

O Futuro das TI

O que os
líderes de IT
precisam de
saber

ESTUDO COMPUWORKS 2025

**IT FUTURE
TRENDS
2035**

ÍNDICE

Introdução

Sumário Executivo

Contextualização do cenário tecnológico português

O Estudo

METODOLOGIA UTILIZADA

- Fase 1 – Mesa Redonda
- Fase 2 – Desk Research
- Fase 3 – Qualitativa
- Fase 4 – Quantitativa
- Fase 5 – Mapeamento de Tendências Específicas e Construção de Cenários:

FASE 3 – ENTREVISTAS EM PROFUNDIDADE: RESULTADOS

- Geopolítica e Inovação
- Mercado e Competitividade
- Cibersegurança e Compliance
- Infraestruturas e Tecnologias Disruptivas
- Inteligência Artificial e Automação
- ESG e Sustentabilidade
- Recursos Humanos e Cultura

Fecho / Conclusão

FASE 4 – QUANTITATIVA – SURVEY: RESULTADOS

- Dimensão da Empresa
- Geopolítica e Inovação Tecnológica
- Contexto Tecnológico em Portugal
- Sobre a Empresa onde desempenha funções
- Sobre Soluções de Cibersegurança na Empresa
- Sobre Satisfação com Soluções de Cibersegurança
- Sobre Soluções baseadas em Inteligência Artificial
- Sobre Modelo de Trabalho
- Sobre Cultura Empresarial, Transformação Digital e Talentos
- Sobre O Profissional de IT da Década 2025 –2035
- Sobre IT, Infraestrutura e Tecnologias Disruptivas
- Sobre Principal Desafio em Infraestruturas
- Sobre Posição da Área de IT nas Empresas até 2035
- Sobre A Evolução das Infraestruturas Digitais até 2035
- Sobre AI, Cybersecurity e Compliance
- Sobre Sustentabilidade, Neutralidade Carbônica e Infraestrutura Digital
- Sobre ESG, Eficiência Energética e Neutralidade Carbônica
- Sobre Relevância de Neutralidade Carbônica de Datacenters

Fecho / Conclusão

FASE 5 – CONSTRUÇÃO DE CENÁRIOS E MAPEAMENTO DE TENDÊNCIAS ESPECÍFICAS

- Cenário Geopolítico e como Portugal está posicionado
- Cenário Tecnológico
- Tendências
 - Megatendências: O pano de fundo estrutural
 - Tendências Comportamentais: Novas lógicas sociais e do trabalho
 - Tendências de Negócio: Novos modelos e estratégias
 - Tendências Específicas

CONCLUSÕES FINAIS

REFERÊNCIAS

01

Introdução



O futuro exige preparação no presente

Por Ricardo Teixeira, CEO da Compuworks

Vivemos tempos de decisões rápidas, incertezas constantes e mudanças tecnológicas que deixam qualquer plano estratégico com prazo de validade curto. Mas se o futuro continua a parecer longínquo, é precisamente agora que temos de começar a prepará-lo.

Foi com esta convicção que nasceu o IT Future Trends 2035, um estudo que desenvolvemos em parceria com o Ecossistema Inova, com um objetivo muito claro: traduzir tendências globais para a realidade portuguesa e apoiar os líderes de tecnologia na construção de guidelines ou linhas estratégicas para a próxima década.

A lacuna é evidente. Portugal continua maioritariamente a depender, quase exclusivamente, de estudos internacionais, feitos à escala dos grandes mercados, úteis, sim, mas muitas vezes desajustados à nossa dimensão, estrutura e maturidade digital.

A maioria das empresas portuguesas não é uma multinacional com departamentos globais, é uma PME com equipas pequenas e desafios muito próprios ao nível da escala, da produtividade e do acesso à inovação. Ignorar estas especificidades significa, na prática, planear às cegas.

E são essas PMEs que representam 99% do tecido empresarial português. É nelas que está a nossa base de geração de riqueza e emprego. São elas que precisam de informação prática, concreta, realista, que as ajude a melhorar produtividade, reduzir o receio tecnológico e planear com confiança.

Este estudo foi pensado exatamente para isso: ser uma ferramenta de planeamento prático para CEOs, CTOs e todos os que lideram a transformação digital no terreno. É um documento orientador, não teórico. Um estudo que quer ajudar, não apenas descrever.

Sabemos que ainda existe receio, hesitação e, por vezes, uma perceção de risco que leva a decisões reativas ou à simples inação. Mas também sabemos que a tecnologia, da cibersegurança à IA, representa um potencial real de aumento de eficácia, produtividade e competitividade. Para que esse potencial se concretize, é fundamental criar condições para que as decisões estratégicas assentem em conhecimento contextualizado e realizável.

Portugal tem, hoje, trunfos geográficos e infraestruturais para se afirmar como um hub tecnológico. Mas para que isso aconteça, é necessário que o valor deixe de ser apenas canalizado e comece a ser efetivamente capturado. E isso depende, em larga medida, da capacidade das nossas empresas de se posicionarem estrategicamente com base em dados, conhecimento e colaboração.

O IT Future Trends 2035 é um primeiro contributo para esse objetivo. Esperamos que sirva como ponto de partida para a reflexão, o planeamento e a preparação de um futuro mais consciente, mais informado e mais alinhado com as reais necessidades do país.

Sumário Executivo

O IT Future Trends 2035 oferece um plano pragmático para que empresas em Portugal antecipem decisões dos próximos 5 a 10 anos, traduzindo tendências globais para a realidade local e reduzindo o “receio tecnológico” com critérios de adoção responsáveis. O estudo parte da constatação de que o país tem ativos importantes, mas precisa de transformar a ambição em execução, sobretudo entre PME's. A mensagem central é direta: preparar hoje é condição para competir em 2035.

No contexto português, o relatório descreve bases sólidas, fibra e 5G difundidos, serviços públicos digitais robustos e agenda alinhada à Década Digital da UE, combinadas a desafios persistentes: assimetrias de adoção entre portes e setores, lacunas de competências em dados e cibersegurança, e a necessidade de converter adoção em produtividade, exportações e emprego qualificado.

A metodologia decorreu por sete meses, organizada em cinco fases complementares. A Fase 1 reuniu lideranças do setor numa mesa-redonda para analisar prioridades; a Fase 2 conduziu desk research com foco em Portugal e leitura europeia, clarificando consensos, divergências e o enquadramento de financiamento e governação. Juntas, ancoram o restante do trabalho e balizam as escolhas que o país terá de fazer (soberania de dados/cloud, competências e aceleração da adoção empresarial).

As fases empíricas consolidam a visão. Na Fase 3 (qualitativa), 60 entrevistas em profundidade detalham perceções e dilemas práticos do ecossistema; na Fase 4 (quantitativa), 141 questionários dimensionam humor e prioridades, reconhecendo que a amostra não é probabilística. A triangulação entre as duas etapas confere robustez às conclusões, ainda que sem representatividade estatística.

A Fase 5 amplia o horizonte com mapeamento de tendências e cenarização: não pretende “prever” o futuro, mas identificar sinais de mudança e testar estratégias em diferentes caminhos possíveis, útil em contextos de alta incerteza. Deste exercício e do desk research emergem prioridades transversais: escalar IA e cloud nas PME's, consolidar soberania de dados/cloud, fechar lacunas de competências e transformar a vantagem atlântica em valor económico local.

A conclusão final é inequívoca: Portugal tem condições reais de subir na cadeia de valor digital se combinar inovação com confiança, agilidade com responsabilidade e propósito com resultados, menos burocracia e mais execução, sem abdicar do diferencial europeu de proteção ao cidadão. Em suma, o futuro exigirá preparação no presente.

Contextualização do cenário tecnológico português

Portugal entrou em 2025 alinhado à agenda europeia da Digital Decade rumo a 2030: metas para competências digitais, digitalização das empresas, dados e cloud, serviços públicos digitais e conectividade avançada. O país consolidou bases de infraestrutura (fibra e 5G) e serviços públicos digitais robustos, e avança de uma fase de “adoção” para outra centrada em produtividade, dados e segurança. A regulação europeia (como gestão do IA e dados) e os programas nacionais, INCoDe.2030, Estratégia Nacional de IA e o Plano de Transição Digital, dão o enquadramento para escalar o que já funciona e corrigir desigualdades de adoção entre grandes empresas e PMEs.

No tecido empresarial, cresce o uso da cloud, análise de dados e IA nas organizações de maior porte, mas persiste assimetria entre setores e escala, sobretudo nas PMEs. O desafio não é apenas “ter tecnologia”, mas integrá-la a processos, talentos e métricas de negócio. A lacuna de competências continua como fator crítico (especialistas TIC, literacia de dados e cibersegurança), ao mesmo tempo em que a digitalização dos pagamentos e a automação de backoffice elevam a eficiência em serviços financeiros, comércio e administração pública. Em paralelo, cibersegurança sobe de prioridade tática para tema estratégico, acompanhando a sofisticação das ameaças e a maior exposição de cadeias de valor digitais.

O ecossistema de inovação amadurece: hubs digitais europeus (EDIH), centros de Investigação e Desenvolvimento (I&D) e redes universidade-empresa (ex.: INESC, programas colaborativos) ancoram projetos em IA, computação avançada, indústria 4.0, saúde digital e energia. O ambiente de startups está mais denso em fintech, software B2B e deep tech, mas ainda precisa de escalar e também capital de crescimento para transformar pipelines promissores em scale-ups globais.

Entre 2025 e 2035, os vetores decisivos serão: expansão de competências (em escala), adoção de IA confiável nas PMEs, gestão e partilha de dados (data spaces), ciberresiliência, e a convergência verde-digital, usando o digital para acelerar descarbonização e eficiência.

Em síntese, Portugal parte de uma base sólida de infraestrutura e serviços digitais, com políticas públicas coerentes e um ecossistema inovador em crescimento. O próximo salto depende de converter adoção em valor económico mensurável, produtividade, exportações tecnológicas e empregos qualificados, reduzindo a distância entre líderes digitais e o restante do tecido empresarial, e garantindo segurança e confiança em todo o percurso.

O Estudo

Este estudo analisa o estado atual do panorama tecnológico português em 2025, e oferece uma visão abrangente das tendências específicas ao setor de IT, funcionando como um documento estratégico de apoio à decisão, especificamente adaptado à realidade portuguesa para a próxima década.

Este relatório destina-se a profissionais e gestores de diferentes áreas do setor de IT que pretendem compreender melhor o ambiente atual e futuro tecnológico em Portugal.

Ao identificar e explorar os principais desafios e tendências, pretende-se fornecer suporte para a tomada de decisões estratégicas, promovendo o desenvolvimento sustentável e a inovação contínua no contexto empresarial português.



**Metodologia
Utilizada**

Metodologia Utilizada

O presente estudo foi realizado ao longo de **7 meses de fevereiro a agosto de 2025, dividido em 5 fases** conforme será detalhado a seguir:

FASE 1 – MESA REDONDA

O ponto de partida aconteceu a 28 de Maio, através da realização de um webinar onde líderes das IT debateram o ‘Futuro das TI’ numa mesa redonda online, moderada pelo Prof. Henrique Carreiro, diretor da IT Insight e contou com os oradores Fábio Ribeiro, Cybersecurity Senior Sales Engineer da Watchguard, Luís Rasquilha, CEO Inova Ecosystem & Board Member da NTT Data Brazil, Ricardo Teixeira, CEO & Founder da Compuworks, Rui Ribeiro, Associate Partner Zertive & Diretor Executivo da LES, Sérgio Carvalho, Executive Director for Tech & CTO da Nova SBE, e Tiago Santos, CEO da AR Telecom.

FASE 2 – DESK RESEARCH

Em paralelo foi realizada uma etapa de desk research que mapeou o estado atual e a trajetória tecnológica em Portugal até 2035, usando fontes oficiais recentes (2024–2025) e análises setoriais europeias. O foco foi Portugal, mas com leitura do contexto europeu para calibrar riscos e oportunidades.

Corpus de fontes.

1. Relatórios oficiais da UE: Digital Decade 2025 – Country Report: Portugal (texto integral e sumários executivos), base para indicadores, metas e avaliação do roteiro nacional (“Portugal records stable growth in digital public services... but can rely on solid connectivity networks.”).
2. Roteiro nacional revisto (2024/25): metas, 157 medidas e orçamento (0,75% do PIB), usado para analisar o alinhamento com prioridades de IA, soberania e competências.
3. Indicadores de adoção tecnológica: tabelas de KPIs (VHCN, 5G, skills, cloud/IA). Ex.: “8,63% das empresas adotaram IA em 2024... com forte diferença entre PMEs e grandes.”
4. Contexto competitivo europeu em IA: relatório Time to place our bets: Europe’s AI opportunity para posicionar Portugal face a lacunas/forças na cadeia de valor da IA (“European cloud companies have <5% market share”).

Os principais pontos elencados nesses relatórios trazem foco nos tópicos a seguir:

CONTEXTUALIZAÇÃO DO CENÁRIO TECNOLÓGICO PORTUGUÊS

Portugal entra em 2025 com uma combinação rara de infraestruturas digitais robustas, serviços públicos digitais maduros e uma agenda nacional alinhada à Década Digital da UE. Os documentos oficiais convergem na leitura de que **o país “regista um crescimento estável nos serviços públicos digitais e desempenho particularmente bom no acesso aos registos de saúde eletrónicos”, mas enfrenta “desafios na adoção de inteligência artificial (IA) pelas empresas” e nas competências digitais de base, embora possa “contar com redes de conectividade sólidas”.**

INFRAESTRUTURA E CONECTIVIDADE: BASE SÓLIDA, USO DESIGUAL

A cobertura das redes de muito alta capacidade (VHCN) atingiu 94,59% das habitações em 2024, com objetivo nacional de 100% até 2030. No 5G, a cobertura global chegou a 98,72% e o país também visa universalização até 2030, com o regulador a preparar redistribuição de espectro remanescente. Além da rede terrestre, Portugal avança no Atlantic CAM, novo anel de cabos submarinos com sensores “SMART” para sismologia e monitorização ambiental, projeto apoiado por fundos europeus e crucial para soberania e resiliência. Apesar da infraestrutura, as próprias fontes destacam “desempenho misto” na adoção: a utilização de banda larga e de 5G pelos utilizadores cresce, mas em ritmos inferiores à média da UE em alguns indicadores.

EMPRESAS E INOVAÇÃO: PMES DIGITAIS, IA AINDA TÍMIDA

O tecido empresarial português, dominado por PMEs, mostra intensidade digital básica ligeiramente acima da média europeia (74,3%), mas adoção de IA ainda modesta (8,6% em 2024, abaixo da UE) e cloud aquém da meta (32,3% das empresas em 2023). Persistem diferenças grandes entre PMEs e grandes empresas.

Como resposta, o roteiro nacional prevê meta de 75% das empresas a usarem cloud e IA em 2030, um plano de cloud soberana para

administração pública e negócios e a plataforma Collaborative Hub for Digital para aproximar oferta e procura de inovação. No ecossistema empreendedor, o país projeta ampliar o número de start-ups de pouco mais de 4.700 (2024) para 6.000 até 2030, mas reconhece escassez de financiamento para fases de crescimento.

COMPETÊNCIAS, TALENTO E SERVIÇOS PÚBLICOS: AVANÇOS E LACUNAS

Nas competências digitais, 56% da população tinha pelo menos competências básicas em 2023, valor próximo da média europeia, mas com grandes diferenças por escolaridade, idade e território (rural). Paralelamente, especialistas em TIC cresceram para 5,2% do emprego e a participação feminina subiu para 22,7%. Nos serviços públicos digitais, Portugal está acima da média da UE e lidera no acesso ao registo eletrónico de saúde, com crescente uso pelos cidadãos.

SOBERANIA, SEGURANÇA E POSIÇÃO ATLÂNTICA

As fontes oficiais realçam a prioridade de soberania digital (dados, cloud, IA) na estratégia nacional atualizada em 2024/25 e recomendam acelerar transposição da diretiva NIS2. A mesa-redonda com líderes do setor converge na necessidade de capacitar talento e consolidar Portugal como hub digital, para deixar de ser apenas ponto de passagem de cabos e tráfego

PRESSÕES E OPORTUNIDADES EUROPEIAS QUE AFETAM PORTUGAL

No plano europeu, contexto incontornável para Portugal, a adoção e o investimento em IA **ficam atrás dos EUA:**

- **O gasto externo em IA na Europa Ocidental é, em média, 61% inferior** ao dos EUA,
- As empresas europeias **investem 45–70% menos** em IA/IT conforme o setor.

A expansão de *data centers* e da IA **eleva a procura de eletricidade na Europa em 20–25% até 2030**, num contexto em que os **preços industriais são ~70% superiores** aos dos EUA, desafio relevante para a localização de *workloads* digitais.

Ainda assim, há uma vantagem europeia em energia limpa que pode ser explorada, inclusive por Portugal, pela sua posição atlântica e projetos de cabos, para atrair investimento digital.

CIBERSEGURANÇA

As empresas portuguesas têm menos incidentes que a média da UE; em 2024, 3,12% relataram indisponibilidade por ataques (UE 3,43%), e 95,6% adotaram alguma medida de segurança, com 65,6% a sensibilizar colaboradores, ambos acima da UE. A adoção de normas seguras da internet é desigual:

- IPv6 está acima da média no lado do utilizador (40% vs. 36% UE), mas muito abaixo no lado servidor (2% vs. 17% UE);
- Validação DNSSEC caiu para 11% (UE 47%).

A transposição da NIS2 está em curso; após a estratégia nacional, prevê-se um plano específico para reforçar a cibersegurança das redes 5G. O CNCS e parceiros lançaram iniciativas financiadas pelo PRR (ex.: C-Academy, C-Network, C-Hub, Cybersecurity Alliance e Observatório) e preparam a campanha "Safer Digital".

Especialistas alertam que NIS2/DORA são "80% processos e 20% tecnologia", com PMEs como elos frágeis na cadeia; é preciso "literacia digital estratégica" e planos para eventos drásticos (ex.: apagão), onde as grandes empresas estão mais bem preparadas.

CONSENSOS E DIVERGÊNCIAS ENTRE AS FONTES

Consensos:

- Infraestrutura: cobertura gigabit e 5G quase universal; cabos submarinos são estratégicos; cobre em retirada até 2030.
- Setor público: serviços digitais e e-Health bem avaliados; cidadãos usam cada vez mais portais e apps.
- Empresas: adoção de IA é o principal "calcanhar de Aquiles"; metas de 2030 incluem 75% das empresas a usar cloud e IA.

Divergências/nuances:

- Uso vs. capacidade. Os relatórios da Comissão sublinham a capacidade (cobertura) e falam em "desempenho misto" na procura (adesão de utilizadores/empresas).
- Hub digital. Os documentos oficiais incidem nos projetos de conectividade; já os especialistas do webinar defendem que Portugal ainda não captura suficiente valor do trânsito internacional de dados, pedindo políticas ativas de cloud soberana e capacitação.
- Contexto europeu. A Comissão centra-se em metas e execução nacionais; a análise setorial independente, chama atenção para custos de energia e o atraso no investimento em IA na Europa, fatores que podem condicionar escolhas de localização e competitividade.

FINANCIAMENTO E GOVERNAÇÃO

Para sustentar a transição, €4,5 mil milhões do PRR e €2,4 mil milhões dos Fundos de Coesão estão afetos ao digital; o roteiro nacional foi revisto em 2024/25, com 157 medidas e forte alinhamento às prioridades de IA, soberania e skills.

SÍNTESE

O retrato que emerge é coerente: infraestrutura e governo digital à frente, capital humano a crescer, mas empresas, sobretudo PMEs, ainda a passo curto em IA e cloud. As prioridades transversais citadas nas fontes incluem escalar a adoção empresarial, consolidar soberania de dados e cloud, fechar lacunas de competências e transformar a vantagem atlântica em valor económico local, sempre atentos ao contexto europeu de custos energéticos e investimento em IA.

FASE 3:

Qualitativa

Instrumento: Entrevistas online, individuais e em profundidade com duração de 1 hora.

Objetivo: compreender em detalhes as perspectivas, opiniões, sentimentos e atitudes dos participantes em relação ao ecossistema tecnológico português e às principais tendências emergentes através da partilha de conhecimento relevante de cada um dos inquiridos.

Amostra: Não é probabilística e nem aleatória. A seleção foi intencional, pois a profundidade da informação e a perspectiva dos participantes são mais importantes do que a generalização dos resultados para uma população maior.

Participantes: A seleção dos inquiridos foi feita considerando que estes possuem características relevantes para o estudo, como experiência, conhecimento, ou parte de um grupo específico. Ao todo foram 60 inquiridos, sendo CTOs, CEOs, membros de conselho, académicos e os restantes profissionais notáveis da área de tecnologia, das principais empresas do mercado tecnológico em atividade no território português.

FASE 4:

Quantitativa

Instrumento: Questionário estruturado com perguntas demográficas para segmentação posterior, baseado nas descobertas da fase qualitativa para desenvolver perguntas pertinentes em questões fechadas, escalas Likert, múltipla escolha e outras técnicas quantitativas, aplicado em plataforma online entre junho e julho de 2025.

Objetivo: Obter insights, dimensionar o humor e a percepção do inquirido em relação realidade atual das empresas e as perspectivas futuras do panorama tecnológico português.

Amostra: Os indivíduos foram convidados, por e-mail, a responder o questionário. A base foi o mailing list de leads da Compuworks e leitores da IT Insight. Vale destacar que não se trata de uma amostra representativa e nem probabilística, já que não condiz ao perfil demográfico das empresas portuguesas. A seleção foi feita por conveniência, usada conforme a facilidade de acesso aos inquiridos e uso de ferramentas tecnológicas no seu quotidiano.

Participantes: Ao todo foram 141 questionários respondidos por CTO's de diferentes empresas de setores diversos, de todo território português.

Nota: As duas fases são complementares: a fase qualitativa oferece profundidade e contexto, enquanto a fase quantitativa oferece amplitude e generalização. A triangulação dos dados, de ambas as fases, oferece uma visão mais robusta e fiável sobre o objeto do estudo a partir da realidade portuguesa, mesmo sem representatividade estatística.

FASE 5:

Mapeamento de Tendências Específicas e Construção de Cenários:

O uso de métodos de mapeamento de tendências e construção de cenários em projetos de investigação permite ampliar o horizonte de análise, ajudando organizações e equipas a prepararem-se melhor para diferentes futuros possíveis. Esse processo não pretende prever o futuro com exatidão, mas sim identificar sinais de mudança no presente que possam impactar o contexto da investigação, permite antecipar riscos e oportunidades que poderiam passar despercebidos em abordagens tradicionais.

Ao mapear tendências, conseguimos compreender quais as transformações tecnológicas, sociais, económicas ou regulatórias estão em curso e como elas podem influenciar o objeto de estudo. Já a construção de cenários ajuda a projetar diferentes caminhos a partir dessas tendências, permitindo testar hipóteses, validar estratégias e enriquecer as decisões com uma visão mais abrangente e estratégica.

Essa etapa contribui, portanto, para tornar a investigação mais ligada com a realidade em transformação, evitando análises presas ao passado ou limitadas ao curto prazo.

Ela é especialmente útil em contextos de alta incerteza, onde pensar de forma antecipada é uma vantagem competitiva e uma necessidade para a sustentabilidade de decisões públicas ou privadas.



03

**Entrevistas em
Profundidade**

FASE 3:

Entrevistas em Profundidade

RESULTADOS

A presente análise qualitativa dá voz aos profissionais que vivem, todos os dias, os desafios e oportunidades da transformação digital em Portugal. Através de entrevistas em profundidade a líderes nas áreas de IT, cibersegurança e inovação, este estudo mapeia percepções, inquietações e apostas para o futuro, revelando um panorama realista, mas também ambicioso, sobre o papel do país no cenário tecnológico europeu e global.

O conteúdo trazido pelos inquiridos revela uma dualidade que atravessa o discurso de forma recorrente: de um lado, a consciência clara das limitações impostas pela burocracia e pelas exigências regulatórias; do outro, o desejo – e a necessidade – de avançar com ousadia, explorando as potencialidades locais, como o crescente ecossistema de startups, os talentos altamente qualificados e a atratividade estratégica de Portugal como hub tecnológico.

A Europa, para muitos, surge como um território com a tendência entre a rigidez normativa e a urgência por inovação. **“O desafio da Europa é desbloquear a burocracia em prol da inovação, sem abdicar da segurança da informação”**, resume um dos inquiridos. Ao mesmo tempo em que se valoriza a solidez regulatória como diferencial competitivo, reconhece-se que a lentidão na adaptação pode custar relevância num cenário global em rápida mutação.

Vários depoimentos também sublinham o papel das infraestruturas digitais resilientes e da computação em cloud no avanço das organizações. Embora a cloud não seja percecionada como mais barata em termos absolutos, destaca-se a sua flexibilidade como trunfo essencial para empresas em crescimento ou em constante adaptação. Ainda assim, “justificar os custos da cloud continua a ser um dos maiores desafios para quem gere IT”, sinaliza um dos profissionais.

A cibersegurança aparece como tema incontornável, especialmente num contexto geopolítico volátil e diante da escalada dos ataques baseados em inteligência artificial. A arquitetura Zero Trust, a descentralização da identidade digital e o uso preditivo de dados são mencionados como pilares de proteção. No entanto, há um alerta sobre o uso oportunista das normas de compliance: “Muitos querem um selo de conformidade rápido, sem antes estruturar a base”.

Ao abordar o fator humano, os inquiridos reconhecem que atrair e reter talentos já não depende apenas de salários competitivos, mas de criar espaços de trabalho significativos, flexíveis e conectados a uma cultura viva. O trabalho híbrido é visto como caminho inevitável, mas que exige redesenho dos ambientes físicos e simbólicos para promover interação e envolvimento.

Esta etapa inaugura, portanto, um mergulho nas percepções de quem está à frente das decisões estratégicas em tecnologia. Não se trata apenas de entender o que pensam os líderes, mas de captar o ritmo, os dilemas e as esperanças que marcam o presente e desenharam o futuro da tecnologia em Portugal.

Quando perguntado a cada inquirido sobre Geopolítica e Inovação: “Qual a sua visão do papel da Europa neste mundo digital político? Acredita que a Europa pode acompanhar o ritmo inovador dos EUA, China e Índia, ou será apenas cliente destes países, procurando assentar e investir numa estratégia regulatória?” aqui estão as principais citações:

GEOPOLÍTICA, INOVAÇÃO E SOBERANIA DIGITAL: O QUE ESTÁ EM JOGO PARA PORTUGAL

Há consenso sobre a urgência de uma postura estratégica da Europa que valorize tanto a inovação quanto a segurança e independência tecnológica.

Verbalizações / Frases representativas:

“A Europa tem que desbloquear a burocracia, mas sem perder sua vantagem em segurança e regulamentação.”
“O futuro pode estar em ecossistemas isolados para experimentação, que depois sejam enquadrados nas regras.”

O avanço tecnológico europeu acontece num tabuleiro geopolítico conturbado. Entre os Estados Unidos, a China e a Índia, a União Europeia (UE) vive pressões externas e divergências internas, enquanto guerras e tensões próximas (como o conflito Rússia–Ucrânia) reacendem prioridades de defesa e segurança. Para Portugal, esse contexto é simultaneamente risco e oportunidade: ou acelera e encontra nichos estratégicos, ou assiste à redefinição do jogo a partir da periferia.

Verbalizações / Frases representativas:

“Ou a Europa muda rápido, ou fica para trás.”

O TABULEIRO GEOPOLÍTICO: RISCOS, DEPENDÊNCIAS E JANELAS DE OPORTUNIDADE

Há consenso de que a UE atua “no meio do tabuleiro” e precisa decidir qual papel quer jogar. O despertar para a área de defesa, um motor histórico de inovação, repõe recursos e prioridades que, durante anos, perderam tração. Ao mesmo tempo, a dependência tecnológica de fornecedores globais (especialmente em cloud e software) expõe vulnerabilidades em cenários de tensão comercial. Soluções de curto prazo, como arquiteturas híbridas ou multicloud, surgem como prática de “soberania operacional” enquanto a autonomia tecnológica não amadurece.

Verbalizações / Frases representativas:

“Dados são o novo ouro, e a Europa pode ser o cofre.”

REGULAÇÃO: "TRAVÃO" OU "CAMINHO" PARA INOVAR?

A regulação europeia (RGPD, NIS2, DORA, e agora a moldura de IA) divide percepções. Para um grupo, as regras encarecem e retardam a adoção de tecnologias, sobretudo de IA. Para outro, funcionam como "guard rails" que obrigam profissionalização e elevam o padrão de segurança, acelerando a maturidade do ecossistema quando integradas "by design", desde a conceção dos sistemas (e não como "remendo" em legacy). Uma pista de convergência aparece: criar sandboxes regulatórios para experimentar com dados não críticos e regular depois, reduzindo a fricção sem renunciar à proteção do cidadão.

Verbalizações / Frases representativas:

"A regulação ajuda, mas dói em recursos."
"Sem regras, muitos não fariam nada."

SOBERANIA TECNOLÓGICA: DO DISCURSO À EXECUÇÃO

A procura por soberania digital, menos dependência externa em dados, infraestruturas e componentes críticos, impõe escolhas. No curto prazo, podem surgir trade-offs com metas de sustentabilidade; no médio e longo prazo, a consolidação de cadeias produtivas e de P&D na Europa é vista como necessária para reduzir riscos e capturar valor de alto impacto (cibersegurança, automação inteligente, infraestruturas resilientes, tecnologias "dual use" com aplicação civil e militar). O caminho passa por desenvolver produtos próprios com regulação inteligente; na ausência disso, consolida alianças tecnológicas de peso para ganhar escala desde o lançamento.

