Universidade de Évora - Escola de Ciências e Tecnologia

Mestrado em Engenharia Informática

Dissertação

A cibersegurança no contexto das pequenas e médias empresas portuguesas: um estudo sobre a consciencialização e investimento na mitigação do cibercrime

Sergio Valente

Orientador(es) | Pedro Patinho

Évora 2022

Esta dissertação não inclui as críticas e as sugestões feitas pelo júri.

Universidade de Évora - Escola de Ciências e Tecnologia

Mestrado em Engenharia Informática

Dissertação

A cibersegurança no contexto das pequenas e médias empresas portuguesas: um estudo sobre a consciencialização e investimento na mitigação do cibercrime

Sergio Valente

Orientador(es) | Pedro Patinho

Évora 2022

Esta dissertação não inclui as críticas e as sugestões feitas pelo júri.

Obrigado à Paula, ao Santiago, ao Rodrigo e
ao Lourenço, por estarem sempre presentes.
Especialmente quando seria mais fácil
deixarem-me sozinho.

Vosso, sempre!

Um agradecimento especial ao professor
Pedro Patinho, por todo o apoio e
ensinamentos.

A Cibersegurança no contexto das pequenas e médias empresas portuguesas: um estudo sobre a consciencialização e investimento na mitigação do cibercrime.

- Resumo -

O tecido empresarial português é constituído maioritariamente por Pequenas e Médias Empresas, cuja prioridade nos investimentos visa o que é essencial à sua actividade. A crescente digitalização dos negócios torna fundamental perceber o seu grau de consciencialização para a Cibersegurança e capacidade de mitigação do cibercrime. Na ausência de estudos neste âmbito – e neste segmento empresarial e geográfico específicos – este trabalho de investigação pretende preencher esta lacuna. As respostas obtidas no questionário construído demonstram que existe um caminho de consciencialização e literacia a fazer junto dos profissionais destas empresas. Permitem também validar que tipo de tecnologias poderão significar um ganho na sua exposição ao cibercrime e qual a propensão para investimentos nesta área. Com base na análise dos resultados foram implementadas soluções técnicas e pedagógicas, numa empresa real, com o propósito de suprimir as fragilidades identificadas e aumentar o seu grau de resiliência no âmbito da Cibersegurança.

PALAVRAS-CHAVE: cibercrime; Cibersegurança; pequenas e médias empresas; realidade portuguesa.

Cybersecurity in the context of small and medium-sized portuguese companies: a study on awareness and investment in cybercrime mitigation.

- Abstract -

The portuguese business fabric is made up mainly of Small and Medium-sized Companies, whose investment priority is oriented towards the essential maintenance of its activity. The growing digitization of business makes it essential to understand its degree of Cybersecurity awareness, and its cybercrime mitigation capacity. Due to the absence of studies in this scope – in this specific business and geographic segment – this research intends to fill this gap. The answers obtained in a questionnaire, show that there is a path of awareness and literacy to be done with this companies' professionals. It also shows what type of technologies could mean a gain in its exposure to cybercrime, and what is the propensity for investments. Based on the results analysis, technical and pedagogical solutions were implemented in a real company, with the purpose of suppressing the identified weaknesses and increasing its degree of resilience in the context of Cybersecurity.

KEYWORDS: cybercrime; cybersecurity; small and medium-sized companies; portuguese reality.

- Índice -

- Índice de Figuras -

- Lista de Abreviaturas -

AD – *Active Diretory*

AP – *Access Point*

ATO – *Account TakeOver*

ATP – *Advanced Threat Protection*

DDoS – *Distributed Denial of Service*

DHCP – *Dynamic Host Configuration Protocol*

DMZ – Demilitarized Zone

IEEE – *Institute of Electrical and Electronics Engineers*

IoT – *Internet of Things*

IP – *Internet Protocol*

IT – *Information Technologies*

LAN – *Local Area Network*

MFA – *Multi-Factor Authentication*

NPS – *Network Policy Server*

PME – Pequenas e Médias Empresas

RADIUS – *Remote Authentication Dial-In User Service*

RH – Recursos Humanos

SD-WAN – *Software-defined Wide Area Network*

SME – *Small and Medium-sized Enterprises*

TI – Tecnologias da Informação

USB – *Universal Serial Bus*

VLAN – *Virtual Local Area Network*

VoIP – *Voice over Internet Protocol*

VPN – *Virtual Private Network*

1. Introdução

Segundo o guia de boas-práticas apresentado pela Gartner (Scholtz, 2021), os responsáveis pela Cibersegurança nas organizações enfrentam novos desafios - e isto aplica-se não só a profissionais das Tecnologias da Informação, mas também a qualquer agente de tomada de decisão dentro das organizações. A exigência de investimento na transformação digital veio para ficar. Conceitos como "Relatórios de violação de dados e ciberataques" ou "Adopção de metodologias e desenvolvimento ágil" passaram a fazer parte do vocabulário das organizações mais preparadas. Sejam elas de que dimensão forem.

A crescente digitalização dos negócios torna fundamental perceber o seu grau de consciencialização para a Cibersegurança e capacidade de mitigação do cibercrime. Para aferi-lo, foi criado um questionário e disponibilizado online para que um conjunto alargado de profissionais pudesse facilmente aceder-lhe e responder. A análise dos dados recolhidos neste questionário permitiu perceber, de forma fundamentada, de que maneira é possível ajudar as PME portuguesas a aumentar o seu grau de consciencialização e mitigação do cibercrime, tornando também possível implementar um plano de acção composto por medidas técnicas efectivas, capazes de eliminar as fragilidades identificadas.

1.1. Motivação

Da análise da pesquisa de literatura efectuada, há um indicador relevante que se destaca: a falta de estudos e dados sobre a temática da Cibersegurança e cibercrime no contexto das pequenas e médias empresas portuguesas. Não existe, de facto, bibliografia relevante com este enquadramento, o que, dada a relevância que tem no tecido empresarial português, implica um impacto directo ou indirecto numa percentagem muito significativa da população. Segundo a PORDATA (2022) trabalham em PME, em Portugal, 3.293.582 pessoas.

São necessários novos recursos e funções de segurança. A digitalização está a gerar a necessidade de um conjunto mais amplo de funções que envolvem novas habilitações e conhecimentos. Isto será necessariamente menos evidente nas Micro empresas do que nas Médias empresas, mas é fundamental que exista a consciência de que este é um contexto em evolução constante e que definir uma estratégia de segurança e comunicá-la perfeitamente a toda a organização é vital para a continuidade do negócio.

É difícil contratar bons profissionais nesta área e quanto mais tempo as organizações estiverem desprovidas de profissionais competentes, capazes de tomar as melhores decisões e implementar as melhores soluções, mais expostas estarão.

Estes dados demonstram e comprovam a importância de aprofundar a pesquisa, no sentido de validar qual o verdadeiro impacto que as fragilidades existentes hoje em dia nas organizações podem ter na sua viabilidade. Para isso, será necessário compreender se este fenómeno tem a capacidade de criar eco nas empresas, qual o verdadeiro nível de consciencialização para o risco da sua exposição ao cibercrime e à capacidade que estas práticas cada vez mais têm de destruir um negócio.

É fundamental também, perceber se os estudos existentes, que indicam claramente que existe um padrão de investimentos-alvo a fazer, seja em infraestruturas, soluções tecnológicas ou formação e consciencialização dos quadros das empresas, são capazes de representar uma aplicabilidade prática, dada a realidade das PME portuguesas. Seja pelos custos económico-financeiros que implicam, seja pelo grau de especialização tecnológica envolvida, ou pela capacidade que têm de demonstrar que estamos perante perigos reais, com consequências potencialmente devastadoras.

Em suma, de forma a concentrar o estudo e restringir o foco da nossa pesquisa ao contexto das pequenas e médias empresas portuguesas, importa aprofundá-lo de forma focada neste grupo específico. É esta a principal nota final a retirar, a de que faz falta um estudo vocacionado especificamente para a realidade das PME portuguesas, capaz de traduzir o seu grau de consciencialização para a Cibersegurança e avaliar a sua capacidade de investimento na mitigação do cibercrime.

2. Revisão Bibliográfica

Com o aumento exponencial da atividade humana assente na utilização de plataformas digitais – e essencialmente online – o fenómeno do cibercrime tem, nos últimos anos, tomado proporções astronómicas. Transformando-se mesmo, em Portugal, na única tipologia de crime com crescimento de incidência desde 2019 (Sistema de Segurança Interna, 2020).

O cibercrime pode ser definido como a actividade criminosa realizada pelo uso da Internet e tecnologias computacionais. Podemos dividi-lo em actividades sociais e actividades cibernéticas, que geralmente têm um alvo específico. No entanto, vamos centrar-nos no tipo de crimes que impactam as organizações. Este tipo de crime organizado dedica-se a explorar as novas tecnologias para colher lucros e expandir o seu alcance criminoso, o que começa a atrair um interesse crescente por parte de agentes e recursos, no sentido de consciencializar e mitigar este fenómeno (Caravelli & Jones, 2019).

De acordo com os dados da PORDATA (2022) (Figura 2.1), a percentagem de Pequenas e Médias Empresas (PME) representava um universo de 99,9% do tecido empresarial português, o que torna relevante traçar um perfil da atividade relacionada com a Cibersegurança no contexto destas empresas, nomeadamente qual o grau de consciencialização dos seus agentes decisores para este fenómeno, e quais as medidas e investimentos efectuados no processo de mitigação do cibercrime.

Tratando-se de um tema absolutamente global e crescentemente transversal a todos os sectores sociais e de actividade, a literatura existente é predominantemente focada nos conceitos de Cibersegurança e cibercrime no seu sentido mais lato. Nas últimas décadas, surgiu um grande número de trabalhos de pesquisa sobre Cibersegurança e ferramentas e tecnologias inerentes. As revisões de literatura, no entanto, são principalmente direcionadas para subdisciplinas dentro da defesa passiva e/ou activa (Goethals & Hunt, 2019).

Segundo Bunker (2020), as principais violações de dados geralmente alertam para a falta de propriedade e responsabilidade pelas informações dentro de uma organização. A Cibersegurança é uma responsabilidade partilhada, comum e transversal a todos os *stakeholders* de uma organização. As empresas, de todas as formas e dimensões, devem aceitar a responsabilidade pela Cibersegurança dos seus negócios e daqueles que fazem parte da sua cadeia de fornecimento de sistemas de informação. Os incidentes/falhas de segurança ocorrem em maior proporção, devido a erros humanos, mas com uma estratégia de segurança abrangente implementada, esses incidentes são largamente reduzidos. Investir em tecnologia é, portanto, uma etapa crucial em qualquer estratégia de segurança, mas a educação e os processos apropriados são igualmente importantes. O objectivo deve ser criar uma cultura

empresarial em que todos os funcionários estejam sintonizados quando se trata das melhores práticas de protecção de informações, bem como de políticas e procedimentos apropriados.

Adoptar uma abordagem cautelosa, responsável e de longo prazo para a Cibersegurança, combinada com uma apreciação pelo investimento em tecnologia e ênfase na educação e consciencialização de toda a organização, é a maneira mais sustentável de acompanhar a evolução e sofisticação do cibercrime de hoje, de forma a estar constantemente apto a mitigá-lo.

Miaoui e Boudriga (2018) propõem a existência de um modelo económico de investimento em Cibersegurança, que distribui o valor gasto em segurança e autodefesa em seguros para cobrir a perda e o custo da recuperação dos danos e na prontidão forense para maximizar o potencial de recolha de evidências que se possa reflectir numa alta taxa de reembolso do seguro. Este modelo analítico proposto usa a teoria da utilidade esperada para calcular a quantidade ideal de investimento em ferramentas de mitigação do cibercrime.

Para calcular a quantia necessária de investimento, são propostas três estratégicas distintas, relativas ao risco: optimista, pessimista e realista. Isto permite inferir que existem modelos considerados óptimos, no que respeita à quantificação do investimento, de acordo com o perfil de cada decisor/empresa. Concretamente de acordo com indicadores como o grau de exposição, o lucro previsto ou o reembolso esperado no caso da activação de um seguro.

Na sua tese de doutoramento, Santos (2018) apresenta a percepção existente em Portugal dos conceitos de Cibersegurança e cibercrime. No entanto, o cruzamento feito destes resultados é feito com a formulação de políticas públicas e não com as medidas efectivas tomadas (ou não), pelas organizações, no sentido de mitigar o seu efeito. Ainda assim, é possível verificar qual a percepção do risco existente. Um dos comportamentos dos indivíduos mais referidos é o "*online service-avoidance*", que consiste na evitação deliberada da utilização de tecnologias. Esta poderá ser, em última análise, uma consequência efectiva da ocorrência do cibercrime, ou seja, a consciencialização para a Cibersegurança estará directamente relacionada com indicadores de infoexclusão. Neste caso, de indivíduos, mas potencialmente também das organizações. Isto poderá estar na origem da falta de digitalização das empresas portuguesas, pois, se relembrarmos que 99,9% das empresas em Portugal são PME (sendo 96% Micro empresas), é facilmente compreensível que a predisposição para o investimento nesta área seja teoricamente diminuta.

Proporção - %

Anos	PME			
	Total	Micro	Pequenas	Médias
2004	99,9	95,4	3,9	0,6
2005	99,9	95,5	3,8	0,6
2006	99,9	95,5	3,9	0,6
2007	99,9	95,6	3,8	0,5
2008	⊥99,9	⊥95,7	⊥3,7	⊥0,5
2009	99,9	95,8	3,6	0,5
2010	99,9	95,7	3,7	0,5
2011	99,9	95,8	3,6	0,5
2012	99,9	96,0	3,4	0,5
2013	99,9	96,2	3,2	0,5
2014	99,9	96,3	3,1	0,5
2015	99,9	96,2	3,2	0,5
2016	99,9	96,2	3,2	0,5
2017	99,9	96,2	3,2	0,5
2018	99,9	96,1	3,3	0,5
2019	99,9	96,0	3,3	0,5
2020	99,9	96,0	3,3	0,5

Fontes/Entidades: INE, PORDATA
Última actualização: 2022-03-30

FIGURA 2.1 - DISTRIBUIÇÃO DE PME POR DIMENSÃO

No decurso da pesquisa bibliográfica inicial, foi possível encontrar vários estudos internacionais com foco na relevância da literacia, no âmbito da Cibersegurança, na consciencialização para esta problemática e em modelos de avaliação que permitem avaliar o grau de exposição das PME ao cibercrime. No entanto, salienta-se mais uma vez a ausência de estudos especificamente elaborados no contexto do tecido empresarial português. Dos estudos encontrados, salientam-se a titulo exemplificativo três estudos, um para o mercado dos Estados Unidos da América, *The Adoption of Cybersecurity in Small - to Medium-Sized Businesses: A correlation Study* (Manns, 2021), outro para os mercados da Tailândia, do Equador e da Itália, *A cybersecurity assessment model for small and medium-sized*

enterprises (Emer et al., 2021) e um para o mercado específico da cidade de Londres, no Reino Unido, *Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs)* (Bada & Nurse, 2019).

Estes estudos diferenciam-se entre si, essencialmente, na abordagem à temática da Cibersegurança com focos distintos. Assim, o primeiro procura estabelecer uma relação entre as percepções existentes da vulnerabilidade e severidade potencial com a intenção comportamental e efectiva adopção de medidas para as mitigar, tudo isto numa perspectiva e análise mais matemática do que propriamente técnica ou vocacionada para a implementação de soluções específicas de engenharia. O segundo tem um objectivo mais direccionado para a criação de uma matriz de qualificação e hierarquização do risco, procurando elencar e ordenar um conjunto de acções e tecnologias que maior influência e importância têm no papel de defender as empresas das ameaças decorrentes do cibercrime, procurando inclusivamente criar uma ferramenta que torne o processo de avaliação mais simples e imediato. E o terceiro foca-se especificamente na questão pedagógica, no sentido de tentar contribuir para o aumento da literacia nesta matéria, recorrendo a eventos como seminários ou *workshops*, tratando-se no entanto de um estudo baseado nos resultados obtidos de um questionário que foi apresentado a um número reduzido de empresas e num âmbito geográfico que poderá ser considerado algo redutor.

Dada a natureza relativamente distinta destes três estudos, importa salientar que todos acabam por corroborar premissas em comum, que são os alvos essenciais do presente estudo. Nomeadamente, o consenso de que as preocupações com Cibersegurança devem ser entendidas como um fenómeno transversal e universal. O facto de as empresas necessitarem de estar preparadas e delinear um plano de acção e implementar medidas constantes, preferencialmente que incluam modelos de avaliação que lhes permita validar onde estão a cada momento, no que refere ao grau de exposição próprio, e o investimento essencial na literacia específica para estas matérias, dos seus colaboradores.

3. Materiais e Métodos

Com a intenção de avaliar o nível de consciencialização das pequenas e médias empresas para a problemática da Cibersegurança, foi criado um questionário, com recurso à plataforma *Google Forms*, e disponibilizado online para que um conjunto alargado de profissionais pudesse facilmente aceder-lhe e responder. Este questionário encontra-se dividido em 5 secções: Identificação da Empresa; Consciencialização para os perigos; Protecção e resiliência; Tecnologias implementadas; e Investimento em Cibersegurança. Perfazendo um total de 39 perguntas.

Este questionário obteve um total de 322 respostas, tendo sido consideradas respostas oriundas apenas do território nacional, segmentadas por região. A saber: Norte, Centro, Sul e Ilhas. Na fase de recolha de dados não foram excluídas respostas de pessoas com ligação a micro empresas, assim como de grandes empresas. Considerando que as micro empresas são genericamente englobadas no contexto das PME, os dados respeitantes a estas serão tratados em conjunto com os restantes. No entanto, na análise dos dados resultantes do questionário não serão considerados os referentes às grandes empresas, pois encontram-se fora do âmbito deste estudo. Ainda assim, foi considerado relevante efectuar a recolha de dados relativos a grandes empresas de forma a permitir um cruzamento comparativo, que permita aferir a existência de alguma diferenciação deste tipo de empresas no posicionamento relativo à Cibersegurança e ao cibercrime. Ou seja, perceber concretamente se, por exemplo, existem diferenças na percepção da exposição ao risco, no investimento, ou no conhecimento técnico. Isto significa que nas 322 respostas, existem 35 cujo enquadramento é no âmbito das grandes empresas, com número de funcionários superior a 249, pelo que a amostra considerada na análise, referente a PME, é de 287 respostas.

Com a análise dos dados recolhidos neste questionário, pretende-se perceber, de forma fundamentada, de que maneira é possível ajudar as PME portuguesas a aumentar o seu grau de consciencialização e mitigação do cibercrime. Ou seja, de acordo com as ilações retiradas, poderá mais facilmente apresentar-se um plano de acção efectivo, que corresponda a um maior grau de protecção destas empresas face à exposição a ameaças do foro da Cibersegurança. Pretende-se concretamente propor um plano de acção que compreenda a implementação de medidas técnicas efectivas, capazes de satisfazer as fragilidades identificadas. Algo que será designado, no âmbito deste projecto de investigação, como "A Cibersegurança em contexto prático". Nessa secção será apresentada a implementação das várias soluções técnicas que permitem aumentar o nível de mitigação identificado como necessário, assim como proposta também uma metodologia

de teor pedagógico, com o intuito de melhorar o grau de consciencialização para a Cibersegurança, adaptado às fragilidades identificadas através da análise dos dados do questionário.

