O "*Work Project*" que seguidamente se apresenta é parte de um requisito para atribuição de grau de Mestre em " Leadership - Executive" da NOVASBE,

Nova School of Business and Economics

O PAPEL DA LIDERANÇA NA CONSTRUÇÃO DE UMA CULTURA DE CIBERSEGURANÇA

Clara Leonor Alexandre Marques

Alumni 56415

Projeto de Trabalho levado a cabo com a supervisão de:

Professora Doutora Filipa Rocha Rodrigues

24/10/2023

It Ain't What You Don't Know That Gets You into Trouble. It's What You Know for Sure That Just Ain't So!

Mark Twain

AGRADECIMENTOS

Em cada jornada a aprendizagem,

Em cada caminho a solidão,

Em cada tempestade uma viagem,

Em cada porto o coração!

Ao meu marido, **Filipe**, por ser o meu apoio, a minha bússola, o meu porto de abrigo;

À minha família, por ser o meu suporte, o meu compasso;

Aos meus amigos e colegas, por me ajudarem a crescer;

Aos meus professores e mentores, por ajudarem no meu desenvolvimento e progresso;

À minha orientadora, Filipa, por ter calcorreado este caminho de aprendizagem comigo.

ÍNDICE

1 Introdução 1

2 Revisão da Literatura 2

3 Método de Investigação 5

3.1 Contexto 5

3.2 Amostra 7

3.3 Recolha e Análise de Dados 7

3.4 Avaliação da Pesquisa 8

4 Resultados 9

5 Discussão 23

6 Conclusão 24

6.1 Contribuição Teórica e Implicações Práticas do Estudo 24

6.2 Limitações do Estudo e Sugestões de Investigação Futura 25

6.3 Considerações Finais 25

7 Referências 26

8 Anexos 30

8.1 Acrónimos e Definições 30

8.2 Caracterização dos Dados Recolhidos 35

8.3 Dados de Apoio ao Tema “o Papel da Liderança na Construção de uma Cultura de Cibersegurança” 40

8.4 Consentimento Informado & Entrevista 66

ÍNDICE DE FIGURAS

Figura 1: Representação esquemática do trabalho de investigação (fonte: Nvivo.14) 6

Figura 2: Estrutura de dados..... 10

Figura 3: Estrutura de Interação 11

Figura 4: Matriz relacional dos fatores de influência da estratégia de cibersegurança..... 12

Figura 5: Primeira análise de estrutura de dados (fonte: Nvivo.14)..... 37

ÍNDICE DE GRÁFICOS

Gráfico 1: Caracterização de género presente na Amostra..... 35

Gráfico 2: Duração (em minutos) das entrevistas realizadas 36

Gráfico 3: Nível de Significância dos Códigos de 1ª ordem 36

ÍNDICE DE TABELAS

Tabela 1: Sectores de Mercado Representados na Amostra..... 35

Tabela 2: Posições Organizacionais representados na Amostra..... 35

Tabela 3: Formação de base dos Entrevistados 35

Tabela 4: Intervalo (em anos) de experiência profissional..... 36

Tabela 5: Intervalo (em anos) de antiguidade na função..... 36

Tabela 6: Estrutura de dados final 38

Tabela 7: Códigos de 1ª ordem, por Entrevistado 39

Tabela 8: Dados de apoio ao tema (Códigos de 1ª Ordem)..... 65

RESUMO

Com a digitalização, as ciberameaças são cada vez mais comuns, colocando desafios à liderança executiva e fazendo da cibersegurança uma questão crítica para qualquer organização. Através de um método qualitativo baseado em 17 entrevistas a líderes de organizações, o presente estudo analisa a relação entre liderança e a estratégia de cibersegurança. Do presente estudo resulta uma matriz relacional dos fatores de influência para a definição / implementação de uma estratégia de cibersegurança nas organizações, destacando-se o papel fundamental de 4 dimensões: Recurso-Chave, Fatores de Influência, Fatores de Sucesso e Principais Desafios, segundo 2 vetores: Líder e Estado.

Palavras-Chave: Estratégia de cibersegurança, conhecimento do negócio, partilha de responsabilidades, gestão do risco, treino e consciencialização.

1 INTRODUÇÃO

Com quase 75% das organizações a sofrerem pelo menos um ciberataque (Microsoft and Marsh 2022), a digitalização faz da cibersegurança uma questão crítica para qualquer organização, colocando desafios à liderança executiva atual (Parenty and Domet 2019). Se a liderança executiva e os conselhos de administração são encarregues de definir a estratégia de negócio da empresa, então não podem descurar este tema, deve estar presente nas suas agendas (Cleveland and Cleveland 2018). Requer-se, assim, por parte destes líderes uma maior compreensão e consciência para os ciber-riscos e potenciais ameaças, esperando-se que saibam agir e que tomem decisões críticas diante de ciberataques (Dobrygowski and O'Halloran 2017). O risco referente à "cibercriminalidade e cibersegurança" aparece na 8ª (oitava) posição, num máximo de 10 (dez), nos riscos globais mais severos enumerados pelo relatório de riscos globais de 2023 do *World of Economic Forum* (Heading et al. 2023). Combater as ciberameaças, por meio de uma correta gestão do risco, tirando partindo dos avanços tecnológicos, representa um desafio estratégico significativo para os líderes de todas as indústrias e setores (Parenty and Domet 2019).

O ano de 2022 revelou-se particularmente fértil e desafiante, tendo em conta a ocorrência de diversos ciberataques de grande impacto social e nas infraestruturas e serviços em Portugal (CNCS Observatório de Cibersegurança 2023), continuando a estimar-se o seu aumento: "O número de incidentes de cibersegurança registados pelo CERT.PT, durante o primeiro trimestre de 2023, decresceu 38% face ao período homólogo. Contudo, este valor representa uma subida de 28% relativamente ao último trimestre de 2022" (CNCS Observatório de Cibersegurança 2023, pág.11). A revisão da literatura efetuada demonstra que o envolvimento dos líderes é fundamental. No entanto, a compreensão dos fatores que conduzem à construção desta cultura e promoção da cibersegurança nas organizações é em grande parte incompleta (Gale, Bongiovanni, and Slapnicar 2022). Surge assim a importância e a necessidade de saber quais

são os fatores que influenciam a promoção de uma cultura de cibersegurança por parte destes líderes e como é que chegamos ao seu correto alinhamento com as necessidades do negócio, não descurando o cumprimento dos requisitos mínimos de segurança que permita às organizações reduzir o ciber-risco associado às ameaças (Marques and Santos 2019).

A presente dissertação encontra-se organizada em diferentes capítulos, secções e anexos, nomeadamente: "Capítulo 1 - Introdução", enquadramento sumário da dissertação e seus objetivos; "Capítulo 2 - Revisão da Literatura", apresentação do tema, seus constituintes, regras e procedimentos internos para facilitar o seu entendimento e a maximizar a confiança dos seus leitores; "Capítulo 3 - Método de Investigação", descrição das várias etapas do processo de investigação, nomeadamente contexto, caracterização da amostra, forma de recolha e análise de dados e avaliação da pesquisa efetuada; "Capítulo 4 - Resultados", apresentação das várias etapas do processo de análise; "Capítulo 5 - Discussão", descrição e discussão dos resultados óbitos; por fim, no último capítulo, "Capítulo 6 - Conclusão", é apresentada a conclusão juntamente com a contribuição teórica / implicações práticas, limitações / sugestões para investigação futura e considerações finais.

2 REVISÃO DA LITERATURA

Cibersegurança, segundo Schatz, Bashroush, e Wall define-se como a "abordagem e ações associadas ao processo de gestão de risco de segurança seguido por organizações e estados para proteger a confidencialidade, integridade e disponibilidade dos dados e ativos utilizados no ciberespaço, suportado por diretrizes, políticas, tecnologias, ferramentas e formação para proporcionar proteção de cibersegurança dos seus utilizadores" (Schatz, Bashroush, and Wall 2017, pág.64).

A rápida evolução tecnológica e transferência de serviços para o ciberespaço leva, inevitavelmente, a um aumento do número dos ciberataques que acabam por afetar a estabilidade económica e política nacional, provocando interrupções de serviços com impactos

financeiros e reputacionais. Sendo o seu impacto cada vez maior, com tendência para aumentar tendo em conta o processo de digitalização de todos os setores da indústria (Parenty and Domet 2019) a gestão estratégica de cibersegurança acaba por ser fundamental para minimizar esse risco e diminuir o impacto (Marques and Santos 2019). Com esta crescente dependência surge uma vulnerabilidade aumentada (Carafano and Sayers 2008), recaindo a proteção dos sistemas sobre os especialistas em cibersegurança e as suas competências (Bukauskas et al. 2022).

Em 2021 a empresa de consultoria Gartner previu que os gastos globais com cibersegurança ultrapassariam 150 bilhões de US$, representando um crescimento de 12,4% em relação a 2020 (Moore 2021).

Sabendo que os ciberataques não vêm com agendamento prévio, espera-se que os líderes das organizações estejam preparados para gerir crises de cibersegurança, pois estes ciberataques poderão impactar toda a organização (Cleveland and Cleveland 2018).

Ciberataques, que são cada vez mais destrutivos e fatais para as organizações, exigem que os seus conselhos de administração, intensifiquem os seus esforços defensivos e aprovem orçamentos cada vez mais ajustados para se protegerem, e simultaneamente direcionam os seus líderes para uma prática mais ativa e eficaz do governo da cibersegurança (IBM 2023).

Este pensamento estratégico e de governo não são lineares nem imediatos. "*Ouvir não é o mesmo que escutar*" é com esta destrinça que o relatório sobre cibersegurança do *World of Economic Forum* introduz a relação comparativa entre os líderes de cibersegurança e outros líderes de negócio comparando a forma como ambos sentem e abordam a exposição das suas organizações ao crescendo do ciber-risco (Bueermann et al. 2023). Indica também que os líderes de negócio, ainda que mais conscientes, continuam longe da necessária visão articulada entre os problemas e os ciber-riscos, já efetuada pelos líderes de cibersegurança (Parenty and Domet 2019).

Mais de 39% dos líderes da organização concordam que "*a cibersegurança é um facilitador*

chave para os negócios" (Bueermann et al. 2023), o que torna como recorrente a prática de recurso a líderes de cibersegurança, tais como diretores de segurança da informação (*CISOs*), para a proteção contra ciberataques (Anderson, Ahmad, and Chang 2022) e alinhamento com referenciais (Marques and Santos 2019) e *frameworks* de cibersegurança segundo as melhores práticas de mercado (NIST 2023).

Em 2014, Luis Aguilar, fez uma síntese, que ainda se mantém atual, de que "as evidências sugerem que pode haver uma lacuna [...] entre a magnitude da exposição apresentada pelos ciber-riscos e as medidas, ou a falta delas, que muitos líderes das organizações tomam para lidar com os mesmos" (Aguilar 2014, pág.5). A lacuna entre as estruturas de conhecimento de cibersegurança e a liderança em cibersegurança surge porque os papéis dos líderes de cibersegurança são mais recentes do que os papéis operacionais de cibersegurança já estabelecidos, como o *Chief Information Officer* (CIO), e não muito bem compreendidos (Anderson, Ahmad, and Chang 2022). Sendo o papel de líder de cibersegurança um papel recente, quando comparado com profissionais da mesma área (profissionais de cibersegurança), e diferente quando comparado com outros cargos de liderança (líderes de negócio), necessita do correto enquadramento para ser entendido. As organizações e instituições de ensino / formação continuam a catalogá-lo como um papel técnico sénior, em vez de um papel estratégico e orientado para os negócios, o que cria uma lacuna entre o que é visto como "negócio" e o que é visto como "IT" deixando as organizações mais vulneráveis a ataques (Anderson, Ahmad, and Chang 2022). Contudo, as capacidades ao nível do conselho de administração para o pensamento estratégico e governo nesta área não conseguem acompanhar tanto os riscos tecnológicos como as soluções que as novas inovações proporcionam (Dobrygowski and O'Halloran 2017). Tudo isto incita os líderes organizacionais de topo a reagirem e a definirem estratégias de cibersegurança (Parenty and Domet 2019).

3 MÉTODO DE INVESTIGAÇÃO

3.1 CONTEXTO

O presente estudo surge em resposta à pergunta: "*Como é que o líder influência a construção de uma cultura de cibersegurança?*". Sendo um tema de interesse e ainda pouco estudado adota-se uma perspetiva exploratória (Tracy 2013) e uma abordagem qualitativa, considerada como a mais adequada para a recolha e análise indutiva de dados (Hastie and Glotova 2012).

Para promover uma compreensão profunda e significativa sobre o tema efetuam-se 17 entrevistas a líderes executivos, na posição de CEO (*Chief Executive Officer*), CISO (*Chief Information Security Officer*) e pessoas com funções impactantes na área da cibersegurança de diversas organizações, representando 15 organizações com presença em Portugal em diversos setores, públicos e privados. Identificam-se os entrevistados seguindo o método *snowballing* (Reis et al. 1997) e determina-se a dimensão da amostra com base no pressuposto de que a saturação teórica é um elemento essencial dentro da pesquisa qualitativa (Sim et al. 2018).

Para atingir os objetivos propostos, este estudo segue a orientação de Stake (Stake 1995) para um desenho de investigação flexível que indica que as questões e perceções levantadas pelos participantes não podem ser conhecidas à partida, ou seja, as questões presentes no guião de entrevista, apenas são dadas a conhecer no momento de realização da entrevista. Identificam-se as questões tendo por base o quadro nacional de referência para a cibersegurança (Marques and Santos 2019) que tem por base *frameworks* transversais a qualquer boa prática de cibersegurança independentemente da sua localização geográfica (Maurer and Morgus 2014).

Para abordar a pergunta de investigação, realiza-se uma pesquisa sistemática de artigos, relatórios, referenciais, regulamentos e literatura sobre a temática da cibersegurança, seguindo, na pesquisa inicial um processo de revisão sistemática (Vom Brocke et al. 2009) e realização de encadeamento reverso e encadeamento direto para encontrar fontes suficientes para uma análise robusta, complementando com pesquisa no Google Académico e EBSCO para

selecionar artigos do setor de fontes de alta qualidade.

O processo de pesquisa acima e seus resultados é apresentado na Figura 1.