Verbalizações / Frases representativas:

"Soberania digital tem de sair do papel."

SEGURANÇA E DEFESA: O NOVO MOTOR DA INOVAÇÃO EUROPEIA

Ciberataques são uma realidade diária, com operadores críticos a reportar centenas de incidentes por semana. A percepção dominante é que o maior risco hoje é "informático", mais do que físico (como o corte de cabos submarinos). O "acordar" europeu para defesa acelera investimentos em capacidades que transbordam para a economia civil, de drones a soluções de comando-e-controlo, criptografia e identidade digital. Para Portugal, esse ciclo é oportunidade de alavancar competências já reconhecidas em ciber e de integrar cadeias europeias de defesa e segurança com produtos exportáveis.

Verbalizações / Frases representativas:

"O maior risco é informático, não o cabo."
"Vemos... à volta de 250 ataques por semana."

TALENTO, CULTURA E GOVERNAÇÃO: VELOCIDADE IMPORTA

Os inquiridos reconhecem massa crítica de talento na Europa, mas mostram dificuldades de coordenação política, burocracia excessiva e aversão ao risco que travam a “tríade” testar-falhar-aprender. A receita destacada: decisões mais integradas (com traços de um “estado federal” em temas estratégicos), simplificação regulatória por consolidação de normas e um impulso cultural para que startups nasçam globais, sem ficarem presas a nichos domésticos.

Verbalizações / Frases representativas:

“Temos talento; falta velocidade e escala.”

“Se a Europa desburocratizar e agir integrada, o poder é muito grande.”

ONDE HÁ CONSENSO, E ONDE HÁ DIVERGÊNCIAS

Consensos

- Risco de atraso por lentidão e fragmentação: a lógica de consenso entre países e processos morosos prejudicam a velocidade tecnológica.
- Regulação é “faca de dois gumes”: traz segurança e padrões, mas consome recursos e pode abrandar a adoção, sobretudo de IA, se mal aplicada.
- Soberania tecnológica como prioridade: reduzir dependências em cloud, dados, chips e IA; produzir e regular no espaço europeu com previsibilidade.
- Segurança e defesa em alta: investimentos crescentes com spillovers para a economia civil e para a resiliência digital.

Divergências

- Europa “atrasada” vs. “capaz de liderar”: uma corrente culpa o excesso de barreiras; outra recorda casos de vanguarda e sustenta que o problema é de mindset e escala, e não de competência.
- Regulação como travão vs. caminho: se embutida desde o desenho (“by design”), ela acelera; como retrofit, trava.

Implicações práticas para Portugal

1. Escolhas de especialização: apoiar hubs nacionais em cibersegurança e identidade digital, com aplicações em setores críticos (energia, finanças, saúde) e rotas de exportação europeias.
2. Arquiteturas híbridas e multicloud no Estado e em operadores críticos: como “ponte” de soberania até que alternativas europeias ganhem escala.
3. Sandboxes regulatórios nacionais alinhados à UE: para testar IA e automação com dados não críticos, reduzindo tempo de validação e aprendizagem antes de regular.
4. Integração em cadeias europeias de defesa e “dual use”: estimular startups e PME a desenvolverem componentes e software com dupla aplicação (civil/militar).
5. Política de talento “born global”: atração e retenção combinadas a programas que empurrem empresas jovens para mercados externos desde o dia 1.
6. Consolidação e clareza regulatória: reduzir sobreposição de normas e sinalizar previsibilidade aos investidores.

CONCLUSÃO

Portugal pode transformar a “desvantagem” geopolítica europeia em vantagem competitiva se jogar bem três cartas: confiança, segurança e resiliência. Isso significa especializar-se onde o mercado valoriza estabilidade (ciber, dados críticos, identidades digitais), acelerar a adoção de arquiteturas híbridas para mitigar dependências e participar ativamente do novo ciclo de inovação alavancado pela defesa e cibersegurança. A condição é política e cultural: simplificar, integrar decisões e trocar a aversão ao risco por uma gestão de risco madura. Por outras palavras, menos burocracia e mais execução, sem abdicar do diferencial europeu de proteção ao cidadão, a combinação que pode posicionar Portugal como um fornecedor de soluções fiáveis para a Europa e além.

Quando questionados sobre ***Mercado e Competitividade: “Diante das grandes aquisições que vemos no mercado nacional e internacional na área tecnológica, qual a sua visão sobre o papel dos operadores de telecomunicações na oferta de serviços de IT? Confiaria o IT da sua empresa a um operador de telecomunicações?”*** aqui estão os principais pontos referidos:

Uma Nova Geopolítica dos Negócios Tecnológicos

O mercado português de tecnologia atravessa um momento de transformação impulsionado por grandes aquisições, reconfigurações estratégicas de operadores de telecomunicações e pela emergência de novos protagonistas globais, como os hyperscalers. Neste cenário, as dinâmicas de competitividade são impactadas por fatores internos, como a qualidade do talento local, e externos, como os movimentos da regulamentação e geoeconómicos que influenciam fusões e aquisições à escala internacional.

A consolidação é inevitável para ganhar escala, indicam os especialistas, mas ela também pode gerar efeitos colaterais no ecossistema. O risco mais frequentemente mencionado é o chamado “fecho de canal”: quando um operador compra um parceiro integrador, outros players podem sentir-se desincentivados a manter relações com esse novo aglomerado, ameaçando a neutralidade e a diversidade do ecossistema de inovação.

Portugal como Alvo Estratégico e os Limites do Mercado Interno

Portugal surge como um mercado atrativo para aquisições “capacitadoras” por grupos estrangeiros. O país oferece hubs já estruturados com entre 100 e 200 engenheiros, que operam sob o modelo de nearshore. Há registos de abordagens semanais de interessados europeus em adquirir operações locais com boa capacidade de entrega. A motivação impulsionadora dessas compras é estratégica: combinar uma carteira de clientes com capacidade técnica instalada para acelerar o crescimento nos mercados empresariais.

Apesar do capital humano reconhecido, o principal entrave competitivo continua a ser a limitação de escala. “Startups focadas só no mercado português não escalam”, observa um dos inquiridos. A ambição internacional, portanto, não é apenas desejável, mas necessária para sustentar a competitividade a longo prazo.

Operadores de Telecom e a Expansão para Serviços de TI

Uma das principais transformações recentes no ecossistema é a tentativa dos operadores de telecomunicações de se reposicionarem como fornecedores de serviços de tecnologia da informação (TI). Essa movimentação, no entanto, divide opiniões:

- Visão cética: operadores seguem focados em conectividade e vendem pacotes agressivos de preço e segurança, mas estão longe de prover soluções de TI completas, como auditoria, roadmap e serviços geridos de ponta a ponta.
- Visão condicional: aquisições de intesegres técnicos locais podem, em alguns casos, aumentar a confiança do mercado, desde que os operadores provem capacidade real de entrega.
- Visão pragmática: em setores críticos, como o de energia, operadores são inevitáveis para a conectividade, mas não para o core operacional, que permanece on-premises.

Esse debate revela que a confiança nas telcos enquanto fornecedores de IT varia significativamente conforme o setor, o histórico da empresa e a qualidade do serviço após fusões.

Confiança em Transformação e Riscos Estratégicos

A confiança dedicada aos operadores de telco em Portugal está em transição. Quando o foco está apenas no “pacote”, ela tende a ser baixa. Porém, cresce quando há provas concretas de entrega, estrutura técnica reconhecida e histórico positivo com parceiros. Ainda assim, há relatos de queda temporária na qualidade do serviço após aquisições, o que leva algumas empresas a migrarem para concorrentes.

A preocupação com o lock-in tecnológico também é recorrente. Boas práticas de arquitetura recomendam múltiplos fornecedores e planos de saída bem estruturados, especialmente no contexto de cloud e telecomunicações.

O Impacto dos Hiperescalers: Redesenhar a Fronteira Competitiva

Um dos maiores desafios estratégicos para os operadores tradicionais é lidar com a concorrência dos hiperescalers, gigantes da tecnologia que já entregam infraestrutura, plataformas (IaaS, PaaS, SaaS), segurança e serviços geridos. “Hipers já comeram as telcos; hoje oferecem rede, cloud e plataformas”, resume um testemunho recolhido. A presença destes atores obriga os operadores locais a reposicionarem-se como integradores de infraestrutura híbrida, evitando confrontos diretos nas camadas aplicacionais.

Recomendações Estratégicas para o Futuro

1. Escolha inteligente do fornecedor: Telcos devem ser consideradas para serviços como SOC, monitorização, continuidade e infraestrutura híbrida. Já aplicações e software devem ser entregues por parceiros especializados.
2. Mitigação de riscos pós-aquisição: Implementar SLAs transitórios, “clean teams” de suporte e estratégias de reversibilidade ajudam a proteger clientes de eventuais degradações temporárias de qualidade.
3. Gestão do ecossistema: Ao trabalhar com operadores que adquiriram integres, é crucial exigir neutralidade de plataforma, paridade de acesso e gestão aberta para preservar a diversidade de parceiros.

Conclusão

Portugal ocupa uma posição estratégica como hub de tecnologia na Europa, mas precisa continuar a internacionalizar-se e a proteger a diversidade do seu ecossistema. O futuro do mercado depende da capacidade de manter a neutralidade nas parcerias, evitar o lock-in, posicionar-se frente aos hyperscalers e transformar fusões e aquisições em vantagens reais de competitividade, não apenas em concentração de mercado.

Como resume uma frase representativa do estudo:

“O mercado das telecom... já não é rentável; operadores têm de arranjar outros serviços”.

A pergunta para o futuro é: quais os serviços, com quais os parceiros, e sob quais condições de confiança.

Quando questionados sobre **Cibersegurança e Compliance**: **“A sua empresa tem um Plano de Cibersegurança formalizado? Já implementou soluções como XDR ou Zero Trust Architecture? Quais os resultados alcançados? Está considerando adotar Identidade Digital Descentralizada (DID) como medida de segurança? Como é que normas como RGPD e NIS2 (DORA também em instituições financeiras), tal como certificações de qualidade, continuam a ter impacto na estratégia de IT da sua empresa? São inibidoras de projetos de inovação?”** aqui estão os principais pontos referidos:

Cibersegurança e Compliance: onde Portugal está hoje, e o que precisa para 2035

A cibersegurança em Portugal vive uma fase de amadurecimento desigual: enquanto grandes organizações e operadores críticos já operam com planos, governação e testes regulares, uma parte relevante do tecido empresarial, sobretudo PME, ainda trata o tema em “parcelas”, atuando conforme os incidentes, orçamento e pressão regulatória. Em comum, porém, há a compreensão de que segurança e conformidade deixaram de ser custo periférico para se tornarem base de continuidade do negócio e de confiança digital.

Maturidade organizacional: do “plano completo” ao “em consolidação”

Nos **casos mais avançados**, as empresas relatam certificação ISO 27001 recente, políticas e procedimentos formalizados, **SOC 24/7** (centro de operações de segurança) com monitorização contínua e **simulações regulares de phishing e testes de continuidade de negócios**. Noutros, o cenário é “em construção”: redesenho de arquitetura, adoção faseada de **Zero Trust** com foco em identidade e **MFA** (autenticação multifator), além de planos para evoluir à ISO 27001 e incorporação de elementos do **NIS2 conforme o roadmap**.

Verbalização / Frase representativa:

“Temos SOC 24x7 a monitorizar tudo o que se passa na rede.”

Divergência por porte:

- **PMEs:** “não estão de todo preparadas... por custos”, prevalece a perceção de baixa preparação e priorização, com segurança feita “aos pedaços”.
- **Grandes empresas e setor público:** planos, equipas e manutenção contínua, com responsabilidades claras e rotinas de auditoria.

Verbalização / Frase representativa:

“PMEs não estão de todo preparadas... por custos.”

Arquiteturas e soluções em prática

O modelo Zero Trust é cada vez mais adotado como padrão de segurança, especialmente em ambientes com múltiplos dispositivos e acessos externos.

Verbalizações / Frases representativas:

“Não temos como controlar os dispositivos dos clientes, mas conseguimos controlar exatamente o que eles acedem dentro da nossa rede.”

“Com o aumento dos ataques automatizados, a arquitetura zero trust e a autenticação multifator tornaram-se essenciais.”

Zero Trust tornou-se a postura de referência: em vez de “confiar por padrão”, cada acesso é verificado, começando por **gestão de identidade e segmentação de acesso** (quem pode aceder a quê, quando e com que perfil). É aqui que **MFA, NAC** e perfis de privilégio mínimo entram.

Verbalização / Frase representativa:

“Zero Trust é fundamental... as grandes falhas muitas vezes vêm de dentro.”

SOC + IA (humano + inteligência artificial): serviços geridos relatam reduções no tempo médio de deteção (de ~30 minutos para poucos minutos), reforçando um modelo híbrido: máquinas aceleram o alerta; pessoas decidem e contêm o risco.

XDR/MDR (deteção e resposta estendidas/geridas): tendência clara de integração entre *endpoint*, rede e automação de resposta. Mesmo quando não nomeadas, as práticas descritas (SOC + IAM + automação) apontam para esse caminho.

IAM e SSO (identidade no centro): o pilar “saber quem acede a quê, quando e com que perfil” é visto como imprescindível na era da IA. Integrações de **SSO** com aplicações de terceiros e **certificados digitais** para assinatura formal já estão difundidas.

Verbalização / Frase representativa:

“IAM é imprescindível... saber quem acede a quê, quando e com que perfil.”

Resiliência de dados: arquiteturas híbridas/multicloud com cláusulas de data residency e backups on-site/off-site para mitigar ransomware e assegurar recuperação.

Identidade Digital Descentralizada (DID): ainda é tema incipiente e gerou interpretações distintas, da confusão com IAM até preocupações com deepfakes e autenticidade. Em ambientes corporativos, a identidade segue centralizada no stack do fabricante (ex.: Microsoft).

Regulamentos (RGPD, NIS2, DORA): travão ou caminhos?

As **certificações** são vistas como **necessárias**, mas muitas vezes **mal compreendidas** e **aplicadas de forma reativa** pelas empresas.

Verbalizações / Frases representativas:

“As certificações não são elegantes, mas são necessárias.”

“Muitos procuram soluções rápidas para obter um certificado de compliance, sem ter sequer o básico implementado.”

O consenso predominante é que **RGPD, NIS2, DORA e ISO não inibem** a inovação: **umentam o custo e exigem investimento**, mas funcionam como **“guard-rails”** que evitam atalhos arriscados, muitas vezes acelerando a digitalização segura. Ao mesmo tempo, alguns apontam **burocracia e fricção**, pedindo simplificação da experiência (por exemplo, nos cookies), sem abdicar de **criptografia, direito ao esquecimento e auditorias**.

Verbalizações / Frases representativas:

“RGPD cria layer de burocracia... deveríamos simplificar mantendo criptografia e auditorias.”

“NIS2/DORA obrigam estratégia, planos e responsabilizam o board.”

Efeitos práticos observados:

- **NIS2/DORA como aceleradores por obrigação:** em setores críticos, os reguladores impulsionam a estratégia, planos e mitigação; conselhos de administração passam a responder por falhas, com multas significativas.
- **Para PMEs, o impacto é mais irregular:** custos pesam e a fiscalização é quase inexistente, protelam os investimentos.
- **“Sem o básico, não há milagre”:** a corrida por certificações sem uma arquitetura coerente resulta em **“compliance por remendos”**.

Inovação com segurança: recomenda-se **sandboxes** isolados para experimentar com dados não críticos e **regular depois**, por forma a evitar “regular antes de inovar”, sobretudo em IA.

Onde há alinhamento, e onde há divergência

Alinhamentos fortes

- Prioridades técnicas mínimas: IAM robusto, Zero Trust, SOC/monitorização 24/7, backups segregados e testes de continuidade.
- Arquitetura antes de papelada: conformidade só é sustentável com desenho sólido de processos e acessos.
- Regulação como motor em setores críticos: acelera maturidade e responsabilização.

Verbalização / Frase representativa:

“NIS2/DORA obrigam estratégia, planos e responsabilizam o board.”

Divergências notáveis

- RGPD: entre “burocrático e conflituoso” vs. “caminho necessário que profissionaliza o mercado”.

DID: do desconhecimento à interpretação ampla; de momento, MFA + gestão de identidade contextual continuam a prática corrente.

Implicações para Portugal até 2035 (perspetiva aplicada)

1. **Da reação à prevenção:** segurança deixa de “apagar incêndios” e passa a integrar o **planeamento estratégico, com KPIs de risco**, testes recorrentes e reporte ao *board*.
2. **SOC com IA como padrão:** redução sustentada do tempo de deteção para poucos minutos, com *playbooks* de resposta orquestrados.
3. **Zero Trust mainstream:** identidade como novo perímetro, **privilégio mínimo** e acesso segmentado por contexto (utilizador, dispositivo, localização, comportamento).
4. **Compliance by design:** RGPD/NIS2/DORA incorporados ao **ciclo de desenvolvimento** e à **gestão de dados**, evitando “compliance por remendos”.
5. **PMEs em foco:** linhas-guia simples, **serviços geridos acessíveis** e incentivos para elevar o patamar mínimo (*backup* segregado, MFA, inventário de ativos, atualizações e formação anti-phishing). Verbalização / Frase representativa: **“PMEs não estão de todo preparadas... por custos.”**
6. **Identidade e autenticidade:** com **deepfakes** e fraude aumentadas, cresce a procura por **verificação de origem** (assinaturas, carimbos de tempo, políticas *anti-prompt-injection*) e educação do utilizador.
7. **Sandboxes regulatórios:** ambientes de teste com **dados não críticos** para acelerar a inovação em IA e automatização, sem comprometer privacidade e segurança.

Conclusão

O retrato que emerge é pragmático: **Portugal dispõe de ilhas de excelência e um núcleo de boas práticas já consolidado, mas precisa democratizar esse patamar entre as PME e evitar a armadilha do “papel sem arquitetura”.** O caminho para 2035 combina **disciplina técnica (IAM, Zero Trust, SOC com IA) com governação viva (dados, processos, responsabilidades) e regulação como caminho, não como travão.** Em última instância, trata-se de reforçar confiança: na identidade de quem acede, na integridade dos dados e na capacidade de o negócio manter-se de pé, mesmo quando o inesperado acontece.

Verbalizações / Frases representativas:

“RGPD cria layer de burocracia... deveríamos simplificar mantendo criptografia e auditorias.”

“Sem o ‘básico’, a conformidade vira uma manta de retalhos.”

“Zero Trust é fundamental.”

Quando questionados sobre **Infraestruturas e Tecnologias Disruptivas: “Qual o modelo de infraestrutura (on premises, híbrido, cloud ou multicloud) que se tem mostrado mais eficaz para atender às necessidades da sua empresa? Quais os resultados práticos que foram alcançados e que casos ou práticas podem ser considerados exemplos a replicar? Como é que a sua organização avalia os custos e o retorno sobre o investimento (ROI) em cloud, mesmo considerando que não seja necessariamente mais barata que o on premise? Já consideraram ou exploraram tecnologias emergentes como Computação Quântica, 6G, Edge Computing ou soluções com inteligência artificial para automação de código, monitorização e administração de sistemas?”** aqui estão os principais pontos abordados:

Infraestruturas Digitais: Uma Evolução Híbrida e Estratégica

O debate sobre qual o melhor modelo de infraestrutura que corresponde/ que atende às exigências das empresas portuguesas revela uma convergência pragmática: o modelo híbrido, frequentemente multicloud, tem sido amplamente adotado como solução mais adaptativa. Como afirmou um dos inquiridos, “híbrido... core on-prem; o resto em cloud”. Este modelo é visto como forma de equilibrar soberania de dados, continuidade de negócio e controlo de custos.

Tendência Maioritária: Híbrido com Multicloud

Entre os inquiridos, a maioria defende ou opera com uma arquitetura híbrida. Este padrão é especialmente comum em setores críticos, como energia ou gestão pública, onde os sistemas core permanecem on-premises e os serviços de colaboração (como Office 365) migram para cloud. O modelo multicloud, por sua vez, surge como resposta direta ao risco de falhas em grandes provedores.

Verbalização / Frase representativa:

“Sempre multicloud, falhas existem”.

Outros fatores influenciam fortemente essa escolha:

- Soberania e regulação, com exigência de dados residirem na União Europeia;
- Capacidade de resposta a falhas (failover e continuidade de negócio);
- Questões financeiras, com a cloud a ser preferida por facilitar o modelo Opex, embora não necessariamente mais barata

Verbalização / Frase representativa:

“É difícil justificar o ROI da cloud se considerada apenas pelos custos diretos”.

Diversidade de Perfis e Estratégias

Apesar da predominância do modelo híbrido, algumas empresas – especialmente fornecedores de tecnologia e de consultoria – operam sob um modelo “cloud-first” ou até “cloud-only”, por pressão de mercado ou vantagens de escalabilidade. Um executivo refere: “99% dos clientes querem cloud”. Contudo, mesmo nesse grupo, há cautela quanto a riscos de “lock-in”, e soluções alternativas como IaaS local são usadas quando a certificação ou a regulação o exige. Em contraste, setores com operações distribuídas por território (como construção civil) adotam soluções híbridas ajustadas ao custo de armazenamento e à conectividade, utilizando links dedicados, 5G e até Starlink para continuidade em áreas remotas.

Lições Práticas e KPIs

Entre as receitas recorrentes estão:

- **Redução de CAPEX e elasticidade via OPEX;**
- **Diminuição de consumo energético e descarte de hardware;**
- **Alta disponibilidade e recuperação de desastres via IaaS/SaaS.**

Entre os **riscos**, destaca-se a **dependência de conectividade, sobretudo no core operacional**, o que reforça a opção por manter cargas críticas on-prem. Como resumido por um inquirido: “multi-ISP e failover são fundamentais”.

O **ROI**, embora difícil de justificar por preço, é **defendido com base em indicadores** como tempo de provisionamento, tempo de restauro, disponibilidade, redução de administração e conformidade regulatória.

Ganhos & KPIs citados

- **Tempo/Produtividade:** *E-mail/colaboração* em cloud → **menos administração e tempo poupado** pela TI; **voz via software** reduz custos móveis.
- **Conectividade em campo:** obras **acedem SharePoint/BIM**; **5G** iguala/dispensa fibra em prazos curtos; **Starlink** como *breaker* em zonas sem cobertura.
- **Disponibilidade/DR:** *Claims* de **99,9% uptime** dos *hyperscalers* e **backups multi-região; backups on/off-site** para ransomware.
- **Sustentabilidade:** *Hyperscalers* otimizam energia/arrefecimento; **redução** de consumo em *housing* próprio.

Riscos & lições

- **Custo de armazenamento** na cloud para **conteúdos massivos** (docs) → mover/replicar **on-prem** (*tiering*) como *quick win* de otimização.
- **Lock-in / “design for exit”:** **migração é “dolorosa”** sem planeamento de saída e **portabilidade de dados**.
- **M&A de operadores:** transição pode **degradar serviço** no curto prazo; mitigar com **planos de reversibilidade e multi-fornecedor**.
- **Soberania/Residência:** exigir **data residency na UE** e **multicloud** para resiliência/regulação.

Casos/boas práticas replicáveis

1. **Hybrid cost-aware:** front-ends/ERP em cloud + **documentos/backups on-prem** (tier por custo/volume) + **DR no Azure**.
2. **Contrato com data residency + multicloud** (redundância entre *hypers*).
3. **Conectividade operator-agnostic:** *SDN, field-tests* com **3 SIMs, 5G/Starlink** para *time-to-serve* e continuidade em obras.

Backups on/off-site segregados contra ransomware.

“Cloud nem sempre é mais barata”: como justificam custos, medem ROI e decidem migração/otimização

Como justificam

- **ROI por TCO completo**, não por “servidor vs cloud”: incluem **equipas de TI/DBA, licenças, tempo de gestão, energia, SLA/DR, risco de ciber**.
- **Agilidade de negócio**: expansão geográfica/filiais sem *capex*; ERP global acessível “de qualquer parte”.
- **Produtividade/colaboração**: *e-mail/Teams/voz* → **menos custos indiretos e mais velocidade**.
- **Resiliência/segurança**: *uptime* multi-região e **soc/controles** do fornecedor superam *in-house* na maioria dos casos.

Como medem

- **Indicadores típicos** (citados/derivados dos relatos):
 - **Tempo de provisionamento** (5G/Starlink vs fibra) e **tempo de restauro** (DR no Azure).
 - **Horas de administração poupadas** (e-mail em cloud).
 - **Custos evitados de downtime** (paragem de recursos = custo/dia).
 - **Conformidade** (residência UE, backups multi-região).

Como decidem migrar/otimizar

- **Critério por workload**:
 - **Cloud/SaaS**: ERP, colaboração, *burst* de tráfego/acessos sazonais.
 - **On-prem/edge**: **dados massivos** (documentos) e **backups** por **custo/latência**.
 - **Evitar single-vendor**: **multicloud** por **redundância** e **bargaining power**.

Planear exit: prever **portabilidade** para reduzir os constrangimentos da migração.

Tecnologias Disruptivas: Entre o Imediato e o Promissor

No campo das tecnologias disruptivas, o cenário português apresenta uma **mistura interessante de pragmatismo e visão estratégica**. Edge Computing desponta como a transformação mais palpável e imediata, enquanto a Computação Quântica é tratada com prudência, e o 6G ainda encontra pouca aplicação prática.

Edge Computing: O Protagonista da Mudança Tangível

A tecnologia de edge computing é unanimemente reconhecida por sua **aplicabilidade imediata**, especialmente em ambientes que exigem latência mínima e resiliência local. Um caso mencionado é o de um dispositivo de vacinação veterinária com processamento de ponta, exemplo real de como “colocar os equipamentos a falar diretamente entre si” pode gerar **ganhos substanciais em eficiência e autonomia**.

A utilização de 5G, Starlink e Wi-Fi 6/7 como **vetores de conectividade ubíqua** fortalece ainda mais a viabilidade do edge, sobretudo em **operações distribuídas ou temporárias**. “A transformação mais imediata [é no] edge”, elenca um dos participantes.

IA em Pilotos Reais: Primeiros Passos, Resultados Visíveis

A **inteligência artificial** já **figura em projetos-piloto** ou **em produção em diversas organizações**, com aplicações que vão da **geração de código à triagem preditiva** em segurança e consumo de energia. Um inquirido relatou: “temos três projetos em curso”, envolvendo **desde conteúdos gerados por IA até ferramentas de automação**.

Apesar disso, **nem todas as empresas estão no mesmo estágio**. Enquanto algumas já capacitam equipas e integram IA a rotinas administrativas, outras ainda priorizam a digitalização de processos básicos. A maioria, contudo, reconhece que “a procura por IA já está a ser universal”.

Casos replicáveis incluem o uso de copilotos com validação humana, IA local para proteção de dados sensíveis e agentes internos (ex. no Teams) que integram sistemas corporativos.

6G: Promessa Ainda em Maturação

As **opiniões sobre o 6G são divergentes**. Enquanto alguns antecipam a próxima geração como um catalisador de colaboração imersiva e descentralizada (“conectividade quase instantânea”), outros a veem apenas como uma evolução incremental do 5G, com ganhos marginais e aplicação limitada no curto prazo.

A ausência de projetos com 6G nas empresas inquiridas corrobora essa **visão cautelosa**. Hoje, o **foco está na expansão do uso do 5G** e no **fortalecimento de redes Wi-Fi 6/7**.

Computação Quântica: Potencial Altíssimo, Horizonte Longo

A computação quântica, por sua vez, é perçecionada como altamente transformadora, mas ainda distante do uso empresarial generalizado. A expectativa de maturidade prevê-se que seja perto de 2030, com destaque para impactos em segurança, criptografia e aceleração de IA. “Vai redefinir encriptação e segurança”, afirma um dos inquiridos.

Entretanto, há também confusão e entusiasmo prematuro: alguns inquiridos atribuem à computação quântica benefícios que, na realidade, decorrem da IA generativa. A recomendação prática é acompanhar o avanço, experimentar pilotos em cloud e iniciar desde já um roadmap de “cripto-agilidade”.

O que muda nos métodos de trabalho e infraestruturas

Mudanças já visíveis

- **Operações de campo: 5G** como *shortcut* de conectividade (elimina espera de fibra), acelera **set-up** de obras/unidades temporárias.
- **Operação com IA: copilotos** a auxiliar **coding, deteção preditiva de vulnerabilidades e automitigações**; humanos validam **falsos positivos**.
- **Edge “event-driven”**: visão/analytics **no local** e só **eventos** escalam para o core, **reduz tráfego e custo**, melhora **latência** e **privacidade**.

Mudanças esperadas (próximos anos)

- **Agentes corporativos** (front-end conversacional único) a **integrar aplicações** de RH, compras, ITSM, etc., reduzindo “*app-hopping*”.
- **Quântica** a acelerar **IA** e a exigir **criptografia pós-quântica**; possível “*corrida à supremacia*” *ataque vs defesa* com IA + quântica.

Conclusão e Caminhos Recomendados

Portugal mostra-se atento e progressivo na adoção de infraestruturas digitais e tecnologias disruptivas. As empresas estão a avançar na inovação com prudência, adaptando os seus modelos à realidade local de regulação, conectividade e risco.

Recomendações práticas para o ecossistema empresarial português:

- **Adotar o modelo híbrido com consciência de custo e risco**, priorizando multicloud quando a continuidade de negócio é crítica.
- **Investir em edge computing** onde latência, privacidade ou resiliência são prioridades.
- **Usar IA com “cinto de segurança”**, iniciando por tarefas padronizadas e promovendo a formação interna.
- **Planear para a computação quântica**, iniciando avaliações de impacto em segurança e algoritmos críticos.
- **Avaliar com critério o salto para 6G**, focando no que 5G e Wi-Fi 6/7 já entregam com bom custo-benefício.

