.), Costa, A.P. (Org.), Moreira, A. (Org.), Alves, A.T.A. da R.B.A., Nascimento, A., Ulhôa, A., Batista, B., Capela, C., Venturine, C., Rodrigues, D., Moreira, E., Ribeiro, E., Silva, F., Demba, J., Lapa, L.D.P., Mota, M., Fortunato, M. & Silva, P.C.B. da (2021). *Reflexões em torno de Metodologias de Investigação: recolha de dados*. 1.ª. [Em linha]. UA Editora. Disponível em: http://hdl.handle.net/10773/30772. [Acesso em: 27 maio 2022].

Sêmola, M. (2014). *Gestão da Segurança da Informação - Uma Visão Executiva - 2ª Ed. 2014*. 2ª edição-8.º tir. [Em linha]. Rio de Janeiro: Elsevier Editora Ltda. Disponível em: https://www.marcossemola.com/. [Acesso em: 5 outubro 2022].

Silva, P.T., Carvalho, H. & Torres, C.B. (2003). *Segurança dos Sistemas de Informação - Gestão Estratégica da Segurança Empresarial*. Portuguese Edition. Lisboa - Porto: Edições Centro Atlântico.

Summers, R. (1997). *Secure Computing: Threats and Safeguards*. New Yor: McGraw-Hill.

Teotônio, Í.D. (2013). *Entendendo os Fundamentos da Segurança da Informação*. [Em linha]. 31 outubro 2013. Disponível em: https://www.profissionaisti.com.br/entendendo-os-fundamentos-da-seguranca-da-informacao/. [Acesso em: 10 outubro 2023].

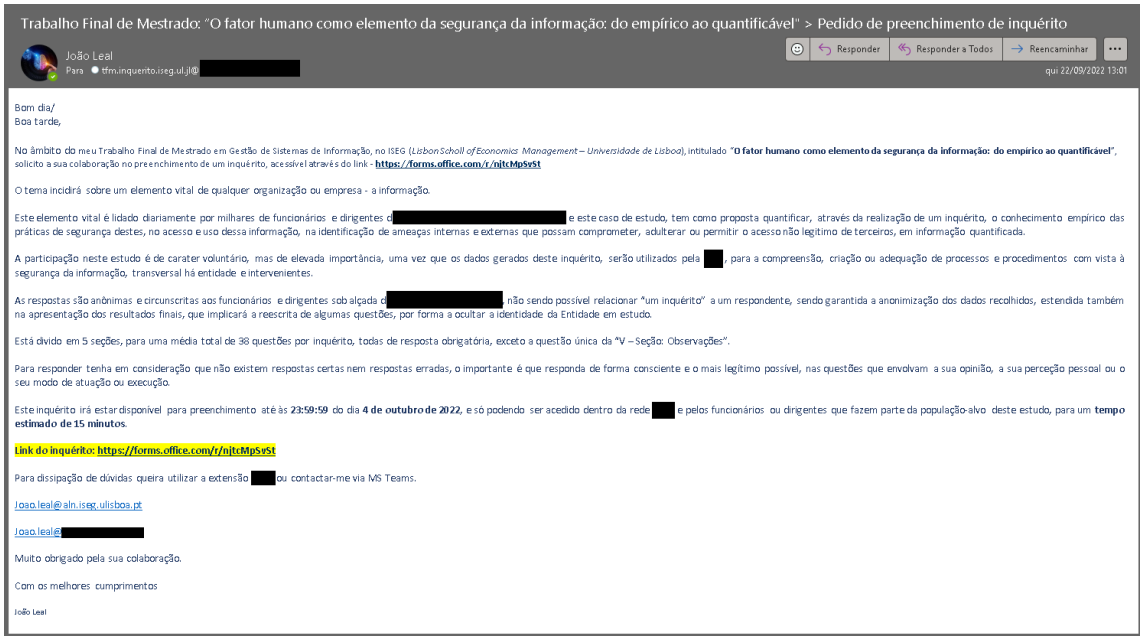
Vicente, J.J. (2017). *A Segurança da Informação - Informação ao Colaborador*. [Em linha]. p.pp. 1–28. Disponível em: https://www.cncs.gov.pt/docs/seguranca-informo-brochura.pdf. [Acesso em: 25 fevereiro 2023].