As características técnicas da infraestrutura que serviu de base às implementações técnicas referidas, encontram-se fundamentadas pelo resultado da análise de dados que se segue e será apresentada, em maior detalhe, na secção correspondente (ver 5.1. A Cibersegurança em contexto prático). Aqui, o fundamental a referir é que, a fim de manter a máxima coerência com o âmbito da investigação, estas implementações decorreram no contexto de uma PME, em cenário real de produção.

4. Resultados

4.1. Resultados Gerais

Após a conclusão da fase de recolha de dados, os resultados finais apurados, ainda sem qualquer tratamento, reflectem, de imediato, a realidade do panorama nacional empresarial português. Desde logo, a distribuição estatística das respostas por sector de actividade e por número de funcionários encontra-se em alinhamento com as estatísticas oficiais (PORDATA, 2022), onde se reflecte a prevalência de empresas do sector terciário e a esmagadora maioria de PME, no tecido empresarial nacional. Estes dados, obtidos através do questionário, cuja composição integral se segue, podem ser consultados no Anexo II.

Conforme indicado anteriormente, o questionário utilizado é constituído por cinco secções, cada uma com um conjunto de questões.

Secção 1: Identificação da Empresa.

Composta por 4 questões, que têm por objectivo enquadrar a tipologia da empresa e segmentar as respostas por funções do colaborador. Tornando possível, por exemplo, comparar respostas entre empresas de maior e menor dimensão, ou de colaboradores com responsabilidades ao nível do processo de tomada de decisão.

Questão 1.1: Sector de atividade da empresa. (Figura 8.13)

Questão 1.2: Área geográfica da empresa. (Figura 8.14)

Questão 1.3: Número de funcionários da empresa. (Figura 8.15)

Questão 1.4: Relação profissional com a empresa. (Figura 8.16)

Secção 2: Consciencialização para os perigos.

Composta por 12 questões, cujo intuito é avaliar o grau de literacia dos colaboradores em matéria de Cibersegurança, nomeadamente que tipologias de ataques lhes é familiar e qual a maior vulnerabilidade da empresa neste contexto.

Questão 2.1: Já foi alvo, ou tem conhecimento de alguma empresa que tenha sido alvo, de um ataque informático? (Figura 8.17)

Questão 2.2: Sabe o que caracteriza um ataque de *phishing*? (Figura 8.18)

Questão 2.3: Sabe o que caracteriza um ataque de *ransomware*? (Figura 8.19)

Questão 2.4: Sabe o que caracteriza um ataque de DDoS (*Distributed Denial of Service*)? (Figura 8.20)

Questão 2.5: Sabe o que caracteriza um ataque do tipo ATO (*Account TakeOver*)? (Figura 8.21)

Questão 2.6: Sabe o que caracteriza um ataque do tipo *Man-in-the-Middle*? (Figura 8.22)

Questão 2.7: Sabe o que caracteriza um ataque de *SQL Injection*? (Figura 8.23)

Questão 2.8: Sabe o que caracteriza um ataque do tipo *Zero-day Exploit*? (Figura 8.24)

Questão 2.9: Sabe o que significa *Malware*? (Figura 8.25)

Questão 2.10: Sabe o que significa *Spyware*? (Figura 8.26)

Questão 2.11: Sabe o que significa *Trojan*? (Figura 8.27)

Questão 2.12: Qual considera o principal vector de entrada de ataques na empresa? (Figura 8.28)

Secção 3: Protecção e resiliência.

Composta por 6 questões, que visam essencialmente validar qual o tipo de acções e investimentos efectuados recentemente nas empresas, com vista a aumentar o nível de resiliência a ataques informáticos, assim como percepcionar de que forma os colaboradores olham para estas empresas em relação ao grau de exposição ao cibercrime, o que poderá permitir tirar algumas ilações sobre o panorama geral que se vive no tecido empresarial português.

Questão 3.1: Nos últimos 2 anos ocorreu alguma sessão de formação ou esclarecimento sobre Cibersegurança no âmbito, ou patrocinada, pela empresa? (Figura 8.29)

Questão 3.2: Nos últimos 2 anos foi adquirido equipamento informático no sentido de aumentar a segurança informática da empresa? (Figura 8.30)

Questão 3.3: Nos últimos 2 anos foram contratados recursos humanos com formação ou conhecimentos específicos na área da Cibersegurança? (Figura 8.31)

Questão 3.4: Nos últimos 2 anos foram implementadas alterações ou melhoramentos nos processos internos para aumentar a segurança informática? (Figura 8.32)

Questão 3.5: Além das medidas mencionadas nas questões anteriores, foram implementadas outras, nos últimos 2 anos? (Figura 8.33)

Questão 3.6: Qual considera ser o grau de proteção geral contra cibercrime na empresa? (Figura 8.34)

Secção 4: Tecnologias implementadas.

Composta por 11 questões, cujo foco é colocado nas tecnologias adoptadas pelas empresas para aumentar os seus níveis de Cibersegurança, assim como avaliar a forma como estas são utilizadas e moldam os próprios processos das empresas. Esta informação poderá ter um papel preponderante no momento em que for necessário apresentar propostas concretas de melhoria, nomeadamente a implementação de tecnologia específica do âmbito da Cibersegurança.

Questão 4.1: Existe algum tipo de tecnologia especificamente dedicada à Cibersegurança na empresa? (Figura 8.35)

Questão 4.2: A rede da empresa está protegida por uma *firewall*? (Figura 8.36)

Questão 4.3: A rede da empresa permite um acesso do exterior, através de VPN? (Figura 8.37)

Questão 4.4: Existe alguma tecnologia de proteção da privacidade documental? (Figura 8.38)

Questão 4.5: A empresa utiliza software antivirus nos seus computadores? (Figura 8.39)

Questão 4.6: É requerida autenticação multifactor (MFA) para aceder aos sistemas e plataformas informáticas da empresa? (Figura 8.40)

Questão 4.7: A empresa utiliza recursos/ferramentas na *Cloud*? (Figura 8.41)

Questão 4.8: As ferramentas utilizadas na *Cloud* têm algum tipo de proteção específica no que refere à segurança? (Figura 8.42)

Questão 4.9: Existem regras específicas para a utilização de meios tecnológicos, relativas à segurança informática? (por exemplo: é proibida a utilização de *pendrives* USB) (Figura 8.43)

Questão 4.10: Os colaboradores utilizam os seus próprios dispositivos móveis para aceder à rede, sistemas, plataformas ou documentação da empresa? (Figura 8.44)

Questão 4.11: Qual a relevância que as soluções/tecnologias *Cloud* têm actualmente nos processos da empresa? (Figura 8.45)

Secção 5: Investimento em Cibersegurança.

Composta por 6 questões, onde se pretende averiguar a propensão para investir na mitigação do cibercrime. Em particular, que tipo de investimentos, financeiros, tecnológicos, etc. Assim como, muito especificamente, perceber também qual o posicionamento destas empresas face à relação valor dos dados/custo para os proteger.

Questão 5.1: Qual o investimento aproximado, feito em Cibersegurança, nos últimos dois anos? (Figura 8.46)

Questão 5.2: Qual o investimento estimado, para Cibersegurança, no prazo de um ano? (Figura 8.47)

Questão 5.3: Existe intenção de contratar ou requalificar profissionais para a área da segurança informática, no prazo de um ano? (Figura 8.48)

Questão 5.4: Qual a importância que considera ter atualmente o investimento em Cibersegurança para a continuidade do negócio? (Figura 8.49)

Questão 5.5: Qual considera ser a probabilidade de investimento futuro em soluções/tecnologias *Cloud*? (Figura 8.50)

Questão 5.6: Como considera ser o valor financeiro/comercial dos dados/informação, face ao investimento necessário para os proteger? (Figura 8.51)

4.2. Análise de resultados tratados, PME

O tratamento dos dados, passou primeiramente pela filtragem das respostas obtidas de profissionais ligados a PME, de acordo com o âmbito definido para o estudo. Separando as respostas por dimensão da empresa, conseguimos fazer o conjunto de análises que se seguem, incluindo algumas comparativas com a realidade de empresas de maiores dimensões e com dados apenas de alguns grupos específicos dentro da nossa amostra, como são o caso dos Profissionais de IT ou os Administradores das empresas.

Desde logo, um dos indicadores mais interessantes, que nos permite ter uma ideia do grau de incidência de ataques informáticos a PME, conhecidos em Portugal. Ou seja, 76,31% dos inquiridos admite ter sido alvo de um ataque informático, ou conhecer alguém ou alguma organização que tenha sido (Figura 4.1).

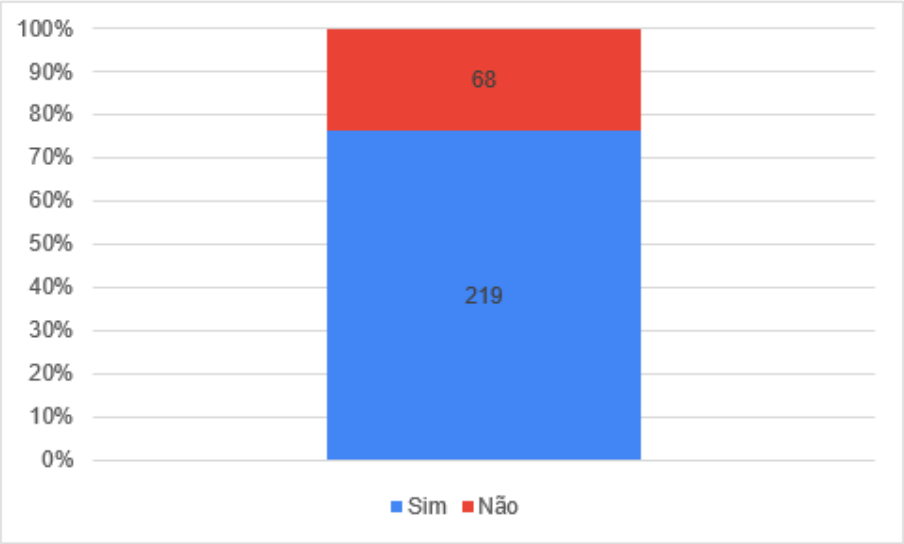

FIGURA 4.1 - GRÁFICO: JÁ FOI ALVO, OU TEM CONHECIMENTO DE ALGUMA EMPRESA QUE TENHA SIDO ALVO, DE UM ATAQUE INFORMÁTICO?

No que refere ao conhecimento técnico específico nesta área, nomeadamente no que respeita à tipologia de ataques e ao género de software malicioso, reparamos que existe alguma discrepância. Ou seja, conseguimos ver que a maioria esmagadora dos inquiridos está familiarizada com os conceitos de *Phishing*, *Malware*, *Spyware* e *Trojan*. Por

contraponto, verifica-se que apenas 58,89% dos inquiridos admitem conhecer em que consiste um ataque de *Ransomware*, que é um dos tipos de ataque mais comuns actualmente, e cujas quantias financeiras envolvidas assumem valores astronómicos à escala global. Além disto, para as restantes tipologias de ataques referidas no estudo, há um enorme desconhecimento, como é possível observar, por exemplo para os casos dos ataques do tipo *Man-in-the-Middle* e *Zero-day-Exploit*, que apenas menos de 30% dos inquiridos indica conhecer (Figuras 4.2 e 4.3).

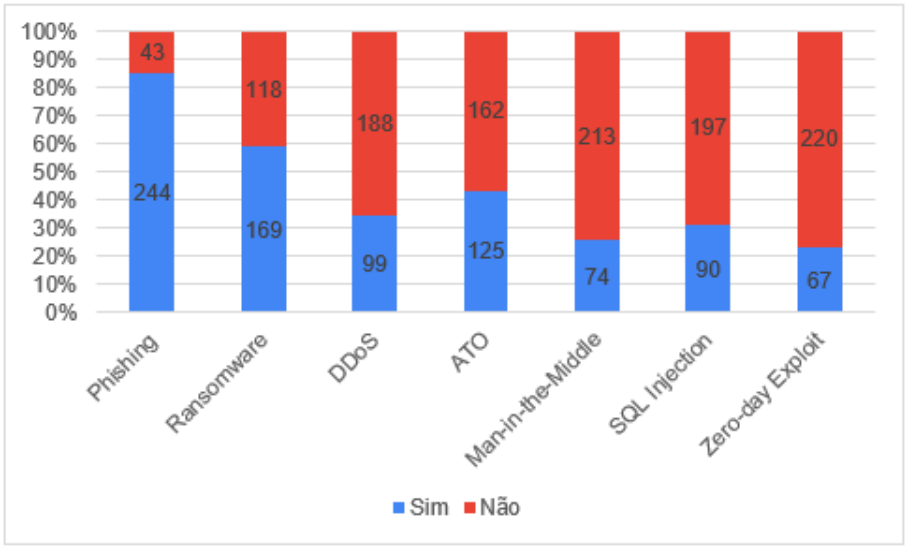

FIGURA 4.2 - GRÁFICO: CONHECE OU ESTÁ FAMILIARIZADO COM ESTE TIPO DE ATAQUE

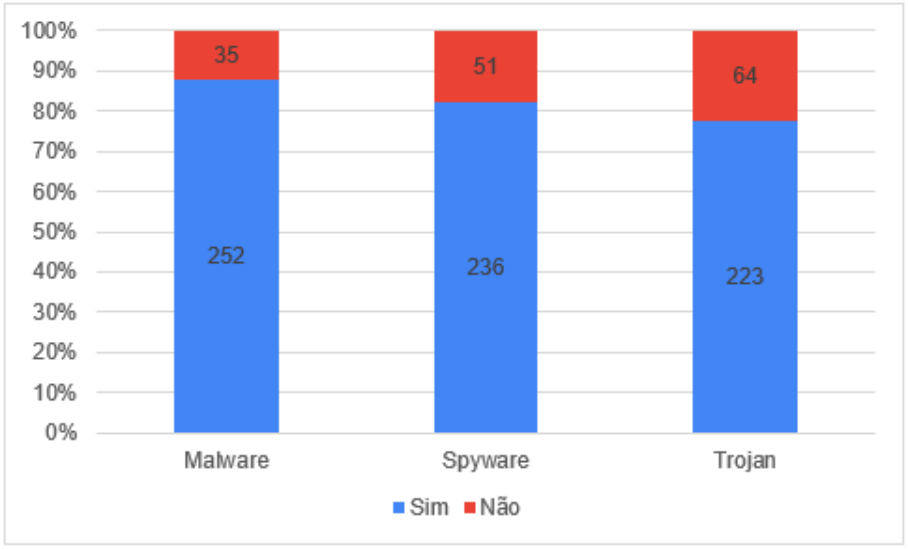

FIGURA 4.3 - GRÁFICO: CONHECE OU ESTÁ FAMILIARIZADO COM ESTE TIPO DE SOFTWARE MALICIOSO

O vector de entrada de ataques nas empresas é um indicador com uma enorme relevância, dado que permite localizar o foco com maior preponderância nas acções preventivas. Assim, é fundamental olhar para os dados que indicam que, genericamente, 47,04% dos inquiridos indica que são as pessoas, enquanto 44,60% indica que é a rede, que serve de porta de entrada a estes ataques. Neste particular, foi feito um comparativo com a opinião dos profissionais de IT, ou seja, quando consideradas apenas as respostas deste grupo, conseguimos verificar que a grande preponderância vai para o vector de entrada, pessoas. Com 78,95% destes profissionais a considerar que são os próprios funcionários das PME que acabam por funcionar como meio para as atacar (Figuras 4.4 e 4.5).

Quando cruzamos estes dados com os obtidos nas respostas dos profissionais ligados a Grande Empresas, percebemos que estes se encontram mais alinhados com a opinião dos Profissionais de TI das PME, no entanto, há a realçar que o factor "rede", volta a aparecer com alguma importância, obtendo 25,71% das respostas (Figura 4.6).

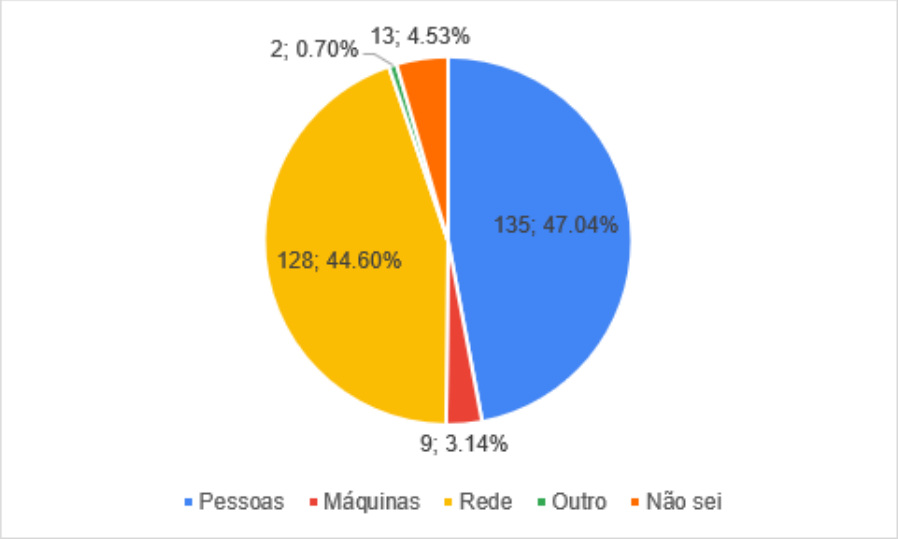

FIGURA 4.4 - GRÁFICO: QUAL CONSIDERA O PRINCIPAL VECTOR DE ENTRADA DE ATAQUES NA EMPRESA?