Como resume um dos inquiridos: “*Híbrido (muitas vezes multicloud) é o padrão mais adaptativo*”. O futuro tecnológico de Portugal será construído sobre essa base de flexibilidade estratégica e inovação responsável.

Quando questionados sobre **Inteligência Artificial e Automação**: “*Com o papel crescente da IA na automação de funções, como imagina a estrutura das equipas de IT nos próximos anos? Como avalia o impacto da IA na cibersegurança, considerando tanto os ataques como as soluções de defesa?*” aqui estão os principais pontos referidos:

Inteligência Artificial e Automação, Um Futuro Integrado entre Máquinas e Humanos

A inteligência artificial (IA) está a remodelar silenciosamente os bastidores das empresas. Não se trata de uma substituição em massa de empregos, mas de uma **profunda reorganização de tarefas e competências**. Há um consenso entre os inquiridos de que a IA está a **automatizar atividades repetitivas e operacionais**, como triagem de tickets, help desk e administração de bases de dados, permitindo que os **humanos se concentrem na análise, curadoria e supervisão dos processos automatizados**.

“Muitas funções serão substituídas; novas irão surgir” resume uma das declarações. A IA, nesse contexto, atua como um **copiloto**: acelera decisões, melhora a produtividade e permite a realocação do **tempo humano para tarefas mais estratégicas**. Essa visão não é especulativa; já há relatos de rádios inteiramente geridos por IA, bem como de sistemas que sugerem soluções operacionais com base em manuais e dados históricos.

Contudo, há divergência quanto à velocidade e profundidade dessas transformações. Um inquirido sublinha que a estrutura das empresas **“não vai mudar assim tanto... haverá mais especialização”**, sinalizando que a requalificação será mais relevante do que uma reinvenção total dos organogramas.

O Futuro das Equipas de TI: De executores a integradores

A evolução das equipas de TI tende a seguir o princípio da “integração”. Os profissionais deixam de ser executores de tarefas manuais para se tornarem gestores de agentes automatizados. As previsões apontam para equipas mais pequenas, focadas na gestão de processos inteligentes, validação de outputs e integração de sistemas.

Funções tradicionais como programadores, analistas e gestores de projeto serão parcialmente automatizadas. Um novo perfil profissional emerge, com competências em *prompt engineering*, *data/ML Ops*, gestão de modelos e segurança por design. A automação do suporte de primeiro nível (L1) será uma realidade, **“agente de ajuda informática como primeira linha antes de ligar para o suporte”** —, enquanto os humanos ficam responsáveis por casos mais complexos (níveis L2 e L3).

A atratividade das empresas também será impactada. Organizações que apostam em IA e automação já são perçecionadas como mais inovadoras e, portanto, mais capazes de atrair talentos.

Hipótese: a automação com IA **acelera** o movimento de sair do “mão-na-massa de servidores” para **operações integradas por software**, com papéis novos na **gestão de modelos, engenharia de dados e observabilidade** (derivado das menções a “regular, afinar, direcionar” modelos).

Novas competências citadas/implícitas: gestão e tuning de modelos, engenharia de prompts/processos, data/ML Ops, segurança por design (mencionado como “regular/afinar modelos” e maior foco em dados).

Visão “mix humano-máquina” (1/7): integração crescente entre capacidades humanas e sistemas inteligentes (“*veja bem o homem biónico*”).

Hipótese: funções puramente operacionais (ex.: instalação manual em massa) **tendem a diminuir**; crescem funções de **arquitetura, integração, SRE/observabilidade e gestão de risco** (derivado do argumento de que o trabalho “manual” já foi deslocado na transição para cloud e seguirá com IA).

Cibersegurança: A Corrida IA contra IA

Se por um lado a IA impulsiona a eficiência, por outro amplia os desafios na cibersegurança. A **“corrida à supremacia IA↔IA”** já começou. Ferramentas de IA estão a ser utilizadas para criar ataques com mais velocidade, volume e verossimilhança, desde e-mails de phishing a chamadas com voz falsificada (voice phishing). **“Criação de e-mails maliciosos muito mais rápida”**, alertou um dos participantes.

Em contrapartida, a IA também fortalece a defesa. Com a sua capacidade de análise em tempo real, a deteção de ameaças pode ser reduzida de 30 minutos para menos de 5, uma redução drástica no Mean Time To Detect (MTTD). A aplicação da IA em Security Operations Centers (SOCs), com *machine learning* para detetar padrões comportamentais e prever ataques, transforma o cenário defensivo: **“dados são o ouro; padrões antecipam ataques”**.

Além disso, práticas como monitorização 24/7, adoção de princípios Zero Trust (**“não confiar em ninguém”**) e autenticação sem password (passwordless) são vistas como essenciais. A cultura de risco precisa ser proativa, com simulações internas regulares (*red/blue teaming*) e clareza sobre a responsabilidade na tomada de decisões automatizadas.

Adoção Prática: Pilotos, Copilotos e AIOps

Vários inquiridos relatam que a adoção da IA já saiu da teoria e está em curso, com projetos piloto e aplicações em produção em áreas como geração de conteúdos, ferramentas internas e automação de decisões operacionais. O termo “copilotos” tornou-se comum, indicando assistentes de IA que apoiam funções como logística, marketing e desenvolvimento de produtos. A universalização da procura por soluções e capacitação é outro sinal claro de que a IA entrou na agenda estratégica das empresas portuguesas. A integração com sistemas de monitorização (AIOps) é apontada como um próximo passo natural, dado o volume crescente de dados e a necessidade de correlacioná-los com agilidade.

Boas Práticas e Caminhos para Replicação

Com base nas práticas mencionadas pelos inquiridos, destacam-se algumas recomendações replicáveis para empresas que desejam avançar na adoção da IA:

- **Automatizar o nível I de suporte** com agentes inteligentes e manter validação humana nos níveis mais complexos.
- **Implementar Zero Trust real**, com privilégios mínimos e autenticação multifator robusta.
- **Integrar IA nos SOCs**, com telemetria contínua, deteção comportamental e resposta automatizada.
- **Executar testes internos contínuos (red/blue teams)** para fortalecer a maturidade de segurança.
- **Documentar a política de propensão ao risco**, assegurando que o board compreenda e aprove as decisões estratégicas.

Conclusão

A inteligência artificial está a assumir o papel de coautora da transformação digital em Portugal. Em vez de substituir pessoas, ela reorganiza o trabalho, eleva o nível das tarefas humanas e fortalece as defesas digitais. À medida que mais empresas adotem agentes inteligentes e copilotos, emerge um novo paradigma: o da integração entre máquinas e humanos, onde a responsabilidade, a ética e a estratégia continuam a ser humanas.

“A IA não substitui as pessoas; a decisão final é humana”, essa frase, repetida em diferentes variações ao longo das entrevistas, resume não só a prudência, mas também a esperança com que os líderes tecnológicos portugueses olham para o futuro.

Quando questionados sobre **ESG e Sustentabilidade**: **“Na sua empresa o tema da sustentabilidade é efetivamente uma prioridade hoje? E em que medida o departamento de TI pode ou não contribuir para os objetivos ESG da empresa até 2035? Quando pensa em Cloud ou Housing, já avalia se o data center tem objetivos de neutralidade carbónica e em que medida este será um fator decisivo na escolha de parceiros tecnológicos?”** aqui estão os principais pontos elencados:

ESG e Sustentabilidade – Entre o Compromisso e a Transição

Nos últimos anos, a sustentabilidade e os princípios ESG (ambiental, social e de governação) deixaram de ser temas periféricos para ocupar um papel central na estratégia de muitas empresas em Portugal, especialmente no setor tecnológico. No entanto, o grau de maturidade e implementação dessas práticas ainda é heterogéneo, variando conforme a dimensão da empresa, o setor de atividade e as exigências dos stakeholders. Como refere um testemunho analisado, “os clientes já pedem reporting... se não cumprimos, somos excluídos”, revelando o peso crescente da sustentabilidade como critério de competitividade.

Apesar da crescente pressão por sustentabilidade, a prática ainda esbarra em desafios de investimento e viabilidade, especialmente fora do setor industrial.

Verbalização / Frase representativa:

“Fala-se muito sobre sustentabilidade nos edifícios, mas o custo de adequação é altíssimo e pouco tangível fora do setor industrial.”

“Hoje não há avaliação formal sobre neutralidade carbónica de data centers nos processos de contratação, embora já haja sinais de mudança em organismos públicos.”

Conclusão

A inteligência artificial está a assumir o papel de coautora da transformação digital em Portugal. Em vez de substituir pessoas, ela reorganiza o trabalho, eleva o nível das tarefas humanas e fortalece as defesas digitais. À medida que mais empresas adotem agentes inteligentes e copilotos, emerge um novo paradigma: o da integração entre máquinas e humanos, onde a responsabilidade, a ética e a estratégia continuam a ser humanas.

“A IA não substitui as pessoas; a decisão final é humana”, essa frase, repetida em diferentes variações ao longo das entrevistas, resume não só a prudência, mas também a esperança com que os líderes tecnológicos portugueses olham para o futuro.

Quando questionados sobre **ESG e Sustentabilidade**: **“Na sua empresa o tema da sustentabilidade é efetivamente uma prioridade hoje? E em que medida o departamento de TI pode ou não contribuir para os objetivos ESG da empresa até 2035? Quando pensa em Cloud ou Housing, já avalia se o data center tem objetivos de neutralidade carbónica e em que medida este será um fator decisivo na escolha de parceiros tecnológicos?”** aqui estão os principais pontos elencados:

ESG e Sustentabilidade – Entre o Compromisso e a Transição

Nos últimos anos, a sustentabilidade e os princípios ESG (ambiental, social e de governação) deixaram de ser temas periféricos para ocupar um papel central na estratégia de muitas empresas em Portugal, especialmente no setor tecnológico. No entanto, o grau de maturidade e implementação dessas práticas ainda é heterogéneo, variando conforme a dimensão da empresa, o setor de atividade e as exigências dos stakeholders. Como refere um testemunho analisado, “os clientes já pedem reporting... se não cumprimos, somos excluídos”, revelando o peso crescente da sustentabilidade como critério de competitividade.

Apesar da crescente pressão por sustentabilidade, a prática ainda esbarra em desafios de investimento e viabilidade, especialmente fora do setor industrial.

Verbalização / Frase representativa:

“Fala-se muito sobre sustentabilidade nos edifícios, mas o custo de adequação é altíssimo e pouco tangível fora do setor industrial.”

“Hoje não há avaliação formal sobre neutralidade carbónica de data centers nos processos de contratação, embora já haja sinais de mudança em organismos públicos.”

Sustentabilidade de Hoje: Uma Prioridade Ainda em Construção

A maioria dos inquiridos considera a sustentabilidade uma prioridade formalizada, com indicadores concretos como reporting anual de energia, auditorias ambientais e metas internas de eficiência energética. Em alguns casos, a agenda é impulsionada por **obrigações regulatórias, certificações ambientais e pressões dos clientes**. “Temos programas muito fortes... somos obrigados a reportar anualmente os consumos energéticos”, afirmou um dos inquiridos. Por outro lado, há organizações que reconhecem lacunas, especialmente entre PMEs. Nessas, a sustentabilidade ainda não é tratada como eixo estratégico. Como expresso por um dos inquiridos: “Deveria ser. Ainda não estamos aí.” Soma-se a isso a percepção de que o investimento em infraestruturas verdes impõe um alto CAPEX, dificultando avanços mais acelerados. Outra preocupação emergente é a possível **tensão entre metas climáticas e as urgências macroeconómicas**. “Os EUA vão ignorar... a Europa tem que se definir”, disse um participante, sugerindo que a geopolítica pode impactar os compromissos ambientais no curto prazo.

A Contribuição da Tecnologia para os Objetivos ESG até 2035

A visão predominante entre os inquiridos é que a tecnologia, especialmente o setor de TI, será uma das principais alavancas para viabilizar metas ESG. Foram mencionadas diversas práticas já em curso ou em expansão:

- **Eficiência energética** como critério essencial na compra e operação de soluções de TI.
 - “Temos de procurar eficiência energética em novos serviços de IT.”
- **Virtualização e consolidação de servidores**, reduzindo hardware e consumo de energia.
 - “Virtualização reduziu muito o hardware.”
- **Digitalização e eliminação de papel**, com processos paperless integrados ao dia a dia operacional.
 - “Sem papel na produção... e painéis solares a alimentar a operação.”
- **Edifícios inteligentes e infraestrutura verde**, com uso de painéis solares, sensores e sistemas de climatização otimizados.
 - “Data center é o maior consumo... olhar para cooling e solar.”
- **Ciclo de vida de equipamentos**: extensão do uso, reutilização, e abate responsável como forma de reduzir o impacto ambiental.
- **Gestão ambiental**: contratos com cláusulas de sustentabilidade, exigência de reporting de fornecedores e uso de práticas como FinOps/GreenOps para calcular custos e emissões por workload.

Há consenso de que a pegada energética do setor de TI está a crescer, especialmente com a expansão dos data centers. Como observou um inquirido: “Somos um dos grandes consumidores energéticos... temos de mudar e melhorar.”

Neste contexto, tecnologias como AIOps e práticas combinadas de custo e carbono (FinOps + CarbonOps) surgem como hipóteses para reduzir emissões até 2035.

Data centers, Cloud e a Corrida pela Neutralidade Carbônica

A neutralidade carbônica dos data centers (DCs) começa a ganhar peso como critério de contratação, sobretudo entre grandes empresas e setores regulados como telecomunicações, finanças e seguros.

Verbalização / Frase representativa:

“Fator decisivo na escolha do parceiro? Acredito que sim.”

Em contas públicas ou grandes RFPs (Request for Proposal), já se exige que fornecedores demonstrem eficiência energética e compromissos ambientais. Além disso, hyperscalers estão a elaborar contratos de longo prazo com fornecedores de energia renovável para garantir uma operação de baixo carbono, “Data centers comprem energia 100% verde... contratos de 30 anos”. Ainda assim, o critério “verde” ainda não é padrão dominante em empresas privadas de menor porte. A redundância, o Tier III e a segurança continuam a ser os fatores principais na seleção de parceiros de cloud e housing. Como resumido por um inquirido: “À data de hoje? Não [avaliamos neutralidade]... interessa redundância/Tier.”

A tendência, no entanto, é de evolução. Os especialistas acreditam que até 2035 a neutralidade carbônica e os indicadores de sustentabilidade tornar-se-ão mandatórios em toda a cadeia de valor, arrastados pela regulação, auditorias e pressão dos clientes.

Divergências claras

- Grau de prioridade: de “DNA + reporting obrigatório” a “deveria ser, ainda não é”.
- Velocidade da transição energética: preocupação com ritmo “rápido demais” vs. urgência climática.
- Critérios de contratação de DC/Cloud: redundância/Tier ainda domina vs. “verde conta e tende a crescer”, solicitados pelo público e clientes.

Boas Práticas Replicáveis para o Futuro Sustentável

Diversas práticas já consolidadas emergem como modelos replicáveis para empresas que desejam acelerar a agenda ESG com suporte da tecnologia:

- **Governança e métricas:** manter reporting ESG anual, com auditorias regulares.
- **Virtualização e arquitetura eficiente:** consolidar servidores, otimizar climatização e reduzir ociosidade.
- **Digital workplaces:** metas claras de eliminação de papel e cultura paperless.
- **Cloud com evidência de carbono:** exigir relatórios de emissões e cláusulas contratuais de sustentabilidade.
- **Supply Chain com baixa emissão:** critérios de eficiência e logística eficiente nos processos de compra.
- **FinOps e GreenOps:** cálculo e gestão do custo e da pegada de carbono por aplicação e carga de trabalho.

Conclusão: Entre a Urgência e a Oportunidade

A sustentabilidade já **não é uma escolha opcional**, é um imperativo competitivo e regulatório. Embora o avanço seja desigual, especialmente entre PMEs, há uma **tendência clara** de incorporação dos princípios **ESG no coração das operações tecnológicas em Portugal**.

Até 2035, espera-se que a tecnologia não apenas contribua, mas lidere a transformação.

Como refere um dos testemunhos: *“Uma das maneiras é a cloud... está a baixar a pegada energética.”* Nesse cenário, eficiência energética, digitalização, governação ambiental e escolhas conscientes de infraestrutura serão pilares de uma **nova lógica empresarial: mais verde, mais ética e mais preparada para o futuro**.

Quando questionados sobre **Recursos Humanos e Cultura de Trabalho**: **“Quais os principais desafios para atrair e reter talentos na área de IT? Como é que a sua empresa os está a superar? Como vê o equilíbrio entre modelos de trabalho presencial, híbrido e remoto no futuro? A sua empresa cria dinâmicas de convívio, reuniões de colaboração e discussão estratégica ou operacionais de alinhamento das pessoas e passagem de objetivos individuais e coletivos?”** aqui estão os principais pontos elencados:

Recursos Humanos e Cultura: Um novo paradigma para a atração e retenção de talentos

O ecossistema tecnológico em Portugal enfrenta uma encruzilhada estratégica na gestão de pessoas. O país vive uma realidade marcada pela escassez de profissionais qualificados, a crescente competição global e a mudança geracional nas expectativas de trabalho. Como sintetizou um dos inquiridos: *“Portugal sofre canibalização de talento pela Europa”*. Empresas estrangeiras, com capacidade de oferecer salários entre duas a quatro vezes maiores do que o praticado localmente, têm seduzido profissionais portugueses, agravando o chamado *“brain drain”*.

A escassez não é apenas uma questão de fuga de cérebros, mas também de origem estrutural. Há *“menos licenciados e muitos trabalham para fora”*, enquanto funções mais tradicionais de TI são hoje vistas como *“commodity”*. Nesse cenário, as empresas competem por profissionais especializados em dados e inteligência artificial, a nova fronteira da disputa por talentos.

Verbalização / Frase representativa:

“As pessoas veem o trabalho como um meio para financiar a vida pessoal, não como um projeto de realização profissional.”

“Por mais que se pague, se não houver ambiente de trabalho dinâmico e ligação entre as pessoas, o talento vai embora por 50 euros a mais.”

Face a este contexto, torna-se imprescindível a **construção de uma proposta de valor ao colaborador que vá além da remuneração**. Entre as práticas que se têm mostrado eficazes, destaca-se a **flexibilidade real** no modelo de trabalho, especialmente o híbrido —, a **oferta de desafios** técnicos modernos (com foco em IA e automação), oportunidades **de aprendizagem contínua** e a **clareza de propósito** e impacto no trabalho realizado.

Híbrido como padrão: entre confiança e cultura

A forma como as empresas estruturam o trabalho mudou radicalmente. A tendência maioritária, identificada nas entrevistas, aponta o modelo híbrido como solução de equilíbrio entre produtividade, bem-estar e manutenção da cultura organizacional. Para muitos, **“o híbrido resolve o problema”, permitindo que se mantenha “a mesma página” entre as equipas, sem abdicar da flexibilidade**.

O modelo remoto integral, embora adotado para ampliar o acesso a talentos fora do país, levanta alertas quanto à **coesão cultural**. A presença física, mesmo que esporádica, é vista como importante para **preservar vínculos e reforçar a identidade** coletiva. Por outro lado, o trabalho 100% presencial é cada vez mais raro, reservado a funções que exigem intervenção física, como na indústria ou infraestrutura.

Um dos pontos críticos mencionados é a confiança. Parte das empresas recuou do teletrabalho por dificuldade de controle, mas outras sustentam que a produtividade pode ser comprometida se o “dia de escritório” for mal aproveitado, por exemplo, com excesso de reuniões. A lição aprendida: *“Não transformar o ‘dia no escritório’ numa maratona de reuniões”*.

Rituais, encontros e cultura: a cola invisível

Num ambiente cada vez mais distribuído, a **cultura organizacional precisa ser cultivada com intencionalidade**. Práticas como encontros semanais com câmaras ligadas, reuniões semestrais presenciais (offsites), eventos sociais e até passeios são **recursos utilizados para manter a coesão**. *“Rituais semanais e offsites reforçam a cultura”*, resume uma das vozes ouvidas.

O objetivo não é apenas **promover integração social**, mas também **alinhar objetivos individuais e coletivos**. Estratégia, metas e “o porquê” do trabalho são constantemente comunicados, reduzindo ansiedade e reforçando o sentido de propósito. O pragmatismo também se impõe: *“Flexibilidade semanal para conviver é produtividade”*.

Há ainda experiências-piloto como a semana de quatro dias em áreas administrativas, um sinal de que a **inovação em RH também passa por testar novos métodos de trabalho**.

Segmentação e propósito: personalização da proposta de valor

Outro aspeto estratégico é a **segmentação geracional na comunicação e nos benefícios oferecidos**. Inquiridos indicam a adoção de diferentes “narrativas” de **employer branding**, com mensagens ajustadas a perfis distintos, dos mais jovens, que procuram flexibilidade e propósito, aos mais experientes, que valorizam estabilidade e plano de carreira. *“O talento tem de sentir propósito”*, reforça um dos relatos.

Além disso, a **tecnologia** em si torna-se **parte da proposta de valor**. *“Equipa que vai apostar no futuro... é mais atrativa”*, afirma um dos inquiridos. O alinhamento com temas como automação, IA e impacto social amplia o apelo do projeto organizacional.

Implicações e caminhos futuros

O estudo revela uma convergência clara: o futuro do trabalho será híbrido, mas com nuances por função, atividade e perfil. A retenção dependerá da capacidade de alinhar salários e benefícios competitivos, um projeto tecnológico credível e um propósito claro. O talento, hoje, procura mais do que emprego: quer fazer parte, desafio e flexibilidade.

A gestão de cultura deixa de ser espontânea e passa a ser desenhada com rituais regulares, encontros periódicos e escuta ativa. Como resumido numa das falas: “Trabalhamos para um propósito que acrescenta valor”.

Assim, a chave para o futuro de Recursos Humanos em tecnologia não está apenas em atrair, mas em reter, com uma cultura viva, um projeto inovador e uma escuta constante às transformações da sociedade e do trabalho.

FASE 3:

QUALITATIVA

Entrevistas em

Profundidade

Entre o pragmatismo e a ambição,
um futuro a ser moldado

As entrevistas realizadas oferecem um retrato lúcido e realista do momento vivido pelas lideranças de tecnologia em Portugal. Mais do que visões idealizadas, o que emerge é um conjunto de reflexões pautadas pela experiência prática, pelo compromisso com a transformação e, acima de tudo, pela consciência de que o futuro não será apenas herdado, ele terá de ser construído.

Há um fio condutor que atravessa todas as conversas: a urgência por adaptação. A velocidade das mudanças tecnológicas, a pressão por segurança e a fragmentação dos modelos de trabalho impõem decisões complexas, em tempo real, muitas vezes sem margem para erro. Os inquiridos reconhecem que não se trata mais de “escolher” inovar, trata-se de sobreviver com relevância num ecossistema que não espera.

Ao mesmo tempo, o tom geral é de esperança ativa. As soluções existem. As competências também. E Portugal, com sua posição estratégica, ambiente regulatório sólido e crescente reputação como polo de startups e centros de dados, tem condições reais de se destacar como protagonista na nova economia digital europeia. Para isso, será necessário ir além do discurso, libertando a inovação do excesso de burocracia, valorizando os talentos locais, e investindo de forma estruturada em sustentabilidade, cibersegurança e infraestrutura digital.

As lideranças ouvidas indicam que o verdadeiro diferencial competitivo não estará apenas na tecnologia adotada, mas na capacidade de combinar inovação com confiança, agilidade com responsabilidade, e propósito com resultados. O desafio está colocado. E os próximos anos serão decisivos para definir se Portugal ocupará um papel periférico ou central neste novo capítulo da história tecnológica da Europa.

04

**Quantitativa:
Survey**

FASE 4: QUANTITATIVA Survey

Resultados

Como já mencionado no início deste documento o objetivo deste survey foi obter insights, apurar o estado de espírito e a percepção dos inquiridos em relação realidade atual das empresas em que atuam e as perspetivas futuras do panorama tecnológico português.

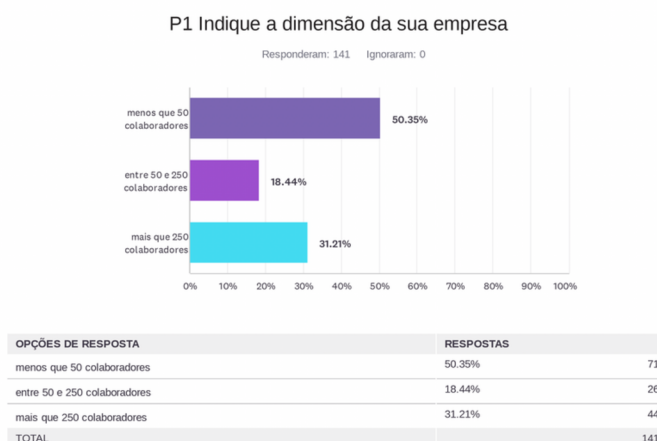
Vale destacar que, não se trata de uma amostra representativa e nem probabilística, já que não condiz ao perfil demográfico das empresas portuguesas. A seleção foi feita por conveniência, usada conforme a facilidade de acesso aos inquiridos e uso de ferramentas tecnológicas no seu quotidiano.

Ao todo foram 141 questionários respondidos por CTO's de diferentes empresas de setores diversos, de todo o território português. O survey foi disponibilizado em plataforma online, entre os meses de junho e julho de 2025.

Esta fase é complementar à fase qualitativa oferecendo amplitude para a triangulação dos dados, de ambas as fases, oferecendo uma visão mais robusta e fiável sobre o objeto do estudo a partir da realidade portuguesa, mesmo sem representatividade estatística.

Dimensão da Empresa

A primeira questão analisa a dimensão das empresas inquiridos, como pode ser observado no gráfico 1.



(Gráfico 1 – Dimensão da Empresa)

A maioria absoluta dos inquiridos (50,35%) atua em empresas com menos de 50 colaboradores, sugerindo que a amostra tem forte peso de micro e pequenas empresas. Isso pode influenciar a percepção sobre temas como recursos disponíveis, estrutura organizacional, processos internos e capacidade de investimento.

Apesar da predominância das pequenas, há 31,21% de grandes empresas, o que garante representatividade de realidades organizacionais mais robustas e complexas.

Empresas de médio porte (50 a 250 colaboradores) formam o menor grupo da amostra (18,44%), o que pode indicar:

- Menor envolvimento deste segmento na investigação.
- Menor quantidade desse perfil no universo investigado.
- Ou ainda, que empresas médias podem estar em transformação, migrando para pequenas (por downsizing) ou grandes (por crescimento).

Implicações e Reflexões

Ações e políticas voltadas ao ecossistema empresarial devem considerar que mais da metade dos inquiridos atua em estruturas reduzidas, com recursos e tempo limitados. Isso exige soluções simplificadas, acessíveis e de fácil implementação.

Por outro lado, um terço da amostra representa empresas maiores, que podem necessitar de tecnologias mais robustas, compliance estruturado, soluções escaláveis e personalizadas.

A baixa representatividade das médias empresas pode sugerir a necessidade de uma escuta mais ativa deste grupo ou de incentivo à sua participação em investigação e processos de decisão.

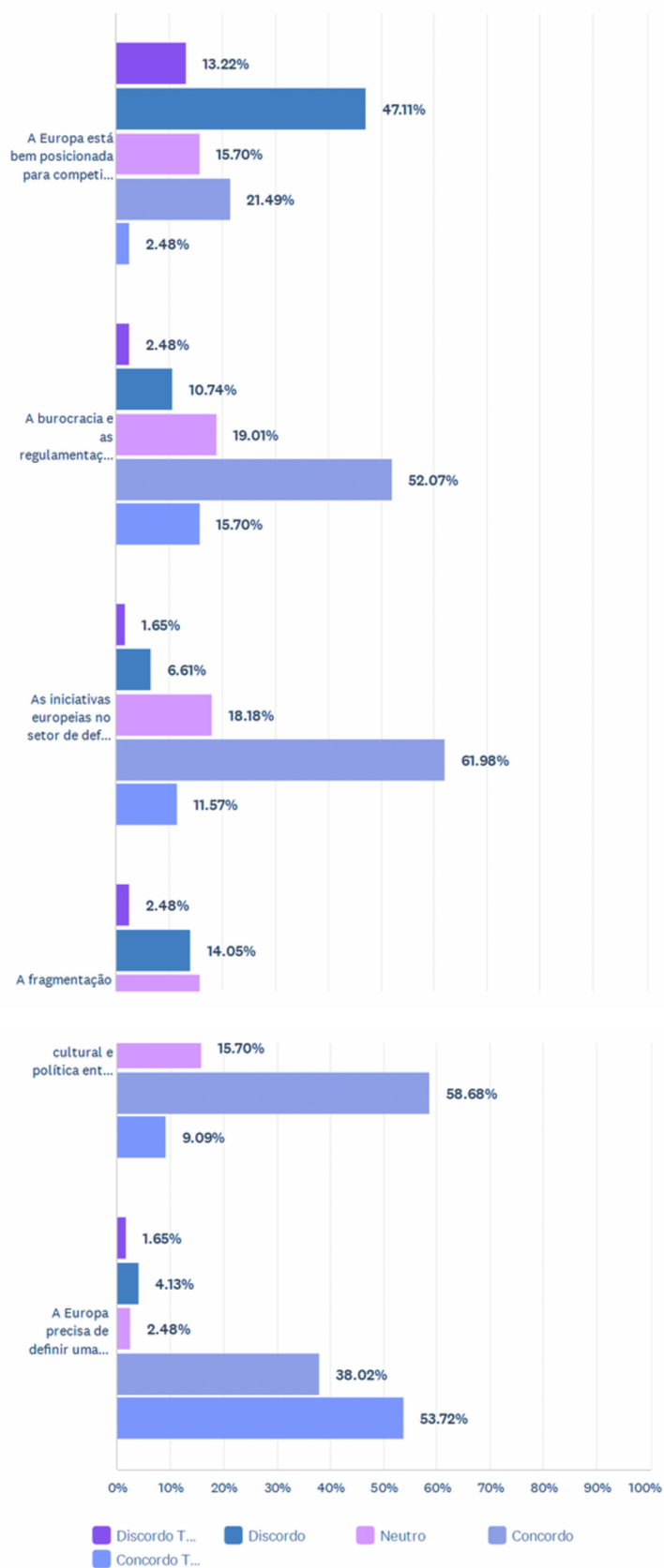
- Adoção de tecnologia e inovação: grandes devem desenvolver projetos estruturados; pequenas, soluções pragmáticas/low-cost.
- Governança e compliance: mais fortes nas grandes; nas pequenas, processos curtos e decisões centralizadas.
- Aquisição de talentos e capacitação: grandes com programas formais; pequenas com polivalência e formação on the job.
- Parceiros/ecossistema: pequenas tendem a parcerias táticas; grandes a alianças estratégicas e RFPs.