Winnefeld Jr., J., Kirchhoff, C. & Upton, and D. (2015). Cybersecurity's Human Factor: Lessons from the Pentagon - How companies can turn themselves into high-reliability organizations. *The Magazine - HBR (Harvard Business Review)*. [Em linha]. p.pp. 86–95. Disponível em: https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon. [Acesso em: 23 abril 2022].

Zorrinho, C. (1991). *Gestão da Informação*. Presença.

Anexos

Anexo I – Primeira mensagem de correio eletrónico



Trabalho Final de Mestrado: "O fator humano como elemento da segurança da informação: do empírico ao quantificável" > Pedido de preenchimento de inquérito

João Leal
Para tfm.inquerito.iseg.ul.pt@[redacted]

Responder | Responder a Todos | Reencaminhar

qui 22/09/2022 13:01

Bom dia/
Boa tarde,

No âmbito do meu Trabalho Final de Mestrado em Gestão de Sistemas de Informação, no ISEG (*Lisbon Scholl of Economics Management – Universidade de Lisboa*), intitulado "**O fator humano como elemento da segurança da informação: do empírico ao quantificável**", solicito a sua colaboração no preenchimento de um inquérito, acessível através do link - **https://forms.office.com/r/njtcMpSr5t**

O tema incidirá sobre um elemento vital de qualquer organização ou empresa - a informação.

Este elemento vital é lidado diariamente por milhares de funcionários e dirigentes d[redacted] e este caso de estudo, tem como proposta quantificar, através da realização de um inquérito, o conhecimento empírico das práticas de segurança destes, no acesso e uso dessa informação, na identificação de ameaças internas e externas que possam comprometer, adulterar ou permitir o acesso não legítimo de terceiros, em informação quantificada.

A participação neste estudo é de carater voluntário, mas de elevada importância, uma vez que os dados gerados deste inquérito, serão utilizados pela [redacted], para a compreensão, criação ou adequação de processos e procedimentos com vista à segurança da informação, transversal há entidade e intervenientes.

As respostas são anónimas e circunscritas aos funcionários e dirigentes sob alçada d[redacted], não sendo possível relacionar "um inquérito" a um respondente, sendo garantida a anonimização dos dados recolhidos, estendida também na apresentação dos resultados finais, que implicará a reescrita de algumas questões, por forma a ocultar a identidade da Entidade em estudo.

Está divido em 5 seções, para uma média total de 38 questões por inquérito, todas de resposta obrigatória, exceto a questão única da "V – Seção: Observações".

Para responder tenha em consideração que não existem respostas certas nem respostas erradas, o importante é que responda de forma consciente e o mais legítimo possível, nas questões que envolvam a sua opinião, a sua perceção pessoal ou o seu modo de atuação ou execução.

Este inquérito irá estar disponível para preenchimento até às **23:59:59** do dia **4 de outubro de 2022**, e só podendo ser acedido dentro da rede [redacted] e pelos funcionários ou dirigentes que fazem parte da população-alvo deste estudo, para um **tempo estimado de 15 minutos**.

Link do inquérito: https://forms.office.com/r/njtcMpSr5t

Para dissipação de dúvidas queira utilizar a extensão [redacted] ou contactar-me via MS Teams.