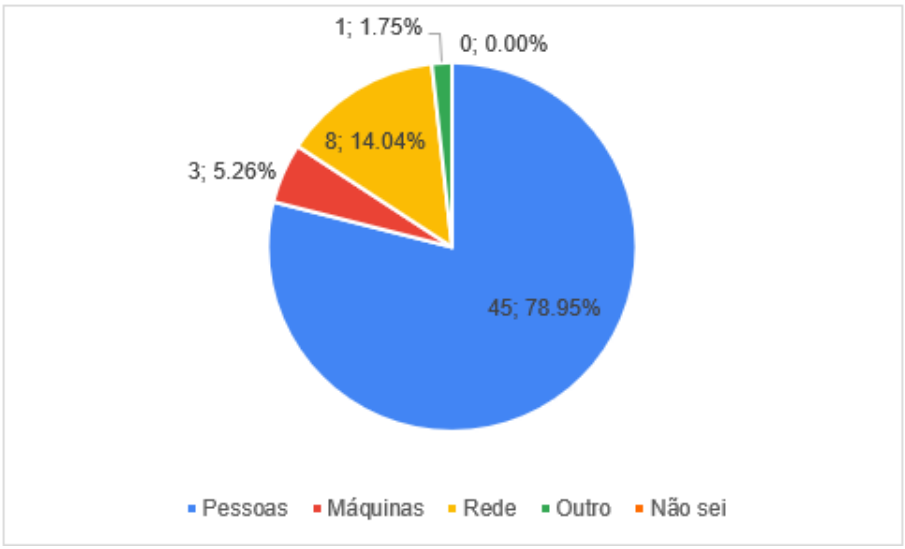

FIGURA 4.5 - GRÁFICO: QUAL CONSIDERA O PRINCIPAL VECTOR DE ENTRADA DE ATAQUES NA EMPRESA? (PROFISSIONAIS DE IT)

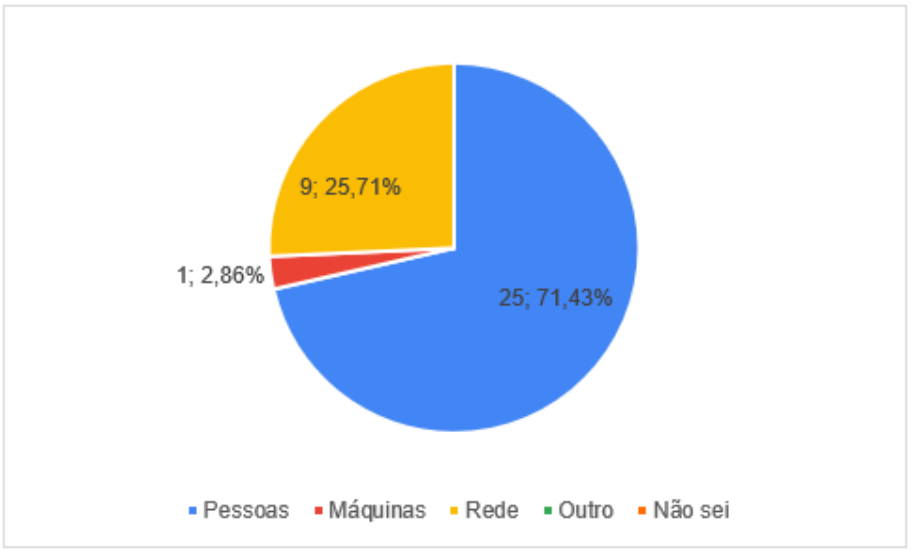

FIGURA 4.6 - GRÁFICO: QUAL CONSIDERA O PRINCIPAL VECTOR DE ENTRADA DE ATAQUES NA EMPRESA? (GRANDES EMPRESAS)

Com vista a perceber que tipo de acções ou investimentos são feitos nas PME, nomeadamente os que sucederam nos últimos dois anos, foi questionado acerca de quatro grupos particulares, que no seu todo abrangem a quase totalidade do que se afigura possível fazer nesta matéria: Formações ou sessões de esclarecimento; Aquisição de equipamentos; Contratação de RH especializados em Cibersegurança; e Melhoria de processos internos.

Verificou-se que o foco do tipo de investimento se encontra essencialmente na aquisição de equipamento e na melhoria dos processos internos das empresas. Por outro lado,

71,43% afirma não terem existido formações ou sessões de esclarecimento relativas a esta matéria, e 72,13% indica que não houve recrutamento de profissionais com perfil ligado à segurança informática, nos últimos 2 anos (Figura 4.7).

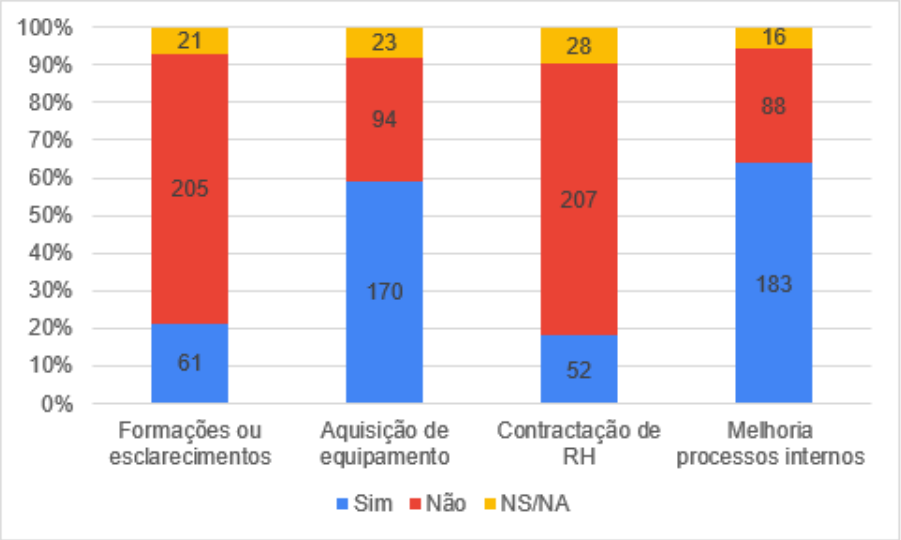

FIGURA 4.7 - GRÁFICO: ACÇÕES OU INVESTIMENTOS EM CIBERSEGURANÇA, NOS ÚLTIMOS 2 ANOS

Genericamente, a perspectiva relativamente ao grau de protecção geral contra o Cibercrime das empresas é, no conjunto de respostas Médio e Elevado, de 70,38%. No entanto, apenas 23,34% tem a percepção de ser Elevado e 22,65% indica mesmo que é Baixo (Figura 4.8).

Estes dados ganham uma relevância suplementar quando comparados com respostas de grupos específicos, como são o caso dos Profissionais de IT das PME ou os Profissionais de IT de Grandes Empresas. Assim, nas PME, 63,16% destes profissionais consideram existir uma protecção Média, e 29,82% uma protecção Elevada, num total conjunto de 92,98%. Já, nas Grande Empresas, é interessante reparar que 65% dos Profissionais de IT consideram que a protecção geral da empresa é elevada, considerando os restantes 35% que é Média (Figuras 4.9 e 4.10).

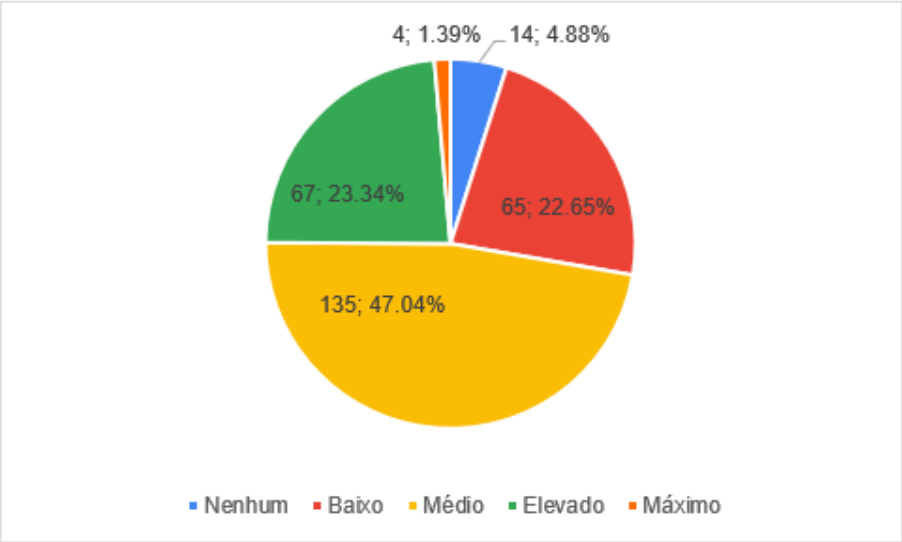

FIGURA 4.8 - GRÁFICO: QUAL CONSIDERA SER O GRAU DE PROTEÇÃO GERAL CONTRA CIBERCRIME NA EMPRESA?

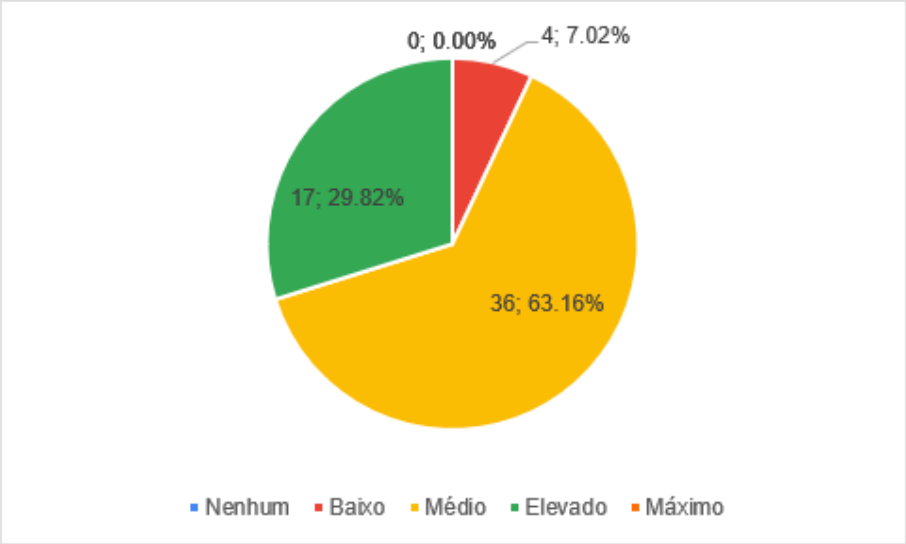

FIGURA 4.9 - GRÁFICO: QUAL CONSIDERA SER O GRAU DE PROTEÇÃO GERAL CONTRA CIBERCRIME NA EMPRESA? (PROFISSIONAIS DE IT)

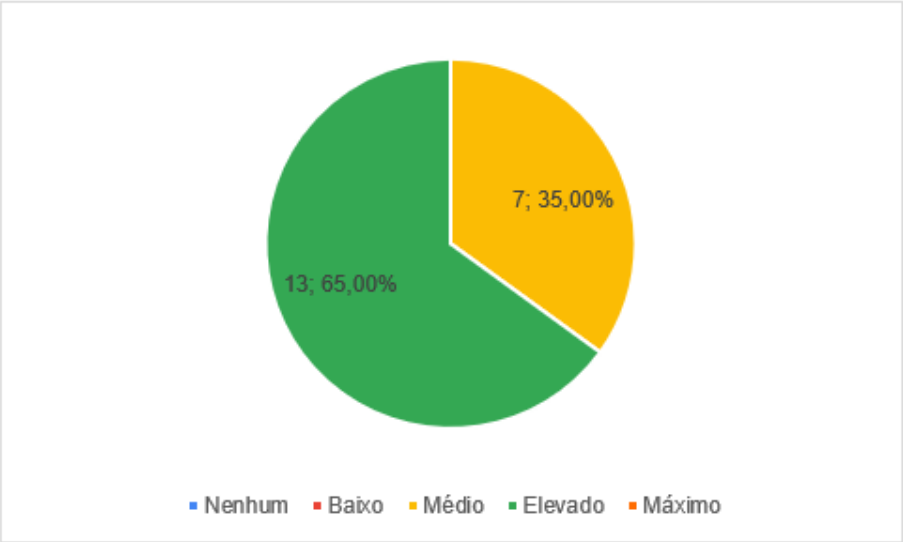

FIGURA 4.10 - GRÁFICO: QUAL CONSIDERA SER O GRAU GERAL DE PROTEÇÃO CONTRA CIBERCRIME NA EMPRESA? (PROFISSIONAIS DE IT EM GRANDES EMPRESAS)

Outro indicador bastante interessante – e potencialmente elucidativo – é o da alocação de tecnologia dedicada à Cibersegurança nas PME. De acordo com os dados obtidos, apenas 45,64% afirma que existe algum tipo de tecnologia deste tipo na empresa. Se a este valor juntarmos os 13,94% que responderam que não sabem ou não se aplica, obtemos uns alarmantes 59,58%. Isto significa que os dados presentes no gráfico seguinte, relativos a tecnologias concretas, respeitam apenas a 40,42% dos inquiridos (os que responderam Sim), onde alguns responderam também, não sei ou não se aplica (Figura 4.11).

Dada a relevância deste indicador, inclui-se a comparação com as respostas dadas por profissionais ligados a Grandes Empresas. Não surpreende a diferença abismal nas respostas, onde 85,71% dos inquiridos respondeu positivamente (Figura 4.12).

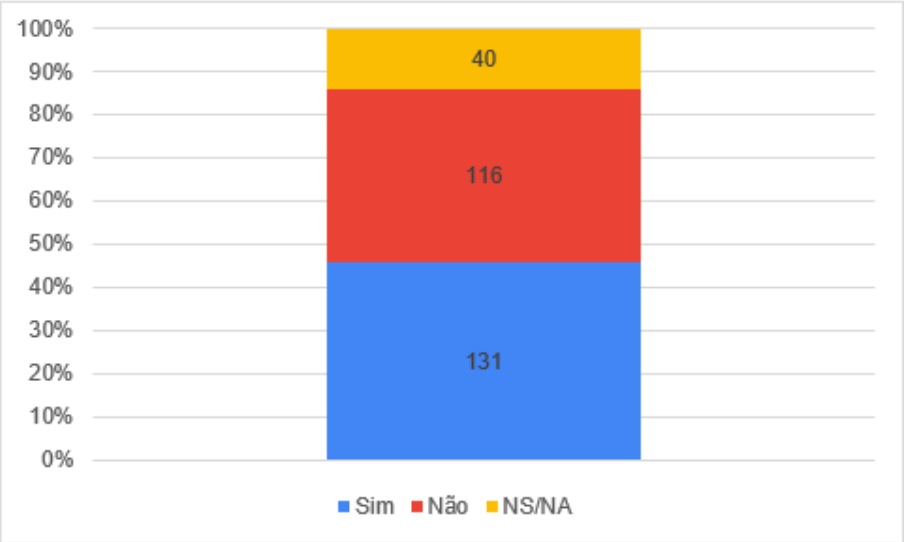

FIGURA 4.11 - GRÁFICO: EXISTE ALGUM TIPO DE TECNOLOGIA ESPECIFICAMENTE DEDICADA À CIBERSEGURANÇA NA EMPRESA?

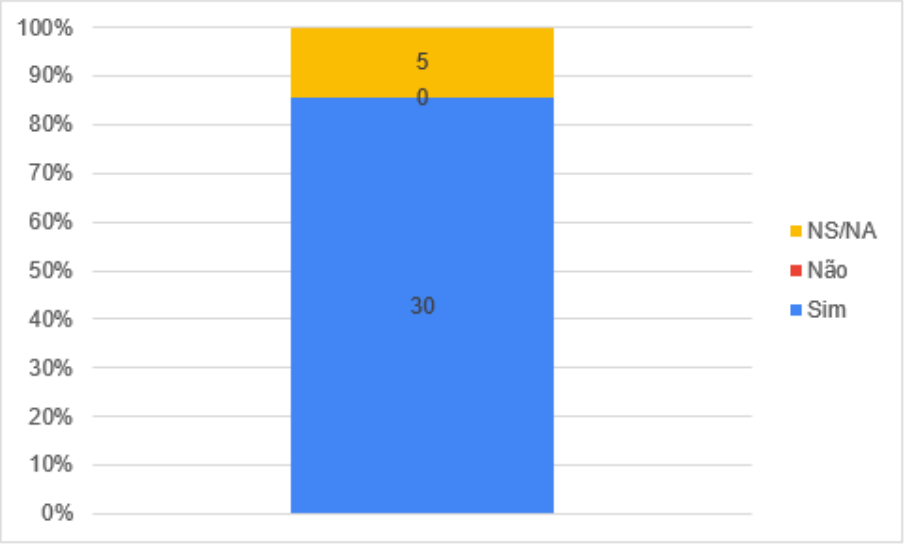

FIGURA 4.12 - GRÁFICO: EXISTE ALGUM TIPO DE TECNOLOGIA ESPECIFICAMENTE DEDICADA À CIBERSEGURANÇA NA EMPRESA? (GRANDES EMPRESAS)

O tipo de tecnologia utilizada nas empresas é uma informação relevante, especialmente porque pode ajudar a compreender o tipo de utilização e dependência de sistemas de informação que existe nas PME. Conseguimos verificar que a utilização de Antivirus, Firewall e VPN se encontra bastante disseminada, com 93,73%, 84,32% e 60,98%, respectivamente, dos inquiridos a afirmar que dispõem destas ferramentas. Por seu lado, nota-se que a privacidade documental e a implementação de sistemas de MFA (Autenticação

Multi-factor) ainda não é uma realidade neste panorama, pois apenas 39,02% dos inquiridos confirmam a existência destes últimos (Figura 4.13).

Por comparação com o cenário vivido nas Grandes Empresas é possível verificar que a utilização de Antivirus é muito menos frequente. No entanto, a existência de Firewall e VPN é muitíssimo elevada, com 97,22% e 88,89%, respectivamente, dos inquiridos a confirmar a presença deste tipo de tecnologia. Já a protecção com MFA aparece com 55,56%, significativamente mais elevado (Figura 4.14).

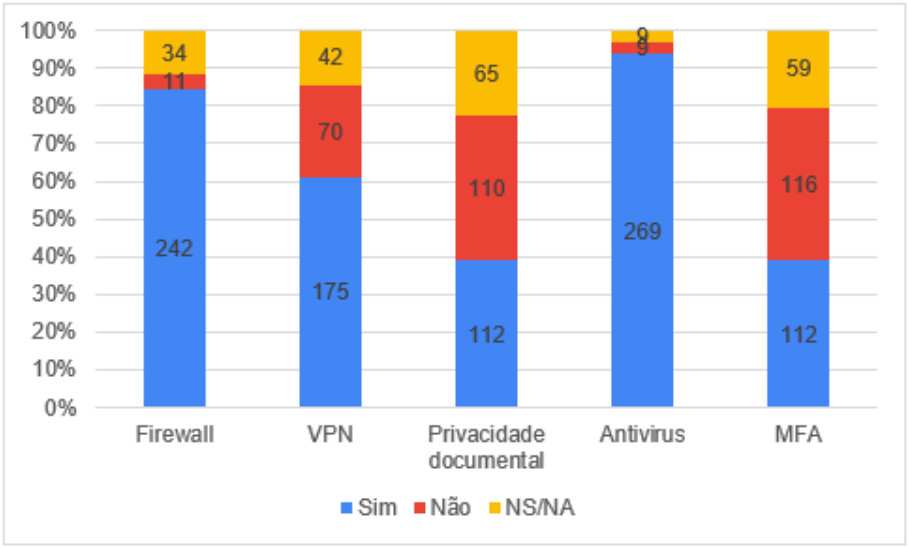

FIGURA 4.13 - GRÁFICO: TECNOLOGIA IMPLEMENTADA NA EMPRESA

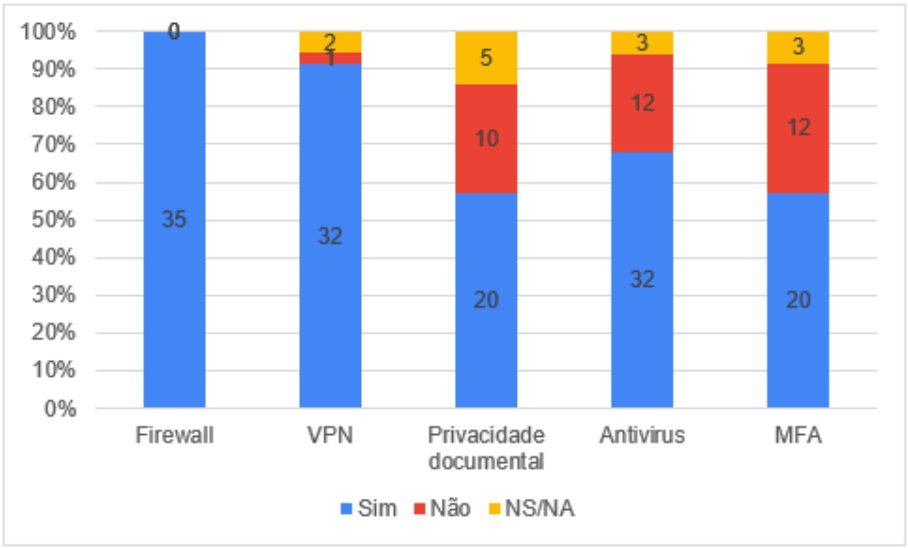

FIGURA 4.14 - GRÁFICO: TECNOLOGIA IMPLEMENTADA NA EMPRESA (GRANDES EMPRESAS)

No que refere às restrições existentes nas PME, relativas à utilização de meios e ferramentas tecnológicas, verificamos que em 68,64%, uma maioria muito significativa, não existe qualquer restrição. Ao mesmo tempo, 37,28% dos inquiridos refere que os profissionais de PME utilizam os seus próprios dispositivos no local de trabalho. Isto significa que um número muito considerável de profissionais destas empresas, utiliza os seus dispositivos pessoais nas instalações e com acesso aos sistemas destas, sem qualquer restrição (Figura 4.15).