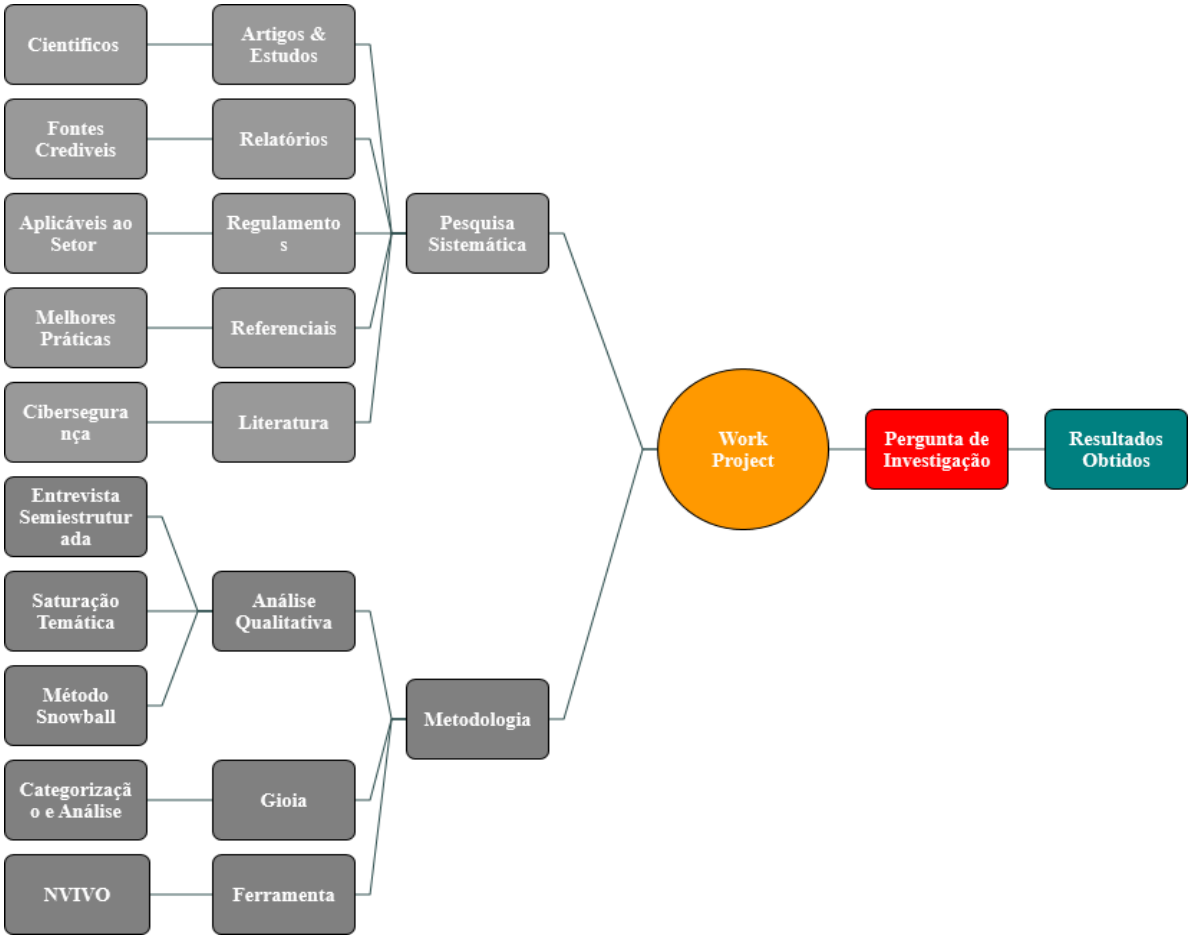

Figura 1: Representação esquemática do trabalho de investigação (fonte: Nvivo.14)

Para tratamento e análise dos dados recorre-se à ferramenta Nvivo.14. De forma a efetuar uma análise de conteúdo e classificação dos elementos constitutivos de cada uma das entrevistas, cria-se uma taxonomia com o objetivo de deduzir dados e fazer refletir uma perspetiva quantitativa de análise de dados, nesta investigação qualitativa (Resende 2016). A representação gráfica do progresso de dados brutos para códigos de primeira ordem, temas teóricos e dimensões teóricas agregadas apura-se com a metodologia de Gioia (Gioia, Corley, and Hamilton 2012).

3.2 AMOSTRA

O método *snowballing* (Reis et al. 1997) identifica os profissionais, com experiência e contacto com a cibersegurança em empresas tanto públicas como privadas, relevantes para participar, e a saturação temática (Sim et al. 2018) determina a dimensão da amostra em estudo (Gráfico 1 e Tabela 1), num total de 17 entrevistados de 15 empresas.

Este estudo não é específico de sector, uma vez que a investigação atual demonstra que as organizações podem ser alvo de ciberataques, independentemente do seu sector, tamanho ou valor (CNCS Observatório de Cibersegurança 2023).

A riqueza dos dados recolhidos é significativamente amplificada pelo facto da maioria dos entrevistados presentes na amostra possuírem uma posição de direção (Tabela 2), formação base diversificada (Tabela 3) e senioridade (Tabela 4 e Tabela 5).

3.3 RECOLHA E ANÁLISE DE DADOS

São adotadas várias estratégias para recrutar os participantes, nomeadamente, contacto direto com conhecidos, contacto através de plataforma de rede social (LinkedIn) e *snowballing* (Reis et al. 1997), no qual um participante identifica outros participantes a incluir.

Obtém-se consentimento prévio para participação neste estudo. Realizam-se entrevistas semiestruturadas, nas quais se fazem perguntas abertas para obter dados informativos, pessoais ou descritivos dos participantes. As entrevistas seguem um protocolo (conforme "Anexo 8.4 - Consentimento Informado & Entrevista") que proporciona padronização, ao mesmo tempo que permite a flexibilidade de seguir pistas e personalizar as perguntas conforme necessário, sendo os entrevistados livres de fornecer informação para além das respostas. A flexibilidade semiestruturada favorece a descoberta das experiências, perceções e envolvimento dos entrevistados. As declarações de confidencialidade e participação voluntária são discutidas com cada participante e o respetivo consentimento é solicitado no

início de cada entrevista (conforme "Anexo 8.4 - Consentimento Informado & Entrevista").

As entrevistas são realizadas presencialmente e virtualmente, conforme disponibilidade do entrevistado, durante 4 meses (entre março e julho de 2023), variando a sua duração entre 31 minutos e 1 hora e 32 minutos, apurando-se uma duração média de 55 minutos (Gráfico 2). Todas as entrevistas são transcritas na integra pelo investigador, que também as revê para manter a precisão, perfazendo um total de 288 páginas transcritas. As transcrições são validadas por cada um dos entrevistados, para garantir que nada se perde e no final são pseudonimizadas para proteger o anonimato dos participantes (que não querem revelar a sua identidade) e a confidencialidade dos dados. Os dados são analisados seguindo uma abordagem de análise temática.

Durante a recolha de dados, e após cada entrevista, o investigador identifica os temas emergentes que são anotados e referidos em cada entrevista subsequente para localizar pontos em comum. Utilizando o método de Gioia (Gioia, Corley, and Hamilton 2012), com suporte da ferramenta Nvivo14, seguiram-se a codificação secundária e a recodificação.

Finalmente, as relações entre os temas foram discutidas entre o investigador e o orientador, e comparadas com a literatura relevante. Este processo foi utilizado para garantir que as perceções e experiências recolhidas foram genuinamente captadas e interpretadas em persecução do objetivo proposto.

3.4 AVALIAÇÃO DA PESQUISA

Conforme recomenda a teoria fundamentada (Gioia, Corley, and Hamilton 2012), a análise dos dados faz-se em três fases:

Fase 1: Produção de categorias provisórias e códigos de primeira ordem.

De forma iterativa, os dados foram simultaneamente codificados e analisados. As entrevistas dos participantes são organizadas tendo em conta as suas semelhanças, formando categorias

provisórias e códigos de primeira ordem. A sua significância é calculada tendo por base o número de vezes que cada um dos códigos é referido e repetido por cada um dos entrevistados ao longo de cada uma das entrevistas efetuadas pelo investigador. O nível de significância entre os codificadores não caiu abaixo de 82% (Gráfico 3). Utiliza-se o software NVivo 14.0 para inserir cotações e organizar códigos. Foram codificadas 208 unidades de significado a partir das 17 entrevistas. Nesta fase, tornou-se claro que independentemente do sector de atividade ou da posição, os aspetos enfatizados eram em todos semelhantes, o que ajuda a agregar e permite focar nos objetos do estudo.

Fase 2: *Criação de temas teóricos*.

Conceitos de primeira ordem são transformados em temas de segunda ordem, apoiando-se na interpretação dos dados recolhidos, bem como na revisão da teoria existente. Em seguida, viajando entre os dados e uma estrutura emergente de argumentos teóricos, as categorias foram consolidadas.

Fase 3: *Agregar dimensões teóricas.*

Procuram-se dimensões subjacentes a estas categorias na tentativa de compreender como diferentes códigos se encaixam num quadro coerente. A Figura 2 fornece uma representação gráfica da evolução de dados brutos para códigos de primeira ordem, temas teóricos e dimensões teóricas agregadas. As dimensões teóricas agregadas explicam como os líderes de cibersegurança, independentemente da sua função, descrevem os fatores que influenciam as estratégias de cibersegurança, sendo a sua estrutura de interação e matriz relacional fornecidas respetivamente pelas Figura 3 e Figura 4.

4 RESULTADOS

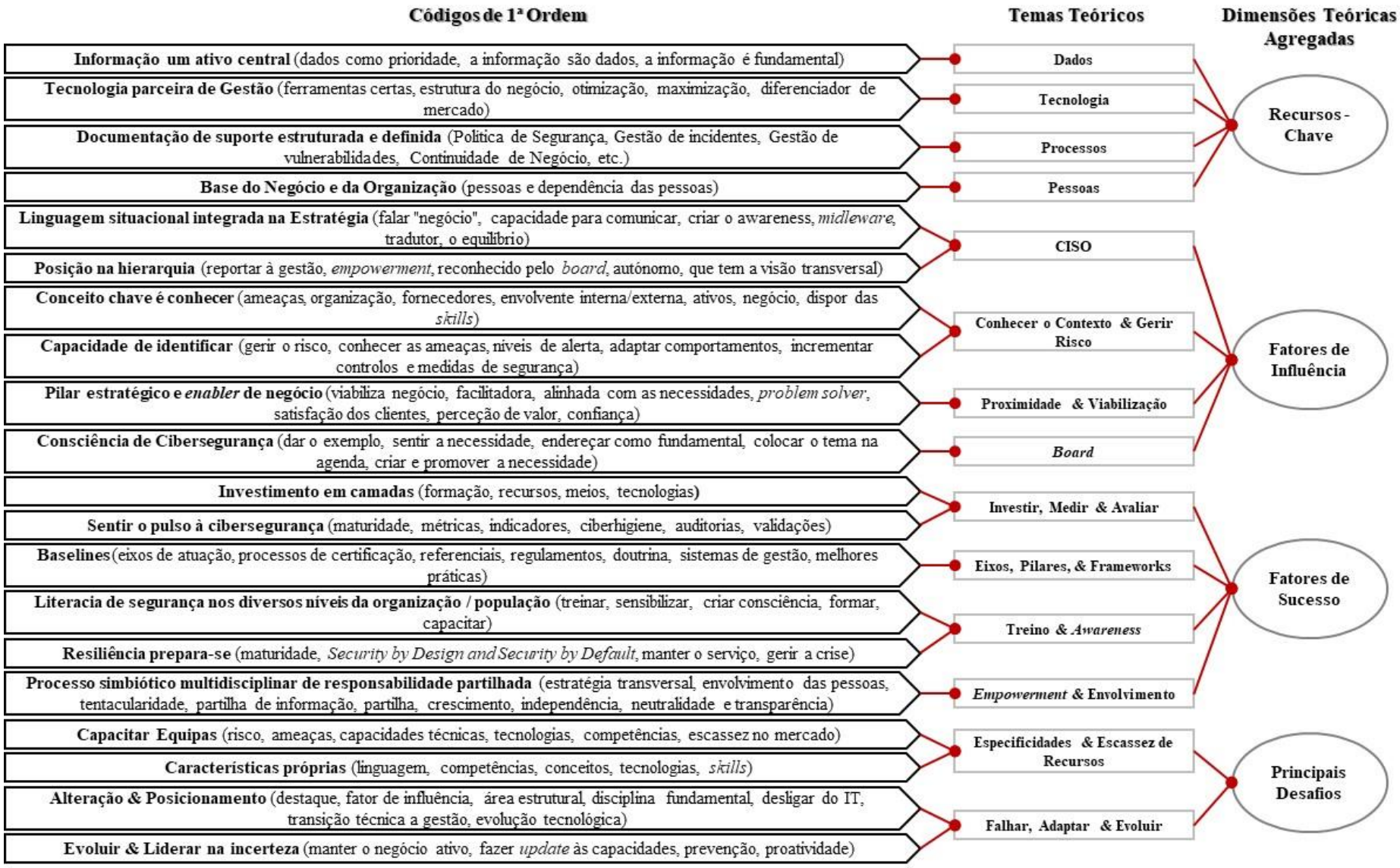

Figura 2: Estrutura de dados

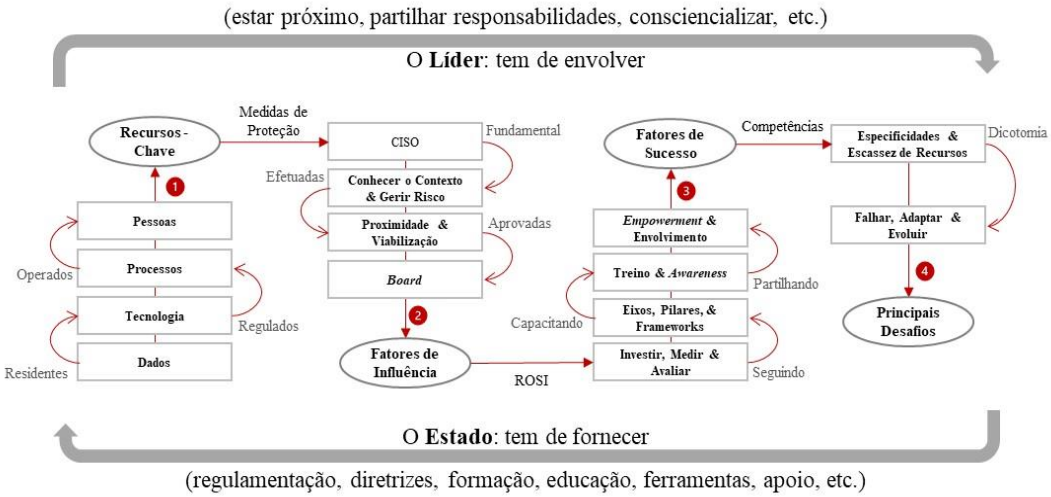

Figura 3: Estrutura de Interação

Ao analisar os dados, tornou-se evidente que os líderes com contacto com a cibersegurança, independentemente da sua função na organização, avaliaram de igual forma os recursos-chave, fatores de influência, fatores de sucesso e principais desafios. Seguindo a literatura (Marques and Santos 2019), questiona-se sobre o papel e a matriz relacional que existe entre cada um. Emergem dois vetores relacionais, igualmente importantes, mas com papéis distintos: numa vertente intrínseca / interna, isto é, com influência sob a organização, o Líder; e numa vertente extrínseca / externa, isto é, com influência sobre a organização, o Estado.

A Figura 3 fornece um quadro de interação entre os recursos-chave, fatores de influência, fatores de sucesso e principais desafios e a Figura 4 a matriz relacional dos fatores de influência da estratégia de cibersegurança.

De uma forma resumida e sistemática, numa lógica de camadas de segurança, todos os líderes descrevem que a definição da estratégia de cibersegurança começa pelo conhecimento profundo do seu negócio, ou seja, por aquilo que querem proteger. Estes recursos-chave traduzem-se nos dados que residem em tecnologia, regulados por processos e operados por pessoas, tendo de se definir medidas para os proteger, determinadas pelos fatores de influência. Na base dos fatores de influência surge o CISO, que é um profundo conhecedor do

contexto e capacidades para efetuar uma boa gestão do risco, cuja existência é fundamental e o papel é facilitado e viabilizado devido à sua proximidade ao negócio e aprovação do *Board*, em alinhamento com a Estratégia, com um custo e por consequência com uma exigência de retorno sob o investimento efetuado (ROSI – *Return on Security Investiment*). Chega-se assim aos fatores de sucesso, ou seja, o investimento tem de ser medido e avaliado, seguindo eixos, pilares e *frameworks* reconhecidas no mercado, sobre as quais as pessoas têm de ser treinadas e consciencializadas para que se sintam envolvidas. E, à semelhança, de outras estratégias, também uma estratégia de cibersegurança, tem desafios, sendo os principais: a escassez de recursos e a dicotomia da falha, adaptação e evolução, isto é, conseguir aprender e crescer com o erro dentro / falha dentro desta área com tantas especificidades. Contanto para isso, por um lado, com o Líder, que tem de envolver toda a organização através da sua proximidade (com as pessoas e com o negócio), partilha de responsabilidade e promoção de consciencialização. E o Estado, por outro, que tem de fornecer apoio, ferramentas, diretrizes, regulamentações, formação e consciencialização transversal para que esta estratégia não seja só organizacional, mas sim nacional.