Geopolítica e Inovação Tecnológica

As respostas, apresentadas no gráfico 2 e na tabela 1, revelam uma visão crítica e ao mesmo tempo construtiva sobre o papel da Europa no cenário de inovação tecnológica global, com concordância significativa em afirmações que apontam entraves e desafios estruturais. A seguir a visualização do gráfico 2 e a tabela 1 com a análise por item:

P2 Nível de concordância com afirmações sobre geopolítica e inovação tecnológica

Responderam: 121 Ignoraram: 20



(Gráfico 2 - Geopolítica e Inovação Tecnológica)

	DISCORDO TOTALMENTE	DISCORDO	NEUTRO	CONCORDO	CONCORDO TOTALMENTE	TOTAL	MÉDIA PONDERADA
▼ A Europa está bem posicionada para competir com Estados Unidos, China e Índia no desenvolvimento de novas tecnologias.	13,22% 16	47,11% 57	15,70% 19	21,49% 26	2,48% 3	121	2,53
▼ A burocracia e as regulamentações europeias dificultam significativamente a inovação tecnológica no continente.	2,48% 3	10,74% 13	19,01% 23	52,07% 63	15,70% 19	121	3,68
▼ As iniciativas europeias no setor de defesa podem impulsionar significativamente a inovação tecnológica nos próximos anos.	1,65% 2	6,61% 8	18,18% 22	61,98% 75	11,57% 14	121	3,75
▼ A fragmentação cultural e política entre os países europeus é uma barreira importante para a construção de uma estratégia conjunta de inovação.	2,48% 3	14,05% 17	15,70% 19	58,68% 71	9,09% 11	121	3,58
▼ A Europa precisa de definir uma estratégia unificada de inovação para não se tornar apenas consumidora de tecnologia externa.	1,65% 2	4,13% 5	2,48% 3	38,02% 46	53,72% 65	121	4,38

(Tabela 1 – Geopolítica e Inovação Tecnológica)

As respostas revelam uma visão crítica e ao mesmo tempo construtiva sobre o papel da Europa no cenário de inovação tecnológica global, com concordância significativa em afirmações que apontam entraves e desafios estruturais. A seguir, a análise por item:

“A Europa está bem posicionada para competir com Estados Unidos, China e Índia no desenvolvimento de novas tecnologias.”

- **Discordância total ou parcial: 60,33% (13,22% + 47,11%)**
- **Concordância total ou parcial: 23,97%**
- **Média ponderada: 2,53 (abaixo da média neutra de 3)**

A maioria acredita que a Europa **não está bem posicionada** na corrida tecnológica global, ficando atrás das potências como EUA, China e Índia.

Possíveis causas:

- Investimentos fragmentados em inovação.
- Ausência de grandes empresas globais de tecnologia europeias com impacto semelhante a Google, Amazon, Tencent ou Infosys.
- Menor velocidade de adoção de tecnologias emergentes.
- Dificuldade em reter talentos frente à concorrência internacional.

“A burocracia e as regulamentações europeias dificultam significativamente a inovação tecnológica no continente.”

- Concordância total ou parcial: 67,77%
- Média ponderada: 3,68

Há uma percepção consolidada de que a Europa é excessivamente reguladora, o que impacta negativamente sua capacidade de inovar.

Possíveis causas:

- Regulamentações rígidas em privacidade, dados e proteção do consumidor (GDPR).
- Dificuldade para startups e PMEs navegarem pelas exigências legais.
- Processos lentos de aprovação e homologação de tecnologias emergentes.

“As iniciativas europeias no setor de defesa podem impulsionar significativamente a inovação tecnológica nos próximos anos.”

- **Concordância total ou parcial: 73,55%**
- **Média ponderada: 3,75**

Existe otimismo quanto ao papel estratégico do setor de defesa como motor de inovação, repetindo modelos como os EUA, onde tecnologias civis derivam de investimentos militares (ex: internet, GPS).

Possíveis causas:

- Aumento de orçamento em defesa na UE.
- Incentivos à inovação dual-use (civil e militar).
- Integração entre universidades, centros de investigação e indústria bélica.

“A fragmentação cultural e política entre os países europeus é uma barreira importante para a construção de uma estratégia conjunta de inovação.”

- **Concordância total ou parcial: 67,77%**
- **Média ponderada: 3,58**

A diversidade política e cultural dentro da UE é percebida como obstáculo à criação de políticas unificadas em inovação.

Possíveis causas:

- Desalinhamento de prioridades entre países membros.
- Diferenças de investimento e maturidade digital.
- Falta de integração entre ecossistemas locais de inovação.

“A Europa precisa definir uma estratégia unificada de inovação para não se tornar apenas consumidora de tecnologia externa.”

- **Concordância total ou parcial: 91,74%**
- **Média ponderada: 4,38, maior de toda a investigação.**

Há quase consenso de que é urgente que a Europa estabeleça uma estratégia de inovação tecnológica unificada para não perder protagonismo.

Possíveis causas:

- Dependência crescente de tecnologia estrangeira.
- Riscos geopolíticos de soberania digital e tecnológica.
- Reconhecimento de que esforços isolados não têm escala competitiva global.

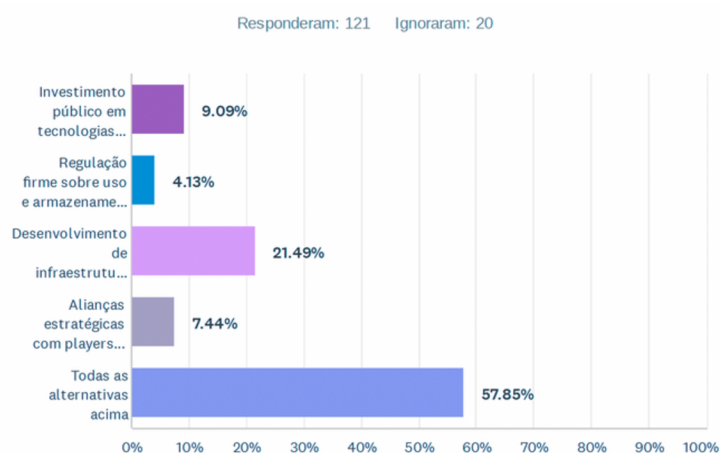
Considerações gerais

A Europa não é vista como líder tecnológica, mas sim como um continente que ainda enfrenta entraves internos para se consolidar nessa posição. Apesar disso, os inquiridos demonstram clareza sobre os caminhos possíveis: aposta em defesa, integração política e redução da burocracia.

Pontos de atenção:

- A divergência interna entre países pode ser um fator crítico a ser enfrentado.
- A burocracia excessiva está a minar a capacidade de resposta rápida às mudanças tecnológicas globais.
- O elevado índice de concordância quanto à necessidade de uma estratégia unificada de inovação mostra que este é a queixa mais forte entre os participantes.

P3 Práticas consideradas essenciais para garantir a soberania digital na Europa até 2035



OPÇÕES DE RESPOSTA	RESPOSTAS
Investimento público em tecnologias emergentes locais	9.09% 11
Regulação firme sobre uso e armazenamento de dados	4.13% 5
Desenvolvimento de infraestrutura própria e segura	21.49% 26
Alianças estratégicas com players não-europeus	7.44% 9
Todas as alternativas acima	57.85% 70
TOTAL	121

(Gráfico 3 – Soberania digital europeia até 2035)

Em contrapartida, a afirmação “Desenvolver infraestrutura própria e segura” é o único item “isolado” que aparece com força marcada por 21,49% dos inquiridos.

- Dependências críticas atuais: cloud, semicondutores, cabos/submarinos, 5G/edge, identidade digital, ciber – onde a Europa ainda depende de fornecedores extra-UE. Construir capacidade local e padrões abertos é visto como a forma mais tangível de autonomia.
- Pressão regulatória/cibernética: requisitos de segurança (ex.: NIS2, setores críticos) empurram empresas para resiliência física e lógica sob governação europeia.
- Efeito para PMEs: metade da amostra é de empresas <50 colaboradores; para quem não tem poder de negociação com “hyperscalers”, uma infraestrutura fiável e acessível resolve problemas práticos (custos, latência, residência de dados, conformidade).

Investimento público isolado tem pouco apelo (9,09%).

- Ceticismo de escala: percepção de que, sozinho, o investimento europeu não iguala EUA/China se não vier acoplado a mercado integrado, compras públicas, talento e escala pan-europeia.
- Efeito de difusão: sem coordenação, o dinheiro pulveriza; com coordenação, ganha tração e escala (programas de missão, consórcios).

Regulação “sozinha” é a menos votada (4,13%).

- Fadiga regulatória: os mesmos inquiridos apontam a burocracia/regulação como barreira. Na prática, mais regra sem instrumentos de execução (infra, capital, escala) não entrega soberania – e pode atrasar.

- Preferência por “regulação habilitadora”: sandboxes, padrões de interoperabilidade, gestão de dados setoriais, acoplada a investimento e adoção pública.

Alianças com não-europeus (7,44%): úteis, mas não como eixo único

- Soberania ≠ autarquia: parcerias são bem-vindas, porém a amostra rejeita dependência. O recado: alianças, desde que preservem o controlo sobre os dados, IP e supply chain (contratos, cláusulas de portabilidade, open standards).

Por outras palavras: a amostra rejeita soluções monodimensionais e, se fosse para escolher apenas um vetor, infraestrutura soberana é o preferido.

Contexto Tecnológico em Portugal

No gráfico 4 e na Tabela 2 é possível observar as perceções da amostra sobre o contexto tecnológico português. A mensagem central da amostra aponta que há otimismo com o ecossistema tech, mas fricções no elo telecom (concentração/qualidade) e desafios de internacionalização de startups.

Para a amostra, Portugal possui potencial para ser um polo relevante de startups (especialmente em cybersecurity e IA) 86,49% concordam totalmente ou parcialmente; média 4,23 (a mais alta). Esse otimismo evidente sobre as capacidades do país, pode refletir:

- Ecossistema crescente de startups e investimento em hubs como Lisboa e Porto.
- Visibilidade internacional crescente (ex: Web Summit).
- Interesse europeu em descentralizar a inovação e aproveitar países menores com bom nível de talento e custo competitivo.

Causa provável: capital humano qualificado, políticas de apoio a startups e visibilidade internacional como “tech-friendly nation”.

Há uma perceção contraditória: reconhece-se o papel estrutural das operadoras, mas falta confiança na sua atuação atual. 74,78% concordam com a afirmação “As operadoras atuam de forma pouco competitiva, prejudicando inovação e qualidade” (média 3,95).

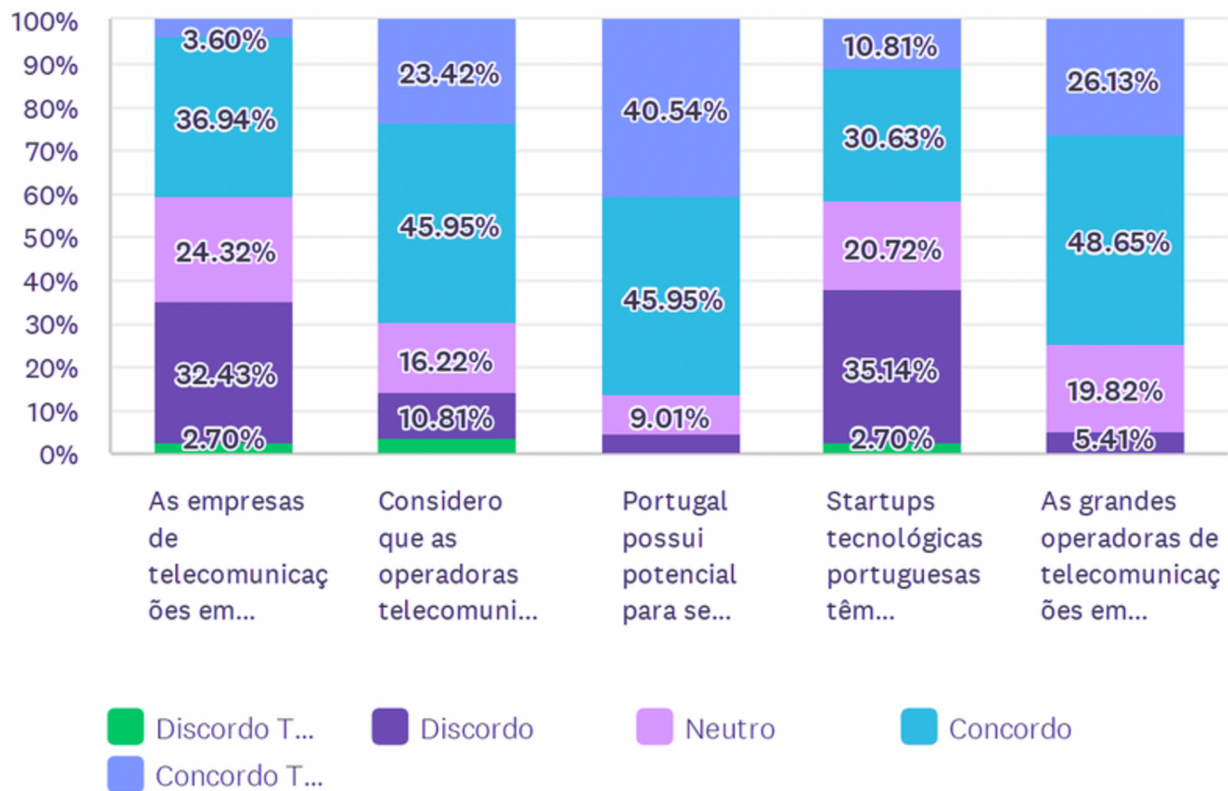
69,37% concordam que “As operadoras são cruciais para a transformação digital” (média 3,75). Mas apenas 40,54% consideram que elas estão de fato entregando serviços à altura.

Causas possíveis:

- Alta concentração de mercado em poucas operadoras (oligopólio).
- Dificuldade de oferta customizada para PMEs/startups, que compõem grande parte da amostra (metade tem <50 colaboradores).
- Lentidão para atualizar ofertas com novas tecnologias (cloud, 5G corporativo, soluções IoT...).
- Reclamações recorrentes de atendimento, preços e transparência (ecoam avaliações públicas).

P4 Nível de concordância com afirmações sobre o contexto português

Responderam: 111 Ignoraram: 30



(Gráfico 4 - Contexto tecnológico em Portugal)

O painel vê Portugal com alto potencial em tech, mas identifica travões no elo telecom (concentração e entrega) e desafios de escala para startups. A agenda vencedora combina mais competição e interoperabilidade em telecom, orquestração telco-startup para soluções B2B exportáveis e instrumentos de capital e procurement que acelerem a transição do “potencial” para produto global.

Apenas 41,44% concordam que “Startups têm dificuldade de escalar por estarem voltadas ao mercado interno”. Esta é a afirmação mais dividida: 35% discordam, 21% neutros, e 31% apenas concordam parcialmente.

Isso indica divergência de experiências:

- Startups mais digitalizadas e com modelo SaaS ou exportável tendem a não ver o mercado interno como barreira.
- Startups em áreas reguladas, govtechs ou com produtos físicos veem limitação real de escala dentro de Portugal.

Causa provável: Portugal é um mercado pequeno, o que exige internacionalização rápida – mas nem todas as startups estão preparadas para isso ou têm apoio para fazê-lo.

	DISCORDO TOTALMENTE	DISCORDO	NEUTRO	CONCORDO	CONCORDO TOTALMENTE	TOTAL	MÉDIA PONDERADA
As empresas de telecomunicações em Portugal oferecem serviços de IT e conectividade que respondem às necessidades atuais do mercado corporativo.	2.70% 3	32.43% 36	24.32% 27	36.94% 41	3.60% 4	111	3.06
Considero que as operadoras de telecomunicações têm um papel crucial na transformação digital das empresas em Portugal.	3.60% 4	10.81% 12	16.22% 18	45.95% 51	23.42% 26	111	3.75
Portugal possui potencial para se tornar um polo relevante no desenvolvimento de startups de tecnologia, especialmente em cybersecurity e inteligência artificial.	0.00% 0	4.50% 5	9.01% 10	45.95% 51	40.54% 45	111	4.23
Startups tecnológicas portuguesas têm dificuldades em escalar por estarem excessivamente voltadas para o mercado interno.	2.70% 3	35.14% 39	20.72% 23	30.63% 34	10.81% 12	111	3.12
As grandes operadoras de telecomunicações em Portugal atuam de forma concertada e pouco competitiva, o que prejudica a inovação e a qualidade dos serviços.	0.00% 0	5.41% 6	19.82% 22	48.65% 54	26.13% 29	111	3.95

(Tabela 2 – Contexto tecnológico em Portugal)

Há um ecossistema promissor, mas atores incumbentes (como as telcos) não são percebidos como parceiros ativos da inovação.

O papel das operadoras é reconhecido, mas é visto mais como necessidade estrutural do que como liderança inovadora.

A dificuldade de escalar mostra que o mercado interno é insuficiente para startups com ambição global, reforçando a importância de infraestrutura, parcerias e políticas públicas que facilitem a internacionalização.

O contexto português é percebido como maduro em talento e potencial, mas ainda limitado por atores tradicionais pouco dinâmicos e desafios de escala do mercado interno. Há um desejo coletivo de mudança estrutural, com expectativas de que grandes empresas e políticas públicas se tornem catalisadoras, e não apenas observadoras, da transformação digital.

Sobre a empresa onde desempenha funções

O gráfico 5 e a Tabela 3 indicam qual a percepção sobre a empresa em que desempenham funções em relação a preparação para segurança digital. Os resultados indicam uma percepção positiva da preparação das empresas para segurança digital. Mais da metade 64,15% (51,89% concordam + 12,26% concordam totalmente) acredita que a sua organização está pronta para os desafios dessa área.

Causas possíveis:

- Investimentos recentes em cibersegurança.
- Aumento da sensibilização sobre riscos digitais após incidentes globais.
- Existência de protocolos básicos ou ferramentas de proteção já implementadas.

Sobre a existência de plano formalizado e eficaz de cybersecurity, há concordância moderada, 51,88% (concordam e concordam totalmente) enquanto há 47,17% de neutros e céticos. Isso indica que há um reconhecimento de que planos existem, mas a eficácia ainda é questionada por muitos.

Causas possíveis:

- Planos que não estão totalmente implementados ou atualizados.
- Falta de comunicação interna sobre os planos.
- Ausência de testes práticos (simulações de ataques, por exemplo).

Sobre a adoção de Identidade Digital Descentralizada (DID) a Concordância é relativamente baixa, apenas 44,34% (31,13% concordam + 13,21% concordam totalmente). Há 39,62% de neutros indicando uma maior indecisão. Muito provavelmente pelo fato do tema ainda ser novo para muitos colaboradores ou não estar em discussão na empresa.

Causas possíveis:

- Desconhecimento técnico sobre o conceito de DID.
- Adoção ainda incipiente no mercado local.
- Falta de urgência percebida em adotar soluções de identidade digital.

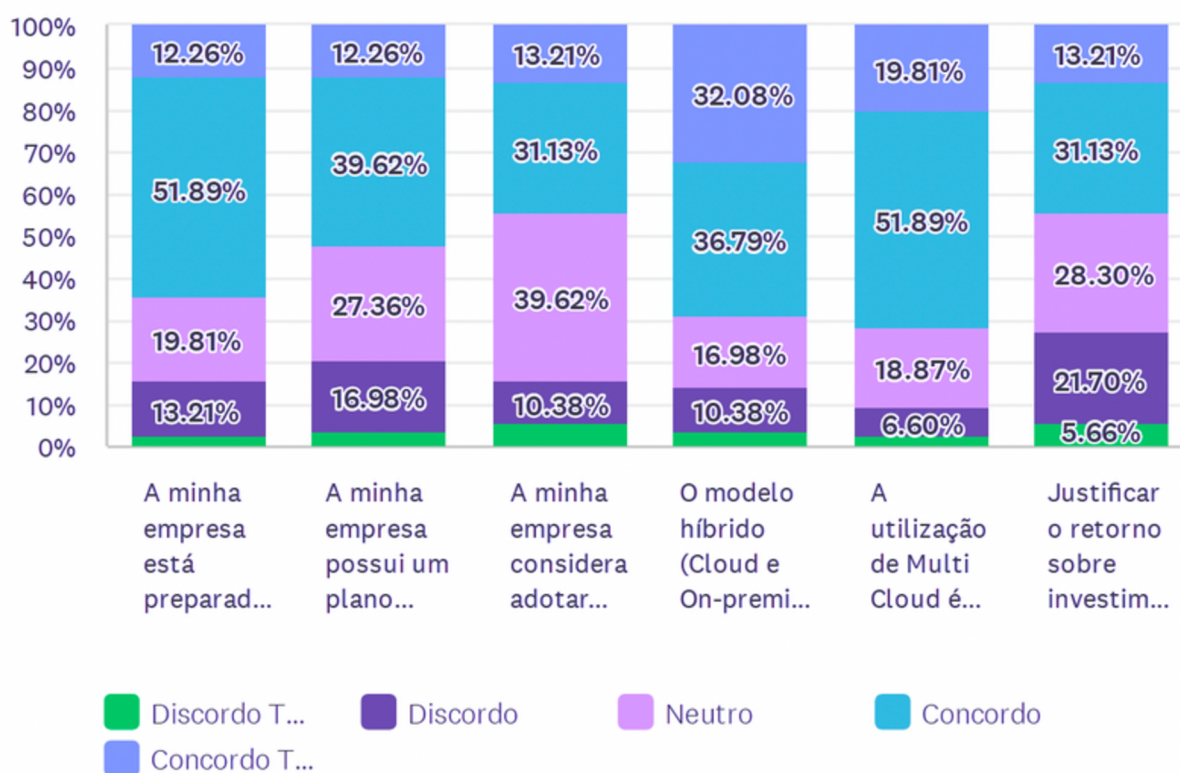
O modelo híbrido (Cloud + On-premise) é amplamente percebido como o mais flexível e adaptável. O nível de concordância é alto 68,87% (36,79% concordam + 32,08% concordam totalmente).

Causas possíveis:

- Realidade comum das empresas ainda manterem parte das operações on-premise.
- A flexibilidade do modelo híbrido para lidar com diferentes níveis de maturidade digital e orçamental.

P5 Nível de concordância com afirmações sobre a empresa onde exerce funções

Responderam: 106 Ignoraram: 35



(Gráfico 5 - Empresa Onde Desempenha Funções)

Há uma percepção consolidada de que o Multi Cloud é estratégico para resiliência. O índice de concordância é elevado 71,7% (51,89% concordam + 19,81% concordam totalmente).

Causas possíveis:

- Dependência percebida de fornecedores únicos.
- Aumento da criticidade de continuidade de serviços digitais.
- Estratégia de mitigação de falhas e riscos operacionais.

	DISCORDO TOTALMENTE	DISCORDO	NEUTRO	CONCORDO	CONCORDO TOTALMENTE	TOTAL	MÉDIA PONDERADA
A minha empresa está preparada para lidar com os desafios de segurança digital.	2.83% 3	13.21% 14	19.81% 21	51.89% 55	12.26% 13	106	3.58
A minha empresa possui um plano formalizado e eficaz de soluções avançadas de cybersecurity.	3.77% 4	16.98% 18	27.36% 29	39.62% 42	12.26% 13	106	3.40
A minha empresa considera adotar Identidade Digital Descentralizada (DID) como medida de segurança.	5.66% 6	10.38% 11	39.62% 42	31.13% 33	13.21% 14	106	3.36
O modelo híbrido (Cloud e On-premise) é o mais adaptável às necessidades da minha empresa.	3.77% 4	10.38% 11	16.98% 18	36.79% 39	32.08% 34	106	3.83
A utilização de Multi Cloud é fundamental para evitar riscos operacionais relacionados à falha de fornecedores específicos.	2.83% 3	6.60% 7	18.87% 20	51.89% 55	19.81% 21	106	3.79
Justificar o retorno sobre investimento (ROI) de infraestruturas em Cloud é fácil na minha organização.	5.66% 6	21.70% 23	28.30% 30	31.13% 33	13.21% 14	106	3.25

(Tabela 3 – Empresa Onde Desempenha Funções)

A razão do retorno sobre investimento em Cloud é um ponto de dor nas organizações. É onde há a maior polarização e menor média ponderada: 44,34% concordam ou concordam totalmente, enquanto 49,06% estão entre neutros e discordantes.

Causas possíveis:

- Dificuldade em avaliar os ganhos intangíveis (segurança, escalabilidade, flexibilidade).
- Falta de métricas claras ou dashboards de desempenho financeiro da cloud.
- Percepção de que os custos da Cloud são altos e não tão visíveis em benefícios imediatos.

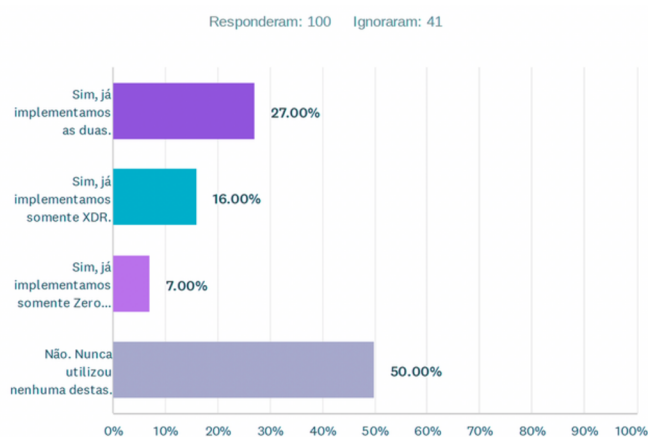
Conclusão

As empresas aparentam estar num nível intermédio de maturidade digital. Há uma boa percepção quanto à preparação para segurança digital e estratégias como Multi Cloud e modelos híbridos são bem avaliadas. Contudo, temas mais avançados ou técnicos, como Identidade Digital Descentralizada e justificativa de ROI em cloud, ainda enfrentam barreiras, o que pode refletir falta de conhecimento, clareza estratégica ou desafios de governação e avaliação. **O dado mais crítico é a dificuldade em justificar ROI, o que pode limitar a adoção mais ampla e sustentada da Cloud, mesmo quando as soluções são vistas como fundamentais.**

Sobre soluções de cibersegurança na empresa

O gráfico 6 revela um cenário polarizado: enquanto uma parcela relevante das empresas já caminha em direção a uma postura madura e integrada de cibersegurança, uma metade ainda permanece sem qualquer adoção dessas tecnologias. Este é um sinal claro de que há desigualdade na maturidade digital e cibernética entre as empresas, o que pode colocar em risco cadeias produtivas inteiras, especialmente se as organizações menos preparadas estiverem conectadas a ecossistemas maiores.

P6 Implementação de soluções como XDR ou Zero Trust Architecture na empresa



OPÇÕES DE RESPOSTA	RESPOSTAS
Sim, já implementamos as duas.	27.00% 27
Sim, já implementamos somente XDR.	16.00% 16
Sim, já implementamos somente Zero Trust Architecture.	7.00% 7
Não. Nunca utilizou nenhuma destas.	50.00% 50
TOTAL	100

(Gráfico 6 – Soluções em Cibersegurança)

50% das organizações que responderam ao inquérito afirma que nunca implementou nenhuma das soluções XDR ou Zero Trust. Esse é um dado significativo que revela uma lacuna importante na adoção de tecnologias modernas de segurança, podendo indicar:

- Falta de maturidade em cibersegurança;
- Barreiras orçamentais ou técnicas;
- Desconhecimento sobre os benefícios dessas soluções;
- Empresas em segmentos menos regulamentados ou com menor exposição a riscos digitais.

Em contrapartida **27% já implementaram ambas as soluções (XDR e Zero Trust)**.

Este grupo representa empresas com maior maturidade em segurança da informação, provavelmente com políticas de segurança bem estruturadas e visão estratégica sobre proteção contra ameaças modernas. A implementação combinada de XDR e Zero Trust sugere uma postura proativa e integrada de defesa cibernética.

16% implementaram apenas XDR. As empresas desse grupo optaram por fortalecer a detecção e resposta a ameaças, com foco operacional. É possível que essas organizações priorizem respostas rápidas a incidentes e estejam ainda avaliando o investimento em uma arquitetura de confiança zero.