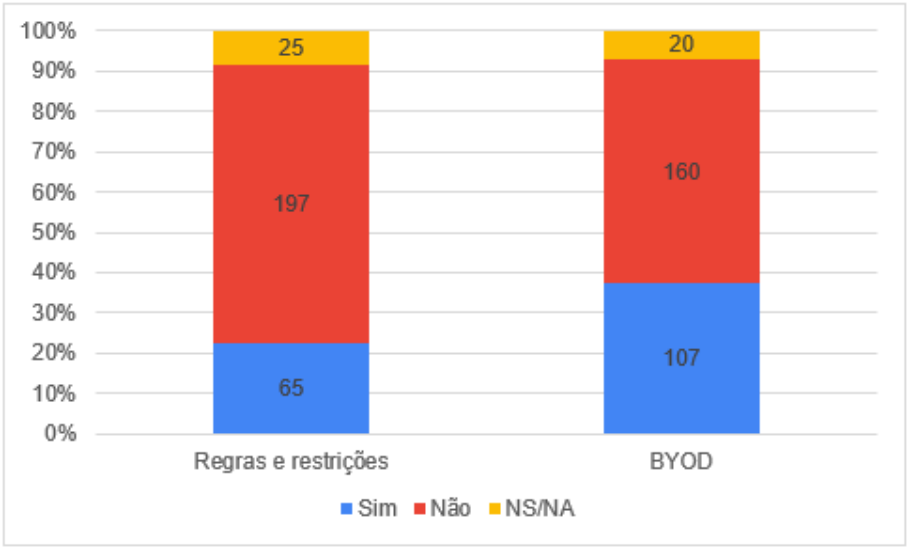

FIGURA 4.15 - GRÁFICO: ACESSO CONDICIONADO A MEIOS TECNOLÓGICOS, REDE E SISTEMAS DA EMPRESA

A utilização de ferramentas e tecnologias Cloud é um indicador com cada vez mais relevância. Neste caso, consideramos para análise apenas as respostas dos Profissionais de IT das PME. Conforme podemos observar, 59,65% indicam que existe recurso a estas plataformas na empresa, mas apenas 49,12% confirma a existência de protecção de segurança associada a elas. Um número muito relevante, 38,60%, afirma que não sabe ou crê que não se aplica se as ferramentas utilizadas na Cloud se encontram protegidas de alguma forma (Figura 4.16).

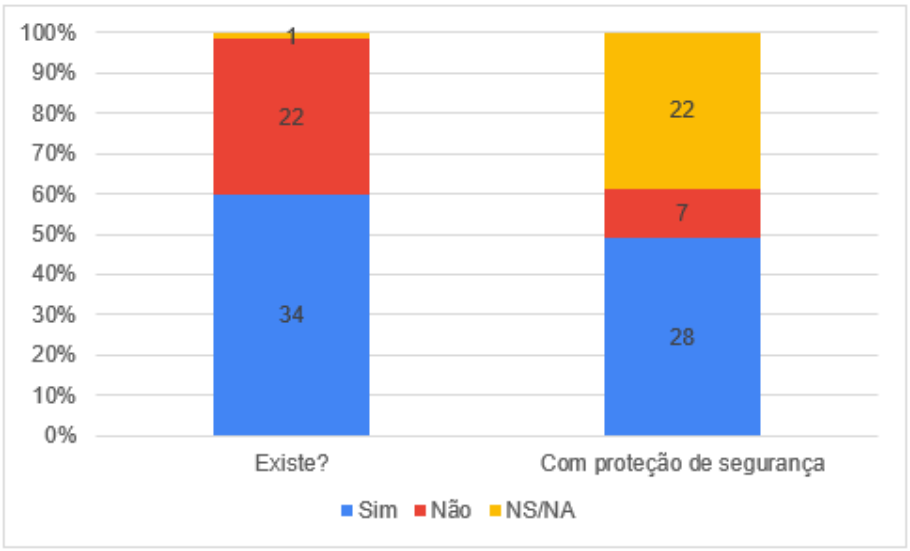

FIGURA 4.16 - GRÁFICO: UTILIZAÇÃO DE FERRAMENTAS OU RECURSOS NA CLOUD (PROFISSIONAIS DE IT)

Outro indicador, onde a opinião específica dos Profissionais de IT das PME poderá ser mais relevante e elucidativa, é o da relevância que as soluções ou tecnologias *Cloud* têm nos processos destas empresas. Isto porque, muitas vezes, os colaboradores não familiarizados com estas tecnologias têm dificuldade em distinguir se uma ferramenta é utilizada na sua versão *Cloud* ou *On-Premises* (localmente). Assim, verificamos que 29,82% afirma ter "Alguma importância", 26,32% diz ter "Muita importância" e 3,51% considera mesmo que tem "Toda a importância". Isto significa que, no seu conjunto, 59,65% destes profissionais considera a Cloud um recurso relevante para o normal funcionamento das PME em Portugal (Figura 4.17).

Uma nota especial para a comparação dos dados obtidos dos Profissionais de IT de Grandes Empresas. Neste contexto empresarial nota-se uma preponderância muitíssimo maior dos ecossistemas Cloud, com um total de 80% destes profissionais a referir que a sua relevância é "Alguma", "Muito" ou mesmo "Toda" (Figura 4.18).

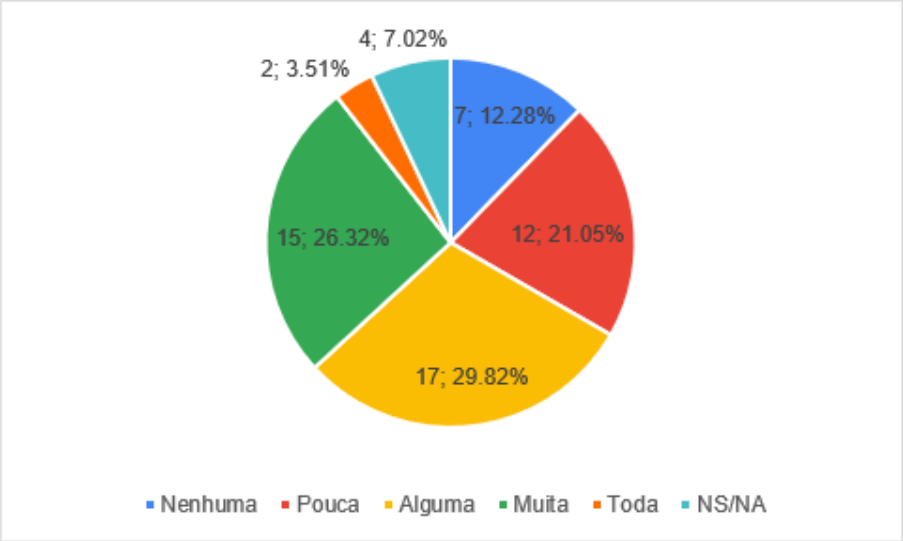

FIGURA 4.17 - GRÁFICO: QUAL A RELEVÂNCIA QUE AS SOLUÇÕES/TECNOLOGIAS CLOUD TÊM ACTUALMENTE NOS PROCESSOS DA EMPRESA? (PROFISSIONAIS DE IT)

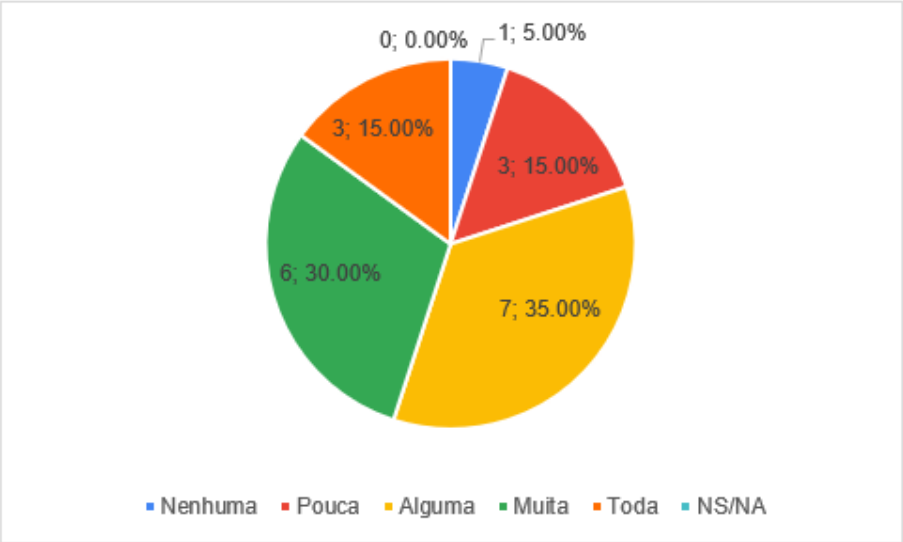

FIGURA 4.18 - GRÁFICO: QUAL A RELEVÂNCIA QUE AS SOLUÇÕES/TECNOLOGIAS CLOUD TÊM ACTUALMENTE NOS PROCESSOS DA EMPRESA? (PROFISSIONAIS DE IT EM GRANDES EMPRESAS)

Concretamente, no que concerne aos investimentos, o *feedback* dos Administradores das PME ganha uma especial relevância, visto que, tipicamente, nestas empresas são estes profissionais que lidam com a questão dos custos. Verificamos então que os investimentos previstos para o curto prazo se encontram alinhados com os efectuados nos últimos dois anos, encontrando-se os valores em causa abaixo dos 1.000€ para cerca de 40% dos inquiridos. Ainda assim, há a denotar que 25,22% dos Administradores admite ter gastado entre 1.000€

e 10.000€ em Cibersegurança nos últimos dois anos, o que são valores bastantes razoáveis para a realidade das PME nacionais (Figura 4.19).

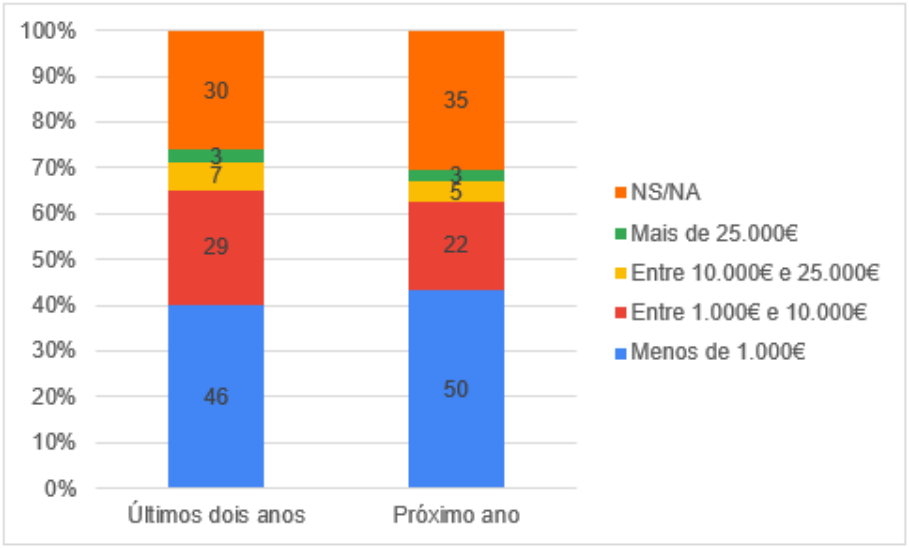

FIGURA 4.19 - GRÁFICO: INVESTIMENTO PASSADO E FUTURO EM CIBERSEGURANÇA (ADMINISTRADORES)

Outro indicador onde as respostas obtidas dos Administradores poderá ser mais elucidativo é o da intenção de contratar ou requalificar profissionais para a área da Cibersegurança. Neste, em particular, existe uma clara prevalência do "Não". O conjunto destes profissionais cuja reposta a esta questão foi "Não" ou "Não sei" ou "Não se aplica" é de 90,43%, pelo que parece não haver margem para qualquer dúvida acerca desta matéria (Figura 4.20).

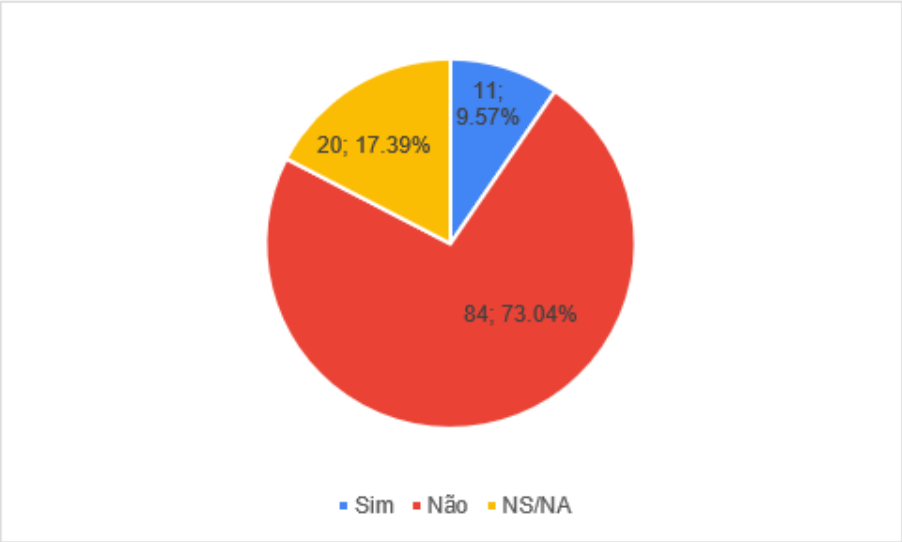

FIGURA 4.20 - GRÁFICO: EXISTE INTENÇÃO DE CONTRATAR OU REQUALIFICAR PROFISSIONAIS PARA A ÁREA DA SEGURANÇA, NO PRAZO DE UM ANO? (ADMINISTRADORES)

A associação da continuidade do negócio às questões da Cibersegurança parece ser bastante relevante. No seu conjunto, 77,35% dos profissionais de PME consideram que a importância deste tipo de investimento é "Alguma", "Muita", ou mesmo, "Toda". É importante referir que, em último caso, este indicador remete-nos para a possibilidade de deixar de operar devido a um ataque informático (Figura 4.21).

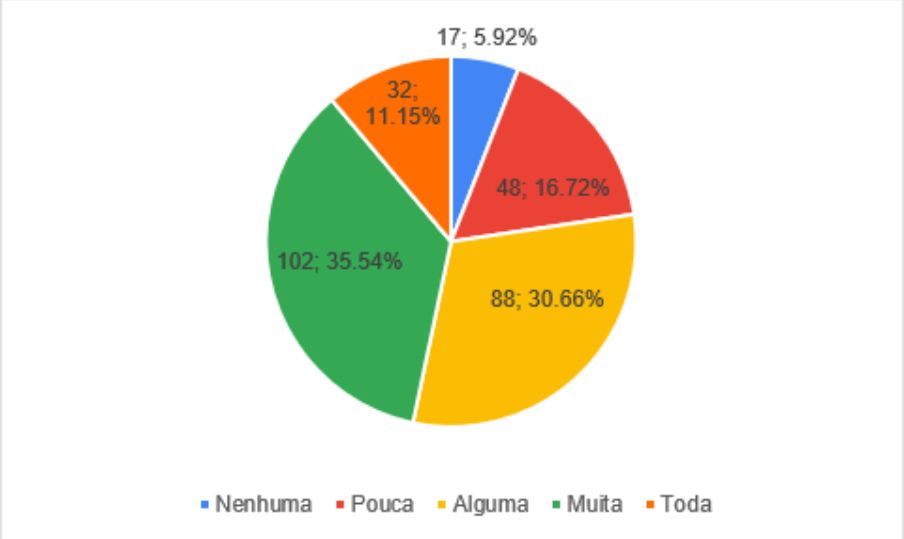

FIGURA 4.21 - GRÁFICO: QUAL A IMPORTÂNCIA QUE CONSIDERA TER ACTUALMENTE O INVESTIMENTO EM CIBERSEGURANÇA PARA A CONTINUIDADE DO NEGÓCIO?

Com cada vez mais serviços e produtos a serem disponibilizados na *Cloud*, validar a previsão de investimento neste tipo de plataformas pode ser significativo. Como é possível verificar, apenas 34,15% dos inquiridos considera que é pouco provável a ocorrência de investimentos futuros neste tipo de soluções (Figura 4.22).

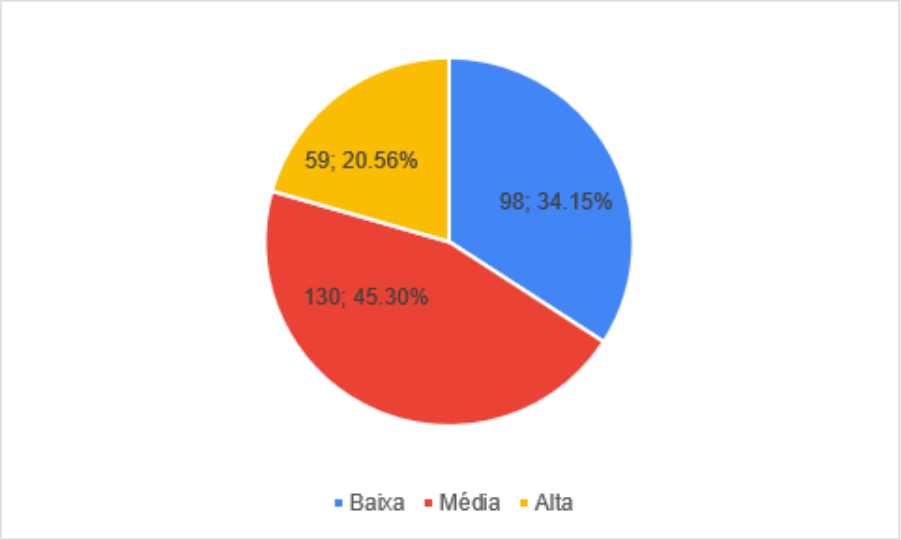

FIGURA 4.22 - GRÁFICO: QUAL A PROBABILIDADE DE INVESTIMENTO FUTURO EM SOLUÇÕES/TECNOLOGIAS *CLOUD*?