Joao.leal@aln.iseg.ulisboa.pt

Joao.leal@[redacted]

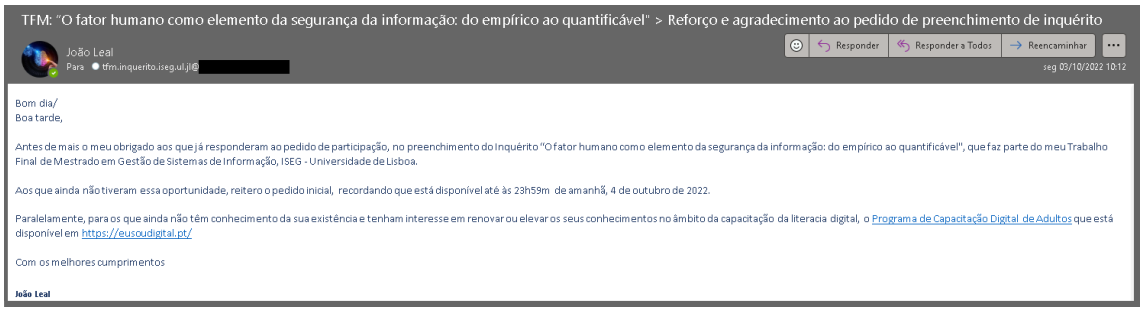
Muito obrigado pela sua colaboração.

Com os melhores cumprimentos

João Leal

Ilustração 3: Primeira mensagem de correio eletrónico a explicar e solicitar à participação

Anexo II – Segunda mensagem de correio eletrónico



TFM: "O fator humano como elemento da segurança da informação: do empírico ao quantificável" > Reforço e agradecimento ao pedido de preenchimento de inquérito

João Leal
Para tfm.inquerito.iseg.ul.pt@[redacted]

Responder | Responder a Todos | Reencaminhar

seg 03/10/2022 10:12

Bom dia/
Boa tarde,

Antes de mais o meu obrigado aos que já responderam ao pedido de participação, no preenchimento do Inquérito "O fator humano como elemento da segurança da informação: do empírico ao quantificável", que faz parte do meu Trabalho Final de Mestrado em Gestão de Sistemas de Informação, ISEG - Universidade de Lisboa.

Aos que ainda não tiveram essa oportunidade, reitero o pedido inicial, recordando que está disponível até às 23h59m de amanhã, 4 de outubro de 2022.

Paralelamente, para os que ainda não têm conhecimento da sua existência e tenham interesse em renovar ou elevar os seus conhecimentos no âmbito da capacitação da literacia digital, o Programa de Capacitação Digital de Adultos que está disponível em https://eusoudigital.pt/

Com os melhores cumprimentos

João Leal

Ilustração 4: Mensagem de correio eletrónio a agradecer e a reiterar o pedido de participação

Anexo III – Questionário

Q#	Questão	Opções de resposta	Ramificação
I - Presença e literacia digital			
1	Tem contacto diário com plataformas de serviços *online* ou redes sociais?	Sim	Q2
		Não	Q5
2	Tendo respondido de forma afirmativa, identifique para cada uma das situações ou plataformas, o principal acesso que utiliza como login: • Meta Inc • TVDE • Banca Digital • …	Email Pessoal	Q3
		Email Corporativo	
		Número associado ao telemóvel	
		Email Pessoal e Número associado ao telemóvel	
		Email Corporativo e Número associado ao telemóvel	
		Não se aplica	

3	A(s) palavra(s)-passe que utiliza nos acessos que indicou na questão anterior são, ou já foram, genericamente idênticas?	Sim, utilizo a mesma palavra-passe para diferentes acessos	Q4
		Sim, em algum momento no tempo foram Idênticas para diferentes acessos	
		Não, nunca foram idênticas	
		Não me recordo, mas é bastante provável	
4	Utiliza algum mecanismo de segurança adicional, como por exemplo o "segundo fator de autenticação" (2FA/MFA), no acesso ao seu correio eletrónico pessoal (email pessoal):	Sim	Q5
		Não	
		Não sei responder	
5	Como classifica, de forma genérica, a sua literacia digital?	Tenho fracos conhecimentos informáticos *(…)*	Q6
		Tenho alguns conhecimentos informáticos *(…)*	