Por fim, apenas 7% implementaram Zero Trust Architecture

Embora minoritário, esse grupo mostra uma preocupação estrutural com o acesso seguro aos recursos, adotando uma filosofia de segurança baseada na verificação contínua, mesmo em ambientes internos.

Comentários sobre Cibersegurança:

“Desconheço e estou a preparar um breve inquérito interno”

“Vamos implementar brevemente”

“Projeto em desenvolvimento”

“Estamos em fase de implementação e testes”

Possíveis Causas

Adoção ainda incipiente (50%) pode estar relacionada a:

- Falta de conhecimento técnico ou estratégico sobre os conceitos de XDR e Zero Trust;
- Perceção de que tais soluções são complexas ou com custos altos para a dimensão da empresa;
- Falta de pressão regulatória ou ausência de histórico de incidentes graves;
- Segmentos que ainda não sofreram grandes impactos com ciberataques.

Adoção mais avançada (27%) esse grupo tende a:

- Estar em setores críticos como finanças, saúde, tecnologia ou indústria;
- Ser empresas maiores, com mais recursos e compliance mais exigente;
- Ter sofrido ou testemunhado incidentes que motivaram investimentos robustos em segurança.

Adoção parcial (somente XDR ou somente Zero Trust) pode indicar:

- Adoção gradual ou faseada;
- Estratégia de priorização por riscos mais urgentes;
- Projetos-piloto em curso;
- Limitações de integração entre sistemas legacy e novas arquiteturas.

Reflexões Estratégicas

Há oportunidade significativa para crescimento na adoção dessas tecnologias, especialmente entre os 50% que ainda não começaram esse trajeto.

A integração entre XDR e Zero Trust é um diferencial competitivo, pois permite não apenas detectar ameaças, mas limitar os danos através de políticas rigorosas de acesso e segmentação de redes.

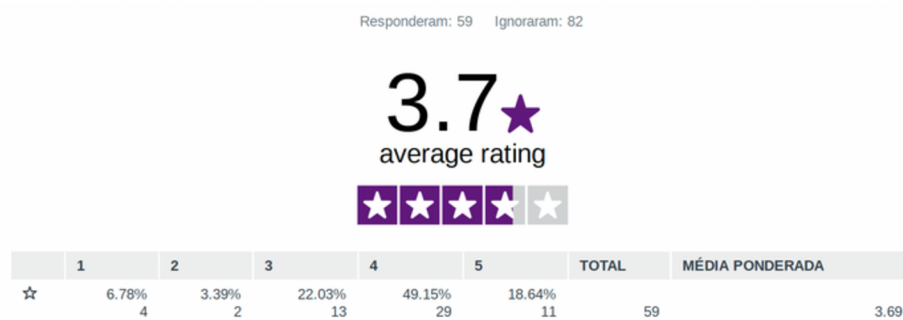
Programas de capacitação, sensibilização e avaliação de maturidade em cibersegurança podem ajudar a reduzir a inércia identificada entre os não adotantes.

Sobre satisfação com soluções de cibersegurança

Após responderem às questões anteriores, referentes a soluções de cibersegurança, os inquiridos foram convidados a classificar os resultados alcançados pela sua empresa com a solução utilizada. Os participantes deveriam atribuir a quantidade de estrelas correspondente à sua experiência.

A avaliação de uma solução implementada numa empresa pode revelar muito mais do que um simples número. Ela expõe percepções reais sobre eficácia, valor estimado e até as expectativas que influenciam a sua adoção.

P7 Classificação dos resultados obtidos com as soluções implementadas



(Figura 1- Estrelas Correspondentes à Solução Cibersegurança)

Na Figura 1- Estrelas Correspondentes à Solução Cibersegurança, temos um termómetro importante: a média ponderada de satisfação com a solução utilizada foi de 3,7 estrelas (de 5 possíveis), com destaque para as avaliações de 4 e 5 estrelas, mas ainda com uma parcela considerável de insatisfeitos. Entender essas nuances é essencial para aprimorar a experiência dos utilizadores e aumentar a adesão às soluções tecnológicas adotadas.

A distribuição das respostas mostra que a maioria dos inquiridos avaliou a solução com 4 estrelas (49,15%), uma nota positiva, mas que sugere a existência de pontos de melhoria. Além disso, 18,64% deram nota máxima, o que reforça que há um grupo satisfeito com os resultados obtidos.

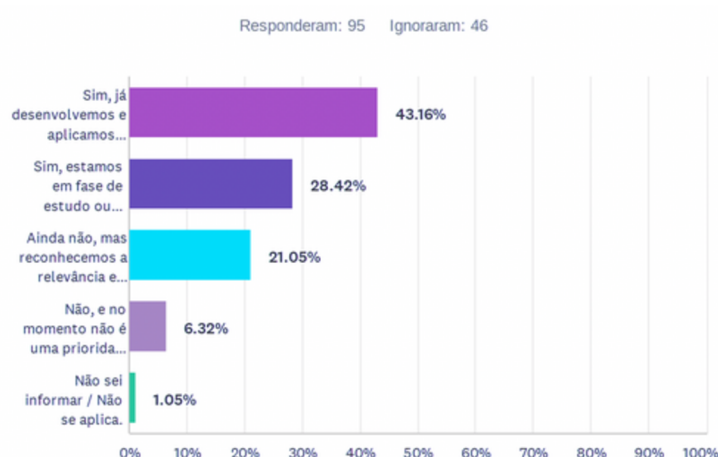
No entanto, chama atenção que 6,78% atribuíram apenas 1 estrela e 3,39% deram 2 estrelas, indicando experiências prejudiciais ou muito abaixo do expectável. Esse dado não pode ser ignorado, pois revela que, apesar da média estar num patamar satisfatório (3,69), a solução ainda não atinge um nível de excelência para todos os perfis de utilizadores.

Algumas hipóteses para explicar essa variação incluem diferenças na forma de uso da solução entre as áreas da empresa, níveis distintos de maturidade digital, falta de formação adequada ou falhas no suporte. É possível que a solução seja tecnicamente robusta, mas não esteja totalmente alinhada às necessidades operacionais ou estratégicas de alguns departamentos. A elevada taxa de respostas com 4 estrelas também pode indicar que há reconhecimento de valor, mas com ressalvas, como limitações de funcionalidade, integração ou usabilidade. Mesmo sem ser uma amostra representativa, nem probabilística, seria interessante aprofundar a escuta qualitativa com os grupos que atribuíram notas mais baixas, procurando identificar pontos específicos de frustração ou barreiras no uso. Ao mesmo tempo, vale apenas investigar o que os utilizadores que deram 5 estrelas consideram diferencial, de forma a replicar boas práticas internas. Também é indicado reforçar ações de formação, suporte contínuo e comunicação de melhorias da solução, para aumentar o envolvimento e a percepção de valor. Em resumo, a média de 3,7 estrelas aponta para uma aceitação moderadamente positiva da solução, com espaço claro para evolução. A leitura atenta desses dados permite transformar feedback em direcionamento estratégico para alcançar níveis mais altos de satisfação e impacto.

Sobre soluções baseadas em inteligência artificial

O gráfico 7 revela um cenário relativamente avançado de adoção de soluções de inteligência artificial em diversas empresas do setor. Combinando os dois primeiros grupos, temos mais de 70% das empresas já envolvidas em alguma etapa do processo de incorporação da IA, o que demonstra um amadurecimento relevante em relação a este tema.

P8 Estado de desenvolvimento/avaliação de soluções de IA na empresa e no setor, como como geração automática de códigos, ferramentas de monitorização e administração de sistemas



OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim, já desenvolvemos e aplicamos projetos piloto com essas tecnologias.	43.16%	41
Sim, estamos em fase de estudo ou planeamento para adoção.	28.42%	27
Ainda não, mas reconhecemos a relevância e estamos a acompanhar o tema.	21.05%	20
Não, e no momento não é uma prioridade para a empresa.	6.32%	6
Não sei informar / Não se aplica.	1.05%	1
TOTAL		95

(Gráfico 7 – Soluções Baseadas em IA)

Adoção em curso (43,16%) – A maior parcela dos inquiridos indica que já está a desenvolver e aplicar projetos com IA, o que demonstra um avanço concreto no setor. Este dado sugere que:

- A IA já deixou de ser apenas uma tendência e se tornou um diferencial competitivo.
- Setores mais pressionados por eficiência (como tecnologia, telecomunicações, serviços financeiros, indústria avançada) provavelmente lideram essa adoção.
- Pode haver incentivos internos como automação de tarefas repetitivas, redução de custos operacionais, ou melhoria da escalabilidade de serviços.
- A existência de talentos especializados ou parcerias com empresas de tecnologia também pode ter acelerado essa implementação.

Planeamento e estudo (28,42%) – Este grupo está em fase de preparação:

- As empresas provavelmente enfrentam barreiras como restrições orçamentais, falta de conhecimento técnico interno ou necessidade de avaliar o ROI com mais clareza antes de investir.
- Também pode indicar que algumas áreas da empresa estão mais prontas do que outras, e que a implementação pode ser gradual.
- Essa fase é típica de setores mais regulados ou que dependem de mudanças culturais antes de implementar automações baseadas em IA.

Reconhecimento da relevância, mas ainda sem ação (21,05%) – Aqui, vemos empresas que estão conscientes da importância, mas ainda não iniciaram nada concreto:

- Pode haver cautela diante da velocidade das mudanças tecnológicas ou incertezas quanto à maturidade dessas soluções.
- Algumas organizações podem estar à espera de “casos de estudo fidedignos” antes de avançar.
- Possivelmente há uma lacuna de formação interna ou ausência de liderança envolvida na agenda digital.

Não é prioridade (6,32%) Um número pequeno de empresas declara explicitamente que IA não é uma prioridade:

- Esse resultado pode ser atribuído a setores com baixa maturidade digital ou que ainda operam de forma analógica.
- Pode refletir também empresas pequenas ou tradicionais que ainda não sentiram pressão competitiva ou regulatória para inovar.
- A crise económica ou instabilidades podem forçar essas empresas a focarem no core business e adiar investimentos mais estratégicos.

Não sei informar / Não se aplica (1,05%) Margem residual, provavelmente de pessoas que:

- Não ocupam cargos técnicos ou estratégicos, e, portanto, não têm visibilidade sobre o tema;
- Ou de empresas para as quais o tema realmente não é aplicável, como setores muito específicos sem base tecnológica relevante.

Causas Possíveis para o Cenário Atual

- Pressão competitiva crescente: A procura por eficiência operacional e diferenciação de mercado está a impulsionar a adoção de IA.
- Disponibilidade de soluções maduras no mercado: Ferramentas baseadas em IA estão mais acessíveis, inclusive via SaaS, o que reduz barreiras técnicas.
- Procura por automação e produtividade: A IA tem se mostrado eficaz em reduzir custos com tarefas repetitivas e melhorar a assertividade de decisões.
- Capacitação interna desigual: Empresas com maior disponibilidade de talentos digitais ou parcerias com fornecedores inovadores saem na frente.
- Cultura organizacional e mindset digital: Empresas mais abertas à experimentação e inovação adotam projetos-piloto mais rapidamente.

Sobre modelo de trabalho

A análise do gráfico 8 revela tendências claras e permite inferir possíveis causas para as percepções manifestadas sobre Modelo de Trabalho. A larga maioria acredita que o modelo híbrido com flexibilidade será o formato predominante até 2035. Possíveis razões incluem:

- Mudança cultural consolidada durante e após a pandemia, que mostrou ser possível manter produtividade fora do escritório.
- Alcançar o equilíbrio entre vida pessoal e profissional, principalmente entre gerações mais jovens.
- Diferentes perfis de trabalho necessitam de abordagens flexíveis, reuniões presenciais para colaboração criativa e trabalho remoto para foco individual.
- Custo-benefício: empresas podem reduzir infraestrutura física sem perder a participação das pessoas.
- Percepção de que o híbrido é o “meio termo ideal”, conciliando as vantagens do remoto com a necessidade de convivência presencial.

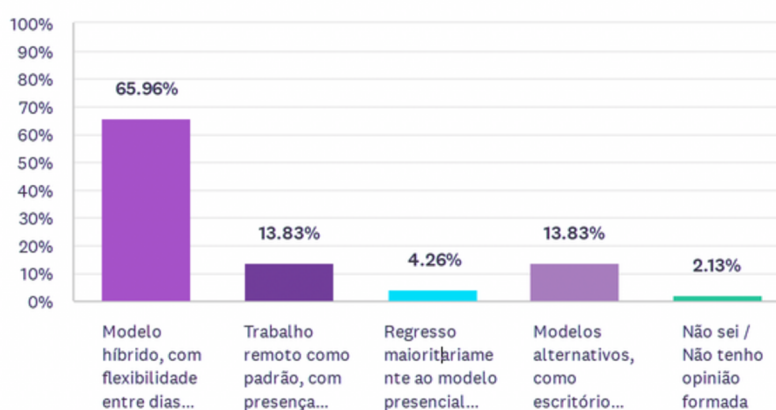
Trabalho remoto como padrão (13,83%)

A parcela que acredita no remoto como norma com presenças pontuais também é significativa. Isso pode estar associado a:

- Empresas e setores que já operam majoritariamente em ambientes digitais.
- Profissionais que valorizam autonomia total, ausência de deslocação e ganhos de produtividade.
- Evolução de ferramentas de colaboração digital que dispensam a necessidade da presença física para boa parte das funções.

P9 Modelo de trabalho que se prevê predominante nas empresas até 2035

Responderam: 94 Ignoraram: 47



OPÇÕES DE RESPOSTA	RESPOSTAS
Modelo híbrido, com flexibilidade entre dias presenciais e remotos	65.96% 62
Trabalho remoto como padrão, com presença pontual em escritórios	13.83% 13
Retorno majoritariamente ao modelo presencial tradicional	4.26% 4
Modelos alternativos, como escritórios descentralizados ou trabalho nômade digital	13.83% 13
Não sei / Não tenho opinião formada	2.13% 2
TOTAL	94

(Gráfico 7 – Soluções Baseadas em IA)

Modelos alternativos e nômadas digitais (13,83%). Mesma percentagem do item anterior, essa resposta indica abertura à inovação estrutural, com causas como:

- **Internacionalização do trabalho** e aumento de freelancers e trabalhadores independentes.
- Consolidação de modelos como **coworkings, hubs descentralizados e esquemas "work from anywhere"**.
- Crescimento de novas gerações que priorizam experiências e mobilidade geográfica.

Regresso ao modelo presencial tradicional (4,26%). A baixa adesão à volta ao modelo 100% presencial sinaliza:

- **Rejeição da rigidez** dos antigos formatos de trabalho.
- Sensação de que este modelo **não é mais compatível com as transformações sociais e tecnológicas**.
- Pode representar segmentos específicos (como produção industrial, saúde, etc.), onde o trabalho remoto é menos aplicável.

Indefinição (2,13%). A pequena parcela de indecisos pode refletir:

- Falta de exposição a debates ou práticas mais modernas de trabalho.
- Incerteza sobre como o cenário político, económico e tecnológico vai evoluir até 2035.

Causas possíveis dos resultados alcançados

1. **Legado da pandemia:** A experiência forçada de trabalho remoto durante a COVID-19 abriu espaço para novas mentalidades organizacionais.
2. **Mudança geracional:** Gerações mais jovens (millennials e gen Z) valorizam flexibilidade e propósito, pressionando empresas a adaptarem-se.
3. **Transformação digital acelerada:** Ferramentas como cloud, videoconferência e IA facilitam a descentralização do trabalho.
4. **Concorrência por talentos:** Empresas que oferecem modelos flexíveis tornam-se mais atrativas.
5. **Evidências de produtividade:** Estudos recentes mostram que regimes flexíveis podem ser mais eficazes em determinadas atividades.
6. **Redução de custos fixos:** Organizações encontram no modelo híbrido ou remoto uma forma de reduzir despesas com grandes sedes físicas.

Conclusão

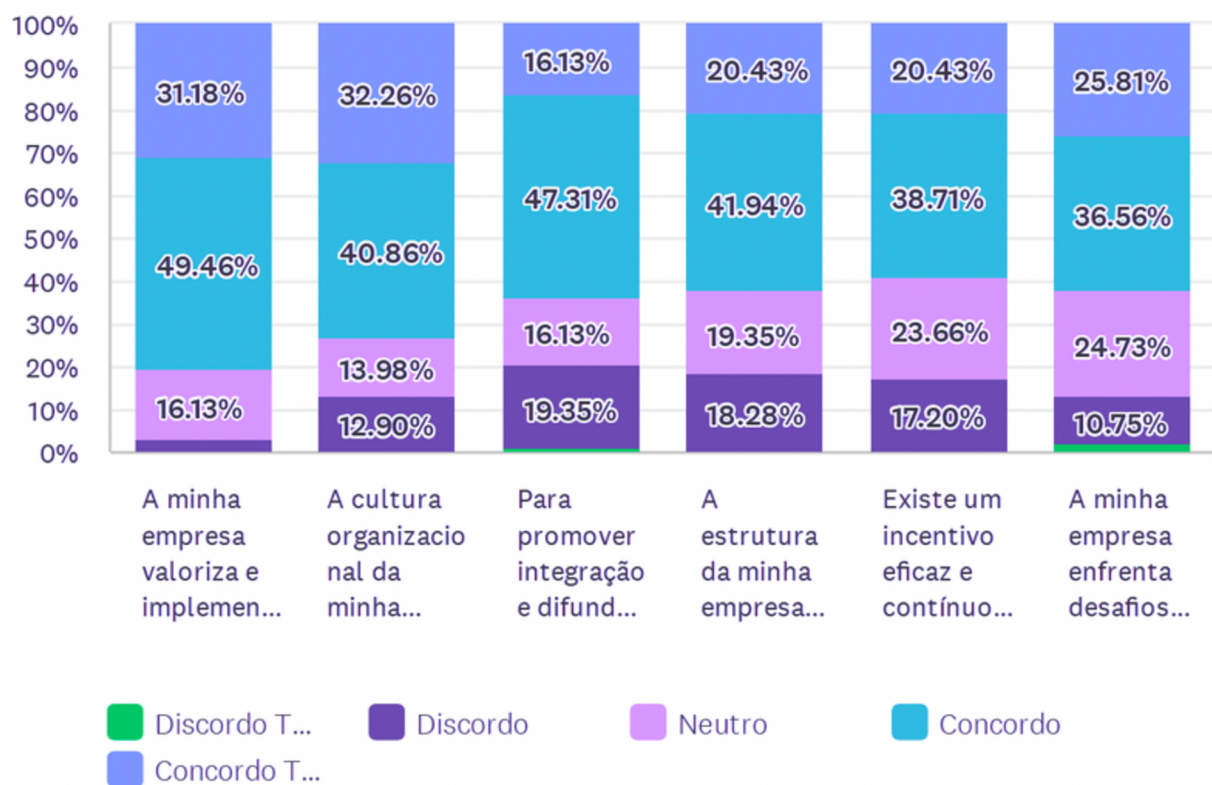
O estudo indica que o **futuro do trabalho caminha para formatos flexíveis**, especialmente o híbrido, que tende a consolidar-se como norma organizacional até 2035. Há uma valorização crescente da autonomia, adaptabilidade e qualidade de vida, refletindo um cenário onde o colaborador ganha protagonismo na definição do seu período de trabalho.

Sobre cultura empresarial, transformação digital e talentos

A análise dos dados apresentados no Gráfico 9 e Tabela 4 – Cultura Empresarial, Transformação Digital e Talentos, revela percepções importantes sobre o ambiente organizacional em relação à transformação digital e à capacidade das empresas em promover mudanças tecnológicas significativas. De forma geral, o sentimento predominante é positivo, com a maioria dos inquiridos a expressarem concordância com as afirmações, mas os índices de neutralidade e discordância em certos pontos indicam áreas com potencial de melhoria e reforço estratégico.

P10 Nível de concordância com afirmações selecionadas

Responderam: 93 Ignoraram: 48



(Gráfico 9 - Cultura Empresarial, Transformação Digital e Talentos)

A afirmação com maior média ponderada (4,09) e **índice de concordância total (mais de 80%) foi: “A minha empresa valoriza e implementa ativamente iniciativas de transformação digital”**. Isso demonstra um compromisso institucional claro com a inovação e a modernização dos processos. A cultura organizacional também é vista de forma relativamente positiva nesse sentido, **com 73% de concordância (média 3,92)**, o que sugere uma disposição das empresas em absorver mudanças, embora 12,9% ainda discordem dessa visão, o que pode sinalizar que nem todos estão igualmente alinhados com essa receptividade.

Entretanto, quando se trata de **estruturas e práticas que facilitam a disseminação da cultura digital e o envolvimento das pessoas**, os índices caem. A afirmação sobre a promoção da integração e a difusão da cultura organizacional tem a **menor média ponderada (3,58)**, e é também a que **apresenta a maior percentagem de discordância somada (mais de 20%)**. Isso pode indicar que, apesar de haver valorização da transformação digital em nível institucional, ainda faltam mecanismos concretos, como dinâmicas de colaboração, rituais de alinhamento e espaços de escuta, que garantam a participação ampla dos colaboradores nas mudanças. O mesmo padrão é observado na avaliação da **estrutura organizacional** (média 3,65) e dos incentivos à formação (média 3,62). Embora mais de 60% dos inquiridos reconheçam avanços nessas áreas, **aproximadamente 40% estão entre a neutralidade e a discordância**, o que demonstra que **existe uma lacuna entre o discurso institucional e a experiência prática vivida por parte dos profissionais**. A ausência de políticas mais claras de reconhecimento, recompensas e desenvolvimento contínuo pode ser um fator que limita uma adesão mais entusiástica.

Por fim, a afirmação de que **as empresas enfrentam desafios significativos para atrair e reter talentos em tecnologia** apresentou uma média ponderada de 3,73, refletindo uma percepção realista e crítica por parte dos colaboradores. Embora mais da metade concorde com essa dificuldade, um quarto dos inquiridos mantém-se neutro, o que pode significar que esses desafios ainda não são discutidos de forma transparente com todas as equipas, ou que não são percebidos da mesma forma em todos os níveis hierárquicos.

	DISCORDO TOTALMENTE	DISCORDO	NEUTRO	CONCORDO	CONCORDO TOTALMENTE	TOTAL	MÉDIA PONDERADA
A minha empresa valoriza e implementa ativamente iniciativas de transformação digital.	0.00% 0	3.23% 3	16.13% 15	49.46% 46	31.18% 29	93	4.09
A cultura organizacional da minha empresa é receptiva às mudanças tecnológicas significativas.	0.00% 0	12.90% 12	13.98% 13	40.86% 38	32.26% 30	93	3.92
Para promover integração e difundir a cultura organizacional da minha empresa cria dinâmicas de convívio, reuniões de colaboração e discussão estratégica ou operacionais de alinhamento das pessoas e passagem de objetivos individuais e coletivos.	1.08% 1	19.35% 18	16.13% 15	47.31% 44	16.13% 15	93	3.58
A estrutura da minha empresa favorece a rápida adoção de novas tecnologias e práticas digitais.	0.00% 0	18.28% 17	19.35% 18	41.94% 39	20.43% 19	93	3.65
Existe um incentivo eficaz e contínuo para desenvolvimento das competências digitais necessárias ao futuro, bem como a formação tecnológica dos colaboradores na minha empresa.	0.00% 0	17.20% 16	23.66% 22	38.71% 36	20.43% 19	93	3.62
A minha empresa enfrenta desafios significativos para atrair e reter talentos em tecnologia.	2.15% 2	10.75% 10	24.73% 23	36.56% 34	25.81% 24	93	3.73

(Tabela 4 - Cultura Empresarial, Transformação Digital e Talentos)

Possíveis causas

- **Forte presença de PMEs:** Em PMEs, patrocínio existe, mas faltam **recursos, processos e governação formais**, o que prejudica “rotinas”, “estrutura” e “incentivos”.
- **Burocracia/fragmentação** percecionadas na Europa: Resultados anteriores mostraram **burocracia e fragmentação** como barreiras. Isso tende a atrasar **time-to-adopt** e desincentivar práticas consistentes de upskilling.
- Dificuldade de provar **ROI em cloud e gaps de programa de segurança**. Sem **métricas claras e runbooks**, líderes ficam hesitantes em escalar a formação e mudanças estruturais.
- **Mercado de talentos:** Competição com big techs/scale-ups, **salários europeus assimétricos, brain drain** e **políticas híbridas ainda em ajuste** elevam a perceção de **dificuldade para atrair/reter**.
- **Modelo operacional em transição:** Muitas empresas ainda operam em **silos funcionais**; a adoção de **product operating model / platform engineering** avança lentamente, o que limita velocidade e rituais de colaboração efetivos.

Onde estão os “pontos críticos”

- **Rituais/canais de difusão cultural:** integrações, comunidades de prática, cadências de decisão ainda irregulares, especialmente no **híbrido**.
- **Estrutura para adoção rápida:** falta **padrão de plataforma**, governação de arquitetura e **autonomia** das equipas.
- **Incentivos à formação:** verbas e caminhos de aprendizagem **não contínuas**; upskilling visto como custo, não como **KPI de negócio**.
- **Talento tech:** employer branding e pacotes de valor **pouco competitivos**; pouca **mobilidade interna**.

Em síntese, os resultados indicam que, de modo geral, as empresas estão no caminho certo ao valorizar a transformação digital, mas precisam **fortalecer os mecanismos internos de comunicação, integração e formação contínua**, além de **enfrentar com mais assertividade os desafios de atração e retenção de talentos em tecnologia**. A chave para avançar está em traduzir o alinhamento estratégico em ações concretas, visíveis e acessíveis no cotidiano de todos os colaboradores.

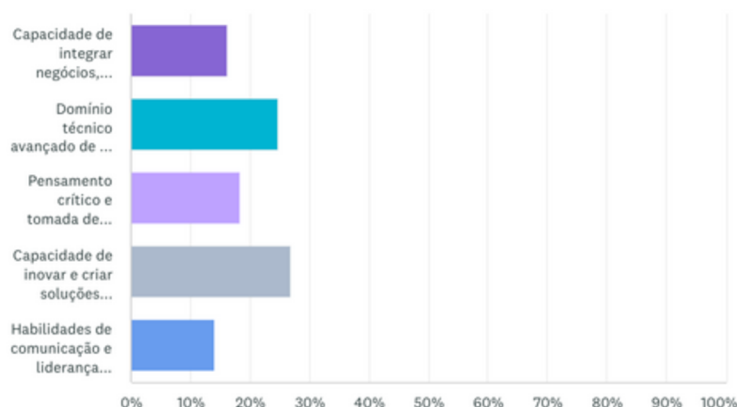
A vontade de transformar já está em andamento; o próximo salto depende de **organização para escalar**, rituais consistentes, arquitetura de plataforma, incentivos de habilidades e uma estratégia de talento que torne o digital uma prática diária, não apenas intenção.

Sobre o profissional da IT da década 2025–2035

O futuro do profissional de IT passa por quem consegue imaginar, construir e liderar o novo, e não apenas por quem domina a tecnologia em si. Essa é a principal mensagem que emerge da análise dos dados apresentados no gráfico 10 – O Profissional de IT da década 2025 – 2035.

P11 Competências mais valorizadas no profissional de IT até 2035

Responderam: 93 Ignoraram: 48



OPÇÕES DE RESPOSTA	RESPOSTAS	
Capacidade de integrar negócios, tecnologia e ESG	16,13%	15
Domínio técnico avançado de IA, computação quântica e 6G	24,73%	23
Pensamento crítico e tomada de decisão baseada em dados	18,28%	17
Capacidade de inovar e criar soluções escaláveis	26,88%	25
Habilidades de comunicação e liderança adaptativa	13,98%	13
TOTAL		93

(Gráfico 10 – O Profissional de IT da década 2025 – 2035)

A pergunta direcionada aos inquiridos foi objetiva: “O que acredita que será mais valorizado no profissional de IT de hoje até 2035?”. Entre as respostas válidas, o destaque ficou com a opção **“Capacidade de inovar e criar soluções escaláveis”**, com 26,88% das menções. Essa resposta sinaliza que, embora o domínio técnico continue a ser essencial, ele está a deixar de ser o único fator diferencial, a inovação consolidou-se como **o pilar central** da agenda futura do setor. Na segunda posição, com 24,73%, aparece o **“Domínio técnico avançado de IA, computação quântica e 6G”**, o que confirma que a base técnica continuará relevante, especialmente em áreas emergentes de alta complexidade. Essa combinação entre tecnologia de ponta e capacidade de escalar soluções revela que o mercado não procura apenas técnicos, mas **arquitetos do futuro digital**.

Já o **pensamento crítico e a tomada de decisão baseada em dados** obtiveram 18,28%, demonstrando que saber interpretar e agir estrategicamente a partir de dados se consolidou como uma competência transversal e cada vez mais exigida em diferentes níveis hierárquicos. A **capacidade de integrar negócios, tecnologia e ESG** ficou em quarto lugar, com 16,13%. Apesar de ser uma competência estratégica, especialmente num cenário de digitalização com foco em sustentabilidade e governança —, ainda enfrenta desafios de incorporação plena nas rotinas profissionais e nos critérios tradicionais de avaliação de desempenho.

Por fim, **as habilidades de comunicação e liderança adaptativa** foram apontadas por 13,98% dos inquiridos, indicando que, embora ainda sejam entendidas como importantes, podem estar subvalorizadas diante da crença de que aspectos técnicos e inovadores “falam mais alto”. No entanto, esse é um dado que merece atenção: à medida que as equipas se tornam mais híbridas e multiculturais, essa habilidade pode crescer em relevância ao longo da década. A amostra prioriza **escala + técnica deep tech**; as competências “socio técnicas” ficam abaixo, mas ainda relevantes.