Por último, um indicador muito interessante, que respeita ao valor atribuído aos dados a proteger. Quando questionados sobre se os dados da empresa têm mais, menos ou o mesmo valor, do que o custo que representa protegê-los, as respostas parecem não deixar grandes dúvidas. Aqui, apenas 23% dos profissionais de PME em Portugal acredita que os dados são menos valiosos do que o custo do investimento para os manter seguros. Isto significa que, por outro lado, 77% dos inquiridos atribui o mesmo ou mais valor aos dados, do que o custo necessário para assegurar a sua segurança (Figura 4.23).

FIGURA 4.23 - GRÁFICO: COMO CONSIDERA SER O VALOR FINANCEIRO/COMERCIAL DOS DADOS/INFORMAÇÃO, FACE AO INVESTIMENTO NECESSÁRIO PARA OS PROTEGER?

5. Discussão

Quando olhamos para os resultados há, desde logo, um conjunto de interpretações que é possível fazer. Umas mais imediatas e lógicas, outras que carecerão naturalmente de uma visão mais holística do contexto em que as PME portuguesas operam. Desde logo da sua dimensão, sabemos que mais de 90% destas são Micro empresas (PORDATA, 2022), mas também a sua capacidade financeira ou o âmbito da sua actividade, por exemplo.

O facto de existirem 76,31% de inquiridos a admitir ter sido alvo de um ataque informático ou, pelo menos, ter tido conhecimento de um ataque deste género, é revelador do grau de disseminação e frequência com que estes sucedem. E deve alertar-nos para a necessidade de criar as medidas e implementar os mecanismos de defesa apropriados.

Se observarmos o nível de literacia existente nas PME, no que concerne às terminologias usadas no contexto dos ciberataques, percebe-se claramente que os inquiridos estão familiarizados com os tipos de software malicioso e ataques mais comuns – ainda que se pudesse esperar que mais do que 58,89% soubessem o que é *Ransomware*, visto tratar-se de um dos tipos de ataque mais mediáticos à escala global nos dias de hoje. No entanto, há muito desconhecimento acerca de outras tipologias de ataques, cuja ocorrência tem aumentado bastante nos últimos anos, o que remete para a eventual necessidade de melhorar o nível de conhecimento geral acerca desta matéria. Algo que poderá passar pela educação e sensibilização destes profissionais para o tema da Cibersegurança, por intermédio, por exemplo, de acções de formação neste âmbito.

Neste particular, encontramos um outro indicador, cujos resultados vêm reforçar esta ideia de que poderá ser importante considerar investir na formação dos colaboradores. Falamos do vector de entrada dos ataques nas empresas. Assim, quando 44,60% dos inquiridos afirma que as pessoas são o principal vector de entrada destes ataques, e 78,95% dos Profissionais de IT indicam que são também as pessoas, estamos perante um sinal claro de que o conhecimento que estas detêm acerca desta matéria será preponderante na mitigação das consequências dos mesmos.

As acções e investimentos feitos pelas PME nos últimos dois anos surgem com um foco evidente na aquisição de equipamentos e na melhoria dos processos internos das empresas. Deixando de parte, em 71,43% dos casos a formação dos colaboradores em matéria de Cibersegurança, e a contratação de profissionais com conhecimento nesta área específica, em 72,13% dos casos. Daqui podemos reforçar a ideia referida anteriormente de que a educação dos colaboradores é algo descurada, mas também que a presença de profissionais especializados nestas matérias, nos quadros destas empresas, não é algo que venha sendo considerado relevante.

Este facto poderá estar a ser influenciado por um outro indicador, que é o da percepção do grau de protecção existente contra o cibercrime. Querendo com isto dizer que a justificação para o tipo de investimentos e acções implementadas, que verificámos anteriormente, poderão ser um efeito do facto de 70,38% dos inquiridos considerar que as PME se encontram com grau Médio ou Elevado de protecção. De resto, quando olhamos para as respostas dos Profissionais de IT apenas, este valor sobe para 92,98%, o que poderá indiciar uma potencialmente falsa sensação de protecção, que acaba por levar a uma despreocupação acima do que seria desejável.

Quando questionados acerca da existência de tecnologia específica e dedicada à Cibersegurança nas PME, os 59,58% de respostas "Não" em conjunto com "Não sei ou Não se aplica", remetem para uma realidade potencialmente desastrosa. Estes dados poderão ter uma correlação directa com os factores referidos inicialmente nesta secção, relativos ao contexto socioeconómico em que estas empresas se inserem. E isto parece reforçado quando analisamos os mesmos dados, mas, desta feita, relativos apenas a Grandes Empresas, onde uma esmagadora maioria de 85,71% respondeu "Sim". Dando, portanto, a entender que, pelo menos em parte, isto poderá dever-se a uma menor capacidade de investimento financeiro em ferramentas e soluções consideradas secundárias.

No que respeita então às ferramentas e tecnologias efectivamente utilizadas pelas PME, percebe-se que as soluções mais tradicionais – no sentido temporal do termo – são as prevalentes, aparecendo a Privacidade documental e os sistemas MFA com valores mais modestos, ainda que perto dos 40%, o que é um valor razoável e já algo surpreendente pela positiva. Ainda que, segundo Phan (2018), a autenticação via MFA é uma das pedras basilares, um dos mínimos a assegurar, para qualquer sistema que se proponha manter minimamente seguro nos dias de hoje.

Isto ganha uma reforçada importância quando olhamos para os dados do indicador de acesso condicionado aos meios tecnológicos das empresas. Ou seja, 68,64% dos inquiridos refere não haver qualquer restrição no acesso, e, a juntar a isto, 37,28% indica que acede através dos seus dispositivos pessoais. Conseguimos, portanto, ter uma ideia clara do grau de risco a que as PME se encontram expostas, simplesmente pela adopção destas abordagens ou estratégias, o que revela algum facilitismo na gestão de algo que poderá ter uma acção directa na continuidade do negócio.

Uma das tecnologias que mais adopção de mercado tem tido nos últimos anos, são as ferramentas disponibilizadas na *Cloud*. Estes ecossistemas transformaram a forma como as empresas e os utilizadores individuais consomem e utilizam muitos produtos e serviços.

Passámos para um paradigma de "tudo como um serviço" (XaaS, *Everything as a Service*). Dada a relevância que as ferramentas e recursos na *Cloud* assumem hoje em dia, olhamos para alguns indicadores relativos a esta área específica com grande interesse. Desde logo, o facto de 59,65% dos profissionais de IT das PME indicar que existe algum tipo de utilização destas soluções, quando cruzado com apenas 49,12% confirmarem que estas contemplam algum tipo de protecção de segurança, apresenta-se como um indício claro de exposição eminente ao cibercrime.

E isto assume um destaque ainda maior quando olhamos para o indicador que revela que 59,65% destes profissionais considera que os recursos utilizados pela empresa, na *Cloud*, têm "Alguma", "Muita" ou "Toda" a importância nos processos desta. O que significa que, mais uma vez, a continuidade do negócio depende, em grande medida da segurança e resiliência destes recursos.

Entrando agora numa análise mais relacionada com os custos e investimentos financeiros, consideramos os *inputs* dos Administradores das PME portuguesas para verificarmos que existe uma linha de continuidade entre os últimos dois anos e o futuro próximo (um ano). E aqui confirmamos a perspectiva já referida de que os factores económicos desempenham um papel decisivo no processo de tomada de decisão, visto que cerca de 40% deste profissionais indica ter existido, ou prever um investimento menor do que 1.000€ em Cibersegurança.

Num evidente alinhamento com o referido, encontram-se os dados do indicador que mostra que apenas 9,57% dos Administradores de PME em Portugal tem intenção de contratar ou requalificar recursos humanos para a área da Cibersegurança, no prazo de um ano. Claramente, mais uma vez podemos interpretar isto como um factor relacionado com o contexto económico e a própria dimensão destas empresas.

Ainda assim, os profissionais das PME demonstram ter uma clara noção da importância que o investimento em Cibersegurança representa para a continuidade do negócio. Quando questionados acerca deste aspecto particular, 77,35% distribuem a sua opinião entre "Alguma", "Muita" e "Toda". O que nos permite depreender que provavelmente não será apenas por uma questão de consciencialização para o fenómeno em si que este tipo de investimento não é maior.

No entanto, há um indicador onde a probabilidade de investimento futuro parece ter uma importância significativa. De acordo com o que já verificámos, as soluções *Cloud* aparecem como uma tendência que veio para ficar, e 65,85% dos inquiridos admite que existe uma probabilidade "Média" ou "Alta" de investir nelas.

Por fim, uma nota muito relevante. Os dados das empresas sempre foram – e continuam a ser – um dos seus bens mais valiosos. E, seguramente, a disponibilidade e propensão para os proteger será tanto maior quanto mais valor lhe for conferido por quem está nas empresas, diariamente, a tomar decisões, a criar e a acrescentar valor a partir desses dados. Assim, é com alguma naturalidade que verificamos que apenas 23% dos profissionais de PME em Portugal assume que o valor dos dados destas é menor do que o custo necessário para os proteger. Por um lado, isto poderá indicar que a falta de investimento poderá estar relacionada, em parte, com questões socioeconómicas da natureza própria deste tipo de empresas – conforme de resto já vimos, mas, por outro lado, poderá também ser um indício de alguma abstracção relativamente aos reais custos envolvidos na implementação de tecnologia relacionada com Cibersegurança e mitigação de cibercrime.

5.1. A Cibersegurança em contexto prático

Num mundo ideal, os sistemas de TI (Tecnologias da Informação) devem garantir – por defeito – que nenhum comportamento indesejável é possível, e que qualquer ataque informático é devidamente mitigado. No entanto, mesmo nos melhores sistemas de TI, que apresentam um elevado grau de flexibilidade e robustez, existe a necessidade de serem tomadas medidas para limitar esses comportamentos indesejáveis, em determinadas circunstâncias. Conforme observado por Lessig (2009), isso pode ser feito por intermédio de sistemas que excluem o risco associado ao comportamento, que violará certas regras. Esperando-se que os utilizadores rejam as suas acções por códigos de conduta especificamente desenhados para eliminar falhas. Em caso de ocorrência destas falhas, há então lugar a processos disciplinares que focam aqueles que quebraram as regras. Este é um contexto e visão para a autenticação, autorização e responsabilidade (Rashid et al., 2019).

No entanto, sabemos que não vivemos num mundo ideal. Aliás, como é possível verificar pelas respostas ao questionário apresentadas anteriormente, é bastante visível o nível de dependência que existe hoje dos sistemas digitais, onde a questão da segurança está eminentemente interligada com os conceitos de identidade, autorização e autenticação. De resto, num contexto onde os profissionais têm as suas tarefas quotidianas cada vez mais dependentes da robustez destes sistemas, e considerando que a sua autonomia, em teoria, deverá manter-se, ou preferencialmente aumentar, é fundamental que, por um lado, os sistemas sejam o mais seguros possível, por outro, que as pessoas possuam o maior grau de literacia digital possível.

De maneira a incrementar a capacidade das PME de resistir a um nível de ameaças crescente, que é parte integrante de um mundo cada vez mais digital e dependente das TI, propõe-se um conjunto de implementações que, de forma transversal, se pretende que sirvam o propósito da mitigação do cibercrime nestas empresas. Podendo todas as implementações ser feitas em conjunto ou separadamente, mediante a capacidade e disponibilidade de cada empresa para este tipo de investimento. Assim, com o intuito de exemplificar a efectivação do aumento do grau de Cibersegurança nas PME, foram introduzidas numa empresa real as seguintes medidas de protecção:

- Segmentação de rede estruturada com várias VLAN (Criação de rede DMZ, Configuração de equipamentos de rede como switchs e firewall);
- Autenticação de dispositivos clientes, na rede wireless da VLAN de domínio (Active Directory), efetuada via RADIUS, num NPS (Network Policy Server);
- Implementação de MFA (MultiFactor Authentication) e Microsoft ATP (Advanced Threat Protection) em ambiente híbrido Cloud-OnPremises (Hybrid Azure AD joined);
- Encriptação de discos rígidos de computadores através de política de grupo, via Microsoft Intune (Bitlocker);
- Formação aos utilizadores sobre Cibersegurança.

A infraestrutura de TI da empresa em questão assenta essencialmente num Cluster Microsoft Hyper-V, onde existem vários servidores virtuais, com funções e serviços diversos. A base da arquitectura é um domínio Active Diretory on-premises, com sincronização para Azure Active Directory (serviço Cloud), e subscrições de Microsoft 365 para o serviço de email em Microsoft Exchange Online e utilização de várias ferramentas de Office, entre outras. No que respeita ao *networking*, a empresa tem uma rede estruturada, com vários switchs ligados entre si e cujo tráfego é gerido numa firewall física (Fortinet Fortigate).

Uma nota particular, e muito importante, para o facto de se seguirem vários recortes de ecrã, retirados dos vários processos de configuração dos vários sistemas elencados anteriormente. Nestes recortes, todas as informações relativas à identidade da empresa em causa foram ocultadas, de forma a garantir a manutenção do seu anonimato. Aproveito também para agradecer à empresa em questão a disponibilidade e abertura demonstradas para acolher a implementação destas tecnologias, assim como para disponibilizar aos seus colaboradores a informação (proposta de formação) contida no ANEXO I.

5.1.1. Segmentação de rede estruturada

Conforme verificámos na questão 2.12 do nosso questionário, sobre o principal vector de entrada de ataques nas empresas, onde 44,60% dos inquiridos (25,71% se considerarmos apenas profissionais de TI) respondeu a opção “Rede”, este é um elemento cuja proteção podemos considerar absolutamente primordial assegurar nestas organizações. Arriscaria mesmo dizer, em qualquer organização. Assim, a implementação específica aqui passou pela segmentação da rede em várias VLAN, com o intuito de direccionar o tipo de tráfego, os acessos às plataformas e a utilização das ferramentas pelos canais próprios (Figuras 5.1 e 5.2).

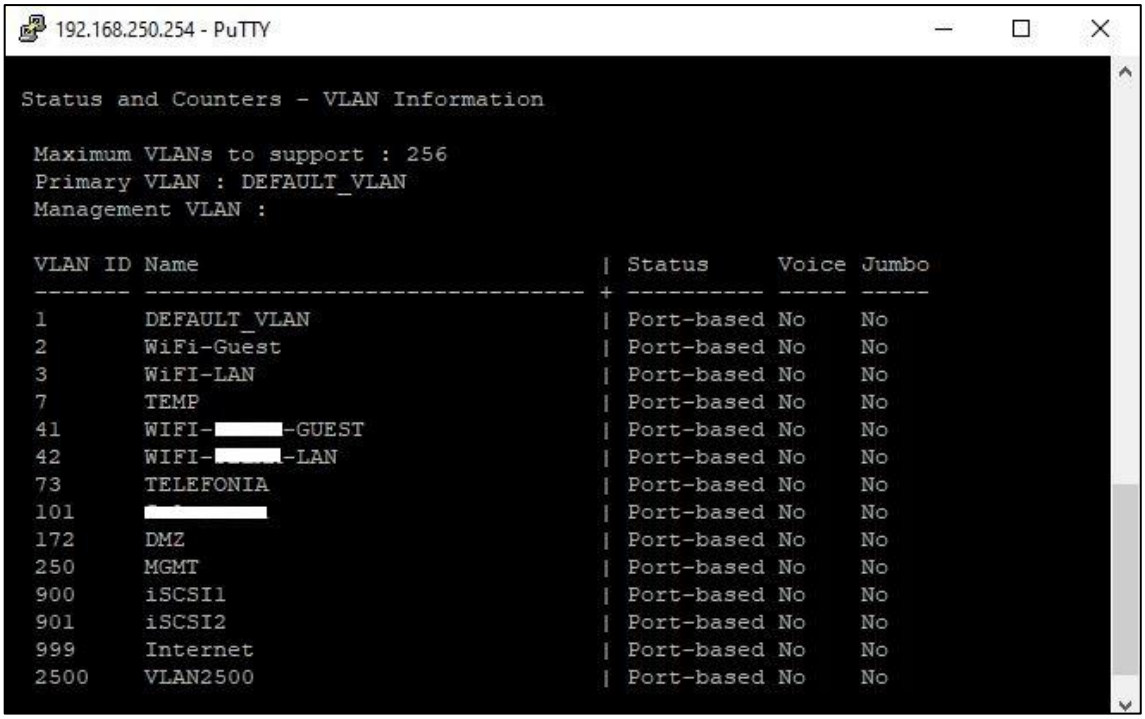

FIGURA 5.1 - VLANS CONFIGURADAS NO CORE SWITCH DA EMPRESA

FIGURA 5.2 - HELPER ADDRESSES DA VLAN DEFAULT (EXEMPLO DE IP DE DHCP SERVER)

Depois de criadas as VLAN, onde se incluiu uma especificamente para a rede DMZ (demilitarized zone), foi também configurada esta rede na firewall, onde é dedicada uma interface física ao tráfego *inbound* e *outbound*, parametrizado o serviço DHCP (Dynamic Host Configuration Protocol) associado à respectiva VLAN, e criadas as regras de comunicação com a rede LAN (Local Area Network) e com a Internet (sd-wan) (Figuras 5.3, 5.4 e 5.5).