		Tenho conhecimentos informáticos genéricos, na ótica do utilizador *(…)*	
		Tenho conhecimentos informáticos acima da média dos utilizadores comuns *(…)*	
		Tenho conhecimentos informáticos especializados *(…)*	
II – Segurança da Informação			
6	Na sua opinião, considera o teletrabalho ou o trabalho híbrido uma ameaça à informação?	Sim	Q7
		Não	
		Não tenho opinião formada	
7	Utiliza equipamento(s) eletrónico(s) pessoa(l/is) em contexto de trabalho?	Sim	Q8
		Não	Q9
8	Tendo respondido de forma afirmativa, indique qua(l/is): *(Pode selecionar mais de uma opção)*	Telemóvel (*smartphone*)	Q9
		Computador portátil (*laptop*)	

		Computador fixo (*desktop*)	
		Tablet	
		"Outro"	
9	*A Entidade* atribuiu-lhe algum(ns) equipamento(s) eletrónico(s) para contexto/utilização em teletrabalho?	Sim	Q10
		Não	Q11
10	Tendo respondido de forma afirmativa, indique qual(is): *(Pode selecionar mais de uma opção)*	Telemóvel (*smartphone*)	Q11
		Computador portátil (*laptop*)	
		Computador fixo (*desktop*)	
		Tablet	
		"Outro"	
11	Quando se encontra fora das instalações *da Entidade*, no acesso ao correio eletrónico corporativo ou Microsoft Teams, utiliza o "duplo fator de autenticação" ou *token (físico ou no telemóvel)*?	Sim	Q12
		Não, porque ainda não me foi atribuído	
		Tenho, mas não acedo fora das instalações	
12		Sim	Q13

	Tem acesso remoto por VPN ao seu equipamento de trabalho n*a Entidade*?	Não	Q15
13	Tendo respondido de forma afirmativa, foi-lhe dado conhecimento e explicado os procedimentos de como gerir e garantir um ambiente seguro, no seu acesso remoto por VPN ao seu equipamento n*a Entidade?*	Sim	Q14
		Não	
		Não me recordo	
14	Já necessitou de recorrer à ajuda de elementos externos ao MNE na resolução de algum problema ou situação para a utilização do acesso remoto por VPN ao seu equipamento n*a Entidade*?	Sim	Q15
		Não	
15	Quanto está em trabalho presencial ou teletrabalho, indique a opção que melhor qualifica a sua ação:		Q16
	Bloqueio a sessão no computador, mesmo por curtíssimos períodos de tempo	Nunca/Não	
		Ocasionalmente	
		Sempre/Sim	
		Nunca/Não	

	Guardo os documentos impressos fora de olhares curiosos, mesmo por curtíssimos períodos de tempo	Ocasionalmente	
		Sempre/Sim	
	Ao imprimir utilizo a opção "Impressão segura"	Nunca/Não	
		Ocasionalmente	
		Sempre/Sim	
	Quando necessito de ausentar-me por um período de tempo superior a +/- 15 minutos guardo os documentos de modo a impedir o acesso por terceiros	Nunca/Não	
		Ocasionalmente	
		Sempre/Sim	
	Já enviei documentos de trabalho para o meu correio eletrónico pessoal	Nunca/Não	
		Ocasionalmente	
		Sempre/Sim	
	Já levei documento impressos de trabalho para fora do ambiente d*a Entidade* (exclui-se situações similares a reuniões de trabalho externas)	Nunca/Não	
		Ocasionalmente	
		Sempre/Sim	
		Nunca/Não	

	Aplico diariamente os conceitos "Secretária limpa" e "Tela limpa"	Ocasionalmente	
		Sempre/Sim	
	Já dei a conhecer a um(a) colega meu/minha a minha palavra-passe de acesso ao computador de serviço ou aplicativo	Nunca/Não	
		Ocasionalmente	
		Sempre/Sim	
	Já guardei, ou ainda guardo, as minhas palavras-passe no meu telemóvel ou *tablet*, seja em forma de texto ou imagem	Nunca/Não	
		Ocasionalmente	
		Sempre/Sim	
16	Quando se desloca ou viaja, se necessitar de transportar um computador portátil, este é transportado: *(Seja de uso pessoal ou atribuído pelo serviço)*	Sempre comigo, nunca o perdendo de vista	Q17
		Pode haver períodos em que não está comigo ou próximo	
		Não se aplica	
17		Sim	Q18