Premissas para este resultado

- **Pressões de escala e complexidade:** Cloud híbrida/multi-cloud, plataformas de dados, ciber e IA exigem **arquiteturas escaláveis** e **engenharia de produto/plataforma**; isso empurra “escala” para o topo.
- **Onda de automação com IA:** O valor migra de “programar” para **integrar sistemas com IA** (AIOps, copilotos, agentes). Profissionais com **domínio técnico avançado** ganham prêmio.
- **Ambiente regulatório e soberania digital:** Requisitos de segurança, residência de dados e confiabilidade aumentam a procura por **engenheiros capazes de escalar com as necessidades** (não apenas protótipos).
- **Trajetória recente das empresas (insights anteriores):** Dificuldade de provar ROI da cloud e lacunas do programa de segurança fazem o mercado procurar **capacidade de escalar com eficiência e resiliência**, antes de ampliar frentes de liderança.
- **Propensão do inquirido:** A pergunta é **de escolha única**; perfis técnicos tendem a “privilegiar” o eixo **técnico/escala** e **subestimar** soft skills que consideram “baseline”.

Pontos de atenção

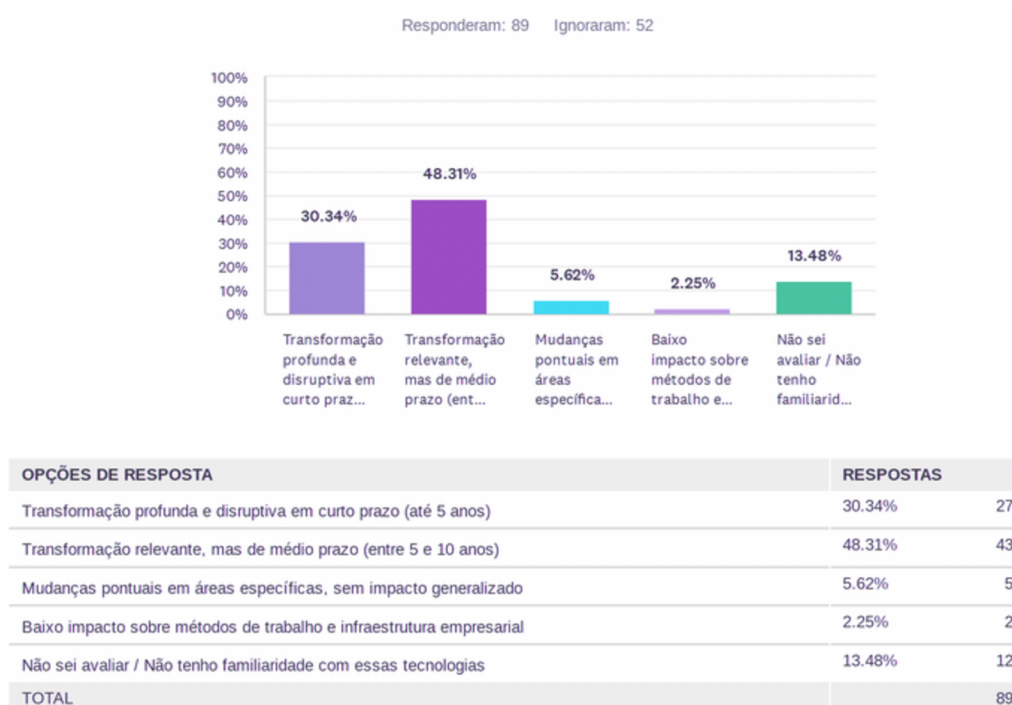
- **Subestimar o humano:** comunicação/liderança e integração negócio–tech aparecem em último, mas são **habilitadores** do próprio scaling (priorização, gestão de mudança, compra executiva).
- **Lag indicator:** conforme IA automatizar parte da codificação, **pensamento crítico** e **liderança adaptativa** tendem a ganhar peso relativo.

Em síntese, os resultados revelam um claro recado do ecossistema de tecnologia: a amostra valoriza quem **inova com escala** e domina **tecnologias de fronteira**, sem descartar as competências humanas e de negócio. O profissional de 2035 é **técnico forte**, mas com **visão de produto e métricas**, capaz de transformar hype em **resultado repetível**. Será aquele capaz de **aliar conhecimento técnico a visão estratégica, pensamento inovador e capacidade de articulação entre diferentes áreas**. Num cenário em constante transformação, quem for capaz de aprender continuamente, adaptar-se rapidamente e propor soluções de impacto terá lugar garantido no centro das decisões.

Sobre IT, infraestrutura e tecnologias disruptivas

Neste momento de transformações aceleradas no universo digital, tecnologias emergentes como Computação Quântica, 6G e Edge Computing prometem remodelar profundamente a forma como empresas operam e estruturam os seus ambientes de trabalho. Mas até que ponto os profissionais já conseguem vislumbrar essa disrupção? O gráfico II– IT, Infraestrutura e Tecnologias Disruptivas, capta essa percepção e revela um cenário de expectativas realistas, mas com um forte sentido de urgência. A seguir, os principais resultados e suas principais constatações.

P12 Impacto esperado da Computação Quântica, 6G e Edge Computing nos métodos de trabalho e nas infraestruturas das empresas



(Gráfico 11 – IT, Infraestrutura e Tecnologias Disruptivas)

A maioria dos inquiridos (48,31%) acredita que as tecnologias citadas provocarão uma **transformação relevante, porém a médio prazo**, ou seja, num horizonte de 5 a 10 anos. Esse dado sugere que, embora se reconheça o potencial disruptivo dessas inovações, há uma percepção de que sua maturação e implementação em larga escala ainda dependem de avanços técnicos, regulações e custos mais acessíveis. É uma visão que combina entusiasmo com cautela, talvez reflexo de experiências passadas com outras inovações tecnológicas que levaram mais tempo do que o previsto para se consolidar.

Ainda assim, **30,34% dos inquiridos acreditam numa transformação profunda e disruptiva já no curto prazo (até 5 anos)**. Esse grupo representa uma parcela mais visionária ou, possivelmente, mais exposta a ambientes onde essas tecnologias já estão a ser testadas ou discutidas de forma prática. Esses profissionais podem estar ligados a setores de ponta, como telecomunicações, cibersegurança ou investigação tecnológica, onde a curva de adoção tende a ser mais acelerada.

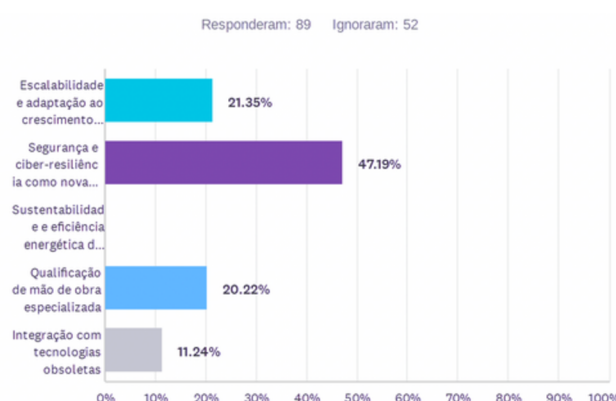
Por outro lado, uma minoria expressiva revela **dúvidas ou desconhecimento: 13,48% afirmaram não saber avaliar ou não ter familiaridade com as tecnologias** em questão. Esse número não deve ser subestimado, pois revela um desafio real: a lacuna de conhecimento técnico e estratégico que ainda persiste em parte das organizações e que pode dificultar o planejamento futuro. Soma-se a isso os 5,62% que consideram que as mudanças ocorrerão apenas de forma pontual e os 2,25% que veem **baixo impacto**, visões que, embora minoritárias, indicam a presença de ceticismo ou foco em áreas menos impactadas a curto prazo.

O gráfico revela um campo fértil para aprofundamento técnico e estratégico nas empresas. A maioria reconhece que estamos diante de uma transformação significativa, mas há incertezas quanto ao ritmo e à abrangência dessas mudanças. A construção de estratégias empresariais mais robustas dependerá da capacidade das lideranças de traduzir o potencial dessas tecnologias em planos concretos, ao mesmo tempo em que promovem a **capacitação interna** e reduzem o desconhecimento que ainda afeta parte dos profissionais. Em resumo: o futuro está próximo, mas ainda exige preparação.

Sobre principal desafio em infraestruturas

Diante da aceleração digital e do surgimento constante de novas tecnologias, as empresas enfrentam o desafio de manter suas infraestruturas digitais robustas, seguras e escaláveis até 2035. O Gráfico 12 – Principais Desafios em Infraestrutura, sintetiza a percepção sobre qual será o principal obstáculo nesse caminho. O resultado revela uma preocupação clara com a segurança e a resiliência cibernética, destacando como os riscos digitais se tornaram uma ameaça permanente e estratégica. Além disso, surgem outras questões relevantes, como o aumento exponencial dos dados, a carência de mão de obra qualificada e a dificuldade de integração com sistemas legados.

P13 Principal desafio para as empresas em relação às infraestruturas digitais até 2035



OPÇÕES DE RESPOSTA	RESPOSTAS	
Escalabilidade e adaptação ao crescimento exponencial de dados	21.35%	19
Segurança e ciber-resiliência como novas ameaças constantes	47.19%	42
Sustentabilidade e eficiência energética dos data centers	0.00%	0
Qualificação de mão de obra especializada	20.22%	18
Integração com tecnologias obsoletas	11.24%	10
TOTAL		89

(Gráfico 12 – Principais Desafios em Infraestrutura)

A análise dos dados mostra que 47,19% dos participantes apontaram a segurança e a ciber-resiliência como o maior desafio até 2035, refletindo a crescente sofisticação das ameaças digitais. A consolidação do trabalho remoto, a ampliação do uso de dispositivos conectados (IoT), a dependência de serviços em cloud e o avanço da inteligência artificial ampliaram exponencialmente a superfície de ataque das empresas. O receio não se limita a invasões externas: fugas de dados, falhas de configuração e riscos internos também estão na mira, exigindo um novo patamar de vigilância contínua e capacidade de resposta rápida, daí a menção à resiliência, e não apenas à segurança.

O segundo maior desafio, com 21,35% das respostas, foi a escalabilidade e a adaptação ao crescimento exponencial de dados. Essa preocupação reflete o impacto direto do Big Data nos negócios, em especial nos setores mais intensivos em informação, como finanças, saúde, retalho e logística. A simples capacidade de armazenar, processar e recuperar grandes volumes de dados não é mais suficiente: é preciso garantir desempenho, disponibilidade e elasticidade, especialmente frente a eventos sazonais ou crises. A transformação digital deixou de ser um diferencial e se tornou pré-requisito de competitividade, e a infraestrutura precisa de acompanhar.

Com 20,22% das menções, a qualificação de mão de obra especializada aparece como uma barreira igualmente crítica. A escassez de profissionais capacitados para lidar com ambientes complexos, como multicloud, DevOps, cibersegurança e inteligência artificial, representa um obstáculo para a evolução tecnológica sustentável das empresas. Trata-se de um problema estrutural, que envolve desde falhas na formação acadêmica até a alta rotatividade no setor de tecnologia, além da crescente procura por requalificação constante.

Curiosamente, a sustentabilidade e a eficiência energética dos data centers não foram apontadas por nenhum dos inquiridos, o que pode sugerir uma percepção de que essa agenda ainda é secundária frente às restantes urgências, ou então que as empresas acreditam que já estão a fazer o suficiente nesse campo, especialmente perante a pressão regulatória e da automação dos sistemas.

Por fim, a integração com tecnologias obsoletas aparece com 11,24%, revelando que o legado ainda é uma pedra no sapato das transformações digitais. Muitas empresas convivem com sistemas antigos que não dialogam com plataformas modernas, criando barreiras de integração, vulnerabilidades de segurança e custos operacionais elevados.

Portanto, o gráfico 12 revela um cenário em que os desafios técnicos, humanos e estratégicos estão entrelaçados. A infraestrutura digital do futuro exigirá não apenas investimentos em tecnologia, mas também uma mudança de cultura organizacional, foco em prevenção e um ecossistema colaborativo capaz de reagir de forma ágil a ameaças e oportunidades.

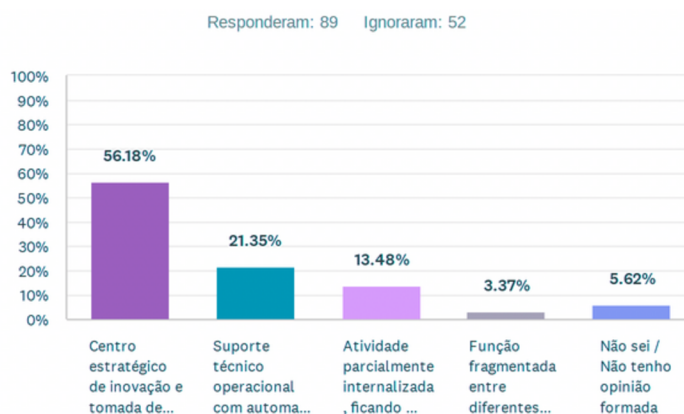
Sobre posição da área de IT nas empresas até 2035

A forma como as empresas projetam o papel da área de Tecnologia da Informação (TI) tem passado por uma transformação significativa, impulsionada tanto pelos avanços tecnológicos quanto pela necessidade de adaptação estratégica diante de um ambiente de negócios volátil e altamente competitivo.

Os dados apresentados no Gráfico 13 – Posição da Área de IT nas Empresas até 2035, revelam de maneira clara essa tendência: o futuro da IT não será apenas operacional, mas fundamentalmente estratégico. Ao analisar as respostas recolhidas, é possível perceber que há uma visão majoritária de que a área ocupará um papel central na inovação e na tomada de decisões até 2035.

A resposta mais expressiva, com 56,18%, aponta que a área de TI será vista como um centro estratégico de inovação e tomada de decisão. Esse dado reflete uma mudança de paradigma: a IT deixa de ser apenas uma área de suporte e passa a ser motor de competitividade e diferenciação. Essa percepção pode estar ligada à crescente importância de temas como inteligência artificial, analytics, automação e cibersegurança, que, por sua vez, exigem uma abordagem integrada à estratégia corporativa.

PI4 Posicionamento da área de IT nas empresas até 2035



OPÇÕES DE RESPOSTA	RESPOSTAS
Centro estratégico de inovação e tomada de decisão	56.18% 50
Suporte técnico operacional com automação predominante	21.35% 19
Atividade parcialmente internalizada, ficando o restante em outsourcing	13.48% 12
Função fragmentada entre diferentes áreas de negócio	3.37% 3
Não sei / Não tenho opinião formada	5.62% 5
TOTAL	89

(Gráfico 13 – Posição da Área de IT nas Empresas até 2035)

Na segunda posição, com 21,35% das respostas, aparece a visão mais tradicional da TI como **suporte técnico operacional com automação predominante**. Embora ainda relevante, essa leitura indica um entendimento mais restrito da atividade da área, centrado na eficiência e não na inovação. Isso pode refletir o perfil de empresas que ainda estão em fase de transição digital ou com maturidade tecnológica mais baixa.

Na sequência, com 13,48% das respostas, está a ideia de uma TI **parcialmente internalizada e parcialmente terceirizada (outsourcing)**. Este modelo aponta para uma gestão mista, onde atividades mais rotineiras ou padronizadas são delegadas a parceiros, enquanto a empresa retém o controle de áreas mais críticas. Essa abordagem sugere uma procura por equilíbrio entre custo e controle estratégico.

Já as opções com menor adesão, **função fragmentada entre áreas de negócio** (3,37%) e **não sei / não tenho opinião formada** (5,62%), revelam visões mais incertas ou descentralizadas sobre o futuro da TI, possivelmente refletindo realidades organizacionais menos estruturadas ou falta de clareza sobre o papel que a tecnologia deve exercer nas empresas.

Possíveis Causas

O otimismo em relação ao posicionamento estratégico da TI pode ser explicado por diversos fatores:

- **A aceleração digital provocada pela pandemia** levou muitas empresas a perceberem a tecnologia como eixo central para continuidade e reinvenção dos negócios.
- **O avanço de tecnologias disruptivas**, como IA generativa, computação em cloud e análise preditiva, reforça a necessidade de integração entre tecnologia e estratégia.
- **A pressão por inovação e diferenciação competitiva**, especialmente em mercados saturados ou altamente regulados, leva a TI a ocupar posição de destaque.
- **A maior valorização do papel dos CIOs, CTOs e líderes de tecnologia**, que passaram a ter lugar nas decisões estratégicas das empresas.

Recomendações

- **Fomentar o protagonismo da TI desde já**, preparando as lideranças da área para atuarem de forma mais consultiva e estratégica dentro das empresas.
- **Integrar tecnologia ao planejamento corporativo**, garantindo que decisões de negócios e investimentos em TI caminhem de forma alinhada.
- **Investir em capacitação e retenção de talentos**, pois o novo posicionamento da área exigirá profissionais com habilidades híbridas (técnicas e de negócios).
- **Evitar a fragmentação da TI**, promovendo uma gestão clara, mesmo em estruturas descentralizadas, para não perder sinergia e agilidade.
- **Mapear o grau de maturidade digital atual** da empresa para definir o ritmo e os marcos de transição rumo a esse novo papel estratégico.

Este retrato aponta para um horizonte em que a TI deixa de ser apenas um apoio técnico para se tornar protagonista na construção do futuro das empresas. A consolidação dessa visão exigirá não apenas investimento em tecnologia, mas principalmente em cultura organizacional, liderança e visão de longo prazo.

Sobre a evolução das infraestruturas digitais até 2035

A discussão sobre o futuro das infraestruturas digitais até 2035 desperta diferentes visões entre os profissionais da área, mas o levantamento apresentado no Gráfico 14 – Evolução das Infraestruturas Digitais até 2035, revela uma tendência clara e dominante: quase metade dos inquiridos aposta na predominância de soluções em cloud híbrida com edge computing.

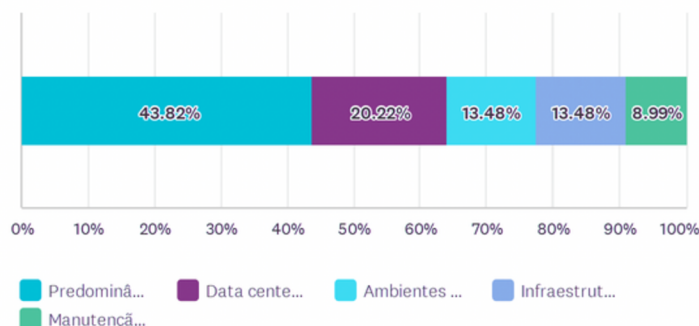
Essa expectativa, além de refletir uma procura por mais flexibilidade e escalabilidade, sinaliza também uma mudança cultural nas empresas em direção a modelos mais dinâmicos, descentralizados e orientados à inovação. Estes dados expõem como os diferentes modelos de infraestrutura estão posicionados diante dos desafios e oportunidades da próxima década.

A cloud híbrida com edge computing, apontada por 43,82% dos inquiridos, lidera com margem. Essa escolha parece ancorada em dois fatores principais: a necessidade de equilibrar segurança e performance com escalabilidade e agilidade, e o avanço das tecnologias que permitem o processamento de dados mais próximo da ponta (edge), reduzindo latências e otimizando recursos.

Num cenário onde a experiência do utilizador, a análise em tempo real e a eficiência operacional ganham protagonismo, essa abordagem mostra-se altamente adaptável. Além disso, muitas organizações ainda mantêm equipamentos legacy ou requisitos de regulamentação que inviabilizam uma migração completa para cloud pública, o que reforça a escolha pela hibridização.

P15 Análise da evolução das infraestruturas digitais até 2035

Responderam: 89 Ignoraram: 52



OPÇÕES DE RESPOSTA	RESPOSTAS
Predominância de soluções em cloud híbrida com edge computing	43.82% 39
Data centers tradicionais otimizados com IA e IoT	20.22% 18
Ambientes 100% descentralizados e conectados via 6G	13.48% 12
Infraestruturas IaaS, contratadas como serviço	13.48% 12
Manutenção do modelo atual com melhorias incrementais	8.99% 8
TOTAL	89

(Gráfico 14 – Evolução das Infraestruturas Digitais até 2035)

A segunda opção mais citada, data centers tradicionais otimizados com IA e IoT (20,22%), mostra que há uma parcela significativa das empresas que ainda confia nas estruturas mais convencionais, desde que modernizadas. Esse dado sugere que, apesar do apelo da cloud, muitos ambientes corporativos preferem manter um certo controle físico sobre os seus dados e processos, especialmente em setores críticos ou regulados, apostando em tecnologias que aumentem a inteligência e a eficiência desses centros.

Em seguida, dois cenários mais disruptivos aparecem empatados com 13,48% cada: ambientes 100% descentralizados e conectados via 6G, e infraestruturas IaaS contratadas como serviço. No primeiro caso, a proposta de um ecossistema totalmente distribuído, impulsionado por conectividade ultrarrápida, ainda parece distante da realidade atual, embora seja promissora em termos de autonomia e inovação. Já no segundo, o modelo “as a service” reforça uma tendência de terceirização e elasticidade dos recursos, embora talvez ainda enfrente resistências relacionadas à dependência de fornecedores externos.

Por fim, a manutenção do modelo atual com melhorias incrementais foi a aposta de apenas 8,99% dos inquiridos, o que indica um consenso maioritário sobre a necessidade de transformação significativa nas infraestruturas digitais. Esse número pode refletir uma percepção de que o modelo vigente já está em processo de obsolescência diante da aceleração tecnológica e das novas exigências de mercado.

A leitura desses dados aponta para alguns caminhos estratégicos. As organizações que ainda não iniciaram sua o seu caminho rumo à cloud híbrida devem considerar esse movimento como prioritário, especialmente se desejam manter competitividade e resiliência digital até 2035. Ao mesmo tempo, é fundamental investir em capacitação técnica para operar e gerir ambientes complexos e distribuídos, e também avaliar com cautela os riscos de regulamentação e de segurança de cada modelo. Assim, é recomendável que empresas mantenham uma mentalidade aberta à experimentação, testando gradualmente soluções emergentes como edge, 6G e IaaS, de forma a prepararem-se para cenários mais descentralizados e interconectados que, embora ainda não dominem, estão no horizonte.

Sobre AI, cybersecurity e compliance

Os dados apresentados no Gráfico 15 – AI, Cybersecurity e Compliance, revelam a percepção dos inquiridos sobre temas sensíveis e estratégicos como Inteligência Artificial (IA), cibersegurança e compliance em meio a um cenário de instabilidade global. As afirmações abordam desde pressões geopolíticas até o impacto prático de tecnologias emergentes, apontando o grau de concordância dos profissionais com esses desafios e oportunidades.

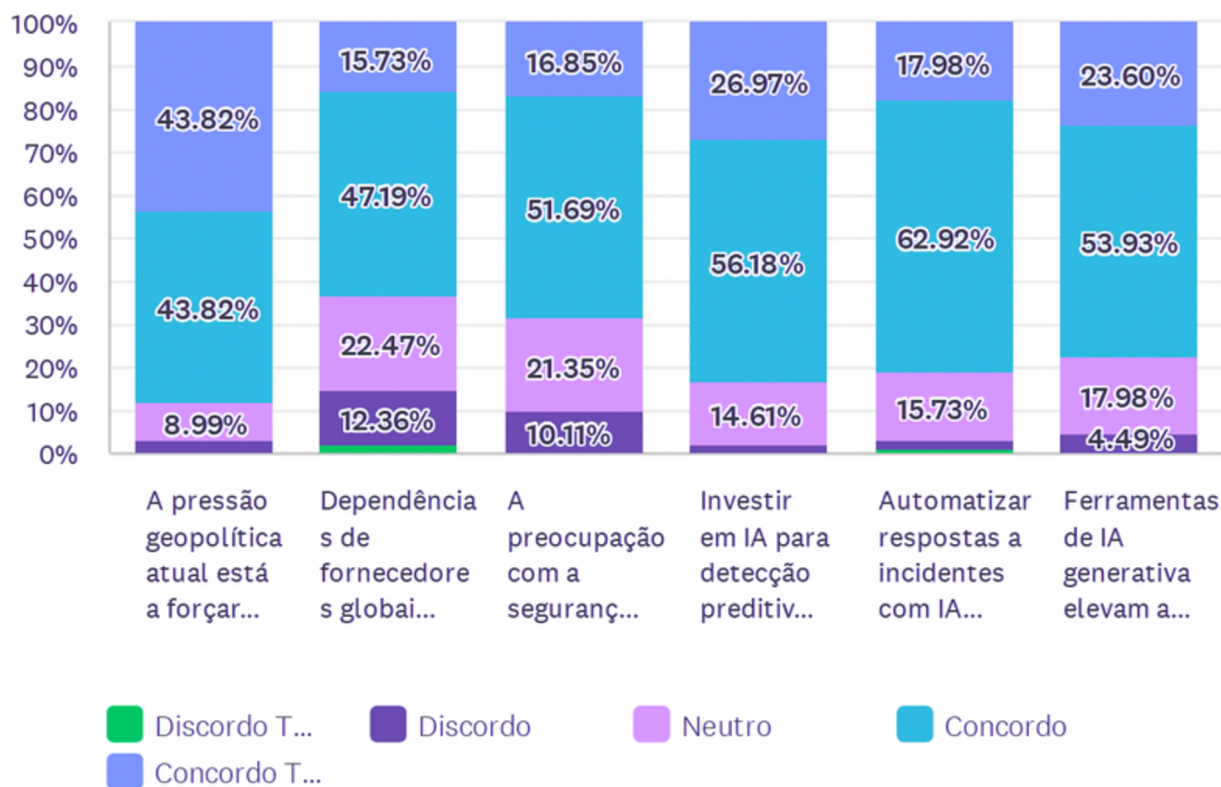
Em geral, observa-se uma forte tendência de alinhamento com a urgência de adoção de IA e estratégias de segurança digital, embora alguma conflitualidade éticas e operacionais ainda gerem posições mais neutras ou cautelosas. A seguir, a análise detalhada dos principais resultados.

Pressão geopolítica acelera independência tecnológica

A afirmação de que as tensões geopolíticas estão forçando a Europa a acelerar sua independência tecnológica em áreas críticas como IA e cibersegurança recebeu **altíssima concordância: 87,64% dos inquiridos** concordam ou concordam totalmente, com **média ponderada de 4,28 – a mais alta entre todas as questões**. Esse resultado pode ser interpretado como reflexo da guerra na Ucrânia, das sanções contra grandes potências tecnológicas e da **crescente preocupação com soberania digital**. O medo de interrupções em cadeias de fornecimento críticas e o risco de espionagem industrial colocam a Europa em alerta, impulsionando investimentos em infraestrutura própria e tecnologias estratégicas. A perspectiva é que as organizações devem acompanhar atentamente políticas da União Europeia como o AI Act e iniciativas como GAIA-X para alinhamento com movimentos de soberania digital e compliance regulatório.

P16 Nível de concordância com afirmações sobre AI, Cibersegurança e Compliance

Responderam: 89 Ignoraram: 52



(Gráfico 15 – AI, Cybersecurity e Compliance)

Riscos das dependências de fornecedores globais

Quase metade dos inquiridos (47,19%) concorda que depender de grandes fornecedores como Microsoft ou Amazon representa um risco, mas essa visão é acompanhada por 22,47% de respostas neutras e 14,61% de discordância. A média ponderada (3,62) sugere um grau menor de consenso, indicando que parte dos profissionais ainda vê essas parcerias como inevitáveis ou vantajosas.

É possível que a baixa percepção de risco esteja relacionada à comodidade, performance ou custo-benefício das soluções oferecidas por big techs, mesmo que isso contrarie os princípios de soberania digital e diversificação.

Fomentar estratégias de vendor diversification e investir em soluções open source ou europeias pode mitigar riscos e alinhar melhor a organização às exigências regulatórias futuras.

Segurança de dados como travão à inovação

Mais da metade (68,54%) acredita que a preocupação com segurança dos dados inibe a velocidade da inovação na Europa. Esse dado revela um dilema real: ao mesmo tempo que a proteção é essencial, o excesso de regulação ou medo de falhas pode travar avanços. A média ponderada (3,75) confirma este equilíbrio instável.

Adotar uma abordagem de “segurança by design” nas inovações tecnológicas pode ajudar a reduzir esse atrito. Isso inclui formação contínua e integração de especialistas em segurança desde as fases iniciais de projetos.

IA como aliada da cibersegurança – com custo

A proposta de investir em IA para fortalecer a cibersegurança teve ampla adesão: 83,15% de concordância e média de 4,08. Isso sinaliza maturidade e reconhecimento de que, apesar de exigente em compliance e custos, a IA é vista como indispensável para combater ameaças avançadas. O destaque para exigências como RGPD, NIS2 e DORA revela uma preocupação não apenas técnica, mas também regulatória.

Uma boa alternativa para este desafio passa por estruturar uma abordagem integrada entre equipes de TI, jurídico e compliance para garantir que os investimentos em IA estejam alinhados com as exigências legais e mitiguem riscos operacionais.