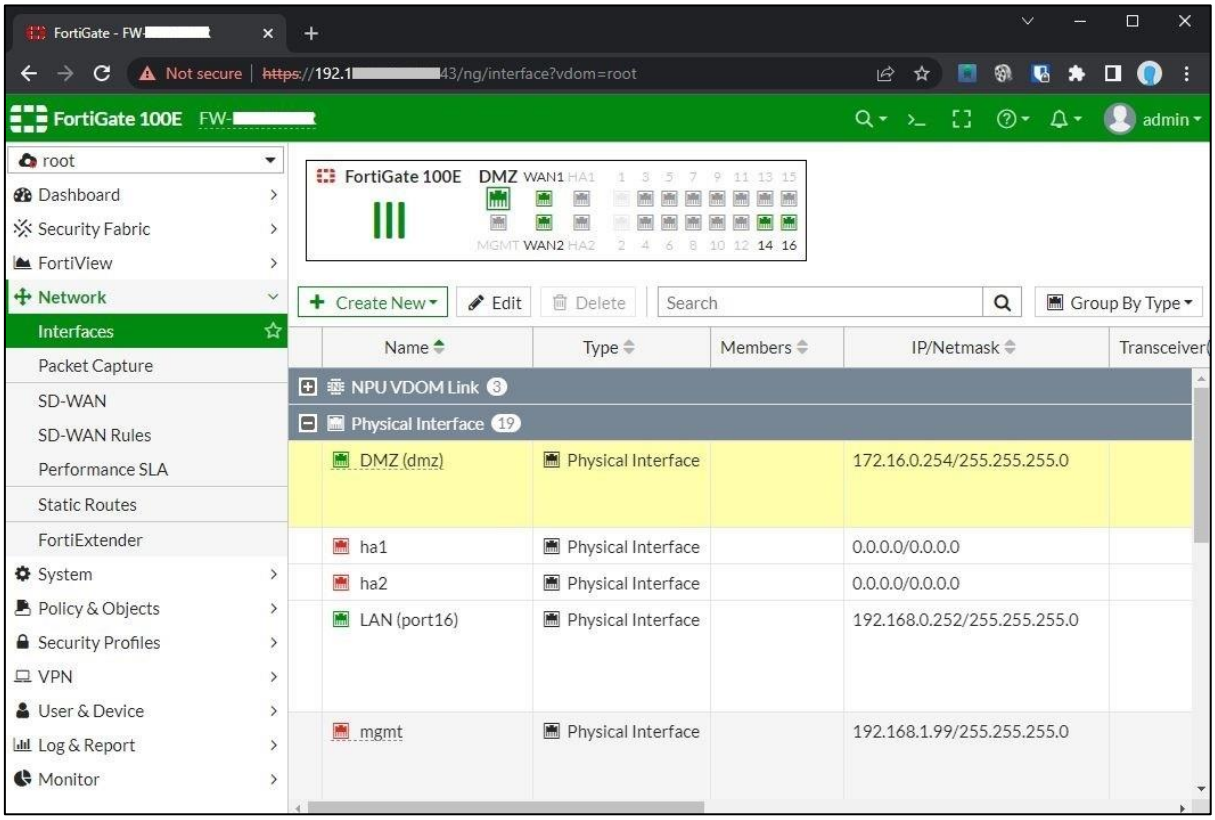

FIGURA 5.3 - INTERFACE PARA DMZ, NA FIREWALL (FORTIGATE)

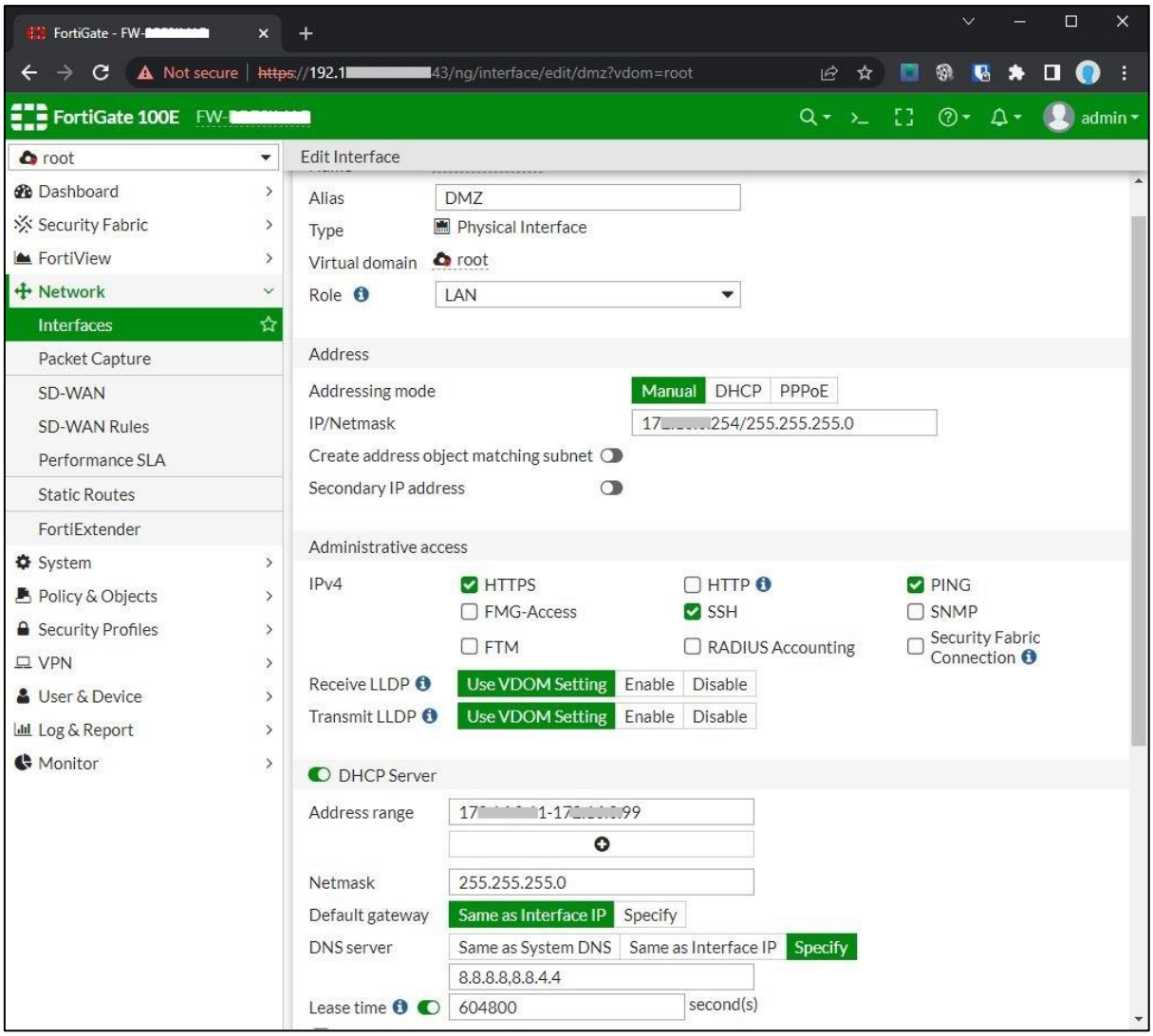

FIGURA 5.4 - CONFIGURAÇÃO DE DMZ NA FIREWALL (FORTIGATE)

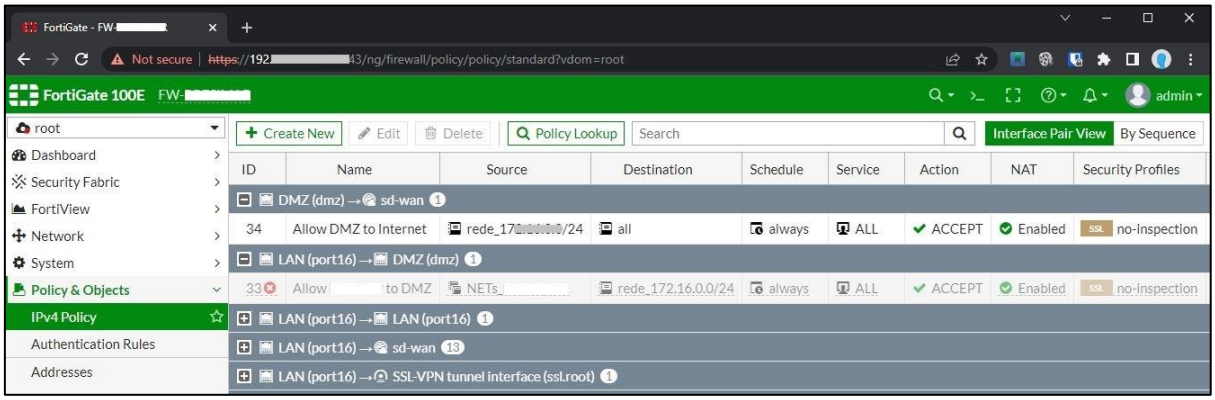

FIGURA 5.5 - CRIAÇÃO DE REGRAS PARA REDE DMZ, NA FIREWALL (FORTIGATE)

Desta forma, conseguimos ter não só uma rede dedicada ao domínio interno da empresa, como também várias dedicadas, por exemplo à rede wireless de convidados, ou à solução de telefonia VoIP (Voice over Internet Protocol) existente, por exemplo. Simultaneamente, com a configuração da rede DMZ, temos um acesso totalmente aberto da rede interna (LAN) à Internet, e vice-versa, necessária para utilizações específicas de profissionais que necessitam colocar online equipamentos industriais, IoT, ou outros, sem terem de o fazer através das restantes redes protegidas.

5.1.2. Autenticação wireless via RADIUS/NPS

Quando olhamos para o indicador relativo à questão 4.9, do nosso questionário, que remete para o tipo de acesso que é feito à rede e sistemas das empresas, reparamos que 68,64% dos inquiridos indica que não existe qualquer condicionamento. Ainda relacionado com este indicador, também verificamos que 37,28% dos profissionais das PME em Portugal utilizam os seus próprios equipamentos para aceder a meios tecnológicos das organizações. Assim, e uma vez que os acessos via redes wireless são cada vez mais comuns, muitas vezes mesmo o modo de acesso à rede primordial nas empresas, e também porque já implementámos tecnologia que nos permite proteger contra acessos indevidos através de rede cablada (ver ponto anterior deste capítulo), apresentamos agora uma implementação ao nível da autenticação na rede wireless (VLAN de domínio) da empresa.

Para isso, foi instalado e configurado o serviço NPS (Network Policy Server), no servidor Controlador de Domínio, seguido da configuração de um cliente RADIUS (Remote Authentication Dial In User Service), seguido da parametrização das opções de segurança da rede wireless de domínio, na Controladora Wireless responsável por gerir os AP (Access Point) da empresa, tendo também sido acrescentados os dispositivos pretendidos aos grupos de segurança Active Directory (Figuras 5.6, 5.7, 5.8 e 5.9).

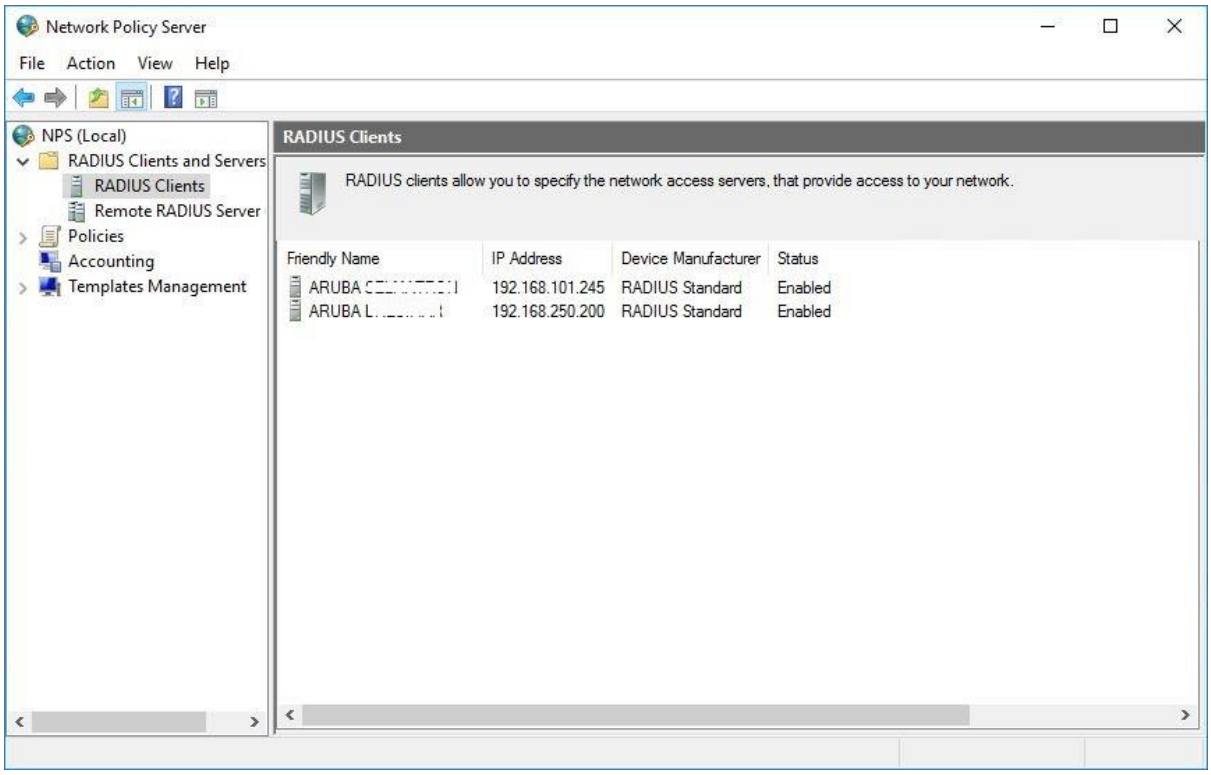

FIGURA 5.6 - CRIAÇÃO DE CLIENTES RADIUS EM WINDOWS NPS

Um dos passos da configuração dos clientes RADIUS é a definição de um *Token* (Shared secret) que é necessário para adicionar este cliente no equipamento de rede responsável por difundir a rede wireless. Neste caso, trata-se de uma Controladora Wireless Aruba (virtual), acessível através de um dos vários *Access Points* distribuídos pelo parque industrial da empresa (Figura 5.7).