	Se necessitar de aceder à Internet num espaço público, estabelecimento comercial, hotel, centro de convenções, e houver disponível uma rede *wifi* aberta, utiliza-a?	Sim, mesmo tendo dados móveis próprios	
		Não	
18	Considera segura a utilização para acesso à Internet de redes *wifi* abertas?	Sim	Q19
		Não	
		Não tenho opinião formada	
19	Se necessitar de aceder à Internet num espaço público, estabelecimento comercial, hotel, centro de convenções, por uma rede wifi na qual necessita de digitar a palavra-passe que lhe é fornecida ou está visível, ou efetuar um pré-registo (com ou sem termos de aceitação) sente-se mais segur(o/a) e protegid(o/a) para a sua utilização?	Sim	Q20
		Sim, mesmo tendo dados móveis próprios	
		Não	
		Não tenho opinião formada	
20	Se tiver de utilizar o computador portátil, telemóvel (*smartphone)* ou *tablet,* num ambiente público ou durante	Sim	Q21
		Não	
		Nunca tinha pensado nisso	

	uma reunião, tem o cuidado proteger o conteúdo que está a visionar da visão/leitura de terceiros?		
21	Sabe o que a PUA d*a Entidade*?	Sim	Q22
		Não	
22	Já foi alvo de alguma tentativa de *phishing*, *smishing* ou v*ishing*?	Sim	Q23
		Não	
		Não sei responder	
23	Considera segura a utilização dos seus dados pessoais na rede informática *da Entidade*	Sim	Q24
		Não	
		Não tenho opinião formada	
24	A sua perceção da "segurança informática da rede d*a Entidade*" é:	Globalmente má	Q25
		Tem alguns aspetos que necessitam de melhorias	
		Globalmente boa	
		Não tenho opinião formada	

25	A sua perceção dos "serviços de informática *da Entidade*" é:	Globalmente má	Q26
		Tem alguns aspetos que necessitam de melhorias	
		Globalmente boa	
		Não tenho opinião formada	
26	Na sua opinião, considera que *a Entidade* dispões dos meios técnicos e humanos de proteção e segurança contra ciberataques?	Sim	Q27
		Não	
		Não tenho opinião formada	
27	Nos últimos 5 anos teve alguma formação que abordasse sobre as temáticas de: • Segurança da Informação (e …) • Utilização do Sistema Operativo • Segurança e utilização de uma VPN	Sim, pelo menos uma das temáticas foi abordada	Q28
		De outro conteúdo em que a temática principal não foi nenhuma das indicadas, mas houve breves abordagens ou contextualização	Q28

	• Utilização segura do correio eletrónico • Identificação de ameaças cibernéticas • *Cloud* • Segurança em redes sociais	Não tive nenhuma formação no âmbito das temáticas indicadas	Q30
28	Tendo respondido de forma afirmativa, identifique qual(is): (Pode selecionar mais do que uma opção)	Segurança da Informação e *(conteúdo omitido)*	Q29
		Utilização do Sistema Operativo	
		Segurança e utilização de uma VPN	
		Utilização segura do correio eletrónico	
		Identificação de ameaças cibernéticas	
		Cloud	
		Segurança em redes sociais	
29	Da(s) que indicou, identifique se fo(i/ram) ministrada(s) ou paga(s):	Pela Entidade	Q30
		Por outra(s) do setor público	
		Por outra(s) do setor privado	

		Não sei responder	
III - Caracterização			
30	Identificação do género:	Feminino	Q31
		Masculino	
31	Faixa etária:	[18-24] anos	Q32
		[25-34] anos	
		[35-44] anos	
		[45-54] anos	
		[55-64] anos	
		65 anos ou +	
32	Qualificações Académicas (*De acordo com o QNQ (Quadro Nacional de Qualificações, Portaria n.º 78/2009, de 23 de julho)*	Nível 1 (2.º ciclo do ensino básico)	Q33
		Nível 2 (3.º ciclo do ensino básico)	
		Nível 3 (Ensino secundário, via de ensino)	