Para orientar o leitor, resumimos agora as nossas descobertas pelos fatores que influenciam a estratégia de cibersegurança.

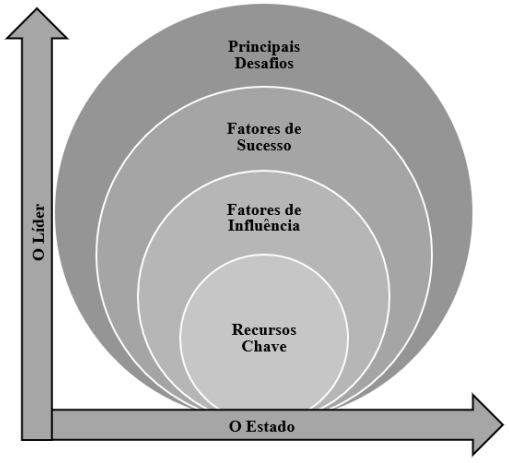

Figura 4: Matriz relacional dos fatores de influência da estratégia de cibersegurança

1) RECURSOS – CHAVE

Os entrevistados definem os recursos-chave como sendo o que norteia o seu negócio e aquilo que é primordial e essencial proteger.

Dados

Dados como um ativo central, sendo a base da informação, torna-se fundamental a sua proteção.

"*(...) é muito importante percebermos primeiro a estrutura de dados que temos na organização, e esse é o primeiro passo*".

[Alexandre Fonseca #03, Co-CEO do Grupo Altice]

"No mundo da digitalização, a segurança da informação é fundamental que nós começamos a ter o ativo de informação central".

[Bruno Soares #11, *Board Adviser* da IDC]

Tecnologia

A tecnologia surge como parceira de Gestão pois são necessárias as ferramentas certas para estruturar e otimizar o negócio para que o mesmo se possa distinguir dos restantes que operam no mesmo segmento de mercado, destacando-se sendo pioneiro e exemplar.

"(...) tenho de ter referenciais, no fundo eu tenho de perceber, perante aquilo que a organização entrega à sociedade, quer seja um produto ou serviço vendável, que processos existem na organização, que pessoas existem na organização, que com a tecnologia fazem produzir aqueles produtos ou serviços".

[Gameiro Marques #15, Diretor do GNS - Gabinete Nacional de Segurança]

Processos

A importância de possuir documentação de suporte estruturada e definida, na qual se incluem

política de segurança, processo de gestão de incidentes, processo de gestão de vulnerabilidades, processos de continuidade de negócio, entre outros.

"A organização tem implementado um conjunto de medidas (…) para proteção de toda a informação. E um conjunto de processos e procedimentos que vamos seguindo para garantir que efetivamente aquilo que vai sendo feito, do ponto de vista da resiliência".

[Luis Martins #04, Vice-Presidente da CIPHER Portugal]

Pessoas

A importância de dar formação, consciencializar e envolver as pessoas, uma vez que a organização e a sua resiliência dependem das mesmas: pessoas como sendo toda a base do Negócio e da Organização.

"Os recursos chave, são claramente as pessoas (…). Eu não tenho condições (…), de desenhar uma estratégia, nem que seja de uma macro, sem perceber a minha organização, sem perceber o meu negócio, sem perceber as minhas pessoas"

[Ricardo Rodrigues #07, Diretor de *Compliance* da Balwurk]

"Por recursos-chave entendemos não só os nossos Arbelievers, portanto, as pessoas que nos ajudam a construir (…) sem dúvida que é uma componente muito importante."

[Margarida Partidário #10, CEO & Founder da Arboreall]

"*Olhando para o nosso negócio, os recursos chave, são sem dúvida as pessoas, cujo a diferenciação do trabalho desenvolvido advém do conhecimento e da experiência, fatores estes que estão nas pessoas e que são difíceis de transferir*".

[Nelson Escrava #12, Diretor de Segurança e Administrador do INOV INESC]

"*Todos os seres humanos, não há nenhum que não seja chave na cibersegurança, desde o rececionista ao Presidente do Conselho de Administração*".

[Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança]

2) FATORES DE INFLUÊNCIA

Os entrevistados definem os fatores de influência como sendo o os elementos que potenciam e contribuem para a implementação de uma estratégia de cibersegurança.

CISO

O CISO (*Chief Information Security Officer*) emerge como o elemento que tem de possuir uma linguagem situacional integrada na Estratégia, isto é, tem de ter uma boa capacidade de comunicar, conseguir falar "negócio" e "técnico" para assim ser o *midleware*, o tradutor, e o que ajuda e contribui para a criação do *awareness* geral, isto é, a construção de uma consciência de cibersegurança partilhada.

"O CISO tem de ser capaz de falar com o IT de forma técnica e detalhada, assim como tem que ser capaz de falar com o board de forma ajustada ao negócio"

[Jorge Vicente #14, CISO do LIDL Portugal]

"*O CISO é quase um middleware que está entre as camadas técnicas e as camadas executivas, e tem que fazer esse balanço de uma forma bastante transparente e bastante pragmática*".

[Nuno Teodoro #16, CISO da HUAWEI]

No entanto, só possível, caso o CISO se encontre numa posição hierárquica com visão transversal da organização e *report* direto à gestão, com o devido *empowerment*, reconhecimento e autonomia dada pelo *board*.

"*Encontrar a pessoa certa. É preciso haver uma empatia de racionalidade entre a Comissão Executiva e o CISO, isto é, a Comissão Executiva tem de confiar no CISO, tanto pela sua honestidade intelectual como pela capacidade de trabalho*."

[Entrevistado #06, CISO de Telecomunicações e/ ou informática]

Conhecer o Contexto & Gerir Risco

Conhecer o contexto surge como sendo o conceito chave, isto é, não é possível influenciar o que não conheço; logo, para a definição da correta estratégia, tenho de conhecer a minha organização/negócio, as ameaças à qual está exposta (o), quem são os meus fornecedores, a envolvente interna/externa, ou seja, o ecossistema no qual me situo.

"*O estabelecimento de uma estratégia implica efetivamente o conhecimento da nossa realidade, o conhecimento da nossa organização e daquilo que existe lá fora."*.

[Hélder Jesus #17, Oficial da Marinha e PhD do Instituto Universitário Militar]

Depois, tenho de ter a capacidade de identificar, ou seja, para efetuar uma boa gestão do risco tenho de conhecer as ameaças e, consequentemente, definir os níveis de alerta, adaptar comportamentos, incrementar controlos e medidas de segurança.

"*Aquilo que nós fazemos, obviamente eu tenho consciência, assim como qualquer pessoa que trabalha nesta área, tenho consciência que nunca nos protegemos a 100%, há sempre riscos, há sempre tentativas de ataque, há sempre ataques que são bem-sucedidos.*"

[Nuno Neves #02, CISO da Associação Nacional de Farmácias]

"*Assumimos que os incidentes vão acontecer e acho que esse é o principal ponto. Nós temos de estar preparados, e face a uma determinada análise de risco e face a um determinado panorama de ameaças, que vamos acompanhando para puder estar preparado porque as ameaças vão-se concretizar* (…) *O tema principal da nossa resiliência, é estar preparados para recuperar, porque os incidentes acontecem"*.

[Nelson Escrava #12, Diretor de Segurança e Administrador do INOV INESC]

Proximidade & Viabilização

A cibersegurança tem de ser vista como um pilar estratégico e *enabler* de negócio, ou seja, tem de viabilizar o negócio, ser facilitadora, estar alinhada com as necessidades, ser um *problem solver*, potenciar a satisfação dos clientes, perceção de valor e a confiança.

"*(…) a cibersegurança não deve ser algo que a organização considere como um problema menor. (…) Isto é, todas as decisões dependem da mesma*".

[Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança]

Board

É fundamental que o *board* tenha uma consciência de Cibersegurança, ou seja, este tem de dar o exemplo, endereçá-la como fundamental, colocar o tema na agenda e acima de tudo criar e promover a necessidade.

"*O Líder (…) tem muita influência na cibersegurança, porque se o líder não está consciente de que algo pode acontecer, ou que tem de ser realizado, não vai acontecer. Porque o líder é a imagem de toda a organização, aliás, a organização rege-se muito pela forma como líder é e como pensa as coisas*".

[Jéssica Domingues #09, CNCS - Certificação no Centro Nacional de Cibersegurança]

"*Senão começar no board, não há nenhuma estratégia de cibersegurança que tenha resiliência ou capacidade de sobrevivência, há de ser sempre um esforço, ou uma luta contínua contra o principal adversário, que é a capacidade de investimento e a disponibilidade de investimento*".

[Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança]

3) FATORES DE SUCESSO

Os entrevistados definem os fatores de sucesso como sendo os elementos que viabilizam a

implementação de uma estratégia de cibersegurança e consolidam a posição da sua organização no mercado.

Investir, Medir & Avaliar

O investimento em cibersegurança deve ser feito por camadas, isto é, investe-se em tecnologias, mas depois têm de se investir nos meios, recursos e formação para operar os mesmos.

"(*...) há um investimento muito grande em tecnologia para ajudar a prevenir as ameaças que foram identificadas como sendo as mais prioritárias."*

[Paulo Rosado #08, CEO da Balwurk]

"*Eu diria que a resiliência tem várias camadas, uma camada mais tecnológica de desenvolvimento de produtos resilientes, uma camada de suporte a esse produto, que gere o ciclo de vida desse produto, que o continua a manter resiliente, e depois uma camada organizacional que, em caso de algo acontecer que potencialmente impacte a resiliência desse produto, sabe responder de uma forma adequada.*"

[Nuno Teodoro #16, CISO da HUAWEI]

O investimento efetuado tem de ser medido para que se possa aferir o seu retorno, isto é, há que sentir o pulso à cibersegurança, para assim perceber o grau de maturidade e ciberhigiene da organização através de métricas, indicadores, auditorias e validações.

"O CISO trabalha com métricas. Métricas essas que são sujeitas ao escrutínio dos seus executores, quer para baixo, quer dos seus pares, que para cima (Comissão Executiva). Dessas métricas há um conjunto de indicadores que são aquelas que num determinado momento o CISO considera relevantes".

[Entrevistado #06, CISO de Telecomunicações e/ ou informática]

"*tem de ter performance indicators, tal como tem para outras áreas (…) enfim, encontrar um conjunto de indicadores que lhe dê o palpitar ou batimento cardíaco sob o ponto de vista de cibersegurança da organização."*

[Gameiro Marques #15, Diretor do GNS - Gabinete Nacional de Segurança]

Eixos, Pilares, & Frameworks

Segundo os entrevistados, tem de haver uma *baseline* (linha orientadora) entendível e de linguagem universal, isto é, um eixo de atuação que siga as melhores práticas, referenciais, regulamentos, doutrina, sistemas de gestão, podendo colmatar num processo de certificação.

"O grande desafio é adaptar todas essas políticas, todos esses processos, todos esses procedimentos, todos esses controlos à nossa estratégia da organização. Ao quê? O negócio e às pessoas (…) porque todo o resto é seguir frameworks."

[Ricardo Rodrigues #07, Diretor de *Compliance* da Balwurk]

"*O principal desafio, uma questão de maturidade das organizações, isto é, maturidade em perceber a necessidade de colocar a cibersegurança como um pilar estratégico do seu negócio (…) Claramente deveria de ser um papel mais ativo e mais proativo. Deveria ser um papel que entendia também enquanto soberania digital, que a cibersegurança é um pilar da nossa sociedade, e não o entende neste momento"*.

[Nuno Teodoro #16, CISO da HUAWEI]

Treino & Awareness

Tem de existir, literacia de segurança nos diversos níveis da organização / população, isto é, as pessoas têm de ser treinadas, formadas e capacitadas para que possam entender e ter sensibilidade para a cibersegurança.

"*Temos de garantir a sensibilização de todas as pessoas, para o que são os temas de segurança, e isso faz-se com comunicação e mais comunicação, e mais comunicação*".

[Nuno Neves #02, CISO da Associação Nacional de Farmácias]

"*Garantir os níveis de conhecimento, de awareness, de consciência aos diversos níveis de organização. Desde os níveis mais baixos, porque são portas de entrada, até aos níveis mais altos, porque são níveis de decisão*".

[Alexandre Fonseca #03, Co-CEO do Grupo Altice]

"*O estado não é relevante, é crítico, não se consegue ter uma sociedade resiliente se o Estado, ele próprio, não tiver investido na educação para a criação dessa resiliência".*

[Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança]

A resiliência prepara-se, ou seja, organizações maduras que incorporem o *Security by Design and Security by Default* conseguem, em caso de eventos disruptivos, manter o serviço enquanto gerem a crise.

"Até situações mais graves ao nível do due diligence ou do due care, nas quais são os próprios responsáveis organizacionais, isto é, de topo, que efetivamente estão um pouco distantes deste tema da segurança".

[Ricardo Rodrigues #07, Diretor de *Compliance* da Balwurk]

Empowerment & Envolvimento

A cibersegurança é um processo simbiótico multidisciplinar de responsabilidade partilhada. Por isso, é importante que a estratégia seja transversal, desenhada com o envolvimento das pessoas. Caracterizada pela sua tentacularidade, partilha de informação, crescimento, independência, neutralidade e transparência.

"*Procuramos precisamente ter na nossa equipa pessoas das mais diversas áreas do conhecimento. E onde é que nos inspiramos para fazer isso, e não foi um processo, mas se nós pensarmos bem, na natureza os ecossistemas mais resilientes são aqueles que têm biodiversidade, porque há umas espécies que se protegem às outras protegem as outras, e que acabam por proteger outras, e assim sucessivamente*".

[Gameiro Marques #15, Diretor do GNS - Gabinete Nacional de Segurança]

4) PRINCIPAIS DESAFIOS

Sendo uma área recente e em constante evolução, os entrevistados referem os principais desafios / fatores de sucesso como sendo os elementos que podem impactar e inviabilizar a estratégia de cibersegurança.

Especificidades & Escassez de Recursos

É fundamental capacitar as Equipas para que as mesmas para fazer face ao risco, ao panorama de ameaças, escassez de recursos no mercado, às especificadas técnicas e tecnológicas.

"Em suma, acho que os dois grandes desafios são o de acompanhar o panorama de ameaças e garantir que os meus investimentos e as minhas decisões sobrevivem às alterações deste panorama, e simultaneamente acompanhar a evolução tecnológica".

[Nelson Escrava #12, Diretor de Segurança e Administrador do INOV INESC]

"*Os desafios continuam a ser os mesmos, ou seja, escolher bem as pessoas, treiná-las, encontrar a capacidade para fazer o investimento e justificá-lo de forma adequada a que o investimento seja o mínimo possível para proteger o máximo de riscos*."

[Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança].

Tendo características próprias no que concerne à linguagem, competências, conceitos, tecnologias e *skills*.

"(…) consequência do crescimento tecnológico, não há recursos humanos suficientes na componente técnica para acompanhar isto, e começam a escassear"

[Hélder Jesus #17, Oficial da Marinha e PhD do Instituto Universitário Militar].

Falhar, Adaptar & Evoluir

A cibersegurança está a mudar. Ao desligar-se do IT está a fazer uma transição da componente mais técnica para abraçar a gestão como uma área estrutural, em linha com a evolução tecnológica, marcando a sua posição através desta alteração.

"*A partir do momento em que a maior parte dos serviços que uma organização presta estão assentes em tecnologia, as preocupações devem estar também na tecnologia que os suportam*".

[Jéssica Domingues #09, CNCS - Centro Nacional de Cibersegurança]

"*(…) e conseguir adaptar a sua organização à medida que o panorama de ameaças muda. O que não é fácil porque nós avaliamos riscos face a ameaças, determinamos controlos, implementamos esses controlos e esses controlos custam, tipicamente, dinheiro (…) Outro dos desafios é a evolução da oferta tecnológica na área de cibersegurança*".