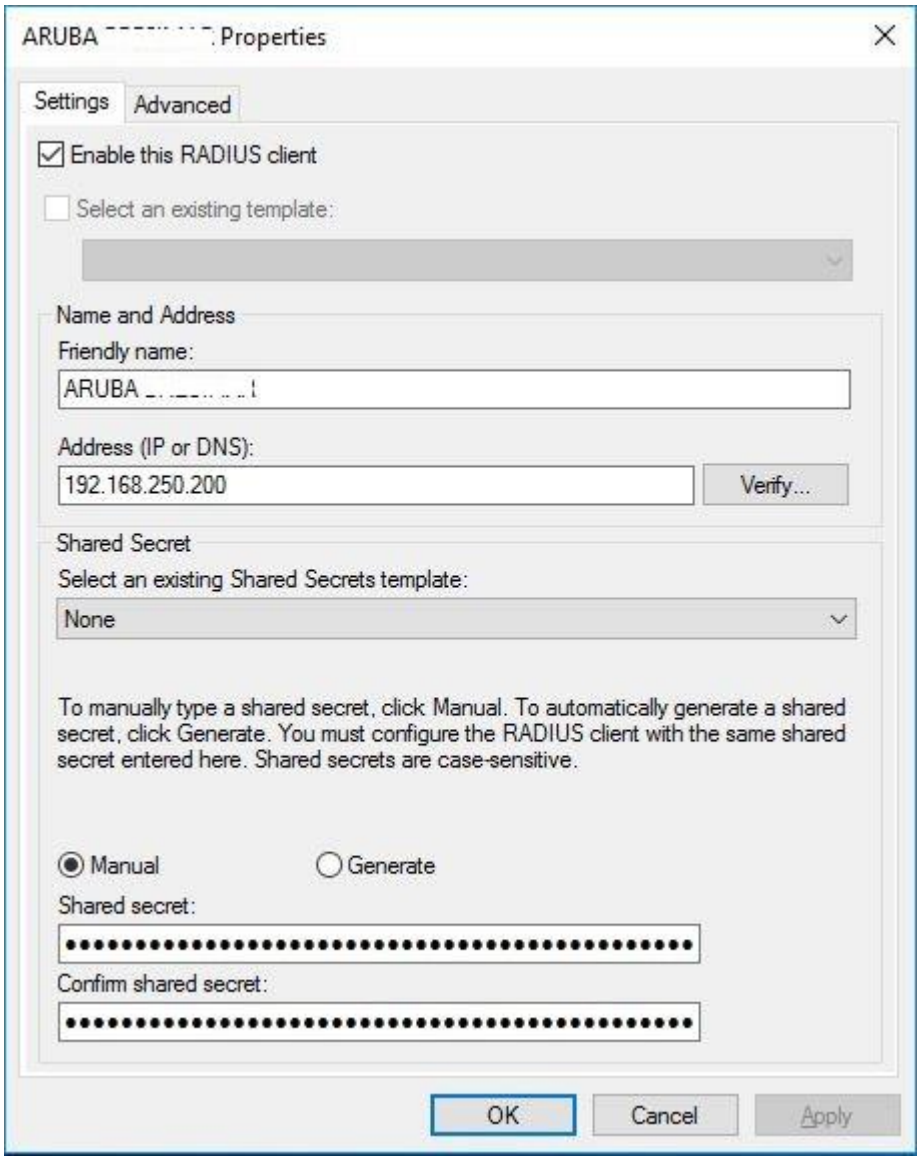

FIGURA 5.7 - CONFIGURAÇÃO DE CLIENTE RADIUS EM WINDOWS NPS

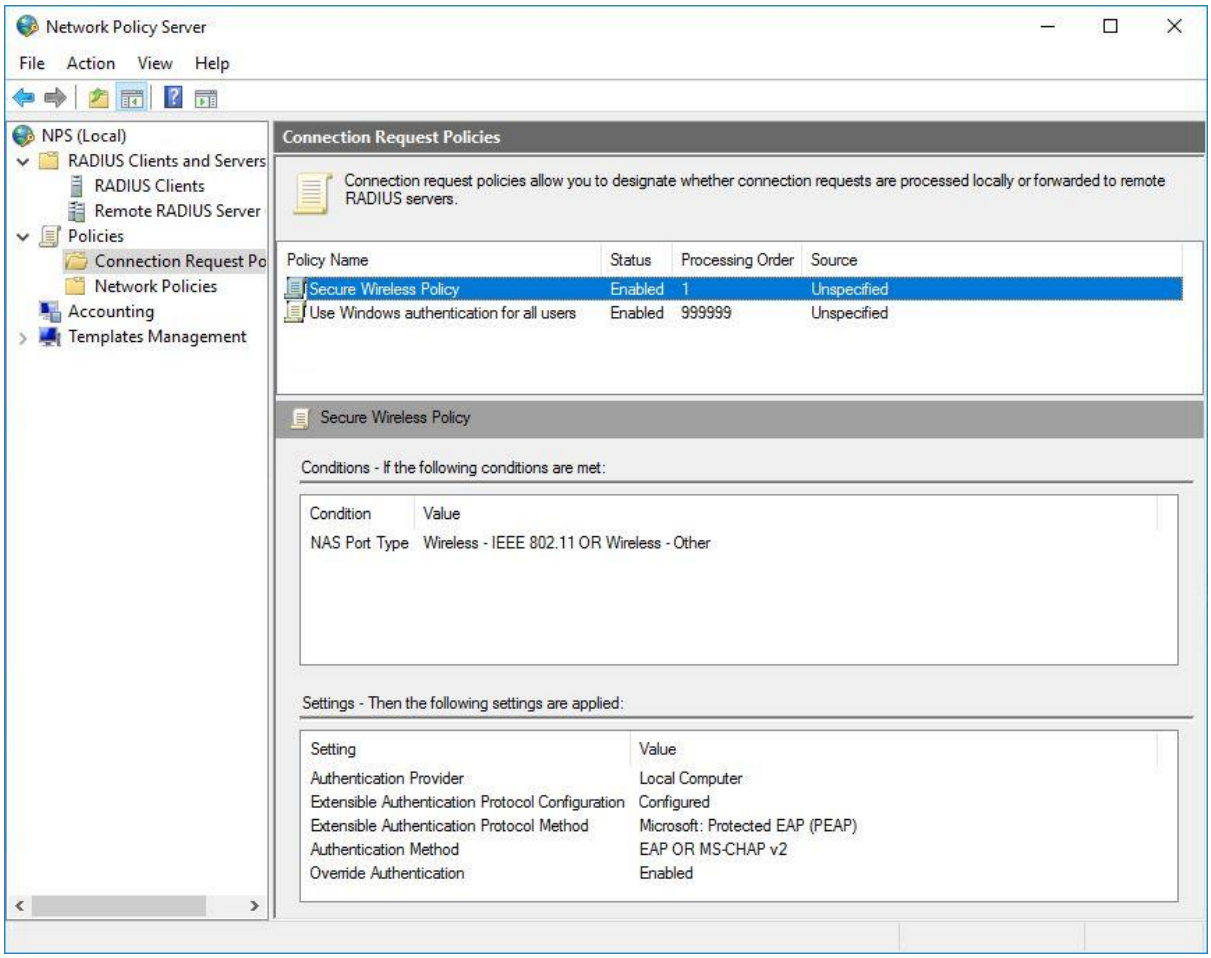

FIGURA 5.8 - CRIAÇÃO DE REGRAS DE AUTENTICAÇÃO EM WINDOWS NPS, 1/2

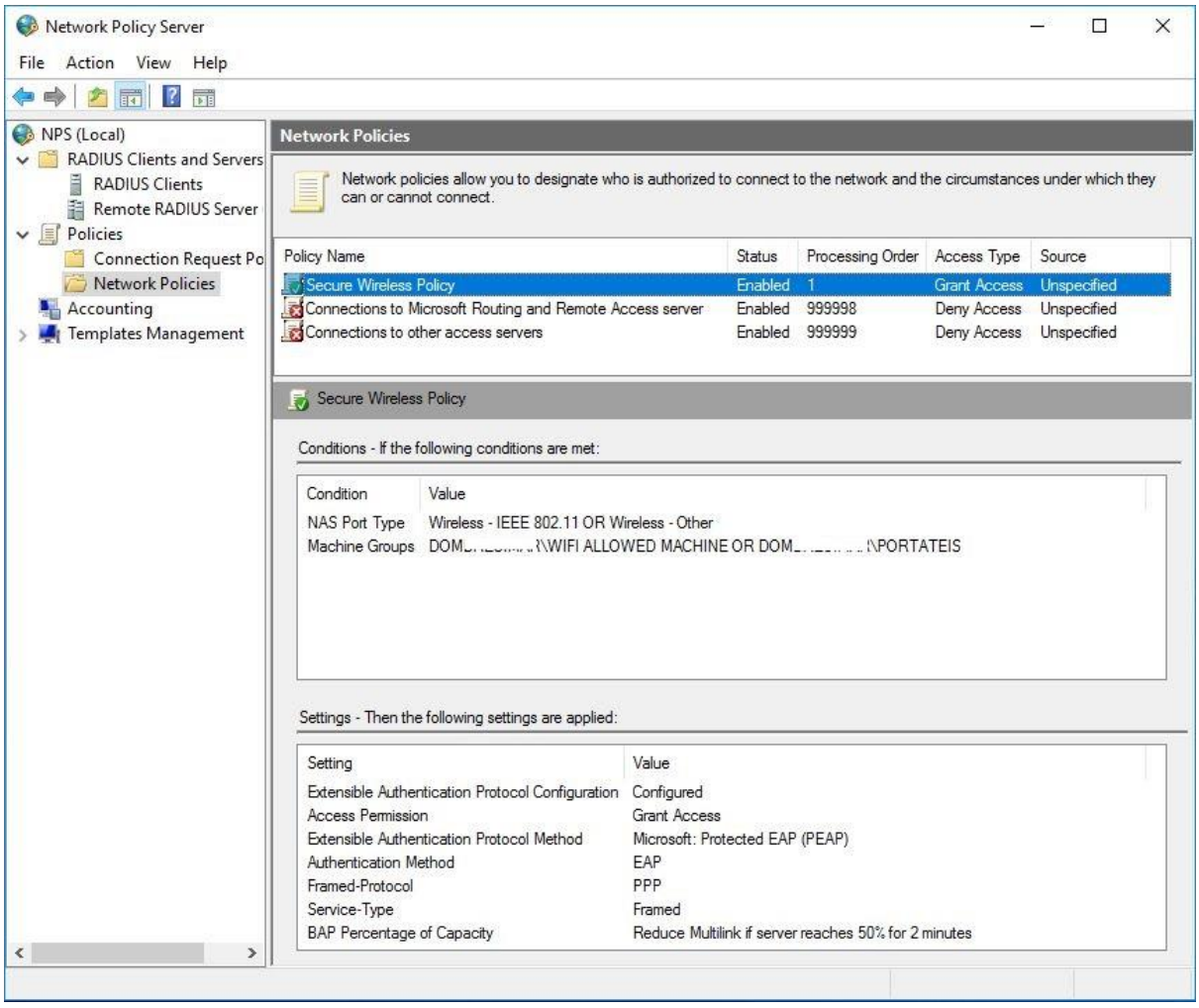

FIGURA 5.9 - CRIAÇÃO DE REGRAS DE AUTENTICAÇÃO EM WINDOWS NPS, 2/2

Para que o NPS autentique os dispositivos na rede de domínio, é necessário definir as regras ou os requisitos que os dispositivos ou utilizadores têm obrigatoriamente que cumprir para tal. Neste caso, além de apenas se conseguirem autenticar dispositivos que utilizem o tipo de autenticação "IEEE 802.1x", é também apenas permitida autenticação, nesta rede, a máquinas que pertençam a um de dois grupos de segurança Active Directory, "WIFI ALLOWED MACHINE" ou "PORTATEIS" (Figura 5.10).

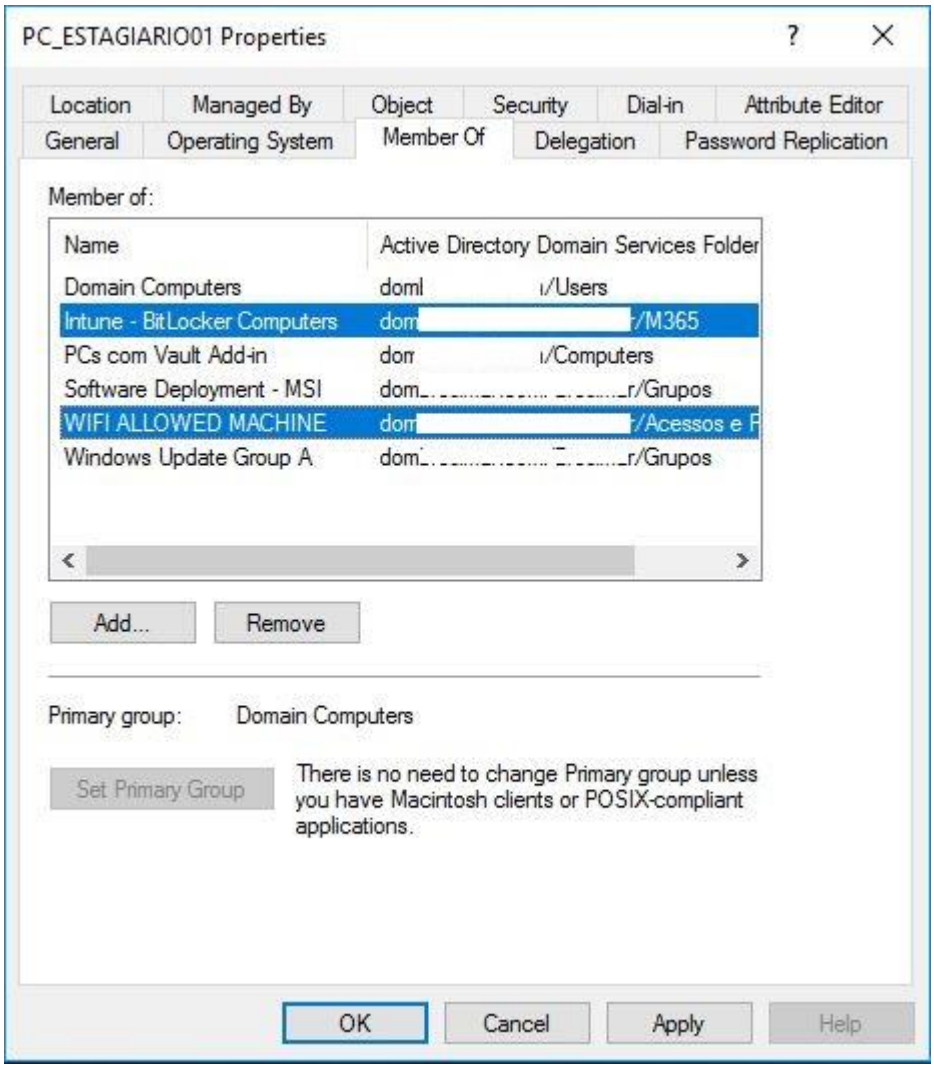

FIGURA 5.10 - ATRIBUIÇÃO DE GRUPOS DE SEGURANÇA A OBJECTOS DA AD, PARA AUTENTICAÇÃO RADIUS

Por último, e conforme referido anteriormente, nas configurações da Controladora Wireless, quando acedemos às definições de segurança da rede cuja autenticação será feita por RADIUS/NPS, parametrizamos o IP do servidor onde se encontra a correr o serviço NPS e introduzimos a chave de segurança, que anteriormente referimos como *Token*. Com estes dados, a controladora irá fazer *bypass* dos pedidos de autenticação que recebe dos clientes que se ligam aos AP para que estes sejam negociados com o servidor (Figuras 5.11 e 5.12).

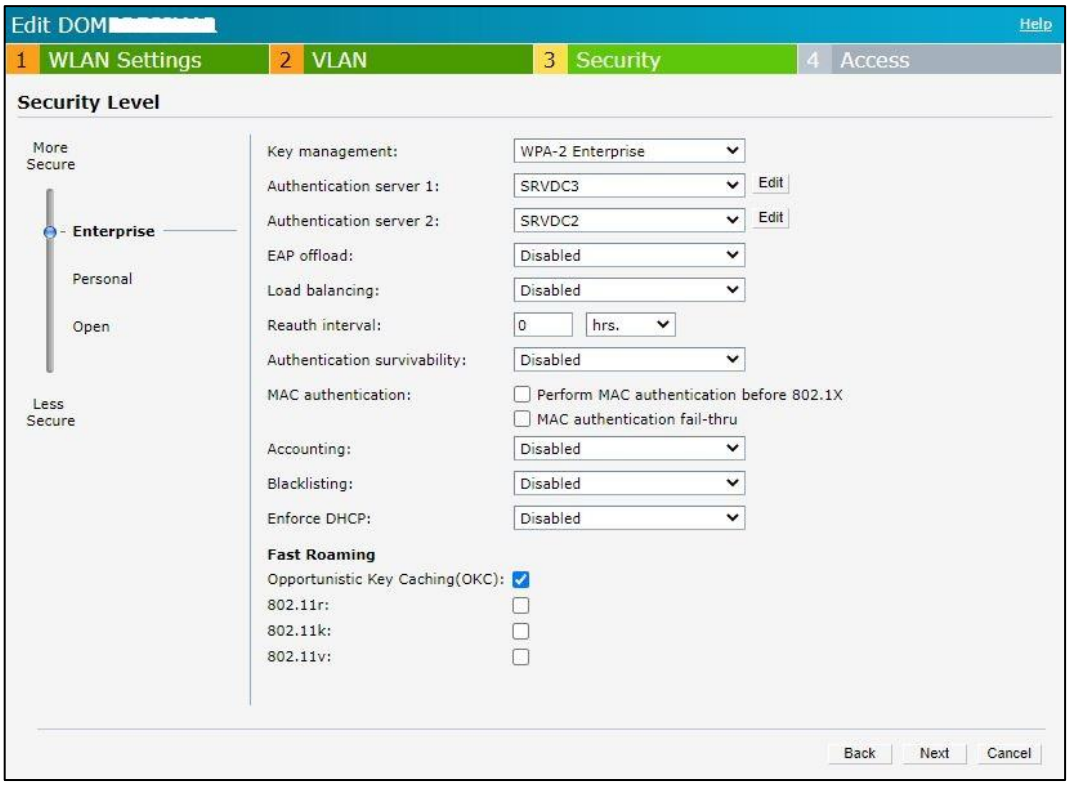

FIGURA 5.11 - DEFINIÇÕES DE SEGURANÇA NA CONTROLADORA WIRELESS (SERVIDOR DE AUTENTICAÇÃO)

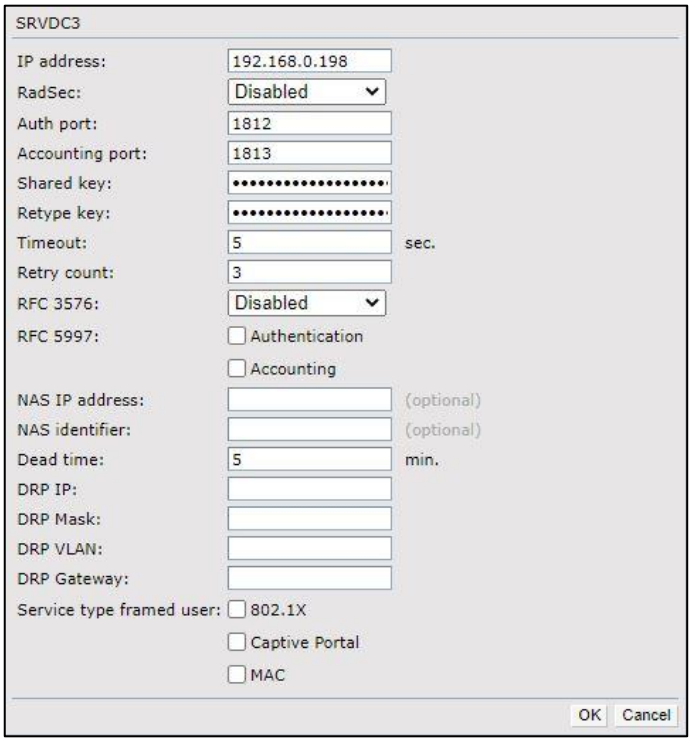

FIGURA 5.12 - PARAMETRIZAÇÃO DE SERVIDOR DE AUTENTICAÇÃO NA CONTROLADORA WIRELESS

5.1.3. Autenticação MFA

Conforme é possível observar pelas respostas às questões 4.7, 4.8, 4.11 e 5.5 do nosso questionário, relativas à relevância e índice de penetração das tecnologias baseadas em Cloud, faz sentido considerar este ecossistema muito particular como meio de implementação de tecnologia específica de protecção contra o cibercrime. Quando cerca de 60% dos profissionais de TI das PME considera as tecnologias *Cloud* "algo", "muito" ou "totalmente" relevantes para os processos das organizações e, simultaneamente, apenas 39,02% dos inquiridos admite a existência de tecnologias MFA nestas, percebemos que um bom passo no caminho da Cibersegurança deste tipo de empresas, em Portugal, poderá ser a implementação de autenticação MFA. No nosso exemplo específico irá incidir sobre as subscrições Microsoft 365, o que se reflecte na plataforma de email (Microsoft Exchange Online) e demais ferramentas utilizadas pela empresa, por exemplo, Sharepoint Online, Office 365, Microsoft Teams, Microsoft OneDrive para Empresas, etc.

Assim, foi implementado um ambiente híbrido entre Active Directory on-premises e Azure Active Directory (*Hybrid Azure AD join*), para que os utilizadores sejam visíveis do lado do Azure Active Directory (*Cloud*) e lá se possa activar e parametrizar o MFA para esses utilizadores.

Para configurar o *Hybrid Azure AD join*, foi utilizada a ferramenta Microsoft Azure Active Directory Connect, onde são parametrizadas as definições específicas da sincronização, por exemplo quais os objectos a sincronizar, que tipo de Exchange, se existir, ou activar a opção *Single Sign-On* (que permite autenticar em várias aplicações ou ferramentas utilizando o mesmo ID). Depois de configurado, é forçada a sincronização com o comando "*Start-ADSyncSyncCycle -PolicyType Initial*". Tendo sido adicionalmente criado um grupo de segurança na Active Directory on-premises, neste caso chamado "Azure - MFA Users", que será alvo das políticas a implementar do lado da Azure Active Directory (*Cloud*) (Figuras 5.13, 5.14 e 5.15).

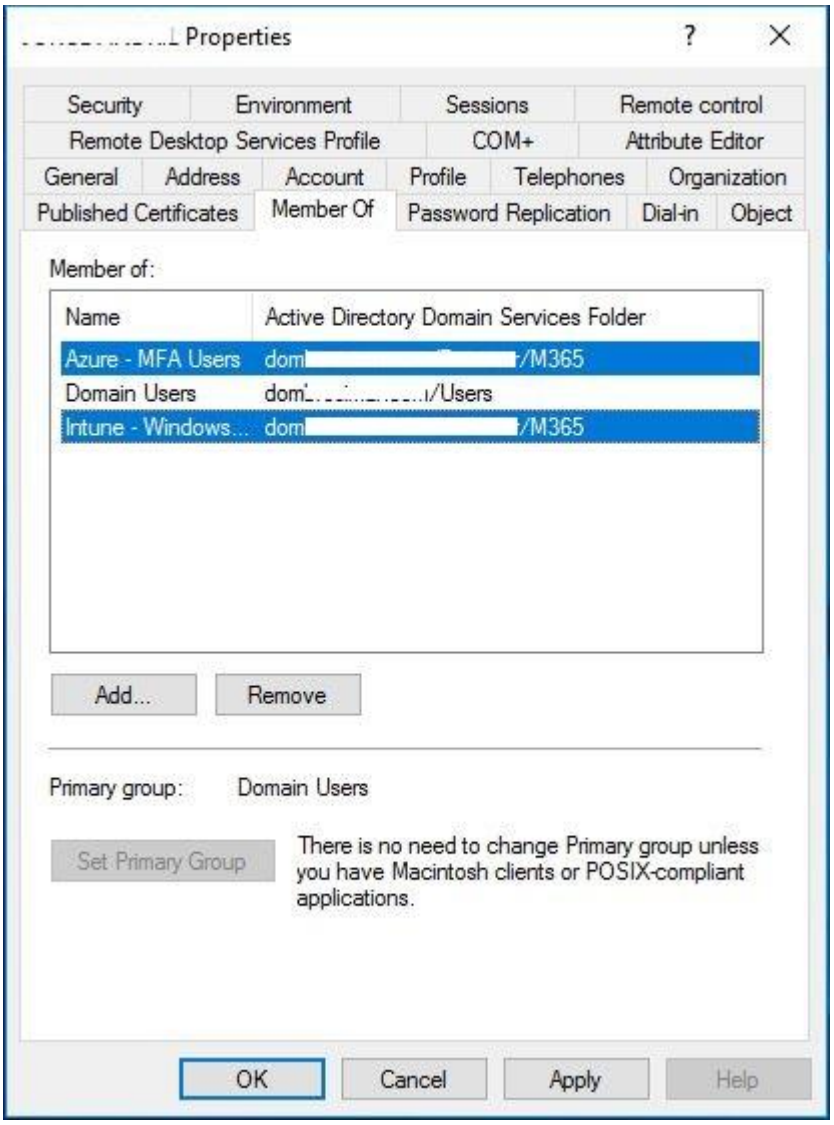

FIGURA 5.13 - ATRIBUIÇÃO DE GRUPOS DE SEGURANÇA A OBJECTOS DA AD (MFA)