	DISCORDO TOTALMENTE	DISCORDO	NEUTRO	CONCORDO	CONCORDO TOTALMENTE	TOTAL	MÉDIA PONDERADA
A pressão geopolítica atual está a forçar a Europa a acelerar sua independência tecnológica em áreas críticas como IA e cybersecurity.	0.00% 0	3.37% 3	8.99% 8	43.82% 39	43.82% 39	89	4.28
Dependências de fornecedores globais (como Microsoft e Amazon) representam um risco controlado e aceitável para a nossa operação.	2.25% 2	12.36% 11	22.47% 20	47.19% 42	15.73% 14	89	3.62
A preocupação com a segurança dos dados inibe significativamente a velocidade das inovações na Europa.	0.00% 0	10.11% 9	21.35% 19	51.69% 46	16.85% 15	89	3.75
Investir em IA para detecção preditiva de ameaças fortalece a postura de cybersecurity, mas requer maiores esforços de compliance (RGPD, NIS2, DORA), elevando os custos operacionais.	0.00% 0	2.25% 2	14.61% 13	56.18% 50	26.97% 24	89	4.08
Automatizar respostas a incidentes com IA reduz o tempo de reação a ataques, porém pode criar dependência excessiva de algoritmos ainda sem governação, transferindo a responsabilidade de decisão para sistemas.	1.12% 1	2.25% 2	15.73% 14	62.92% 56	17.98% 16	89	3.94
Ferramentas de IA generativa elevam a produtividade das equipes de segurança ao acelerar análises, mas também aumentam o risco de fuga ou exposição de dados confidenciais.	0.00% 0	4.49% 4	17.98% 16	53.93% 48	23.60% 21	89	3.97

(Tabela 5 – AI, Cybersecurity e Compliance)

Automatização de respostas a incidentes: agilidade com ressalvas

Com média de 3,94, a **maioria (80,9%)** concorda que automatizar respostas com IA reduz o tempo de reação a incidentes, mas a afirmação também **alerta para riscos éticos** de transferir a responsabilidade de decisões críticas a algoritmos ainda imaturos. Há aqui uma **tensão entre eficiência operacional e responsabilidade**.

Desta forma criar camadas híbridas de resposta – **automação com supervisão humana** – e definir claramente os limites da atuação algorítmica é essencial para **manter accountability e ética nas decisões críticas**.

IA generativa: produtividade e risco

Por fim, a afirmação sobre o uso de IA generativa para aumentar produtividade foi bem recebida (média de 3,97), mas não sem ressalvas: **41,6%** dos inquiridos concordaram totalmente, e **23,6%** concordaram, mas **22,47%** ficaram neutros ou discordaram. A principal preocupação é o **risco de fuga** de informações confidenciais ao utilizarmos ferramentas abertas e pouco controladas. Portanto, desenvolver **políticas claras de uso de IA generativa**, inclusive definindo quais tarefas podem ser delegadas a essas ferramentas e quais dados são sensíveis, é crucial para garantir segurança e ética.

A análise desses dados aponta que o debate sobre IA, cibersegurança e compliance nas empresas europeias está a amadurecer rapidamente. Há alto grau de alinhamento quanto à **urgência dos temas**, mas também surgem **dilemas éticos e operacionais** que procuram políticas claras, investimentos direcionados e formação constante. **O futuro será de maior automação, sim, mas também exigirá mais responsabilidade, governação e decisões estratégicas conscientes**.

Sobre sustentabilidade, neutralidade carbônica e infraestrutura digital

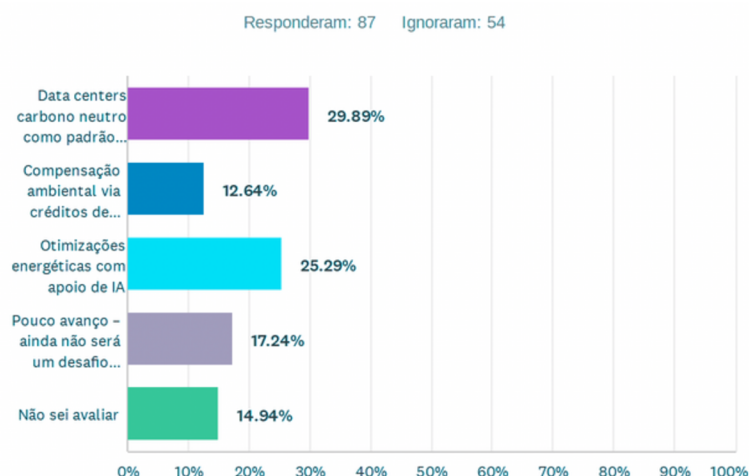
A procura por práticas sustentáveis e pelo cumprimento de metas de neutralidade carbônica tem vindo a intensificar-se nos últimos anos, especialmente em setores altamente dependentes de infraestrutura digital.

No horizonte de 2035, espera-se que a sustentabilidade seja incorporada como premissa central no planeamento tecnológico. O Gráfico 16 – Sustentabilidade, Neutralidade Carbônica e Infraestrutura Digital, traz uma visão importante sobre o que os inquiridos projetam como tendência nesse campo, indicando tanto as apostas mais promissoras quanto as incertezas que ainda pairam sobre o tema.

O destaque dos dados elencados vai para a expectativa de que data centers carbono neutro se tornem o padrão global, com 29,89% das respostas. Isso reflete a crescente pressão regulatória, social e ambiental por operações mais limpas, especialmente num setor que tradicionalmente consome grandes volumes de energia. A consolidação de iniciativas de grandes empresas de tecnologia em direção à neutralidade climática, como os compromissos públicos da Microsoft, Google e Amazon, pode estar a influenciar essa percepção como um “caminho natural” a ser seguido por todo o mercado.

Outro ponto relevante é a aposta nas otimizações energéticas com apoio de inteligência artificial (25,29%), o que indica uma visão de futuro em que a eficiência será cada vez mais automatizada. Essa resposta pode ser explicada pelo avanço das tecnologias preditivas e pela proliferação de sensores inteligentes que tornam os sistemas mais autônomos na identificação e correção de desperdícios. A IA surge, assim, como aliada da sustentabilidade, não apenas como motor de inovação, mas como ferramenta de gestão ambiental.

P17 Expectativas para a infraestrutura digital em matéria de sustentabilidade e neutralidade carbônica até 2035



OPÇÕES DE RESPOSTA	RESPOSTAS
Data centers carbono neutro como padrão global	29.89% 26
Compensação ambiental via créditos de carbono	12.64% 11
Otimizações energéticas com apoio de IA	25.29% 22
Pouco avanço – ainda não será um desafio relevante	17.24% 15
Não sei avaliar	14.94% 13
TOTAL	87

(Gráfico 16 – Sustentabilidade, Neutralidade Carbônica e Infraestrutura Digital)

Por outro lado, a **compensação ambiental via créditos de carbono** foi escolhida por **apenas 12,64% dos inquiridos**, o que pode sinalizar uma certa desconfiança quanto à eficácia dessa abordagem isoladamente. A crítica recorrente a esse modelo é referente à sua **capacidade de gerar impacto real**, já que permite a manutenção de práticas poluentes mediante contrapartidas financeiras, muitas vezes de difícil rastreabilidade ou impacto incerto.

Interessante também notar que **17,24%** dos participantes acreditam que haverá **pouco avanço até 2035**, considerando que o tema ainda não será um desafio relevante para o setor. Essa resposta, embora minoritária, levanta um sinal de alerta: parte do mercado ainda pode estar **subestimando o impacto ambiental da digitalização crescente**. A este grupo, soma-se uma percentagem considerável (**14,94%**) de pessoas que afirmaram não saber avaliar, o que revela uma lacuna de conhecimento técnico ou estratégico sobre o tema.

Diante desses dados, é possível identificar alguns caminhos de ação.

- Ampliar a disseminação de informações sobre **o impacto ambiental da infraestrutura digital é fundamental para ligar os setores** ainda reticentes ou desinformados.
- Fomentar **políticas públicas e incentivos económicos** que impulsionem a adoção de práticas sustentáveis pode acelerar a transformação do setor.
- **Promover uma visão integrada**: data centers mais eficientes, sim, mas acompanhados de mudanças estruturais no modelo energético e no ciclo de vida dos equipamentos.

A expectativa sobre 2035 mostra que **há ambição, mas também dispersão**. O futuro da infraestrutura digital neutra em carbono exigirá mais do que boas intenções, será necessário alinhar inovação, regulação, investimento e sensibilização de forma coordenada.

Sobre ESG, eficiência energética e neutralidade carbônica

Já o Gráfico 17 – ESG, Eficiência Energética e Neutralidade Carbônica, revela como os profissionais estão a perceber a relação entre tecnologia, ESG (ambiental, social e governança) e eficiência energética no contexto de infraestrutura digital, especialmente no que diz respeito ao uso de data centers e inteligência artificial.

As respostas obtidas mostram uma tendência clara de **valorização de soluções tecnológicas sustentáveis e integradas a metas de neutralidade carbônica**. A **alta taxa de concordância em praticamente todas as afirmações** sinaliza que o tema já entrou com força na agenda estratégica das empresas, mas os dados também revelam **nuances que merecem atenção**.

Tendência majoritária de concordância com ESG e eficiência energética

A afirmação com maior média ponderada (4,06) e maior taxa de concordância total (**85%**) foi a de que **“a crescente procura por data centers impõe desafios relevantes à neutralidade carbônica, exigindo soluções energéticas mais sustentáveis”**. Isso demonstra uma sensibilização generalizada de que o crescimento da procura digital, especialmente impulsionado pela inteligência artificial e armazenamento em cloud, tem custos ambientais que precisam ser abordados com estratégias de mitigação, como o uso de energias renováveis e sistemas mais eficientes do arrefecimento.

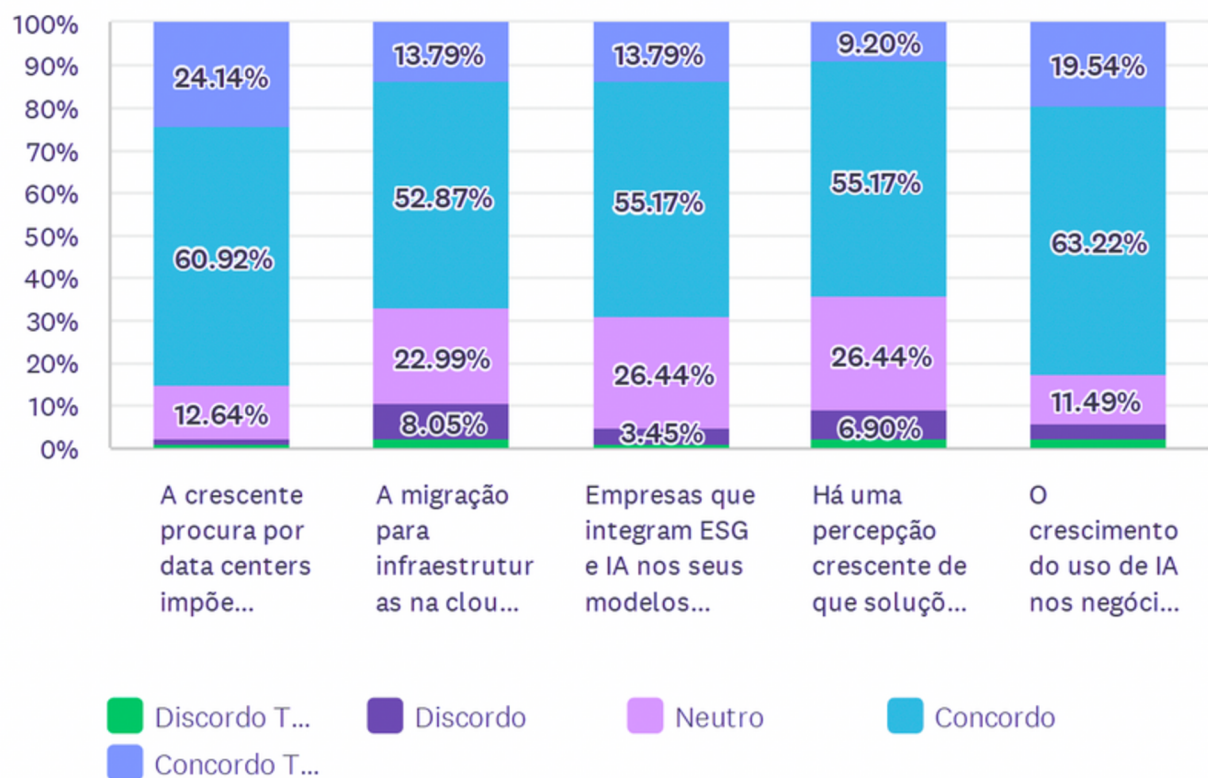
Esse entendimento conecta-se diretamente com outra afirmação de alta concordância: **“o crescimento do uso de IA nos negócios deve ser equilibrado com investimentos em infraestruturas digitais sustentáveis”** (média 3,94). Essa percepção reforça a ideia de que a inovação tecnológica precisa caminhar lado a lado com a responsabilidade ambiental. Aqui, **82,76%** concordaram ou concordaram totalmente com a afirmação.

Complementaridade entre tecnologia e sustentabilidade

Outro destaque é o reconhecimento de que **soluções tecnológicas e metas de sustentabilidade não são contraditórias, mas complementares**, afirmação com **64,37%** de concordância (média 3,62). Ainda que essa seja a de menor média entre as cinco afirmações, o número ainda é expressivo e sugere que há um entendimento crescente de que tecnologia pode, e deve, ser usada como ferramenta a favor da sustentabilidade, e não vista como antagonista.

P18 Nível de concordância com afirmações sobre ESG, eficiência energética e neutralidade carbônica

Responderam: 87 Ignoraram: 54



(Gráfico 17 – ESG, Eficiência Energética e Neutralidade Carbônica)

Percepção de vantagens competitivas para empresas que integram ESG e IA

A terceira afirmação mais bem avaliada (média 3,77) aponta que **empresas que integram ESG e IA nos seus modelos operacionais obtêm vantagem competitiva e reputacional**. Combinando as respostas “concordo” e “concordo totalmente”, **68,96%** dos inquiridos validam essa proposição, indicando que a integração de princípios sustentáveis e tecnologias emergentes não é apenas uma questão de compliance, mas também uma estratégia de diferenciação no mercado.

Possíveis Causas

Essa percepção positiva pode ser explicada por fatores diversos. O primeiro é o **aumento da regulação e da exigência de transparência** nas práticas ESG, que empresas portuguesas estão sujeitas no âmbito do Pacto Ecológico Europeu. Em segundo lugar, há um **amadurecimento das tecnologias de infraestrutura**, como cloud híbrida e data centers verdes, que tornam mais viável alinhar desempenho e sustentabilidade. E, finalmente, a IA tem ganhado papel estratégico nas organizações, o que pressiona pela expansão de infraestrutura digital, mas também gera maior atenção sobre os seus impactos

	DISCORDO TOTALMENTE	DISCORDO	NEUTRO	CONCORDO	CONCORDO TOTALMENTE	TOTAL	MÉDIA PONDERADA
A crescente procura por data centers impõe desafios relevantes à neutralidade carbónica, exigindo soluções energéticas mais sustentáveis.	1.15% 1	1.15% 1	12.64% 11	60.92% 53	24.14% 21	87	4.06
A migração para infraestruturas na cloud e data centers de última geração contribui para maior eficiência energética e redução de emissões.	2.30% 2	8.05% 7	22.99% 20	52.87% 46	13.79% 12	87	3.68
Empresas que integram ESG e IA nos seus modelos operacionais obtêm vantagem competitiva e reputacional no cenário europeu.	1.15% 1	3.45% 3	26.44% 23	55.17% 48	13.79% 12	87	3.77
Há uma percepção crescente de que soluções tecnológicas e metas de sustentabilidade não são contraditórias, mas complementares.	2.30% 2	6.90% 6	26.44% 23	55.17% 48	9.20% 8	87	3.62
O crescimento do uso de IA nos negócios deve ser equilibrado com investimentos em infraestruturas digitais sustentáveis, como data centers verdes.	2.30% 2	3.45% 3	11.49% 10	63.22% 55	19.54% 17	87	3.94

(Tabela 6 – ESG, Eficiência Energética e Neutralidade Carbónica)

Diante estes dados, três caminhos são recomendáveis:

1. **Fortalecer a gestão do ESG ligada à tecnologia**, criando indicadores de impacto energético e ambiental específicos para áreas como TI e inovação.
2. **Investir numa infraestrutura verde desde a fase de planejamento**, adotando critérios de eficiência energética, circularidade e uso de fontes renováveis.
3. **Promover capacitação e sensibilização nas áreas técnicas e de gestão**, para garantir que o crescimento da IA e da digitalização caminhe em equilíbrio com os compromissos climáticos das organizações.

Portanto, há uma janela de oportunidade para empresas que conseguirem alinhar a transformação digital com metas ambientais concretas, não apenas para cumprir exigências regulatórias, mas também para conquistar uma posição mais sólida, fiável e inovadora no mercado.

Sobre relevância de neutralidade carbónica de data centers

Um dos aspetos mais discutidos é a neutralidade carbónica dos data centers, já que existe um alto consumo energético e, portanto, têm impacto direto nas emissões de carbono. Assim, após responder as questões anteriores sobre ESG, os participantes foram convidados a atribuir a quantidade de estrelas compatível a que medida consideram os objetivos de neutralidade carbónica de data centers como fator decisivo na escolha de parceiros tecnológicos, sendo 1 estrela = nada relevante a 5 estrelas = extremamente relevante.

Assim, a Figura 2 analisada mostra como os profissionais avaliam a importância desse critério na escolha de parceiros tecnológicos. A pergunta central é: a procura por data centers mais sustentáveis já é uma prioridade concreta ou ainda é vista como secundária frente a outros fatores, como custo e desempenho?

P19 Relevância dos objetivos de neutralidade carbónica dos data centers na escolha de parceiros tecnológicos

Responderam: 87 Ignoraram: 54

3.3★
average rating



	1	2	3	4	5	TOTAL	MÉDIA PONDERADA
☆	13.79%	8.05%	20.69%	47.13%	10.34%	87	3.32
	12	7	18	41	9		

(Figura 2- Estrelas Correspondentes à Relevância da Neutralidade Carbónica em Data Centers)

A média geral obtida na avaliação foi de **3,3 estrelas**, em uma escala de 1 a 5, indicando uma **relevância moderada**, mas não absoluta, atribuída ao tema. Embora **47,13%** dos inquiridos tenham atribuído 4 estrelas, sinalizando que consideram o critério “relevante” —, apenas **10,34%** deram a nota máxima, de 5 estrelas. Por outro lado, ainda há uma percentagem considerável que não vê grande importância nessa exigência: **13,79%** avaliaram com apenas 1 estrela, indicando que consideram o tema “nada relevante”, e outros 8,05% deram 2 estrelas.

Essa dispersão de respostas revela um cenário em transição. Ainda que a maioria já reconheça a importância dos objetivos de neutralidade carbônica, a força desse fator como **critério decisivo** ainda é limitada. As causas possíveis para esse comportamento podem estar ligadas a três aspectos principais. Primeiro, a percepção de que sustentabilidade ainda encarece as soluções tecnológicas, o que pode ser um impeditivo em contextos orçamentais restritos. Segundo a ausência de métricas claras ou certificações acessíveis pode gerar desconfiança ou dificultar a comparação entre fornecedores. E terceiro, pode haver uma **desconexão entre as áreas técnicas e as diretrizes ESG institucionais**, fazendo com que a preocupação ambiental fique em segundo plano nas decisões mais operacionais.

É importante que as organizações alinhem os seus critérios técnicos com os compromissos ESG já assumidos em nível institucional. A criação de **guidelines claras para contratação de parceiros tecnológicos**, incluindo exigências mínimas de sustentabilidade, pode ajudar a transformar essa percepção intermediária numa prioridade concreta. Além disso, **ações de sensibilização interna** e a valorização de cases de sucesso em redução de carbono no setor de TI podem acelerar esse ponto de viragem.

Em resumo, o gráfico revela um campo fértil para amadurecimento. A neutralidade carbônica nos data centers já está no radar, mas ainda precisa avançar para o centro da tomada de decisão.



FASE 4: QUANTITATIVA Survey

De maneira geral, o estudo revela um ambiente que já internalizou a transformação digital como prioridade estratégica, mas que ainda enfrenta obstáculos práticos e estruturais para materializar essa ambição em larga escala. A valorização de modelos híbridos de trabalho, a aposta em tecnologias emergentes como IA e cloud híbrida, e a percepção da TI como centro estratégico das empresas sinalizam maturidade crescente. Contudo, persistem lacunas relevantes, como:

- Dificuldade de justificar o ROI de soluções em cloud,
- Baixa penetração de práticas avançadas de cibersegurança,
- Disparidade no nível de conhecimento sobre identidade digital e sustentabilidade.

O estudo também aponta para uma tensão latente entre inovação e regulação, especialmente no contexto europeu. A burocracia e a fragmentação política são vistas como entraves à competitividade tecnológica, ao passo que a pressão geopolítica e os riscos de dependência de grandes fornecedores estrangeiros impulsionam um desejo claro por soberania digital e estratégias mais autônomas. A sustentabilidade, por sua vez, começa a ganhar espaço no planeamento tecnológico, embora ainda não figure como critério decisivo na escolha de parceiros, sinal de que há um caminho a percorrer na integração efetiva entre tecnologia e ESG. Outro ponto de destaque é a valorização de competências híbridas no profissional de IT do futuro: dominar tecnologias de ponta e, ao mesmo tempo, ser capaz de inovar com capacidade de expansão. Ainda que soft skills apareçam em menor evidência nas respostas, é notável que pensamento crítico, visão estratégica e capacidade de articulação entre tecnologia e negócios sejam mencionadas como atributos diferenciais até 2035.

Em síntese, os dados quantitativos confirmam e expandem as percepções qualitativas levantadas anteriormente, permitindo uma triangulação robusta de evidências. O panorama que emerge é de um ecossistema em transição, que já compreende a direção a seguir, mas que ainda precisa alinhar discurso e prática, estratégia e execução, ambição e realidade. O futuro está mapeado; a questão que se impõe agora é como, e com que velocidade, as empresas conseguirão percorrê-lo.

Mais do que oferecer respostas definitivas, os dados deste estudo convidam à reflexão contínua e ao diálogo entre os diversos atores envolvidos na transformação digital em Portugal. Trata-se de um ponto de partida valioso para ações futuras, pautadas não apenas pela tecnologia em si, mas pela capacidade coletiva de projetar e construir um futuro mais conectado, sustentável e inclusivo.

05

**Construção
de Cenários e
Mapeamento
de Tendências
Específicas**

FASE 5: CONSTRUÇÃO DE CENÁRIOS E MAPEAMENTO DE TENDÊNCIAS ESPECÍFICAS:

Cenário geopolítico e como Portugal está posicionado

A Europa vive um momento de intensa reconfiguração geopolítica, marcado por múltiplas tensões que moldam profundamente o setor de Tecnologia da Informação. O continente enfrenta um cenário de vácuo de poder global onde nenhuma potência consegue ditar as regras internacionais ou evitar grandes conflitos.

O conflito russo-ucraniano está a reconfigurar fundamentalmente o setor tecnológico na Europa Oriental. A guerra ultrapassou diversas “barreiras geopolíticas” nos últimos anos, desde invasões e ocupações até violações do espaço aéreo e crimes de guerra, criando um ambiente de maior tolerância ao risco e incentivando escaladas para reestabelecer a dissuasão.

A Ucrânia emergiu como um polo inesperado de inovação militar-tecnológica, especialmente em drones. Centenas de empresas ucranianas desenvolveram tecnologias que, apesar de simples em engenharia, acumulam experiência de combate real. O país lançou o programa “Construa com a Ucrânia”, permitindo que aliados europeus acedam essas tecnologias e estabeleçam linhas de produção conjuntas.

O conflito expõe vulnerabilidades críticas na cadeia de suprimentos tecnológica europeia. A Ucrânia fornece mais de 90% do neónio de grau semicondutor para os Estados Unidos, fundamental para a fabricação de chips. A Rússia, por sua vez, é responsável por 35% do paládio global, utilizado em sensores e componentes de memória.

Embora os grandes fabricantes de chips inicialmente relatassem impacto limitado devido aos estoques existentes, especialistas alertam para uma possível “segunda onda” de escassez de semicondutores caso o conflito se prolongue.

Este é um ambiente de guerra ao mesmo tempo, convencional, mas também por meios, como ciberataques, desinformação, interferência política e pressão económica. A Europa intensificou drasticamente esforços para alcançar soberania digital diante das tensões geopolíticas. A União Europeia deve investir €300 mil milhões na próxima década para construir infraestrutura de cloud europeia segura e resiliente, fortalecer capacidades de IA e desenvolver uma indústria de semicondutores autossuficiente.

Atualmente, 92% da infraestrutura de cloud da Europa é controlada por empresas dos EUA, destacando a urgência de reduzir essa dependência. A UE lançou uma nova fase do Programa Europa Digital com €8,1 mil milhões até 2027 para reforçar a adoção de tecnologias emergentes, priorizando IA generativa e cibersegurança.

A geopolítica digital tornou-se inseparável da política global. As tensões entre EUA, China e Europa moldam diretamente as decisões tecnológicas no continente. O CLOUD Act americano confere ao governo dos EUA o poder de aceder a dados globalmente detidos por empresas americanas, mesmo quando armazenados na Europa, criando conflitos com o RGPD europeu.

Empresas europeias formaram uma coligação com mais de 250 assinaturas, incluindo Airbus e Dassault Systèmes, exigindo ações radicais da UE para soberania digital. A iniciativa EuroStack propõe a criação de um Fundo de Infraestrutura Soberana e campanhas “Buy European” para aumentar a procura por soluções tecnológicas europeias.

Neste contexto, Portugal demonstra progressos consistentes na digitalização, ocupando posição de destaque na disponibilização de serviços públicos digitais e liderança no acesso a registos de saúde eletrónicos. O país possui cobertura robusta de conectividade, com 98,7% de cobertura 5G e 94,6% de redes de alta capacidade.

O mercado nacional de tecnologia apresenta resiliência e crescimento contínuos, impulsionado pela necessidade crescente de modernização empresarial e pelo Plano de Recuperação e Resiliência (PRR) na Administração Pública. Portugal dedica 21% do PRR ao digital (€4,5 mil milhões) e 11% dos fundos de coesão (€2,4 mil milhões) a projetos digitais.

Portugal desenvolveu uma Agenda Nacional de IA estruturada em três eixos – Inovação, Talento e Infraestrutura – com visão clara para 2030: garantir um ecossistema robusto de IA baseado na ética e excelência científica. As iniciativas incluem o desenvolvimento do primeiro LLM português e implementação de uma “fábrica de IA”.

A IA generativa está a transformar significativamente o mercado nacional, prometendo impactar não apenas as operações empresariais, mas também os modelos de negócio e toda a economia. As tendências indicam que as áreas de maior crescimento em 2025 serão IA, cibersegurança, computação em cloud e análise de dados.

Portugal consolidou-se como um dos ecossistemas de startups mais vibrantes da Europa. O país registou taxa de sucesso de 9,68% no programa EIC Accelerator, superando a média europeia de 7,16%. A Fábrica de Unicórnios de Lisboa aumentou cinco vezes sua capacidade em dois anos, passando de 50 projetos anuais para mais de 250. O programa Winter Batch 2025 apoiará 50 novas startups, com 40% dos fundadores sendo mulheres e 40% dos projetos tendo fundadores internacionais.

Portugal é reconhecido como modelo a seguir em cibersegurança, posicionando-se entre as nações com níveis mais elevados de desenvolvimento segundo o Global Cybersecurity Index da ITU. A implementação da Diretiva NIS2 representará tanto desafio quanto oportunidade para organizações portuguesas reforçarem investimentos em cibersegurança. A necessidade de proteger dados críticos e garantir resiliência das infraestruturas digitais será prioritária, especialmente em setores estratégicos.

De uma maneira geral, o cenário geopolítico europeu atual caracteriza-se por múltiplas tensões e reconfiguração de alianças, com impactos profundos no setor de Tecnologia da Informação. A guerra na Ucrânia catalisou inovações tecnológicas inesperadas e expôs vulnerabilidades críticas nas cadeias de fornecimento.

Portugal posiciona-se estrategicamente neste contexto, demonstrando liderança em cibersegurança, crescimento do ecossistema de startups e investimentos significativos em digitalização. O país combina vantagens competitivas – conectividade robusta, políticas públicas estruturadas e reconhecimento internacional – com desafios como a necessidade de maior autonomia tecnológica e desenvolvimento de talentos especializados.

O desejo europeu pela soberania digital representa tanto um desafio, como uma oportunidade para Portugal, que pode consolidar-se como hub tecnológico relevante no contexto regional, contribuindo para a redução da dependência externa e fortalecimento da competitividade europeia no cenário global.

Cenário Tecnológico

O panorama tecnológico e geopolítico europeu é fortemente marcado por eventos que exigem o reordenamento de prioridades nacionais e regionais. Em 2025, destacam-se o avanço da cibersegurança diante da guerra híbrida, a dependência tecnológica e a perda de soberania digital, o crescente gap competitivo em relação aos Estados Unidos e China, desafios de regulamentação e de fragmentação do mercado, o risco sistémico da desinformação, a escassez de talentos em TIC, além dos impactos crescentes de riscos climáticos sobre infraestrutura crítica.

Cibersegurança

A cibersegurança ganhou centralidade no contexto das guerras híbridas modernas. Em 2025, estima-se que os gastos europeus em cibersegurança crescerão 11,8%, impulsionados pelo aumento das ameaças digitais e pela instabilidade internacional. A Rússia, notoriamente, tem ampliado o seu arsenal de guerra híbrida, incluindo ataques cibernéticos, espionagem, sabotagem e campanhas de desinformação, ataques como o apagão europeu de abril de 2025 levantaram suspeitas de ciberataques coordenados. Além disso, a vulnerabilidade de infraestruturas críticas permanece alta: falhas como a baixa visibilidade de ativos e autenticação fraca potencializam riscos sistêmicos, já que ataques num país rapidamente se propagam por toda a região. No setor de energia, petróleo, gás e serviços públicos, 80% dos ataques de ransomware em 2024 resultaram na encriptação de dados. Como resposta, regulamentações como NIS2, DORA e RGPD têm um papel vital, ainda que o compliance traga desafios burocráticos.