[Nelson Escrava #12, Diretor de Segurança e Administrador do INOV INESC]

Evoluir e liderar na incerteza para que se mantenha o negócio ativo, é necessário ser proativo trabalhar na prevenção e fazer *update* às capacidades.

"*Que vai falhar, (…) eu sei que vai falhar, portanto aqui a preparação é a chave (…) depois o amanhã é voltar a montar, e voltar a tentar recuperar o que se pode, e avançar*."

[Nuno Neves #02, CISO da Associação Nacional de Farmácias]

5 DISCUSSÃO

O interesse em compreender de que forma a Liderança poderia influenciar a definição de uma estratégia e implementação de uma cultura de cibersegurança, e quais os fatores que a influenciam, foi o objetivo do presente estudo, considerando para esse efeito a realidade portuguesa.

Os resultados obtidos confirmaram a relevância e papel fundamental da Liderança (Cleveland and Cleveland 2018). Líderes com consciência de cibersegurança, ao contrário de outros, contribuem positivamente para a definição de uma estratégia e implementação de uma cultura de cibersegurança. (Gale, Bongiovanni, and Slapnicar 2022) demonstraram que o envolvimento dos líderes é fundamental. No entanto, a compreensão dos fatores que conduzem à definição desta estratégia e implementação de uma cultura de cibersegurança nas organizações é em grande parte incompleta.

O presente estudo demonstrou que existem 4 dimensões (ou fatores) e 2 vetores que as organizações deverão ter em conta para a definição de uma estratégia e implementação de uma cultura de cibersegurança.

Todos os entrevistados referiram que a definição de uma estratégia e implementação de uma cultura de cibersegurança é feita por camadas, cujo raio vai aumentando, e com responsabilidade partilhada, ou seja, na base da mesma ficam os recursos-chave, seguidos os fatores de influência, precedidos pelos fatores de sucesso e testados pelos principais desafios, envolvidos pelo estado e o líder.

As conclusões do estudo, relativas às dimensões e vetores, confirmaram o descrito nos referenciais (Marques and Santos 2019) e *frameworks* de cibersegurança (NIST 2023). O conjunto das melhores práticas permite às organizações reduzir o risco associado às ciberameaças, disponibilizando as bases para que qualquer entidade possa, de uma forma voluntária, cumprir os requisitos mínimos de segurança, nas suas diversas componentes,

designadamente, na identificação, proteção, deteção, resposta e recuperação a ciberincidentes, incluindo a organização necessária para a sua gestão.

Os resultados da análise efetuada, permitiram a identificação dos pilares das *frameworks*, que constituem os vetores de trabalho e os objetivos de controlo que são as regras / indicadores pelas quais faço reger o meu sistema preconizado na matriz relacional dos fatores de influência para a definição / implementação de uma estratégia de cibersegurança.

6 CONCLUSÃO

6.1 CONTRIBUIÇÃO TEÓRICA E IMPLICAÇÕES PRÁTICAS DO ESTUDO

A Cibersegurança é definida na literatura como sendo a abordagem e ações associadas ao processo de gestão de risco de segurança, seguido por organizações e estados para proteger a confidencialidade, integridade e disponibilidade dos dados e ativos utilizados no ciberespaço (Schatz, Bashroush, and Wall 2017). Seguindo as melhores práticas de mercado (NIST 2023) a sua estratégia é definida em alinhamento com referenciais e *frameworks* de cibersegurança (Marques and Santos 2019), e suportada por diretrizes, políticas, tecnologias, ferramentas e formação para proporcionar proteção de cibersegurança dos seus utilizadores (Schatz, Bashroush, and Wall 2017).

Ficou claro com este estudo o peso que a Liderança tem na definição de uma estratégia e implementação de uma cultura de cibersegurança e quais os fatores e vetores que a orientam. Liderança esta que se mostra diferente quando comparada com outros líderes de negócio, diferindo dos anteriores por possuírem uma visão articulada entre as ameaças e os ciber-riscos, isto é, uma consciência de cibersegurança (Bueermann et al. 2023). Mas com lacunas tanto a nível de conhecimento (Anderson, Ahmad, and Chang 2022) como a nível das medidas (ou a falta delas) que muitos líderes das organizações tomam para lidar com os ciber-riscos (Aguilar 2014) e com capacidades limitadas ao nível do conselho de administração para o pensamento estratégico e governo nesta área (Dobrygowski and O'Halloran 2017).

Desta forma, considera-se crucial reorientar o princípio de formação e desenvolvimento disponibilizado às Lideranças por forma a capacitá-las, criando, desenvolvendo e reforçando a sua consciência de cibersegurança, em linha com as melhores práticas de cibersegurança, onde o estado acaba por ter um papel fundamental (Parenty and Domet 2019).

6.2 Limitações do Estudo e Sugestões de Investigação Futura

O período disponível para a realização do presente estudo foi relativamente curto levando à opção de uma recolha de dados num único momento por intermédio da realização de um número limitado de entrevistas. Assinala-se, no entanto, o interesse na sua extensão de, obtendo respostas em pelo menos mais um momento, para consolidação/confirmação dos dados anteriores. Como direção de pesquisa futura, fruto de temas emergentes do presente trabalho de investigação propõe-se estudar: (1) A influência do tipo de liderança na definição de uma estratégia de cibersegurança; (2) Os tipos de liderança exercidos pelos CISOs relacionado com o seu papel dentro de cada uma das organizações; (3) O papel do Estado através de um caso de estudo aplicado à Estónia.

6.3 Considerações Finais

Este estudo demonstrou o papel que a Liderança tem sobre a definição de uma estratégia e implementação de uma cultura de cibersegurança. Comprovou que Liderança promove e influencia a definição da estratégia e implementação da cultura, mas que só acontece se a Liderança tiver consciência de cibersegurança. Consciência que se reflete nas 4 dimensões: Recurso-Chave, Fatores de Influência, Fatores de Sucesso e Principais Desafios, segundo 2 vetores: Líder e Estado e se traduz na matriz relacional dos fatores de influência para a definição / implementação de uma estratégia de cibersegurança.

7 REFERÊNCIAS

Aguilar, Luis A. 2014. “Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus.” *Conference New York Stock Exchange*, June 10, 2014.

Anderson, Ashley Baines, Atif Ahmad, and Shanton Chang. 2022. “Competencies of Cybersecurity Leaders: A Review and Research Agenda.” *AIS Electronic Library (AISeL)*, December.

Brocke, Jan Vom, Björn Niehaves, Kai Riemer, Ralf Plattfaut, Martin Hilti Chair, and Alexander Simons. 2009. “Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process.” *ResearchGate*, June.

Bueermann, Gretchen, Seán Doyle, Daniel Dobrygowski, Akshay Joshi, Luna Rohland, Carlos Aguirre, Taylor Browder, Jim Pruitt, Michael Rohrs, and Lauren Stockton. 2023. “Global Cybersecurity Outlook 2023 Insight Report.” *World Economic Forum*, January 2023. https://www.weforum.org/reports.

Bukauskas, Linas, Agnė Brilingaitė, Aušrius Juozapavičius, Daiva Lepaitė, Kęstutis Ikamas, and Rimantė Andrijauskaitė. 2022. “Competencies of Cybersecurity Leaders: A Review and Research.” *Heliyon*. Vol. 9. Elsevier Ltd.

Carafano, James Jay, and Eric Sayers. 2008. “Building Cyber Security Leadership for 21 Cent.” *Backgrounder* 2218 (December).

Cleveland, Simon, and Marisa Cleveland. 2018. “Toward Cybersecurity Leadership Framework.” *AIS Electronic Library (AISeL)*, May, 1–6.

CNCS Observatório de Cibersegurança. 2023. “Relatório Cibersegurança Portugal – Tema Riscos & Conflitos 2023.” *CNCS - Centro Nacional de Cibersegurança*, June 2023. https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf.

Dobrygowski, Daniel, and Derek O’Halloran. 2017. “Future of Digital Economy and Society System Initiative Advancing Cyber Resilience Principles and Tools for

Boards.” *World Economic Forum*, January 2017. https://www.weforum.org/reports.

Gale, Megan, Ivano Bongiovanni, and Sergeja Slapnicar. 2022. “Governing Cybersecurity from the Boardroom: Challenges, Drivers, and Ways Ahead.” *Computers and Security* 121 (102840).

Gioia, Dennis A., Kevin G. Corley, and Aimee L. Hamilton. 2012. “Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology.” *Organizational Research Methods* 16 (1): 15–31.

Hastie, Peter, and Olga Glotova. 2012. *Analysing Qualitative Data*. 1st ed. London: Routledge Taylor & Francis Group.

Heading, Sophie, Saadia. Zahidi, Klaus Schwab, and Borge Brende. 2023. “The Global Risks Report 2023 18th Edition.” *World Economic Forum*, January 2023. https://www.weforum.org/reports.

IBM, Security. 2023. “Cost of a Data Breach Report 2023.” *Copyright IBM Corporation 2023*, July 2023. https://www.ibm.com/reports/data-breach.

Marques, António, and Lino Santos. 2019. “Quadro Nacional de Referência Para a Cibersegurança.” *CNCS - Centro Nacional de Cibersegurança*, 2019. https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf.

Maurer, Tim, and Robert Morgus. 2014. “Compilation of Existing Cybersecurity and Information Security Related Definitions.” *@NEWAMERICA*, October, 1–126.

Microsoft, and Marsh. 2022. “The State of Cyber Resilience.” *Marsh and Microsoft*, 2022. https://www.marsh.com/us/services/cyber-risk/insights/the-state-of-cyber-resilience.html.

Moore, Susan. 2021. “Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021.” *Gartner Newsroom*, May 17, 2021.

https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem.

NIST. 2023. “The NIST Cybersecurity Framework 2.0.” *NIST - National Institute of Standards and Technology*, August 8, 2023. https://www.nist.gov/cyberframework.

Parenty, Thomas J., and Jack J. Domet. 2019. *A Leader´s Guide to Cybersecurity: “Why Boards Need to Lead and How to Do It.”* Edited by Thomas J. Parenty and Jack J. Domet. 1st ed. Boston, MA: Harverd Business Review Press.

Reis, Elizabeth, Paulo Melo, Rosa Andrade, and Teresa Calapez. 1997. *Estatística Aplicada*. 1st ed. Vol. 2. Lisboa: Edições Sílabo, Lda.

Resende, Rui. 2016. “Técnica de Investigação Qualitativa: ETCI.” *Journal of Sport Pedagogy & Research* 2–1: 50–57.

Schatz, Daniel, Rabih Bashroush, and Julie Wall. 2017. “Towards a More Representative Definition of Cyber Security.” *The Journal of Digital Forensics, Security and Law*.

Sim, Julius, Benjamin Saunders, Jackie Waterfield, and Tom Kingstone. 2018. “Can Sample Size in Qualitative Research Be Determined a Priori?” *International Journal of Social Research Methodology*. Routledge.

Stake, Robert E. 1995. *The Art of Case Study Research*. Edited by Robert E. Stake. 1st ed. Vol. I. California: SAGE Publications.

Tajani, A., and G. Ciamba. 2019. “ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA Relevance) Concerning the Definition of Micro, Small and Medium-Sized Enterprises.” *Official Journal of the European*

Union 151 (June): 15–69. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

Tracy, Sarah J. 2013. *Qualitative Research Methods - Collecting Evidence, Crafting Analysis, Communicating Impact*. Edited by John Wiley & Sons. *Wiley-Blackwell*. 1st ed. Malden: Wiley-Blackwell.

8 ANEXOS

8.1 ACRÓNIMOS E DEFINIÇÕES

Conforme mencionado por alguns dos entrevistados "a cibersegurança tem um jargão próprio, o que as vezes torna difícil a sua compreensão" abaixo se listam um conjunto de conceitos[1] fundamentais à compreensão deste trabalho de investigação:

AMEAÇA: Causa potencial de incidente indesejável que pode resultar em danos para uma organização ou qualquer dos sistemas por ela utilizados. Estas ameaças podem ser acidentais ou deliberadas (com dolo) e caracterizam-se por elementos ameaçadores, alvos potenciais e métodos de ataque.

ATAQUE: Qualquer tipo de atividade maliciosa que tenta coletar, perturbar, negar, degradar ou destruir recursos de sistema de informação ou a informação em si.

AVALIAÇÃO DO RISCO: Identificação das ameaças e vulnerabilidades e realização da análise de risco conexa, ou seja, a análise da probabilidade e do impacto.

CIBER: Termo que conota uma relação com as tecnologias da informação.

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.

CIBERESPAÇO: Ciberespaço consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação.

CIBERSEGURANÇA: Conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir

[1] Fonte e informação disponíveis em: https://www.cncs.gov.pt/pt/glossario/

a confidencialidade, integridade e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem.

CNCS: Centro Nacional de Cibersegurança.

DISPONIBILIDADE: Em tecnologias da informação e da comunicação, capacidade de uma unidade funcional permanecer em estado de realizar uma determinada função dentro de condições determinadas, num dado instante ou num dado intervalo de tempo, supondo que estão assegurados os necessários meios exteriores.

ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERSESPAÇO: A ENSC 2019-2023 assenta em três objetivos estratégicos: maximizar a resiliência, promover a inovação e gerar e garantir recursos. As implicações e necessidades associadas a cada um dos objetivos estratégicos permitem definir uma orientação geral e específica, traduzida em seis eixos de intervenção, que enformam linhas de ação concretas destinadas a reforçar o potencial estratégico nacional no ciberespaço.

EVENTO DISRUPTIVO: Que perturba o normal funcionamento da organização ou impede de continuar a dar serviço. Qualquer circunstância, evento ou ação potencial suscetível de danificar, perturbar ou de outro modo afetar negativamente as redes e os sistemas informáticos, os utilizadores desses sistemas e outras pessoas, tendo por base uma "Ciberameaça" (Tradução livre de (Tajani and Ciamba 2019), pág.32).

HACKTIVISTAS: Atores de ameaças "orientados a realizar ações de protesto contra decisões políticas / geopolíticas que afetam matérias nacionais e internacionais.

INCIDENTE: (1) Um evento com um efeito adverso real na segurança das redes e dos sistemas de informação; (2) Ações tomadas através da utilização de uma rede de computadores que resultam num efeito atual ou potencialmente adverso sobre um sistema de informação e/ou a informação aí armazenada.

INFORMAÇÃO: (1) Conhecimento que pode ser comunicado sob qualquer forma; (2) Dados que foram interpretados ou organizados de forma coerente e posteriormente comunicados sendo então possível tirar conclusões do seu significado.

INTEGRIDADE: Garantia de que os dados ou a informação não sejam alterados de modo não autorizado.

MALWARE (SOFTWARE MALICIOSO): 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.

MODELO DE MATURIDADE E CAPACIDADE: Um conjunto de melhores práticas para diagnóstico e avaliação do grau de maturidade de uma organização, no que respeita à aptidão para o desenvolvimento de software. Neste modelo faz-se uma avaliação contínua, identificação de problemas e ações corretivas, dentro de uma estratégia de melhoria dos processos.

NORMA: Em engenharia de software, requisitos obrigatórios utilizados e impostos para atingir uma abordagem disciplinada e uniforme no desenvolvimento de software.

RANSOMWARE: O *Ransomware* representa um tipo de *malware* (vírus, *trojans*, etc.) que infetam os sistemas informáticos dos utilizadores e manipulam o sistema de forma que a vítima não consiga utilizar, parcial ou totalmente, os dados armazenados que estão armazenados. A vítima geralmente recebe um aviso de chantagem por *pop-up*, pressionando a vítima a pagar um resgate para recuperar o acesso total ao sistema e aos arquivos.