		Nível 4 (Ensino secundário, via profissional)	
		Nível 5 (Ensino técnico-profissional)	
		Nível 6 (Bacharelato, Licenciatura de 1.º ciclo de Bolonha)	
		Nível 7 (Licenciatura pré-Bolonha, Mestrado)	
		Nível 8 (Doutoramento)	
33	Modalidade do vínculo de trabalho ou relação:	Estágio	Q34
		Prestação de serviços (em trabalho subordinado)	
		Prestação de serviços (em trabalho não subordinado/independente)	
		Contrato a termo	
		Contrato sem termo	

		(opção omitida)	
		(opção omitida)	
34	Caracterização da carreira ou função atual:	Assistente Operacional	Q35
		Assistente Técnico	
		Técnico Superior (Nível 6, 7 e 8)	
		Carreira não-revista (Informática)	
		Carreira não-revista (Informática), equivalente a Técnico Superior (Nível 6, 7 e 8)	
		Coordenação, Chefia ou Direção	
35	Tempo na carreira ou na função atual:	< 1 ano	Q36
		[1 - 3] anos	
		[4 - 6] anos	
		7 anos ou +	
36	Identificação do “*Departamento*”:	*(opção omitida)*	Q47

		"Assuntos Jurídicos"	Q38
		"Administração (RH, Economato, …)"	Q37
		"Informática"	Q40
		"Informação e Imprensa"	Q47
		"Administração (Chefia)"	Q47
		"Arquivo e Formação"	Q39
		(opção omitida)	Q47
37	*"Administração (RH, Economato, …)"*	*(opções omitidas)*	Q47
38	*Assuntos Jurídicos"*	*(opções omitidas)*	Q47
39	*Arquivo e Formação"*	*(opções omitidas)*	Q47
40	"*Informática*"	*(opções omitidas)*	Q41
IV – "*Informática*"			
41	Desempenha funções técnicas?	Sim	Q42
		Sim, e também de chefia	Q42
		Não, porque "pertenço à chefia"	Q43

		Não, porque executo apoio ou funções administrativas	Q45
42	Há quanto tempo desempenha funções na área das TIC?	< 1 ano	Q43
		[1 - 3] anos	
		[4 - 6] anos	
		7 anos ou +	
43	Tem formação especifica na área das Tecnologias de Informação e Comunicação (TIC)?	Sim	Q44
		Não	
	Nos últimos 5 anos frequentou alguma(s) formaç(ão/ões) TIC, focada(s) na(s) área(s) das suas funções, que tivesse sido:		
44	Ministrada, paga ou subsidiada pela *Entidade*?	Sim [1 a 2]	Q45
		Sim [3 a 5]	
		Sim [+ 5]	
		Não	
		Não se aplica	

	Ministrada, paga ou subsidiada pela minha Entidade? (Só se aplica aos externos)	Sim [1 a 2]	
		Sim [3 a 5]	
		Sim [+ 5]	
		Não	
		Não se aplica	
	Adquirida a expensas próprias.	Sim [1 a 2]	
		Sim [3 a 5]	
		Sim [+ 5]	
		Não	
		Não se aplica	
45	Aquando do seu início de funções foi-lhe dado conhecimento sobre os processos e procedimentos internos, necessários à execução das suas funções?	Sim	Q46
		Não	
		Não me recordo	
46		Sim	Q47
		Não	

	Aquando do seu início de funções, (texto omitido) teve algum período de adaptação ou o acompanhamento direto, durante algum tempo, por um colega que executa-se essas funções?	Não me recordo	
V - Observações			
47	Utilize esta última "questão", se pretender registar alguma situação ou sugestão que considera importante para este inquérito.	(resposta livre e não obrigatória)	(Fim)