Dependência tecnológica

No âmbito da dependência tecnológica e perda de soberania digital, a Europa encontra-se numa posição delicada: 92% da infraestrutura de cloud do continente está sob controle de empresas dos EUA, e cerca de 80% dos fornecedores de semicondutores utilizados por empresas europeias são de fora da União Europeia. Essa configuração expõe setores estratégicos, como o setor automóvel e das energias renováveis, a riscos graves, trocando a dependência energética tradicional por uma nova dependência digital.

Competitividade

A Europa enfrenta também um crescente gap competitivo com EUA, China e Coreia do Sul. Enquanto apenas 11 empresas europeias estão entre as 100 maiores do setor tecnológico global, as cinco maiores empresas americanas investem mais em P&D do que os 27 membros da UE juntos, ao longo de sete anos. Em tecnologias críticas, a liderança europeia é restrita: no setor de 5G, por exemplo, a China capta quase 60% do financiamento externo, os EUA recebem 27% e a Europa apenas 11%. Especialistas alertam para os riscos económicos, com um valor em jogo estimado em até €4 bilhões por ano até 2040 se essa tendência se mantiver.

Ameaças Regulamentárias e Fragmentação do Mercado

O ambiente de inovação europeu tem sido pressionado por dilemas de regulamentação e fragmentação do mercado. Enquanto a rigidez das regras procura proteger direitos fundamentais e manter padrões éticos, ela pode limitar a capacidade de inovação em escala global. Grandes empresas veem com preocupação a retirada de projetos essenciais de regulamentação de patentes em tecnologias críticas, encarando o movimento como um retrocesso competitivo.

Desinformação e Manipulação da Informação

A desinformação e manipulação de informações figuram como ameaças sistémicas. Segundo a UNESCO, a desinformação é o maior risco global para 2025. A União Europeia aponta a Rússia como responsável por interferência em processos eleitorais via inteligência artificial, com uso de deepfakes e doppelgangers, recursos que tornam mais difícil distinguir realidade de manipulação, prejudicando ainda mais o ambiente geopolítico.

Escassez de Talentos em TIC

A escassez de talentos em TIC também se agrava: 57,5% das empresas da UE relatam dificuldades para recrutar todos os profissionais necessários. Em dez anos, o gap entre oferta e procura cresceu 20%. Os principais obstáculos incluem falta de candidaturas, qualificação insuficiente e altas expectativas salariais, impactos sentidos especialmente em países como Alemanha, Chéquia, Malta, Áustria e Luxemburgo.

Impactos na Infraestrutura Crítica

Os riscos climáticos lançam uma ameaça adicional às infraestruturas críticas europeias. Com a intensificação dos eventos extremos, o dano médio anual provocado por fenómenos climáticos já ultrapassa €15,9 mil milhões (2011-2020) e pode ser dez vezes maior até o fim do século. Essa vulnerabilidade é ampliada pela interdependência dos sistemas, aumentando os riscos de efeitos em cascata sobre toda a infraestrutura do continente.

O atual cenário tecnológico apresenta-se como um grande desafio para Portugal e suas empresas.

Tendências

Entendemos que as decisões de Planeamento de TI em Portugal até 2035 serão fortemente influenciadas pelo Tripé de Tendências apresentado no Inova Trend Map What's Next 2035: Megatendências, Tendências Comportamentais e Tendências de Negócio. Estas dimensões estruturam tanto o diagnóstico estratégico como a priorização das apostas que posicionarão as organizações portuguesas num mundo pós-taylorista, no qual a flexibilidade, a inovação e a adaptabilidade são condições sine qua non para perenidade e competitividade.

DEFINIÇÕES:

Megatendências são movimentos e mudanças (de larga escala) em termos sociais, económicos, políticos, ambientais e tecnológicos, que se manifestam de forma consistente na realidade atual e que influenciarão decisivamente o futuro. **Tendências comportamentais** são processos de mudança que resultam da observação do comportamento dos consumidores e que origina a criação e o desenvolvimento de novas ideias: de negócio, de produto ou serviço, de marca ou de ação. **Tendências de Negócio** são mudanças no mercado resultantes da atuação dos players, do comportamento dos consumidores e das realidades económicas, políticas e sociais que influenciam a forma como as empresas tomam decisões nos seus negócios, considerando áreas de atividade e apostas estratégicas para o futuro. A seguir apresentamos cada uma das tendências do Inova Trend Map What's Next 2035 mais relevantes para os negócios de tecnologia em Portugal.

Megatendências: O pano de fundo estrutural

Mundo 5.0 e Tech Disruption

A transição do paradigma “Tech4Business” para “Tech4People” exige que o planeamento de TI, além de procurar eficiência e automação, coloca o ser humano, a ética e a inclusão digital no centro do desenho de soluções. A disrupção tecnológica, IA, computação quântica, automação avançada, a necessidade de revisão contínua de arquitetura de sistemas, cibersegurança e políticas de dados, além de estratégias robustas para reskilling/upskilling dos colaboradores portugueses. A lógica será sempre antecipar-se às ondas de mudança, promovendo uma cultura data-driven, aberta e resiliente.

Sustentabilidade Integrada

Questões ambientais, regulamentárias e sociais, como ESG, Logística Reversa e Transição Energética, passam a condicionar escolhas de infraestrutura de TI (cloud verde, arquitetura modular, eficiência energética e gestão ambiental de dados). A pressão vinda de consumidores, fundos e regulações europeias reforça a necessidade de consolidação de métricas e sistemas de reporte inteligentes e auditáveis.

Demografia e Trabalho Intergeracional

O envelhecimento acelerado e a coexistência de pelo menos quatro gerações em ambientes laborais criam desafios de desenho inclusivo, usabilidade e customização de soluções. Lifelong learning e aprendizagem adaptativa serão o alicerce da capacitação tecnológica sustentada.

Tendências Comportamentais: Novas lógicas sociais e do trabalho

Pós-Taylorismo, Full Agile e Empowerment

A lógica linear, hierárquica e focada na cadeia de comando do passado cede lugar à governação horizontal, à experimentação contínua, à flexibilidade e ao protagonismo individual e coletivo. Modelos ágeis, squads interdisciplinares, ambientes colaborativos, adoção de métodos DevOps e gestão adaptativa são exemplos claros de resposta comportamental traduzida em novas procuras de TI.

Trabalho Híbrido, Nómadas Digitais e Conectividade Permanente

A digitalização das relações, mobilidade e o trabalho descentralizado impõem desafios e oportunidades ao planeamento de TI: infraestrutura escalável, soluções de colaboração seguras, gestão de identidades híbridas e suporte universalizado a múltiplos dispositivos e contextos culturais.

Segurança Psicológica, Diversidade e Inclusão

O bem-estar digital, a saúde mental, as políticas de diversidade, a inclusão (por idade, cultura, género) e a valorização das soft skills passam a pautar não apenas as práticas de gestão, mas também o desenho e a implementação de sistemas e plataformas digitais que respeitem a multiplicidade do tecido humano português.

Tendências de Negócio: Novos modelos e estratégias

Ambidestria Corporativa

Equilibrar a maximização dos ativos existentes (exploitation) com a inovação contínua (exploration) define a agenda do CIO moderno. É imperativo investir em integração de sistemas legac com novas tecnologias, fomentar laboratórios de inovação, adotar arquitetura orientada a microsserviços, cloud e edge computing, além de parcerias externas estratégicas (open innovation, ecossistemas digitais).

Negócios de Plataforma e Ecossistema

O modelo competitivo em rede exige plataformas abertas, interoperáveis, adaptáveis a múltiplos parceiros e que facilitem a expansão, customização e integração de novos serviços. O foco migrará de projetos verticalizados para a gestão de parcerias, APIs e dados compartilhados, atentos às oportunidades e riscos (segurança, compliance, propriedade intelectual).

Estratégia Prospetiva

O uso sistemático de foresight e análises de tendências, suportado por dados, será ferramenta obrigatória para garantir resiliência. Organizações precisarão de processos e ferramentas para mapear cenários futuros, identificar riscos emergentes (como ataques cibernéticos avançados), avaliar oportunidades de automação e de novos modelos de negócio digital.

Novos Modelos de Operação

A integração de novas práticas como nearshoring de TI, fabrico aditivo, economia circular e personalização em massa irá redefinir não apenas os fluxos operacionais, mas também as prioridades de investimento, governação e capacitação das equipas portuguesas.

Tendências Específicas

Após um abrangente trabalho de pesquisa, entrevistas e levantamento de informações, identificamos os principais conceitos das IT Future Trends 2035. Apresentamos, a seguir, recomendações direcionadas tanto aos decisores empresariais, de tecnologia ou de outros setores, quanto aos responsáveis pela formulação de políticas públicas. Abaixo, destacamos as tendências específicas identificadas.

Inteligência Artificial (IA)

Impacto e Automação: A IA é vista como uma revolução que automatizará tarefas rotineiras, libertando os profissionais de TI para funções mais estratégicas e criativas. A produtividade aumentará e as equipes de TI se tornar-se-ão mais focadas em "gestão de agentes" de IA.

Modelos de IA: Embora modelos maiores (bilhões de parâmetros) tenham sido predominantes, modelos menores e mais eficientes (SLMs), com dez mil milhões ou menos parâmetros, têm-se revelado igualmente eficazes, permitindo a integração de IA em diversos dispositivos.

Riscos e Governança: A IA é uma "faca de dois gumes" devido a riscos de desinformação, deepfakes, e viés algorítmico. A necessidade de validação humana e governança de dados é crítica.

Investimento em IA: A IA liderou as tendências tecnológicas em patentes, pesquisas no Google e publicações de investigação. No primeiro trimestre de 2025, empresas de IA levantaram US\$ 52 bilhões em financiamento global, incluindo um investimento de US\$ 40 bilhões na OpenAI liderado pela SoftBank.

Computação em Cloud e Edge Computing

Modelo Predominante: Há um forte consenso de que o futuro da infraestrutura de TI é híbrido e multi-cloud, oferecendo escalabilidade, flexibilidade, resiliência e otimização de custos.

Desafios: A justificação do Retorno sobre Investimento (ROI) para a cloud em organizações mais tradicionais e o "vendor lock-in" são desafios. A dependência de grandes provedores de soluções cloud e a soberania dos dados continuam a ser a preocupação.

Crescimento da Procura: A evolução da IA impulsionou a procura por data centers, com estimativas de crescimento anual de capacidade entre 19% e 22% de 2023 a 2030, o que triplicaria a procura atual.

Cloud Soberana na Europa: A Europa está a investir em soluções de cloud soberana, como o modelo de cloud distribuída da Hivenet, para garantir que os dados permaneçam dentro das fronteiras europeias, em conformidade com o GDPR. Empresas europeias como Cleura e gridscale estão a ganhar destaque ao priorizar a soberania e segurança dos dados.

Computação Quântica

Potencial Disruptivo: Reconhecida pelo seu potencial para resolver problemas complexos, especialmente em cibersegurança, criptografia, descoberta de medicamentos e modelagem financeira.

Estágio de Maturidade: Ainda está a 5-10 anos de maturidade plena para aplicações amplas. No entanto, houve avanços significativos em 2025, com grandes empresas como AWS, Google, IBM e Microsoft anunciando avanços em chips quânticos e capacidade de correção de erros.

Inovação e Programas Nacionais: O interesse e a inovação em tecnologias quânticas estão a crescer, impulsionados pela expansão de programas nacionais de investigação e o reconhecimento global (2025 declarado Ano Internacional da Ciência e Tecnologia Quânticas pela ONU).

5G/6G e Conectividade Avançada

Uso e Impacto: O 5G está a ser utilizado para garantir conectividade em locais mais remotos e otimizar operações. O 6G é visto como um complemento necessário para o salto tecnológico.

Procura por Fibra Ótica: A explosão de dados gerada pela IA aumenta a procura por infraestrutura de fibra, que é crucial para data centers e aplicações inteligentes.

Cobertura em Portugal: Portugal tem uma excelente cobertura de 5G (98.1% dos domicílios em 2023) e está a caminho de atingir 100% de cobertura em áreas mais povoadas.

Metaverso e Novas Realidades

Evolução: O metaverso está a passar por uma recalibração, com a visão evoluindo de um conceito focado em VR para uma integração mais subtil e prática na vida diária.

Hardware e IA: Há avanços contínuos no desenvolvimento de hardware (óculos inteligentes, headsets) e no uso de IA para criar avatares mais realistas e experiências imersivas.

Oportunidades: Reinvenção de modelos de negócios através da integração de ofertas físicas e digitais, gerando novas fontes de receita e experiências personalizadas.

Desafios: Ameaças de deepfakes e desinformação exigem medidas de segurança robustas e educação para manter a autenticidade.

Biotecnologia

AI e Biologia: A IA está a acelerar descobertas científicas em bioengenharia, impulsionando avanços na medicina e na produção de materiais.

Empresas "Biotech": Organizações de diversos setores estão a tornar-se "empresas de biotecnologia" ao adotar soluções biológicas (ex: materiais biomanufaturados, tratamento de resíduos).

Avanços: Progressos significativos em bioprinting 3D, órgãos cultivados em laboratório e terapias regenerativas. Investigadores estão a desenvolver "computadores vivos" que usam circuitos biológicos para processar dados.

Sustentabilidade (ESG) e TI

Preocupação Crescente: O consumo energético da TI, especialmente de data centers, é uma preocupação crescente.

Eficiência Energética: Grandes provedores da cloud estão a investir em eficiência energética e neutralidade de carbono. A IA, embora consuma muita energia, pode ajudar a otimizar a eficiência.

Fator Competitivo: A sustentabilidade tornou-se um fator decisivo na escolha de parceiros tecnológicos e é vista como um "negócio" em si.

RECOMENDAÇÕES

Fortalecimento do Capital Humano

Intensificar programas de capacitação digital e requalificação para todas as idades, com foco em habilidades avançadas em TIC, inteligência artificial e cibersegurança.

Atrair e reter talentos de TIC, abordando a questão dos salários e oferecendo projetos desafiadores e ambientes de trabalho híbridos que valorizem a interação social e a cultura empresarial.

Promover ativamente a participação feminina em STEM e TIC, com iniciativas desde a educação primária até a integração profissional, para atingir a meta de 30% de mulheres especialistas.

Aceleração da Adoção Tecnológica

Incentivar PME's a adotar soluções digitais avançadas, incluindo IA e serviços cloud, através de programas de sensibilização, mentoria e apoio financeiro, para atingir a meta de 90% de intensidade digital.

Fomentar um ecossistema de startups vibrante que priorize tecnologias de fronteira e contribua para o aumento do número de unicórnios.

Desenvolvimento de Infraestrutura Soberana e Resiliente

Reduzir a dependência de provedores de soluções cloud estrangeiros através do desenvolvimento de uma cloud soberana e do investimento em empresas europeias de cloud.

Fortalecer a cadeia de valor de semicondutores na Europa, apoiando a meta da Lei dos Chips da UE.

Garantir a resiliência da infraestrutura crítica contra ciberataques e riscos climáticos, com planos proativos de cibersegurança e investimento contínuo.

Otimização do Enquadramento Regulatório

Equilibrar a proteção de dados e a ética com a agilidade necessária para a inovação, criando "sandboxes regulamentárias" para testar novas tecnologias.

Assegurar a conformidade com as regulamentações europeias (GDPR, NIS2, DORA, AI Act), garantindo a segurança jurídica e confiança no ambiente digital.

Promoção da Colaboração e Inovação Aberta

Fortalecer as parcerias público-privadas e académicas para o desenvolvimento de soluções digitais inovadoras e a transferência de conhecimento.

Apoiar a investigação e o desenvolvimento em tecnologias emergentes como IA avançada, computação quântica e conectividade 6G, aproveitando o capital intelectual de Portugal.

Combate à Desinformação e Incentivo da Literacia Digital

Desenvolver e implementar ferramentas e estratégias para validar informações e gerir os riscos associados à IA, como deepfakes e enviesamentos algorítmicos.

Promover a literacia mediática e digital para que os cidadãos possam discernir informações falsas e entender como os algoritmos funcionam.

Integração da Sustentabilidade (ESG)

Integrar as metas de ESG nas estratégias de TI das empresas, com foco na eficiência energética de data centers e na gestão de resíduos, tornando a sustentabilidade um fator decisivo na escolha de parceiros tecnológicos.

06

Conclusões Finais Referências

Conclusões Finais

Este estudo mostrou que pensar 2035 é, na prática, decidir 2025–2030 com método. A combinação das cinco fases, mesa-redonda, desk research, entrevistas em profundidade, inquérito quantitativo e mapeamento de tendências e cenários, permitiu cruzar visão estratégica, dados e práticas do terreno. O retrato que emerge é coerente: Portugal parte de bases sólidas de conectividade e governo digital, mas precisa transformar capacidade instalada em produtividade, exportações tecnológicas e confiança, sobretudo entre as PMEs, que compõem a espinha dorsal da economia.

Os resultados convergem em quatro eixos: (1) infraestrutura robusta, porém com assimetrias de uso; (2) adoção ainda tímida de cloud e IA nas empresas, contrastando com casos de excelência; (3) cibersegurança a subir de tema técnico para pilar de continuidade do negócio, com Zero Trust, SOC 24/7 e IAM no centro; e (4) regulamentação europeia (RGPD, NIS2, DORA e enquadramento de IA) como “caminhos” que profissionalizam o ecossistema quando incorporados by design. Em tecnologia de base, o padrão mais adaptativo é o híbrido, muitas vezes multicloud, com desenho de saída planeado para evitar lock-in e cláusulas de residência de dados que conciliem soberania e resiliência.

No plano competitivo, o mercado reconfigura-se entre operadores de telecom, integres, hyperscalers e um pipeline de startups que precisa de escala. O país é atrativo como hub e ponto de passagem, mas ainda capta pouco valor sem especialização clara. Edge computing traz ganhos imediatos em latência e autonomia; IA difunde-se como “copiloto” operacional; 6G permanece no horizonte; e a computação quântica exige desde já cripto-agilidade. A agenda ESG avança, pressionada por clientes e setor público, mas de forma desigual: eficiência energética, FinOps/CarbonOps e critérios “verdes” nos data centers tendem a tornar-se mandatórios até 2035.

Nada disso se sustenta sem gente. A competição global por talento é dura, a preferência por trabalho híbrido consolidou-se e a proposta de valor ao colaborador precisa ir além do salário: aprendizagem contínua, projetos tecnicamente relevantes (IA/automação), autonomia e rituais de cultura que preservem coesão. As equipas de TI estão se a transformar de executoras para integradores de agentes e plataformas, enquanto governance de dados, observabilidade e segurança por design entram no “core” das funções.

Assim, a mensagem final é simples e operativa: o caminho para 2035 passa por escalar competências, adotar IA com “cinto de segurança”, tratar cibersegurança como tema de negócio, governar dados e interoperabilidade, escolher arquiteturas híbridas com design-for-exit, integrar critérios ESG no ciclo de decisão tecnológica, internacionalizar desde o dia um e explorar a vantagem atlântica do país em conectividade e energia limpa. Do lado das empresas e das políticas públicas, a prioridade é transformar ilhas de excelência em padrão mínimo de maturidade. Se 2035 parece longe, começa agora, com decisões sequenciais, mensuráveis e ancoradas em confiança.



Sobre a Compuworks

A Compuworks é uma empresa portuguesa especializada em soluções integradas de tecnologias de informação para organizações de todas as dimensões.

Com **escritórios em Lisboa, Porto e Leiria**, assegura uma cobertura nacional próxima, eficiente e estratégica.

Ao longo de mais de duas décadas de atividade, a Compuworks tem sido um parceiro essencial na operação e segurança tecnológica de centenas de empresas, com serviços como:

- Consultoria e Auditoria Informática
- Outsourcing de Departamento de IT
- Segurança Informática Empresarial
- Assistência Técnica e Suporte 24/7
- Projetos de Infraestrutura
- Managed Services (MSP)

Com um modelo de parceria flexível, que pode complementar ou substituir o departamento de IT interno, a Compuworks garante soluções robustas, adaptadas a cada negócio, sempre com foco na rentabilidade, produtividade e segurança.

Atualmente, a empresa acompanha mais de **23.000 utilizadores**, protege **mais de 5.000 equipamentos móveis**, e assegura **mais de 51.000 horas de assistência técnica por ano**. Este know-how e capacidade de adaptação fazem da Compuworks uma referência no mercado nacional de IT, com uma taxa de crescimento média sustentada de 20%.

Assente no lema **“We work, IT works”**, a Compuworks aposta na excelência técnica, proximidade com o cliente e inovação contínua, trabalhando todos os dias para garantir que a tecnologia é uma mais-valia real no crescimento e resiliência das organizações.

Agradecimentos

A realização deste estudo foi possível graças à colaboração de dezenas de profissionais que partilharam o seu tempo, conhecimento e visão sobre os desafios e caminhos do setor tecnológico em Portugal.

Agradecemos, em particular, ao Rui Ribeiro, pela formulação e seleção das questões estruturantes deste estudo; ao Sérgio Bruno A. Carvalho, pela análise crítica e melhoria contínua do processo de entrevistas; e à Sofia Teixeira, pela revisão cuidada dos conteúdos. Uma palavra especial de reconhecimento ao Luís Rasquilha, pela forma como abraçou este projeto desde o primeiro momento, tornando possível a criação de um estudo verdadeiramente centrado na realidade portuguesa, bem como à Eliane El Badouy (Badu) e ao Renato Jannuzzi Cecchetti pela dedicação, profissionalismo e incansável entrega em todas as fases deste trabalho.

O nosso reconhecimento estende-se a todos os líderes e especialistas que aceitaram o convite para serem entrevistados, às equipas que contribuíram com análises e sugestões valiosas ao longo do projeto, e a todos os parceiros que, direta ou indiretamente, tornaram possível esta reflexão conjunta sobre o futuro das tecnologias em Portugal.

Este estudo é, acima de tudo, um trabalho coletivo, e a cada uma destas contribuições se deve a sua relevância.

ECOSSISTEMA INOVA

Somos um ecossistema global de inteligência estratégica com matriz no Brasil, raízes na Europa e presença nos 5 Continentes. Criamos e desenvolvemos o conceito original de Gestão TrendsInnovation — uma abordagem única que conecta visão de futuro, cenários prospectivos, tendências globais, estratégia e inovação orientada à longevidade de empresas e negócios.

Ajudamos empresas, líderes e instituições a navegar em tempos de transição, antecipar mudanças e transformar incertezas em vantagem competitiva sustentável. Atuamos em múltiplas frentes, integrando pesquisa e mapeamento de tendências, formação de líderes, consultoria estratégica e metodologias próprias que já impactaram uma variedade de organizações.

TRENDSINNOVATION: NOSSO DNA E ESPINHA DORSAL

A essência da nossa atuação está em mapear e identificar as transformações do futuro por meio de prospectiva estratégica e do foresight, interpretando movimentos emergentes e tendências globais. Esse conhecimento é aplicado diretamente à gestão da inovação e ao planejamento estratégico, apoiando líderes na construção de empresas ambidestras, ágeis e preparadas para navegar em cenários complexos.

COMPOSIÇÃO DO ECOSSISTEMA INOVA

GTR – GLOBAL TRENDS RESEARCH

Drivers de Mudança | Estudos Prospectivos | Mapping de Cenários | Estudos de Tendências | Foresight de Negócio | Best Practices | Benchmarks | Trend Tracking | Coolhunting

CONSULTING

Gestão da Inovação | TrendsLator | Cultura de Inovação | Inovação Disruptiva | Inovação Aberta

STRATEGY

Planejamento Estratégico Prospectivo (SBB) | Business Strategy | Strategy Audit | Transformação Digital | Full Agile | Business Pulse | Ambidestria Corporativa | Lid360

N.O.M.A.

Advisor por Projeto | Advisor por Stakeholder (do Board, do C-Level, dos Acionistas) | PCA (Programa de Certificação de Advisors)

BUSINESS SCHOOL

Programas Executivos: MBA TrendsInnovation | Pós-MBA TrendsInnovation | Governança TrendsInnovation em Empresas Familiares | Programa de Ambidestria Corporativa Certificações: Programa de Certificação de Conselheiros (Board Members) | Programa de Certificação de Advisors (PCA) | HIO (Certificação Hole in One) Outros: Masters & Nanodegrees | Programas in Company | Palestras & Seminários | Mentoring

INOVA ONLINE

Cursos Assíncronos | Cursos Híbridos | Plataforma Aberta

PUBLISHING

Livros POD (Print On Demand)

EDUCADORES INOVADORES

Congressos | Eventos | Conteúdos | Estudos | Networking | Missões

INSTITUTO INOVA

Benefícios Fiscais em Impacto Real | Projetos de Impacto Social | Conceção | Integração | Implementação | Suporte | Relatórios | Análises e Dados

CT - CONSELHEIROS TRENDSINNOVATION

Network | Lifelong Learning

Acreditamos que entender o futuro é uma competência estratégica — e que a inovação só é verdadeiramente transformadora quando está conectada às tendências e à inteligência coletiva. Por isso, conectamos pesquisa, estratégia, educação e prática em um só movimento, apoiando organizações na criação de caminhos inovadores e sustentáveis.

www.ecossistemainova.com



AUTORES



Eliane El Badouy (Badu)



**Senior Consultant Ecosystema Inova
Future, Trends & Behavior**



Luis Rasquilha



**CEO
Ecosystema Inova**



Renato Jannuzzi Cecchetti



**Senior Consultant Ecosystema Inova
Scenario Planning**

Referências

- Comissão europeia. (2024). *Digital Decade 2025 – Country Report: Portugal*.
- Governo de Portugal. (2024). *Roteiro nacional para a transição digital 2024/2025*.
- McKinsey & Company. (2023). *Time to place our bets: Europe's AI opportunity*.
- Governo de Portugal. (2020). *Estratégia Nacional de Inteligência Artificial*.
- Governo de Portugal. (2020). *Plano de Ação para a Transição Digital*.
- Governo de Portugal. (2017). *Programa INCoDe.2030 – Iniciativa Nacional de Competências Digitais e.2030*.
- União Europeia. (2022). *NIS2 Directive – Directive on measures for a high common level of cybersecurity across the Union*.
- União Europeia. (2022). *DORA – Digital Operational Resilience Act*.
- União Europeia. (2016). *Regulamento Geral sobre a Proteção de Dados (RGPD) – Regulation (EU) 2016/679*.
- Centro Nacional de Cibersegurança (CNCS). (2024). *Iniciativas de Cibersegurança financiadas pelo PRR: C-Academy, C-Hub, C-Network, Cybersecurity Alliance e Observatório Nacional de Cibersegurança*.
- Comissão Europeia. (2024). *Atlantic CAM – Submarine cable system and SMART sensing*.
- FinOps Foundation. (2023). *FinOps: Cloud Financial Management for Practitioners*.
- GreenOps. (2023). *GreenOps Practices for Sustainable IT Operations*.
- Ecossistema Inova – What's Next – Direção 2035

Números que definem o futuro

IT Future Trends 2035

Geopolítica & Inovação

- 92% da infraestrutura de cloud da Europa é controlada por empresas dos EUA.
- 80% dos semicondutores usados na Europa vêm de fora da União Europeia.
- As 5 maiores empresas americanas investem mais em P&D do que os 27 países da UE juntos.

Cibersegurança

- 3,12% das empresas portuguesas reportaram indisponibilidade por ataques em 2024 (UE: 3,43%).
- 95,6% das empresas já adotaram alguma medida de segurança digital.
- 50% das organizações nunca implementaram XDR ou Zero Trust.
- Apenas 27% já implementaram ambas as soluções.
- 83,15% defendem investir em IA para reforçar a cibersegurança.

Cloud & IA

- Adoção de IA em Portugal: apenas 8,6% das empresas (2024).
- Utilização de cloud: 32,3% das empresas (2023).
- 68,87% preferem modelo híbrido (cloud + on-premises).
- 71,7% veem o multi-cloud como estratégico para resiliência.
- Mais de 70% das empresas já estão a adotar ou planear adotar IA.

Talento & Competências

- Especialistas em TIC: 5,2% do emprego em Portugal.
- Mulheres especialistas em TIC: 22,7%.
- 56% da população portuguesa tinha competências digitais básicas em 2023.
- 57,5% das empresas da UE reportam dificuldades em recrutar todos os profissionais de TIC necessários.

Infraestruturas & Sustentabilidade

- 47,19% apontam a ciber-resiliência como maior desafio.
- 43,82% acreditam que a cloud híbrida com edge computing será o modelo dominante em 2035.
- 29,89% esperam que data centers carbono neutro sejam o padrão até 2035.
- 85% concordam que a procura por data centers impõe desafios de neutralidade carbónica.
- O dano médio anual provocado por fenómenos climáticos já ultrapassa €15,9 mil milhões.


Economia & Startups

- Portugal dedica 21% do PRR ao digital (€4,5 mil milhões).
- Portugal dedica 11% dos fundos de coesão ao digital (€2,4 mil milhões).
- Taxa de sucesso de Portugal no EIC Accelerator: 9,68% (média europeia: 7,16%).
- Portugal projeta aumentar de 4.700 startups (2024) para 6.000 até 2030.
- A Fábrica de Unicórnios de Lisboa aumentou 5 vezes a sua capacidade em dois anos.

Obrigado!

Obrigado por dedicar o seu tempo a ler este relatório.

Se tiver alguma dúvida ou quiser discutir as nossas conclusões mais detalhadamente, não hesite em entrar em contacto connosco.

 Av. Dom João II n.º 17 2.º Piso,
Escritório 1, 1990-078 Lisboa

 +351 213 138 603

 comercial@compuworks.pt

 <https://compuworks.pt>