RESILIÊNCIA: capacidade de adaptação rápida e/ou recuperação de qualquer tipo de disrupção, para permitir a continuidade das operações a um nível aceitável tendo por base os objetivos de missão e o impacto na segurança.

RISCO: (1) Possibilidade de uma ameaça específica explorar as vulnerabilidades internas e externas de uma organização ou de um dos sistemas por ela utilizados, causando assim danos à organização e respetivos ativos corpóreos ou incorpóreos. Mede-se pela combinação entre a probabilidade de as ameaças ocorrerem e o respetivo impacto.

RISCO DE SEGURANÇA: A probabilidade de as vulnerabilidades inerentes a sistemas de comunicação e informação serem exploradas por ameaças, levando ao comprometimento dos sistemas.

RETURN ON SECURITY INVESTMENT (ROSI)[2]: É a relação entre o benefício monetário de um investimento de segurança e seu custo, isto é, o cálculo do ROSI combina a avaliação quantitativa do risco e o custo da implementação de contramedidas de segurança para mitigação desse risco.

"*SECURITY BY DESIGN*" [3]: Abordagem à segurança tecnológica de um produto TIC desde a sua conceção, procurando integrar no mesmo padrões de segurança de forma holística, criativa, proativa, interdisciplinar, robusta, responsável e integrada no desenho da respetiva arquitetura. É tida como o oposto de "segurança através da obscuridade".

"*SECURITY BY DEFAULT*" [4]: Abordagem à configuração de produtos ou serviços TIC, que garante uma configuração segura desde a sua versão base, ou utilização por defeito, mesmo quando esta não é a mais fácil de utilizar, podendo ser definida por normas ou referenciais extraídos de uma análise do risco e/ou de testes de verificação.

---

[2] https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment

[3] Tradução livre de Cavoukian, A., Dixon, M. (2013). "Privacy and Security by Design: An Enterprise Architecture Approach.", Oracle Corporation, disponível em: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf

[4] Tradução livre: REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity A): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

SEGURANÇA DA INFORMAÇÃO: Proteção dos sistemas de informação contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento, processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não autorizados, incluindo as medidas necessárias para detetar, documentar e contrariar tais ameaças.

TECNOLOGIAS DE INFORMAÇÃO E DE COMUNICAÇÃO (TIC) [5]: Conjunto diversificado de ferramentas e recursos tecnológicos utilizados para transmitir, armazenar, criar, compartilhar ou trocar informação. Essas ferramentas e recursos tecnológicos incluem computadores, a Internet, tecnologias de transmissão, tecnologias de gravação e de telecomunicação (fixa ou móvel, satélite, etc.).

TRATAMENTO DE INCIDENTES: Todos os procedimentos de apoio à deteção, análise e contenção de um incidente, e à resposta ao incidente.

TRATAMENTO DO RISCO: Atenuação, eliminação, redução (mediante uma combinação adequada de medidas técnicas, materiais, organizativas e processuais), transferência ou monitorização do risco.

VULNERABILIDADE [6]: Deficiência no produto ou serviço que pode permitir a exploração de ameaças por pessoas não autorizadas ou criar quebras de segurança. Fraqueza de um sistema informático, revelada por um exame à sua segurança (por exemplo, devido a falhas na análise, conceção, implementação ou operação), que se traduz por uma incapacidade de fazer frente às ameaças informáticas que pesam sobre ele.

WIPERWARE: Classe de *malware* destinada a apagar (limpar), de forma maliciosa dados e programas, do disco rígido ou outra memória estática do computador ou infra estrutura que infeta.

---

[5] Tradução livre: http://uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict

[6] Tradução livre: ISO/IEC 27000:2018, disponível em https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27000:ed-5:v1:en

8.2 CARACTERIZAÇÃO DOS DADOS RECOLHIDOS

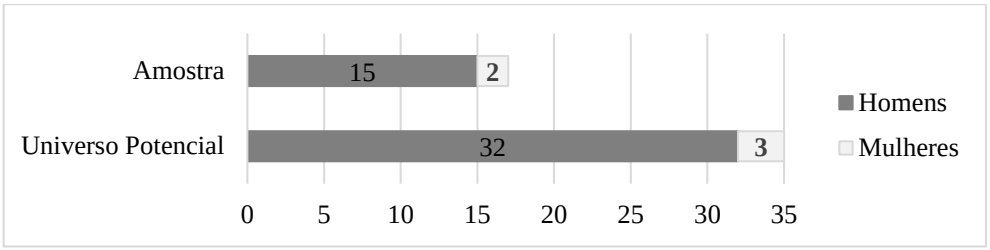

Gráfico 1: Caracterização de género presente na Amostra

Sector de Mercado (INESC)	Qt
Administração Pública	2
Bancos, seguradoras	1
Comércio, Transportes, Distribuição	1
Consultoria	5
Indústria, Produção	1
Militar	1
Outros	2
Saúde	1
Telecomunicações e/ ou informática	3
Total de Organizações	17

Tabela 1: Sectores de Mercado Representados na Amostra

Posição na Organização	Qt
CEO	3
CEO e CISO	1
CISO	5
Co-CEO	1
Diretor de Compliance	1
Diretor de Segurança	1
Diretor de Segurança e Administrador	1
Diretor Geral	1
Oficial e Investigador	1
Regulação, Supervisão e Certificação	1
Vice-Presidente (Portugal)	1
Total	17

Tabela 2: Posições Organizacionais representados na Amostra

Formação de base	Qt
Ciências Militares	1
Engenharia Biomédica	1
Engenharia Informática	8
Engenharia Topográfica	1
Gestão de Sistemas e Tecnologias de Informação	1
Informática	1
Informática e Gestão de Empresas	1
Jurista	1
Licenciatura em Design de Comunicação	1
Oficial da Marinha	1
Total	17

Tabela 3: Formação de base dos Entrevistados

Anos de Experiência	Qt
5 - 10	2
25 - 30	2
20 - 25	7
15 - 20	1
10 - 15	1
> 30	4
Total	17

Tabela 4: Intervalo (em anos) de experiência profissional

Antiguidade na Função	Qt
0 - 5	9
5 - 10	4
10 - 15	2
15 - 20	2
Total	17

Tabela 5: Intervalo (em anos) de antiguidade na função

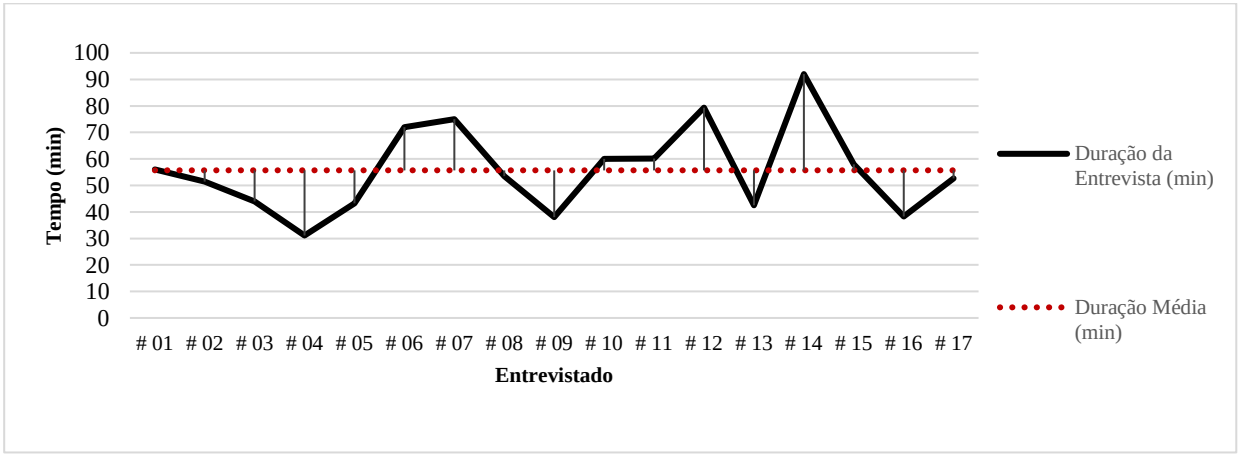

Gráfico 2: Duração (em minutos) das entrevistas realizadas

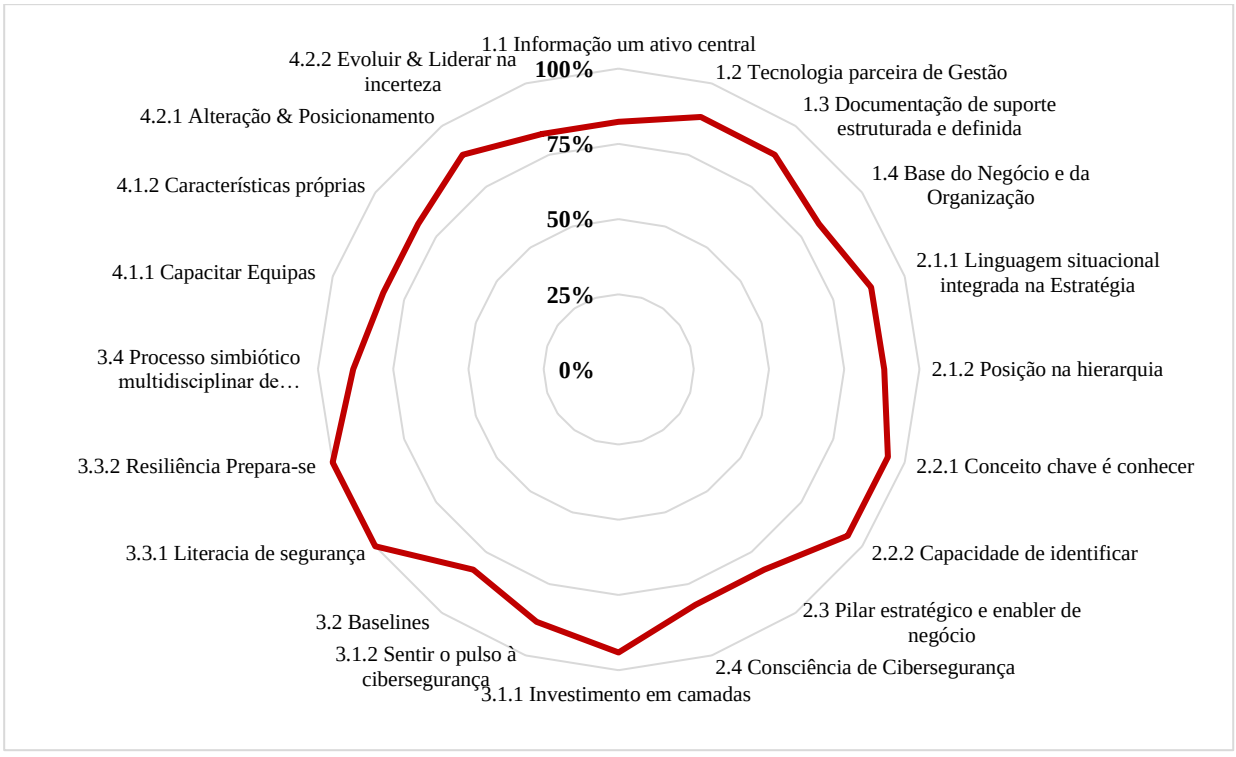

Gráfico 3: Nível de Significância dos Códigos de 1ª ordem

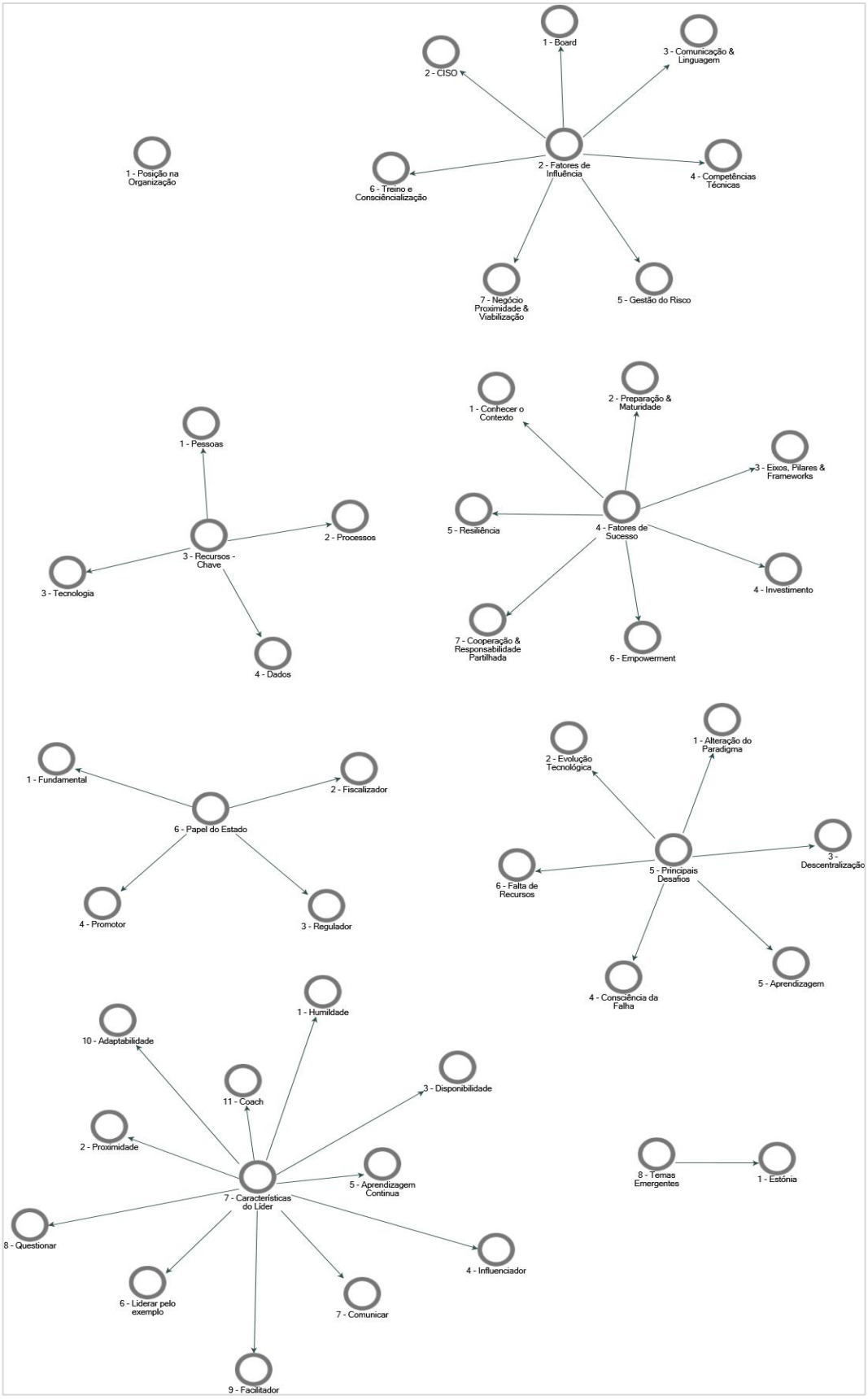

Figura 5: Primeira análise de estrutura de dados (fonte: Nvivo.14)

Códigos (1ªOrdem)	Temas (2ª Ordem)	Dimensões Agregadas
Informação um ativo central (dados como um prioridade, a informação são dados, a informação é fundamental)	Dados	Recursos-Chave
Tecnologia parceira de Gestão (ferramentas certas, estrutura do negócio, otimização, maximização, diferenciador de mercado etc.)	Tecnologia	Recursos-Chave
Documentação de suporte estruturada e definida (Politica de Segurança, Gestão de incidentes, Gestão de vulnerabilidades, Continuidade de Negócio, etc.)	Processos	Recursos-Chave
Base do Negócio e da Organização (pessoas e dependência das pessoas)	Pessoas	Recursos-Chave
Linguagem situacional integrada na Estratégia (falar "negócio", capacidade para comunicar, criar o awareness, midleware, tradutor, o equilibrio)	CISO	Fatores de Influência
Posição na hierarquia (reportar à gestão, empowerment, reconhecido pelo board, autonomo, que tem a visão transversal)	CISO	Fatores de Influência
Conceito chave é conhecer (ameaças, organização, fornecedores, envolvente interna/externa, ativos, negócio, dispor das skills)	Conhecer o Contexto & Gerir Risco	Fatores de Influência
Capacidade de identificar (gerir o risco, conhecer as ameaças, níveis de alerta, adaptar comportamentos, incrementar controlos e medidas de segurança)	Conhecer o Contexto & Gerir Risco	Fatores de Influência
Pilar estratégico e enabler de negócio (viabilizar o negócio, facilitadora, alinhada com as necessidades, *problem solver, s* atisfação dos clientes, percepção de valor, confiança)	Proximidade & Viabilização	Fatores de Influência
Consciência de Cibersegurança (dar o exemplo, sentir a necessidade, endereçar como fundamental, colocar o tema na agenda, criar e promover a necessidade)	Board	Fatores de Influência
Investimento em camadas (formação, recursos, meios, tecnologias)	Investir, Medir & Avaliar	Fatores de Sucesso
Sentir o pulso à cibersegurança (maturidade, métricas, indicadores, ciberhigiene, auditorias, validações)	Investir, Medir & Avaliar	Fatores de Sucesso
Baselines (Eixos de atuação, processos de certificação, refrenciais, regulamentos, doutrina, sistemas de gestão, melhores práticas, etc.)	Eixos, Pilares e Frameworks	Fatores de Sucesso
Literacia de segurança nos diversos niveis da organização / população (treinar, sensibilizar, criar consciência, formar, capacitar)	Treino & Awareness	Fatores de Sucesso
Resiliência Prepara-se (maturidade, *Security by Design and Security by Default* , manter o serviço, gerir a crise)	Treino & Awareness	Fatores de Sucesso
Processo simbiótico multidisciplinar de responsabilidade partilhada (estratégia transversal, envolvimento das pessoas, tentacularidade, partilha de informação, partilha, crescimento, independência, neutralidade e transparência)	Empowerment & Envolvimento	Fatores de Sucesso
Capacitar Equipas (risco, ameaças, capacidades técnicas, tecnologias, competências, escassez no mercado)	Especificidades & Escassez de Recursos	Principais Desafios
Características próprias (linguagem, competências, conceitos, tecnologias, skills, etc)	Especificidades & Escassez de Recursos	Principais Desafios
Alteração & Posicionamento (destaque, fator de influência, área estrutural, disciplina fundamental, desligar do IT, transição técnica a gestão, evolução tecnológica)	Falhar, Adaptar & Evoluir	Principais Desafios
Evoluir & Liderar na incerteza (manter o negócio ativo, fazer update às capacidades, prevenção, proatividade)	Falhar, Adaptar & Evoluir	Principais Desafios

Tabela 6: Estrutura de dados final

Códigos (1ªOrdem)	#01	#02	#03	#04	#05	#06	#07	#08	#09	#10	#11	#12	#13	#14	#15	#16	#17
1.1 Informação um ativo central	1	1	x	1	1	1	1	1	1	0	x	0	0	1	1	1	1
1.2 Tecnologia parceira de Gestão	0	1	1	0	1	1	x	x	1	1	x	1	1	1	x	1	1
1.3 Documentação de suporte estruturada e definida	1	1	1	x	1	1	1	1	1	1	1	1	0	x	1	1	0
1.4 Base do Negócio e da Organização	1	1	1	0	x	0	x	1	1	x	0	x	x	1	x	1	1
2.1.1 Linguagem situacional integrada na Estratégia	x	1	1	1	x	x	1	1	1	0	1	0	1	x	1	x	1
2.1.2 Posição na hierarquia	1	1	x	1	1	1	1	1	1	0	1	0	1	1	x	1	1
2.2.1 Conceito chave é conhecer	1	1	x	0	1	x	x	1	1	1	1	1	x	1	1	1	x
2.2.2 Capacidade de identificar	x	x	1	0	1	1	x	1	x	1	1	x	1	1	1	1	1
2.3 Pilar estratégico e enabler de negócio	x	x	1	1	1	1	1	0	0	1	1	1	x	1	x	1	0
2.4 Consciência de Cibersegurança	0	1	x	1	0	1	1	1	x	x	x	1	x	0	1	1	1
3.1.1 Investimento em camadas	1	1	x	1	1	x	1	x	1	1	1	1	1	1	0	x	1
3.1.2 Sentir o pulso à cibersegurança	1	1	1	1	1	1	x	1	1	0	0	1	1	x	x	1	1
3.2 Baselines	1	1	1	1	1	1	x	1	1	0	0	1	0	1	1	x	1
3.3.1 Literacia de segurança	1	x	x	1	1	1	1	1	1	1	1	x	x	1	x	1	1
3.3.2 Resiliência Prepara-se	1	1	x	1	x	1	x	x	1	1	x	1	1	1	1	x	1
3.4 Processo simbiótico multidisciplinar de responsabilidade partilhada	1	1	x	1	x	0	x	1	1	1	0	1	1	x	x	x	1
4.1.1 Capacitar Equipas	1	1	1	0	1	0	x	1	1	0	1	x	x	1	1	1	x
4.1.2 Características próprias	1	1	x	0	x	1	1	1	0	1	1	x	0	x	1	1	1
4.2.1 Alteração & Posicionamento	1	1	x	1	1	x	1	1	x	x	1	x	1	1	0	0	1
4.2.2 Evoluir & Liderar na incerteza	1	x	x	1	0	1	x	1	1	1	1	x	1	0	0	1	1

0	O Entrevistado **não** referiu o código (1ª Ordem)
1	O Entrevistado referiu o código (1ª Ordem)
x	O Entrevistado referiu o código (1ª Ordem) e há excerto transcrito na presente tese

Tabela 7: Códigos de 1ª ordem, por Entrevistado

8.3 Dados de Apoio ao Tema "o Papel da Liderança na Construção de uma Cultura de Cibersegurança"

Códigos 1ª Ordem	Citações Representativas[7]
1.1 Informação um ativo central (dados como prioridade, a informação como um conjunto de dados, a informação é fundamental)	**1.** "*Antes de dizemos quais são as nossas joias da coroa, é muito importante percebermos primeiro a estrutura de dados que temos na organização, e esse é o primeiro passo*" – Alexandre Fonseca #03, Co-CEO do Grupo Altice (https://www.altice.pt/pt). **2.** "*As pessoas não percebem que se calhar, ao pagar um ransomware, estão a financiar uma organização terrorista, um Estado- nação, que que é menos escrupuloso, ou seja , esta falta de literacia para perceber qual é o impacto, de quanto é que valem os nossos dados, e valem dinheiro na Dark Web, e nesses fóruns, se forem dados de saúde, têm um valor ainda mais alto do que se for de outro tipo*." - Paulo Rosado #08, CEO da Balwurk (https://balwurk.com/). **3.** *"No mundo da digitalização, a segurança da informação é fundamental que nós começamos a ter o ativo de informação central"* – Bruno Soares #11, *Board Adviser* da IDC (https://idcportugal.com/).

[7] **Os *owners* das *quotes* (citações) estão identificados segundo o seguinte padrão**: Nome do entrevistado (p.e. Ricardo Rodrigues), ordem da entrevista (p.e. #07), cargo / posição ocupada (p.e. *Head of GRC*) e nome da organização (p.e. Balwurk). Entrevistados que não autorizam a sua identificação, querendo permanecer anónimos, são designados por "Entrevistado", mantendo a referência à ordem da execução da entrevista, indicando-se o seu cargo / posição na organização a qual também acaba por ficar anonimizada porque o nome é substituído pelo seu sector de atividade conforme classificação INE (Instituto Nacional de Estatística).

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
1.2 Tecnologia parceira de Gestão (ferramentas certas, estrutura do negócio, otimização, maximização, diferenciador de mercado)	**1.** *"O Estado não deve ajudar a impulsionar este desenvolvimento, o Estado deve fazer parte da solução também. O Estado deve ser fator integrante e deve garantir que as organizações têm todas as ferramentas necessárias e toda a informação necessária para conseguirem desenvolver o seu Trabalho Interno"* – Ricardo Rodrigues #07, Diretor de Compliance da Balwurk (https://balwurk.com/). **2.** *Portanto, se nós falarmos de objetivamente estratégia de cibersegurança, e se cibersegurança for mesmo cibersegurança, então nós estamos a falar de um movimento estratégico que é absolutamente necessário, porque a tecnologia passa a ser a plataforma de negócio da organização.* – Bruno Soares #11, Board Adviser da IDC (https://idcportugal.com/). **3.** *"Na minha opinião eu tenho de ter referenciais, no fundo eu tenho de perceber, perante aquilo que a organização entrega à sociedade, quer seja um produto ou serviço vendável, que processos existem na organização, que pessoas existem na organização, que com a tecnologia fazem produzir aqueles produtos ou serviços, e depois na tecnologia tem de perceber que riscos é que aquela tecnologia tem."* - Gameiro Marques #15, Diretor do Gabinete Nacional de Segurança (https://www.gns.gov.pt/).

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
1.3 Documentação de suporte estruturada e definida (Política de Segurança, Gestão de incidentes, Gestão de vulnerabilidades, Continuidade de Negócio, etc.)	**1.** *"A organização tem implementado um conjunto de medidas, quer técnicas, quer organizativas, quer tecnológicas, para proteção de toda a informação. E um conjunto de processos e procedimentos que vamos seguindo para garantir que efetivamente aquilo que vai sendo feito, do ponto de vista da resiliência, tem um mapeamento que nos permita ter conforto naquilo que estamos a fazer"* – Luis Martins #04, Vice-Presidente da CIPHER Portugal (https://cipher.com/pt/). **2.** "*A forma mais correta é envolver as pessoas nos processos, na definição dos processos, na identificação da maturidade e na evolução das pessoas, perceberem como é que estão a evoluir*" – Jorge Vicente #14, CISO do LIDL Portugal (https://www.lidl.pt/).
1.4 Base do Negócio e da Organização (pessoas e dependência das pessoas)	**1.** "*Aqueles que apresentam um risco mais elevado para o nosso negócio*" – Entrevistado#05, Diretor de Segurança do Sector Financeiro. **2.** *"Os recursos chave, são claramente as pessoas e o negócio, não descurando os restantes ativos de toda a organização, mas focam-se essencialmente nestes. Eu não tenho condições (…), de desenhar uma estratégia, nem que seja de uma macro, sem perceber a minha organização, sem perceber o meu negócio, sem perceber as minhas pessoas"* – Ricardo Rodrigues #07, Diretor de *Compliance* da Balwurk

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	(https://balwurk.com/). **3.** "*Por recursos-chave entendemos não só os nossos Arbelievers, portanto, as pessoas que nos ajudam a construir, quer seja, a nível de pensamento, quer seja a nível de desenvolvimento tecnológico, sem dúvida que é uma componente muito importante.*" – Margarida Partidário #10, CEO & Founder da Arboreall (https://arboreall.com/#/). **4.** "*Olhando para o nosso negócio, os recursos chave, são sem dúvida as pessoas, cujo a diferenciação do trabalho desenvolvido advém do conhecimento e da experiência, fatores estes que estão nas pessoas e que são difíceis de transferir*" – Nelson Escrava #12, Diretor de Segurança e Administrador do INOV INESC Inovação (https://www.inov.pt/index.html). **5.** "*Todos os seres humanos, não há nenhum que não seja chave na cibersegurança, desde o rececionista ao Presidente do Conselho de Administração, passando, obviamente pelos técnicos.*" – Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança. **6.** "*A resiliência das organizações não se mede exclusivamente pela forma como elas protegem, na dimensão digital. A resiliência das organizações mede-se sobretudo por aquilo que já referi há pouco em resposta à sua pergunta dos*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	elementos-chave de uma organização e que referi serem as pessoas" – Gameiro Marques #15, Diretor do Gabinete Nacional de Segurança (https://www.gns.gov.pt/).
2.1.1 Linguagem situacional integrada na Estratégia (falar "negócio", capacidade para comunicar, criar o awareness, midleware, tradutor, o equilíbrio)	**1.** "*Talvez tenhamos a influência da cibersegurança na liderança, ou seja, eu acho que a tomada de decisão do líder, como vimos atrás, deve ser realizada tendo presente as inúmeras variáveis da liderança e da gestão, em que a cibersegurança tem de ser uma delas*. (…) *Na cibersegurança eu acho que deve de ser o mesmo, nós devemos ter um nível mínimo básico, que tem de sempre influenciar a gestão e a liderança, mas depois há alturas em que a componente de cibersegurança pode tomar uma relevância muito maior no que toca à tomada de decisão dos líderes*" – Alexandre Fonseca #03, Co-CEO do Grupo Altice (https://www.altice.pt/pt). **2.** "*O líder de segurança, a meu ver é, tem de ter a capacidade de equilibrar as necessidades do negócio com as necessidades internas da organização*" - Entrevistado#05, Diretor de Segurança do Sector Financeiro. **3.** "*Encontrar a pessoa certa. É preciso haver uma empatia de racionalidade entre a Comissão Executiva e o CISO, isto é, a Comissão Executiva tem de confiar no CISO, tanto pela sua honestidade intelectual como pela capacidade de trabalho*."

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	– Entrevistado #06, CISO de Telecomunicações e/ ou informática. **4.** *"O CISO tem de ser capaz de falar com o IT de forma técnica e detalhada, assim como tem que ser capaz de falar com o board de forma ajustada ao negócio*" – Jorge Vicente #14, CISO do LIDL Portugal (https://www.lidl.pt/). **5.** "*O CISO é quase um middleware que está entre as camadas técnicas e as camadas executivas, e tem que fazer esse balanço de uma forma bastante transparente e bastante pragmática*" – Nuno Teodoro #16, CISO da HUAWEI (https://www.huawei.com/en/). **6.** "*Nem todos os CISOs são iguais, porque nem todas as organizações são iguais, nem todos os requisitos e necessidades das organizações são iguais. Se tu fores falar com um CISO de uma ONG, a sua perspetiva de negócio totalmente diferente, se fores falar com um CISO de uma empresa de um qualquer setor altamente regulado. Mas, independentemente da diferenciação setorial, na minha opinião, é inevitável que um CISO tenha de conseguir falar uma linguagem desde a parte mais técnica, como um tradutor para a parte estratégica do negócio.*" – Nuno Teodoro #16, CISO da HUAWEI (https://www.huawei.com/en/).
2.1.2 Posição na	**1.** "*O CISO é alguém que tem um empowerment dentro da*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
hierarquia (reportar à gestão, empowerment, reconhecido pelo board, autónomo, que tem a visão transversal)	*organização, que está mesmo que hierarquicamente não tenha uma linha direta de report ao CEO, tem uma linha de report direto a pelo menos um membro da comissão executiva*" – Alexandre Fonseca #03, Co-CEO do Grupo Altice (https://www.altice.pt/pt). **2.** "*O CISO deve saber comunicar com o board, para que se transmita à organização o que se pretende no que à cibersegurança diz respeito.*" – Gameiro Marques #15, Diretor do Gabinete Nacional de Segurança (https://www.gns.gov.pt/).
2.2.1 Conceito chave é conhecer (ameaças, organização, fornecedores, envolvente interna/externa, ativos, negócio, dispor das skills)	**1.** "*O conceito chave é conhecer, nós nunca podemos, enquanto líderes, influenciar algo que não conhecemos."* - Alexandre Fonseca #03, Co-CEO do Grupo Altice (https://www.altice.pt/pt). **2.** "*Portanto, nós temos de lidar com a cibersegurança como, aliás eu chamo-lhe "ciber-insegurança", a minha doutrina está muito orientada, à "ciber-insegurança", porque nós temos de fazer uma empresa viver, de forma racional e adequada perante a insegurança do contexto em que vivemos.*" – Entrevistado #06, CISO de Telecomunicações e/ ou informática. **3.** *"É estaremos preparados, termos um tal conhecimento de nós próprios e, portanto, das nossas organizações, do nosso*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	negócio e das nossas pessoas, que nos faz definir uma estratégia que implemente processos, tecnologia, controlos que nos permitem de uma forma rápida e eficaz, voltar ao nosso estado normal de funcionamento, após sermos sujeitos a um evento inesperado, incerto, que é precisamente essas ameaças, é o nosso risco." – Ricardo Rodrigues #07, Diretor de *Compliance* da Balwurk (https://balwurk.com/). **4.** "*Primeiro o líder te de ser consciência da necessidade, (…) não necessita de ter formação especifica, tem sim de perceber todos os contextos da cibersegurança*" – Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança. **5.** "*O estabelecimento de uma estratégia implica efetivamente o conhecimento da nossa realidade, o conhecimento da nossa organização e daquilo que existe lá fora."* – Hélder Jesus #17, Oficial da Marinha e Investigador (PhD) do Instituto Universitário Militar (https://www.ium.pt/).
2.2.2 Capacidade de identificar (gerir o risco, conhecer as ameaças, níveis de alerta, adaptar comportamentos, incrementar	**1.** *"A influência da gestão de topo na segurança, é significativa, pela afetação de meios, pela afetação de recursos*." – José Casinha #01, CISO da Outsystems (https://www.outsystems.com/). **2.** "*Se acho que é resiliente, espero que sim, senão não durmo descansado. Portanto, espero que vá sendo resiliente. Aquilo que nós fazemos, obviamente eu tenho consciência, assim*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
controlos e medidas de segurança)	*como qualquer pessoa que trabalha nesta área, tenho consciência que nunca nos protegemos a 100%, há sempre riscos, há sempre tentativas de ataque, há sempre ataques que são bem-sucedidos.*" – Nuno Neves #02, CISO da Associação Nacional de Farmácias (http://www.anf.pt). **3.** "*Porque falar de segurança é falar de risco, é falar de gestão de risco, é saber o quanto as nossas organizações estão a identificar ou têm identificado o seu apetite ao risco, e só a partir daí é que se pode começar a definir todos os restantes processos a nível de segurança*" – Ricardo Rodrigues #07, Diretor de *Compliance* da Balwurk (https://balwurk.com/). **4.** *"Eu diria que os principais desafios em relação à cibersegurança é o aumento da área de risco, a partir desse momento, aumenta-se o número e a e a diversidade de ameaças, e ao mesmo tempo, lidando com a falta de conhecimento e de recursos, no qual rapidamente tiveram de progredir para uma área de tecnologias de informação no qual não tinham as suas bases bem assentes. Diria assim que estes são os principais desafios."* Jéssica Domingues #09, Regulação, Supervisão e Certificação no Centro Nacional de Cibersegurança (https://www.cncs.gov.pt/). **5.** "*Assumimos que os incidentes vão acontecer e acho que esse é o principal ponto. Nós temos de estar preparados, e face a*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	uma determinada análise de risco e face a um determinado panorama de ameaças, que vamos acompanhando para puder estar preparado porque as ameaças vão-se concretizar, mesmo que não seja hoje, pode ser amanhã, porque sabemos que os incidentes acontecem. E face a isso, apostar na recuperação, ou seja, garantir que temos os meios alternativos disponíveis para recuperar caso as ameaças se materializem. (…) *O tema principal da nossa resiliência, é estar preparados para recuperar, porque os incidentes acontecem."* – Nelson Escrava #12, Diretor de Segurança e Administrador do INOV INESC Inovação (https://www.inov.pt/index.html). **6.** "*Em suma a cibersegurança tem de estar alinhada com o risco, o risco tem de estar alinhado com o negócio, e sem haver uma análise de risco adequada a cibersegurança vais ser um custo demasiado elevado e injustificável ou errado.*" – Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança.
2.3 Pilar estratégico e *enabler* de negócio (viabiliza negócio, facilitadora,	**1.** "*A abordagem de segurança na OutSystems teria de ser um enabler de negócio como primeiro fator. Pois sendo um enabler de negócio eu consigo ter amplificadores da minha voz, no bom sentido. Ou seja, quero ter amplificadores da importância da segurança no negócio*" – José Casinha #01,

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
alinhada com as necessidades, *problem solver*, satisfação dos clientes, perceção de valor, confiança)	CISO da Outsystems (https://www.outsystems.com/). **2.** "*Exatamente porque, a ANF, entendeu que a cibersegurança é um tema que tem ligação direta com o negócio.*" – Nuno Neves #02, CISO da Associação Nacional de Farmácias (http://www.anf.pt). **3.** "*Eu tenho como ideia, desde há muito tempo, de que a cibersegurança não deve ser algo que organização considere como um problema menor. (…) Isto é, todas as decisões dependem da mesma, e da equipa de topo, que é basicamente a gerência*." – Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança. **4.** "*Temos de olhar para a cibersegurança como um business enabler, e por isso tem de ter performance indicators, tal como tem para outras áreas, p.e, vendas, produção, taxa de execução de orçamento."* – Gameiro Marques #15, Diretor do Gabinete Nacional de Segurança (https://www.gns.gov.pt/).
2.4 Consciência de Cibersegurança (dar o exemplo, sentir a necessidade, endereçar como fundamental, colocar o tema na	**1.** *"Primeiro o líder tem de conhecer para poder interiorizar, depois para poder influenciar, e tem de influenciar dois níveis, a gestão da organização e toda população. E para o fazer, mais uma vez, temos de voltar ao início, ele tem de conhecer e manter-se atualizado."* - Alexandre Fonseca #03, Co-CEO do Grupo Altice (https://www.altice.pt/pt). **2.** "*O Líder é fundamental, tem muita influência na*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
agenda, criar e promover a necessidade)	*cibersegurança, porque se o líder não está consciente de que algo pode acontecer, ou que tem de ser realizado, não vai acontecer. Porque o líder é a imagem de toda a organização, aliás, a organização rege-se muito pela forma como líder é e como pensa as coisas*" – Jéssica Domingues #09, Regulação, Supervisão e Certificação no Centro Nacional de Cibersegurança (https://www.cncs.gov.pt/). **3.** "*Nós somos muito pequenos, mas há em boa parte por aquilo que é a minha preocupação, vamos tomando estas medidas, aflige-me que empresas com outros recursos ou com outra envergadura não sintam a preocupação multiplicada por 100, porque eles têm muito mais a perder que nós convenhamos. Ou seja, o negócio deles pode sofrer uma pancada brutal. (…) se fala tanto os gestores supostamente têm acesso a uma formação de excelência, contactam e comunicam com outros que também estão a liderar outros negócios. O que é que está a falhar nesta adesão rápida aos serviços de cibersegurança?*" – Margarida Partidário #10, CEO & Founder da Arboreall (https://arboreall.com/#/). **4.** "*Se a organização está preocupada com a resiliência, então a primeira preocupação começa ao nível da governança, começa ao nível da Administração*" – Bruno Soares #11, *Board Adviser* da IDC (https://idcportugal.com/).

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	5. "*Sendo que, senão começar no board, não há nenhuma estratégia de cibersegurança que tenha resiliência ou capacidade de sobrevivência, há de ser sempre um esforço, ou uma luta contínua contra o principal adversário, que é a capacidade de investimento e a disponibilidade de investimento*" – Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança.
3.1.1 Investimento em camadas (formação, recursos, meios, tecnologias)	**1.** "*Agora depois esta questão, é uma questão de cebola, é uma questão das várias capas, depois de vermos o interior, e vamos indo cada vez mais para fora da cebola, vamos chegar obviamente a área que são menos relevantes, agora, depois depende, e como bem sabemos, pois nós já falamos sobre isso no passado, aqui a questão é uma questão de custo-benefício, uma vez mais. Quanto é que custa proteger mais camadas exteriores dessa cebola, e se vale ou não vale a pena, até chegar ao ponto em que nós dizemos, que se calhar aqui, nós não podemos, queremos, mas não podemos lá chegar, pois o nível de investimento é demasiado elevado*" – Alexandre Fonseca #03, Co-CEO do Grupo Altice (https://www.altice.pt/pt). **2.** "*Para que isto possa acontecer tem de haver investimento. Temos de investir em tecnologia, temos de ter processos e como tal o CISO tem de ter a tal responsabilidade de garantir*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	oversight do equilíbrio de todas estas dimensões" – Entrevistado #06, CISO de Telecomunicações e/ ou informática. **3.** "(*...) há um investimento muito grande em tecnologia para ajudar a prevenir as ameaças que foram identificadas como sendo as mais prioritárias."* – Paulo Rosado #08, CEO da Balwurk (https://balwurk.com/). **4.** "*Eu diria que a resiliência tem várias camadas, uma camada mais tecnológica de desenvolvimento de produtos resilientes, uma camada de suporte a esse produto, que gere o ciclo de vida desse produto, que o continua a manter resiliente, e depois uma camada organizacional que, em caso de algo acontecer que potencialmente impacte a resiliência desse produto, sabe responder de uma forma adequada.*" – Nuno Teodoro #16, CISO da HUAWEI (https://www.huawei.com/en/).
3.1.2 Sentir o pulso à cibersegurança (maturidade, métricas, indicadores, ciberhigiene, auditorias,	**1.** *"O CISO é o garante da doutrina, nas suas diversas facetas. Para o efeito, o CISO trabalha com métricas. Métricas essas que são sujeitas ao escrutínio dos seus dos executores, quer para baixo, quer dos seus pares, que para cima (Comissão Executiva). Dessas métricas há um conjunto de indicadores que são aquelas que num determinado momento o CISO considera relevantes. O CISO tem de ser responsável da*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
validações)	*doutrina, tem que assegurar a componente de compliance do ponto de vista formal"* – Entrevistado #06, CISO de Telecomunicações e/ ou informática. **2.** "*O Estado deve agir como regulador, nivelador e auditor na perspetiva de aplicar coimas quando efetivamente as empresas não estão a cumprir com os requisitos mínimos para o seu setor ou para a sua dimensão*" – Jorge Vicente #14, CISO do LIDL Portugal (https://www.lidl.pt/). **3.** "*Temos de olhar para a cibersegurança como um business enabler, e por isso tem de ter performance indicators, tal como tem para outras áreas, p.e, vendas, produção, taxa de execução de orçamento (…) enfim, encontrar um conjunto de indicadores que lhe dê o palpitar ou batimento cardíaco sob o ponto de vista de cibersegurança da organização."* – Gameiro Marques #15, Diretor do Gabinete Nacional de Segurança (https://www.gns.gov.pt/).
3.2 Baselines (eixos de atuação, processos de certificação, referenciais, regulamentos, doutrina, sistemas	**1.** *"O grande desafio é adaptar todas essas políticas, todos esses processos, todos esses procedimentos, todos esses controlos à nossa estratégia da organização. Ao quê? O negócio e às pessoas. É isso que não é feito por qualquer um, porque todo o resto é seguir frameworks."* – Ricardo Rodrigues #07, Diretor de *Compliance* da Balwurk (https://balwurk.com/).

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
de gestão, melhores práticas)	**2.** "*O principal desafio, uma questão de maturidade das organizações, isto é, maturidade em perceber a necessidade de colocar a cibersegurança como um pilar estratégico do seu negócio (…) Claramente deveria de ser um papel mais ativo e mais proativo. Deveria ser um papel que entendia também enquanto soberania digital, que a cibersegurança é um pilar da nossa sociedade, e não o entende neste momento."* – Nuno Teodoro #16, CISO da HUAWEI (https://www.huawei.com/en/).
3.3.1 Literacia de segurança nos diversos níveis da organização / população (treinar, sensibilizar, criar consciência, formar, capacitar)	**1.** "*Temos de garantir a sensibilização de todas as pessoas, para o que são os temas de segurança, e isso faz-se com comunicação e mais comunicação, e mais comunicação*." – Nuno Neves #02, CISO da Associação Nacional de Farmácias (http://www.anf.pt). **2.** "*Garantir os níveis de conhecimento, de awareness, de consciência aos diversos níveis de organização. Desde os níveis mais baixos, porque são portas de entrada, até aos níveis mais altos, porque são níveis de decisão*" – Alexandre Fonseca #03, Co-CEO do Grupo Altice (https://www.altice.pt/pt). **3.** *"A ausência de literacia digital, ou a ilusória literacia digital é um dos fatores mais importantes para a ciber insegurança, ou seja, uma razão para nós estarmos vulneráveis. Porque a*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	maior parte dos ciberataques, ou cibercrime, explora uma fronteira de confiança entre o ser humano e a tecnologia, atividade que designamos de engenharia social. Estes (atacantes) exploram a confiança que o ser humano deposita na tecnologia." – Nelson Escrava #12, Diretor de Segurança e Administrador do INOV INESC Inovação (https://www.inov.pt/index.html). **4.** "*O estado não é relevante, é crítico, não se consegue ter uma sociedade resiliente se o Estado, ele próprio, não tiver investido na educação para a criação dessa resiliência."* – Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança. ***3.*** "*Há determinados princípios fundamentais de liderança, mas um líder que incorpore na sua matriz de liderança a cibersegurança, tem de se modificar. Um exercício de liderança atualmente é um exercício de cooperação, de colaboração, com visão, mas temos de saber que temos de ir com alguém, que não conseguimos fazer nada sozinhos. Na cibersegurança, e a mesma coisa, é muito difícil fazer alguma coisa sozinhos*" – Gameiro Marques #15, Diretor do Gabinete Nacional de Segurança (https://www.gns.gov.pt/).
3.3.2 Resiliência Prepara-se	**1.** *"A resiliência é uma composição de duas variáveis: o Passado e o Presente"* – Alexandre Fonseca #03, Co-CEO do

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
(maturidade, *Security by Design and Security by Default*, manter o serviço, gerir a crise)	Grupo Altice (https://www.altice.pt/pt). **2.** "*A análise do que é que falhou? Porque é que falhou? O que é que devia ser diferente para não falhar novamente? Isto é exatamente o amanhã, o dia seguinte após a recuperação.*" – Entrevistado#05, Diretor de Segurança do Sector Financeiro. **3.** *"Até situações mais graves ao nível do due diligence ou do due care, nas quais são os próprios responsáveis organizacionais, isto é, de topo, que efetivamente estão um pouco distantes deste tema da segurança"* – Ricardo Rodrigues #07, Diretor de *Compliance* da Balwurk (https://balwurk.com/). **4.** "*Bom, e acho que uma organização só pode dizer quem é resiliente, depois de ter sofrido o primeiro grande ciberataque, até lá, as empresas podem dizer o que quiserem, porque até testarem, mesmo a sério, os limites da organização não vão chegar a saber, se são resilientes ou não.*" – Paulo Rosado #08, CEO da Balwurk (https://balwurk.com/). **5.** *"O grande objetivo será sempre a manutenção de serviços e continuidade de negócio, mas que por acréscimos traz a cibersegurança e é assim que ela ganha importância"* – – Bruno Soares #11, Board Adviser da IDC (https://idcportugal.com/).

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	4. "*De uma forma bastante pragmática uma organização é resiliente, e para um determinado contexto, medirmos a sua resiliência através da capacidade de resposta a ataques específicos às tais joias da coroa, que falámos anteriormente. E capacidade de reposição de serviço, dentro de um tempo aceitável, se um incidente acontecer neste determinado âmbito para determinados ativos*." – Nuno Teodoro #16, CISO da HUAWEI (https://www.huawei.com/en/).
3.4 Processo simbiótico multidisciplinar de responsabilidade partilhada (estratégia transversal, envolvimento das pessoas, tentacularidade, partilha de informação, partilha, crescimento, independência,	**1.** "*Primeiro o líder tem de conhecer para poder interiorizar, depois para poder influenciar, e tem de influenciar dois níveis, a gestão da organização e toda população. E para o fazer, mais uma vez, temos de voltar ao início, ele tem de conhecer e manter-se atualizado. São estes os dois grandes passos, que é fundamental que o líder dê, para poder aumentar esses níveis de consciencialização e conhecimento destas temáticas dentro da organização e garantir que elas são práticas correntes*." – Alexandre Fonseca #03, Co-CEO do Grupo Altice (https://www.altice.pt/pt). **2.** *"Esta oposição é capaz de ser o princípio do problema, mas diria que isto tem que ser um equilíbrio, por isso, isto nunca se devia de ver como dois opostos."* – Entrevistado#05, Diretor de Segurança do Sector Financeiro. **3.** "*A tendência aqui é, de facto, a consciencialização das*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
neutralidade e transparência)	*organizações, para estarem preparadas o melhor possível, porque 100% não existe, pois, o risco existirá sempre*" – Ricardo Rodrigues #07, Diretor de Compliance da Balwurk (https://balwurk.com/). **4.** *"A liderança tem um papel primordial, ou seja, a liderança deve ser o principal impulsionador da cibersegurança. Não de pode ser reativo, é necessário ser proativo, e isso parte da liderança."* – Nelson Escrava #12, Diretor de Segurança e Administrador do INOV INESC Inovação (https://www.inov.pt/index.html). **5.** *"Na organização à qual eu pertenço, não só porque trabalha na área de cibersegurança, mas assume a sua necessidade como uma área de responsabilidade interna, da qual todas as estratégias dependem. Isto é, todas as decisões dependem da mesma, e da equipa de topo, que é basicamente a gerência*." – Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança. **6.** "*(…) a implementação de uma estratégia de segurança de informação ou de cibersegurança tem de estar alinhada com o negócio. Não existe uma receita única para uma estratégia de cibersegurança. (…) Todos os colaboradores fazem parte da minha equipa da segurança da informação e é assim que todos os colaboradores entram no Lidl*" – Jorge Vicente #14,

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	CISO do LIDL Portugal (https://www.lidl.pt/). **7.** "*Procuramos precisamente ter na nossa equipa pessoas das mais diversas áreas do conhecimento. E onde é que nos inspiramos para fazer isso, e não foi um processo, mas se nós pensarmos bem, na natureza os ecossistemas mais resilientes são aqueles que têm biodiversidade, porque há umas espécies que se protegem às outras protegem as outras, e que acabam por proteger outras, e assim sucessivamente*" – Gameiro Marques #15, Diretor do Gabinete Nacional de Segurança (https://www.gns.gov.pt/).
4.1.1 Capacitar Equipas (risco, ameaças, capacidades técnicas, tecnologias, competências, escassez no mercado)	**1.** "*Primeiro que tudo, não nos podemos esquecer que a cibersegurança, já é o quinto domínio de guerra, portanto, não estamos aqui a falar de um nicho, não estamos a falar de um problema que não é só nacional*" – Ricardo Rodrigues #07, Diretor de Compliance da Balwurk (https://balwurk.com/). **2.** *"Em suma, acho que os dois grandes desafios são o de acompanhar o panorama de ameaças e garantir que os meus investimentos e as minhas decisões sobrevivem às alterações deste panorama, e simultaneamente acompanhar a evolução tecnológica"* – Nelson Escrava #12, Diretor de Segurança e Administrador do INOV INESC Inovação (https://www.inov.pt/index.html).

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	3. "*Os desafios continuam a ser os mesmos, ou seja, escolher bem as pessoas, treiná-las, encontrar a capacidade para fazer o investimento e justificá-lo de forma adequada a que o investimento seja o mínimo possível para proteger o máximo de riscos*." – Entrevistado #13, CEO & CISO de Empresa de Consultoria de Cibersegurança. **4.** *"(…) consequência do crescimento tecnológico, não há recursos humanos suficientes na componente técnica para acompanhar isto, e começam a escassear"* – Hélder Jesus #17, Oficial da Marinha e Investigador (PhD) do Instituto Universitário Militar (https://www.ium.pt/).
4.1.2 Características próprias (linguagem, competências, conceitos, tecnologias, skills)	**1.** "*Da mesma que os líderes investem na sua formação financeira, em marketing e em vendas, na estrutura das suas operações, devem também investir na sua formação em cibersegurança."* - Alexandre Fonseca #03, Co-CEO do Grupo Altice (https://www.altice.pt/pt). **2.** *"(…) porque a área da cibersegurança tem um jargão muito próprio, e infelizmente, é muito difícil passar para outras empresas, e às vezes para o público em geral." – Entrevistado#05, Diretor de Segurança do Sector Financeiro.* **3.** *"A ausência de literacia digital, ou a ilusória literacia digital é um dos fatores mais importantes para a ciber (in)segurança, ou seja, uma razão para nós estarmos vulneráveis. Porque a*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	maior parte dos ciberataques, ou cibercrime, explora uma fronteira de confiança entre o ser humano e a tecnologia, atividade que designamos de engenharia social" – Nelson Escrava #12, Diretor de Segurança e Administrador do INOV INESC Inovação (https://www.inov.pt/index.html). **4.** "*A primeira coisa que nós temos de fazer é dar o empowerment a pessoa certa, identificar a pessoa certa para o lugar, é fundamental, e depois essa pessoa tem de ter alguma capacidade de perceber que a implementação de uma estratégia de segurança de informação ou de cibersegurança tem de estar alinhada com o negócio. Não existe uma receita única para uma estratégia de cibersegurança."* – Jorge Vicente #14, CISO do LIDL Portugal (https://www.lidl.pt/).
4.2.1 Alteração & Posicionamento (destaque, fator de influência, área estrutural, disciplina fundamental, desligar do IT, transição técnica a gestão, evolução	**1.** "*Da mesma maneira como nós temos essa consciência, quase inata, por anos e anos, gerações e gerações que nos foram ensinando estes comportamentos, também na cibersegurança, é importante que as pessoas comecem a ter noção que apagar a luz, desligar o ar-condicionado e fechar a porta, também tem o seu equivalente no mundo digital.*" - Alexandre Fonseca #03, Co-CEO do Grupo Altice (https://www.altice.pt/pt). **2.** *"Em boa verdade, os desafios são inerentes, e são independentes dos CISOs terem ou não skills, ou terem não*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
tecnológica)	*know-how. Os desafios estão lá. O que mudou foi eventualmente, a evolução do conhecimento, mais racional das pessoas que têm ou devem para que possam exercer uma função de CISO perante ameaças. Sim, é verdade, as ameaças, as ameaças evoluíram, em banda larga, mas também na vertical, e o principal erro de muitos CISOs é tentarem absorver tudo, isto é, querem absorver a área toda."* – *Entrevistado #06, CISO de Telecomunicações e/ ou informática.* **3.** "*Diria que os principais desafios de atualmente nem precisam ser em relação à cibersegurança, mas sim em relação às tecnologias de informação como um todo. A partir do momento em que a maior parte dos serviços que uma organização presta estão assentes em tecnologia, as preocupações devem estar também na tecnologia que os suportam.*" – Jéssica Domingues #09, Regulação, Supervisão e Certificação no Centro Nacional de Cibersegurança (https://www.cncs.gov.pt/). **4.** *"Eu acho que há uma arrogância generalizada, e isto pega com o que eu indiquei ainda agora, ou seja, estas empresas muito grandes partem do princípio de que são intocáveis, que são impenetráveis. E partem do princípio de que são poderosas o suficiente, para de antemão, fazer com que à*

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
	partida não fossem o alvo, ou têm a capacidade de desencorajar, pelo facto de serem grandes o suficiente." – Margarida Partidário #10, CEO & Founder da Arboreall (https://arboreall.com/#/). **5.** "*Os desafios variam de 2 formas. Por um lado, variam face ao panorama de ataques e que chamamos de panorama de ameaças (…) e conseguir adaptar a sua organização à medida que o panorama de ameaças muda. O que não é fácil porque nós avaliamos riscos face a ameaças, determinamos controlos, implementamos esses controlos e esses controlos custam, tipicamente, dinheiro, sejam eles tecnologia ou sejam processos. (…) Outro dos desafios é a evolução da oferta tecnológica na área de cibersegurança, ou seja, nós vamos novos produtos em cibersegurança, para cada uma das dimensões, a serem lançados continuamente*," – Nelson Escrava #12, Diretor de Segurança e Administrador do INOV INESC Inovação (https://www.inov.pt/index.html).
4.2.2 Evoluir & Liderar na incerteza (manter o negócio ativo, fazer update às capacidades, prevenção,	**1.** "*Que vai falhar, (…) eu sei que vai falhar, portanto aqui a preparação é a chave, e aquilo que temos visto também, é que, portanto, se hoje falhar, vamos para que ontem tenhamos preparado as coisas, e que depois o amanhã é voltar a montar, e voltar a tentar recuperar o que se pode, e avançar*." – Nuno Neves #02, CISO da Associação Nacional de

CÓDIGOS 1ª ORDEM	CITAÇÕES REPRESENTATIVAS[7]
proatividade)	Farmácias (http://www.anf.pt). **2.** "*Esta lógica do "fail fast" é muito importante interiorizarmos. Perceber que falhar faz parte do processo de aprendizagem, falhar faz parte do sucesso"* – Alexandre Fonseca #03, Co-CEO do Grupo Altice (https://www.altice.pt/pt). **3.** *"Portanto, faz parte do processo falhar, faz parte do processo de aprendizagem falhar, eu diria mesmo, não há aprendizagem sem falha"* – Ricardo Rodrigues #07, Diretor de Compliance da Balwurk (https://balwurk.com/). **4.** *"A liderança tem um papel primordial, ou seja, a liderança deve ser o principal impulsionador da cibersegurança. Não de pode ser reativo, é necessário ser proativo, e isso parte da liderança."* – Nelson Escrava #12, Diretor de Segurança e Administrador do INOV INESC Inovação (https://www.inov.pt/index.html).

Tabela 8: Dados de apoio ao tema (Códigos de 1ª Ordem)

8.4 CONSENTIMENTO INFORMADO & ENTREVISTA

CONSENTIMENTO INFORMADO

Autorização para tratamento dos dados recolhidos

Eu, _____, dou o meu consentimento à recolha de dados e ao tratamento dos meus dados pessoais nos seguintes termos e condições:

a) A responsável pelo tratamento é Clara Leonor Alexandre Marques, alumni 56415 do Mestrado de Executivo de Liderança da NOVA SBE, com o email 56415@novasbe.pt;

b) Os dados pessoais destinam-se a fundamentar a tese de Mestrado, no ano letivo 2022/2023 subordinado ao tema "*Como é que o líder influência a construção de uma cultura de cibersegurança?*" e os dados não serão tratados de forma incompatível com as respetivas finalidades da recolha;

c) Os dados pessoais são conservados pelo período considerado necessário para a intervenção (prazo ou, se não for possível, critérios usados para definir esse prazo) respeitando a sua conservação as garantias de sigilo e confidencialidade exigidas pelo Regulamento Geral de Proteção de Dados – RGPD em vigor;

d) Assistem-me, na qualidade de titular dos dados pessoais, os seguintes direitos:

- solicitar à pessoa responsável pelo tratamento dos meus dados pessoais, o acesso aos mesmos, a sua atualização, retificação, eliminação, limitação ou oposição ao seu tratamento;
- retirar o consentimento a qualquer momento sem, no entanto, comprometer a licitude do tratamento efetuado com base no consentimento anteriormente dado e sempre que tal seja necessário para efeitos de cumprimento de obrigações do/a responsável pelo tratamento dos dados (que, por definição de prazo legal, têm que ser conservados);
- apresentar reclamação à Comissão Nacional de Proteção de Dados (CNPD);

- não disponibilizar um ou mais dados solicitados no presente instrumento de recolha;
- a opor-me ao tratamento de dados se não tiver sido concedido consentimento para o efeito ou se o tratamento não decorrer, designadamente, de um contrato, de procedimentos judiciais ou defesa dos meus interesses vitais, entre outros;
- a não ficar sujeito a decisões tomadas com base no tratamento automatizado, incluindo a definição de perfis, se esse facto puder produzir efeitos que me venham a afetar na minha esfera jurídica ou outra.

Informação sobre o/a entrevistado(a)

Nome:

Formação Base/ Formações:

Número de Geografias onde exerceu / exerce funções:

Anos de Experiência Profissional:

Posição:

Antiguidade na Função:

Organização:

Origem da Organização:

Dimensão da Organização (nº de funcionários):

Presença em outras geografias:

Sector de mercado:

☐ Não aceito que as informações relativas ao meu "nome" e "organização" sejam divulgadas a elementos terceiros, nos resultados da tese os mesmos devem de figurar anonimizados, isto, é entrevistado X da organização no sector de mercado Y.

☐ Fico disponível para ajudar na aplicação de um estudo quantitativo (inquérito) à minha organização para aferir o seu grau de maturidade na literacia de cibersegurança.

☐ Autorizo a gravação áudio em quaisquer suportes e formatos da minha entrevista.

Assinatura:

_____

Data da recolha: _____/_____/_____

ENQUADRAMENTO

Metodologia & relevância da entrevista para a tese

"*Ouvir não é o mesmo que escutar*" é com esta destrinça que o relatório sobre cibersegurança do *World of Economic Forum* introduz a relação comparativa entre os líderes de cibersegurança e outros líderes de negócio, comparando a forma como ambos sentem e abordam a exposição das suas organizações ao crescendo do risco cyber. Indicando também que os líderes de negócio, ainda que mais conscientes, continuam longe da necessária visão articulada entre os problemas e os ciber-riscos, já efetuada pelos líderes de cibersegurança (Bueermann et al. 2023). Razão esta que faz com grandes organizações tornem como recorrente a prática de recurso a líderes de cibersegurança, tais como diretores de segurança da informação (CISOs), para se proteger contra ciberataques.

Sendo o papel de líder de cibersegurança um papel novo, quando comparado com profissionais da mesma área (profissionais de cibersegurança), e diferente quando comparado com outros cargos de liderança (líderes de negócio), na medida em que exige estratégia, colaboração e requer uma necessidade de manutenção de consciência situacional ativa contra as potenciais ameaças, necessitando de ser corretamente enquadrado para ser

entendido. Isto é, as organizações e educadores continuam a catalogá-lo como um papel tecnológico sênior, em vez de um papel estratégico e orientado para os negócios, o que cria uma lacuna entre o que é visto como "negócio" e o que é visto como "IT" deixando as organizações mais vulneráveis a ataques(Anderson, Ahmad, and Chang 2022).

Surge assim a importância de saber qual a matriz de competências necessárias para os líderes de cibersegurança, e como é o correto alinhamento das mesmas com as necessidades do mercado, não descurando cumprimento dos requisitos mínimos de segurança das redes e sistemas de informação poderá permitir às organizações reduzir o ciber-risco associado às ameaças (Marques and Santos 2019).

É neste contexto que surge a pergunta de investigação: *"Como é que o líder influência a construção de uma cultura de cibersegurança?"*

GUIÃO DE ENTREVISTA

Questões

1. "Como é que o líder influência a construção de uma cultura de cibersegurança?"
2. Quais são os principais desafios da liderança hoje em relação à cibersegurança? Como é que sente que os mesmos se têm alterado?
3. Como define a estratégia de cibersegurança da organização? Como é que o CISO se posiciona?
4. Quais são os recursos chave da organização?
5. A organização é resiliente? / Como é que a organização se protege?
6. Se hoje falhar o que se faz amanhã?
7. O que tem a dizer sobre o seguinte: "*A influência da liderança na cibersegurança ou a influência da cibersegurança na liderança*".