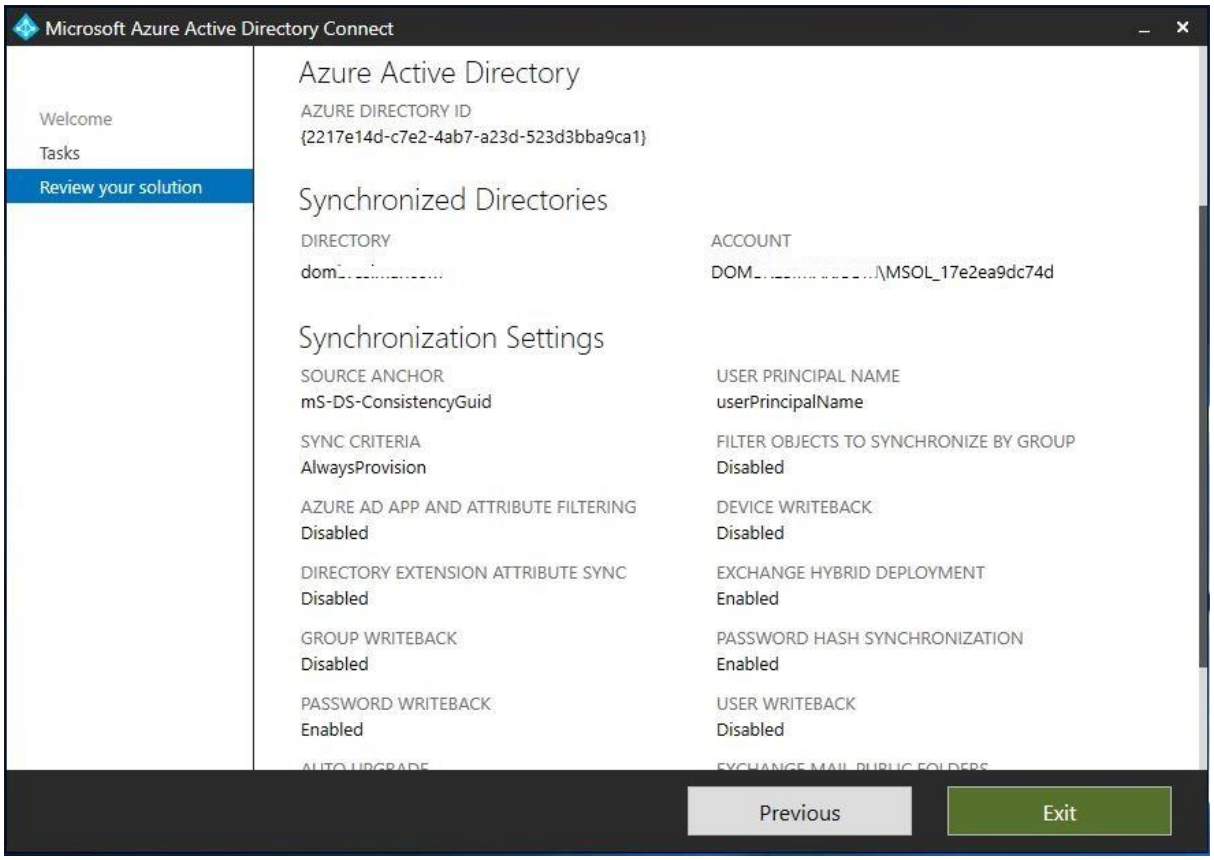

FIGURA 5.14 - PARÂMETROS *HYBRID AZURE AD JOIN* (MICROSOFT AZURE *ACTIVE DIRECTORY CONNECT*)

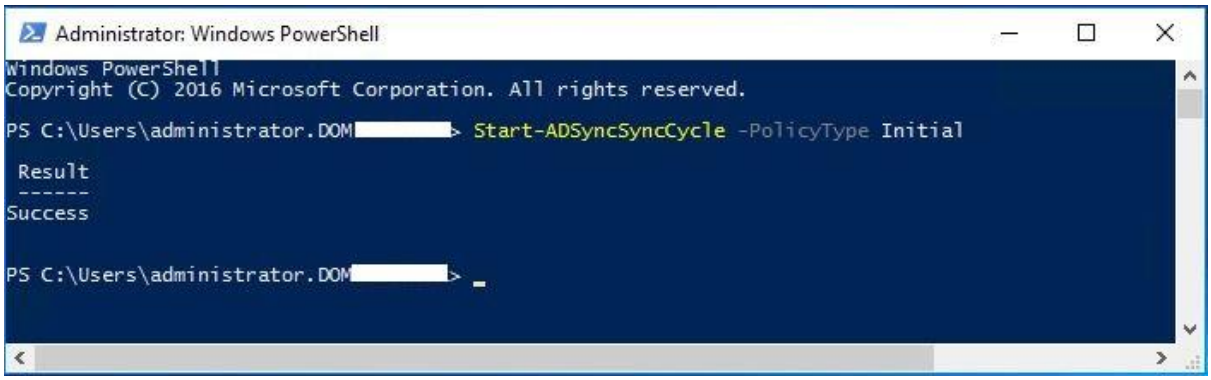

FIGURA 5.15 - COMANDO POWERSHELL DE SINCRONIZAÇÃO FORÇADA DA AD

Depois de sincronizados os utilizadores, no painel "Per-user MFA", definimos as regras que serão aplicadas por esta política de segurança. E avançamos para a activação da funcionalidade, em cada utilizador ou em *bulk* (Figuras 5.16, 5.17, 5.18 e 5.19).

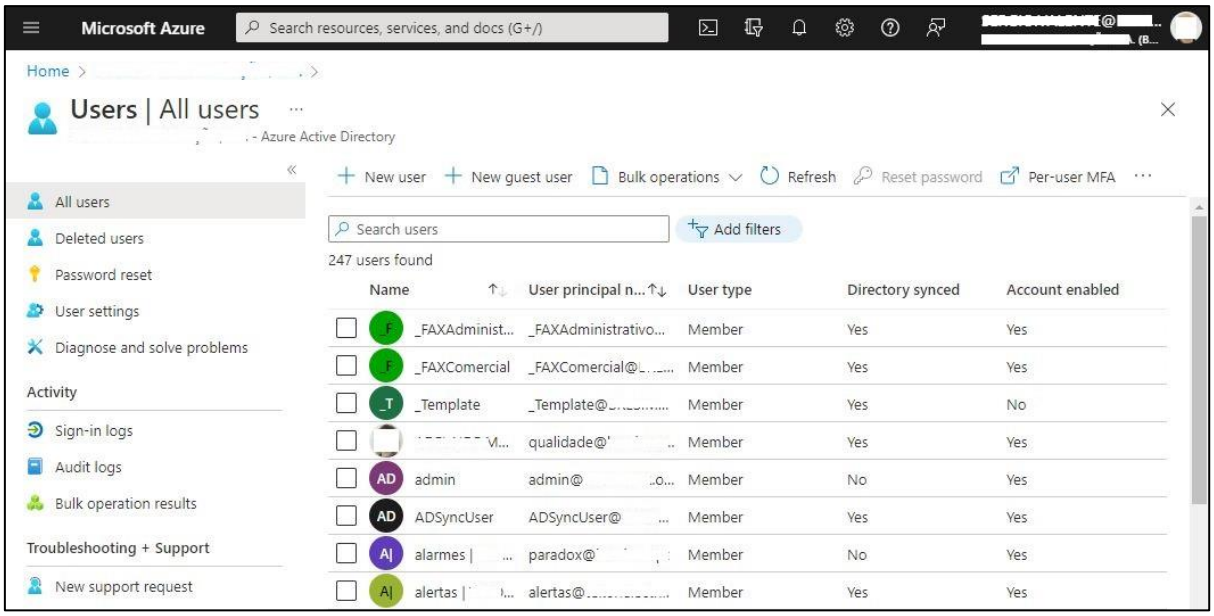

FIGURA 5.16 - MICROSOFT AZURE AD (*USERS*)

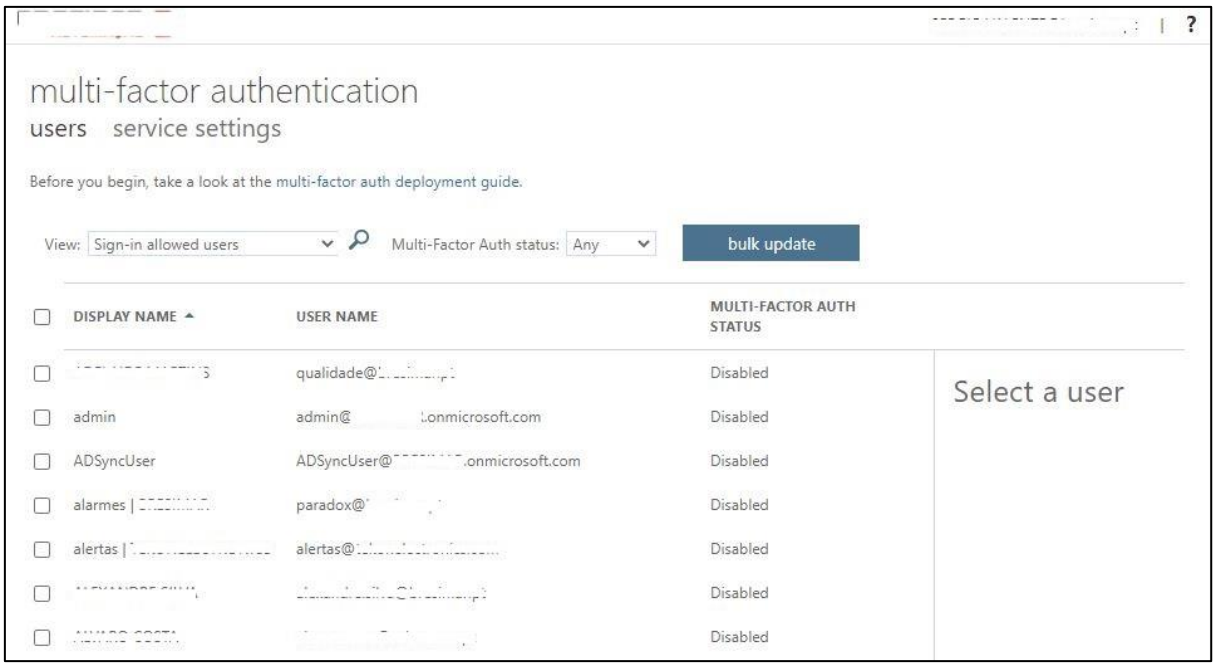

FIGURA 5.17 - MICROSOFT AZURE AD (*PER-USER MFA*)

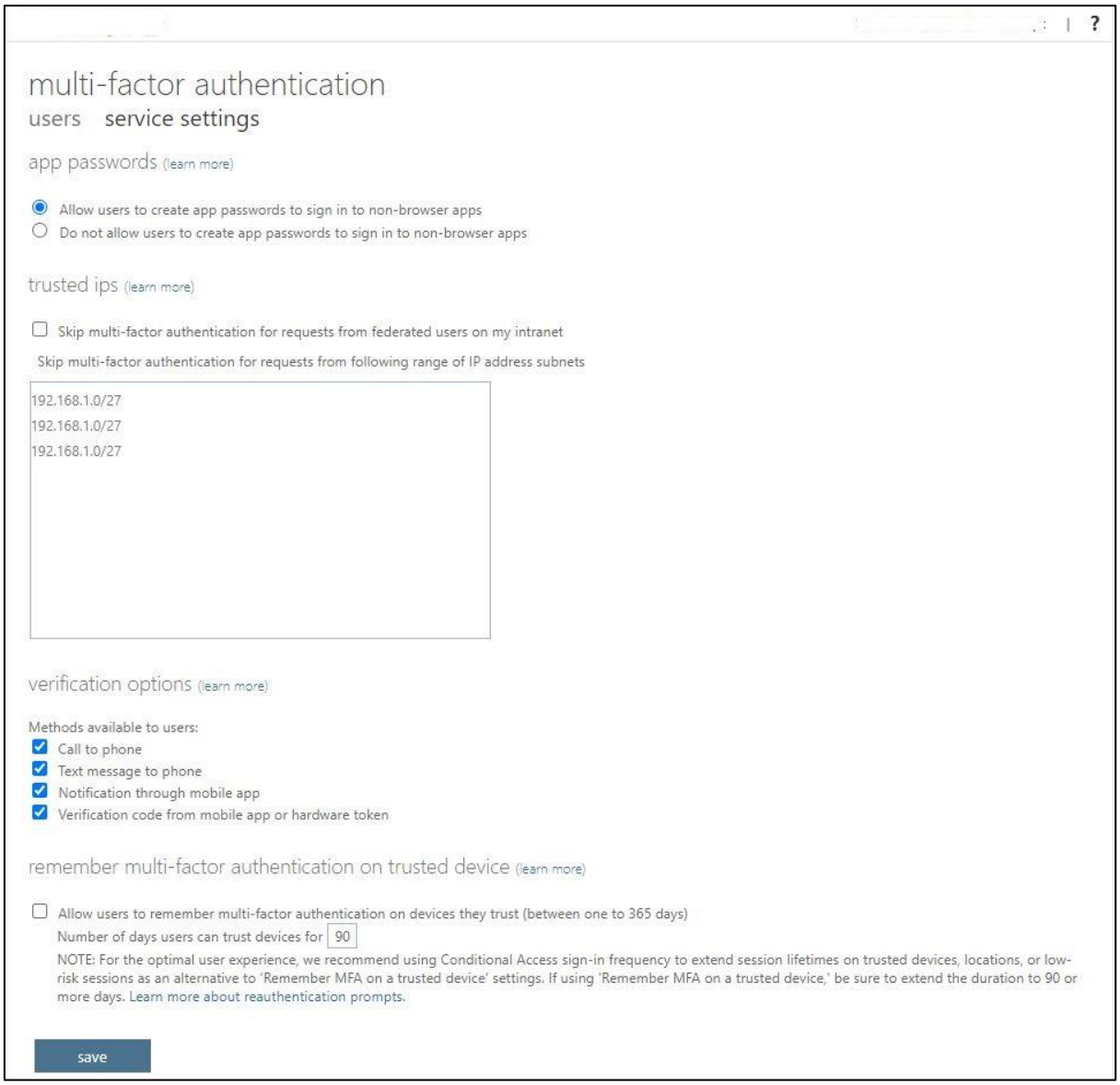

FIGURA 5.18 - MICROSOFT AZURE AD (*MFA SERVICE SETTINGS*)

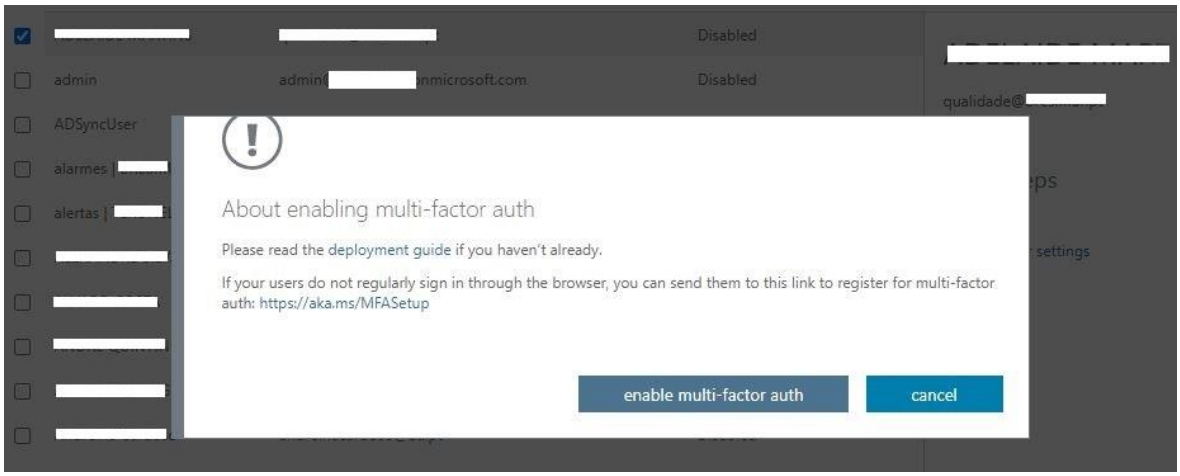

FIGURA 5.19 - MICROSOFT AZURE AD (*ENABLING MULTI-FACTOR AUTH*)

Podemos também fazer esta operação de forma centralizada e aplicada a todos os utilizadores, para isso vamos à área específica "Multi-factor Authentication", no portal do Azure (https://portal.azure.com/) (Figuras 5.20 e 5.21).

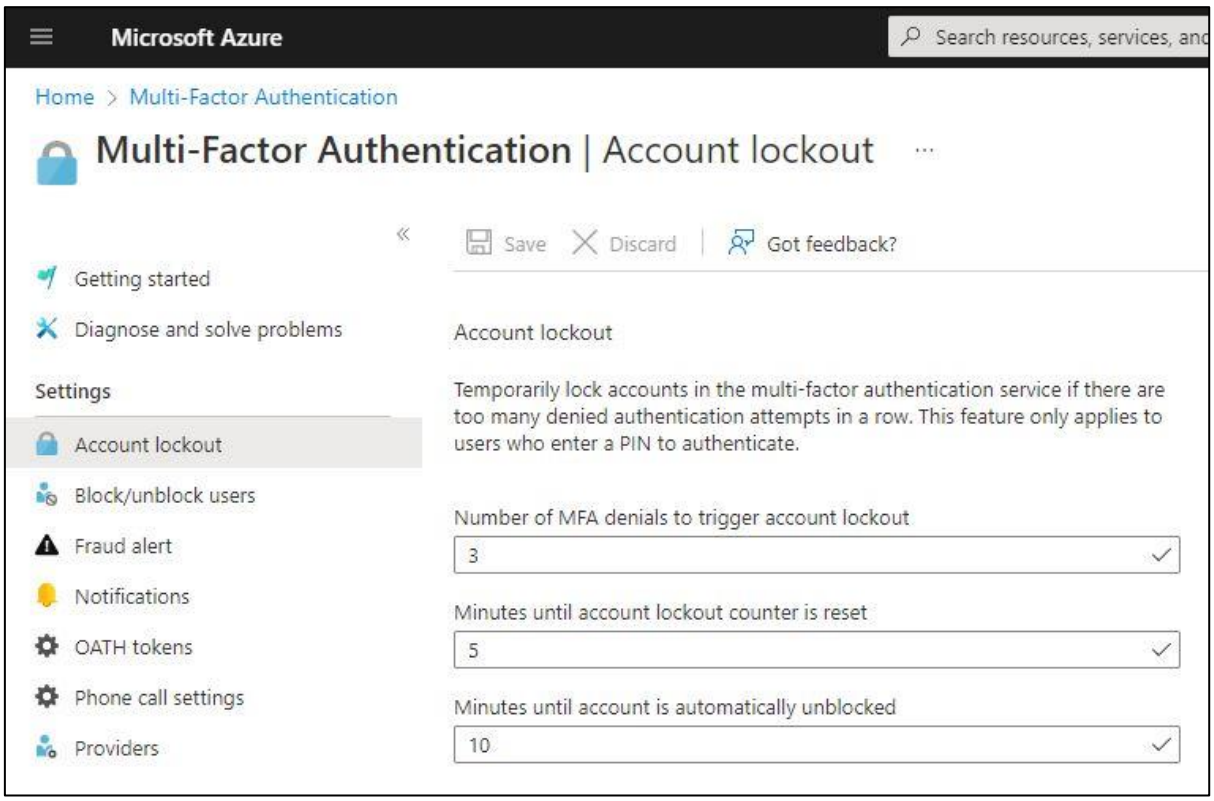

FIGURA 5.20 - MICROSOFT AZURE AD (*ACCOUNT LOCKOUT*)

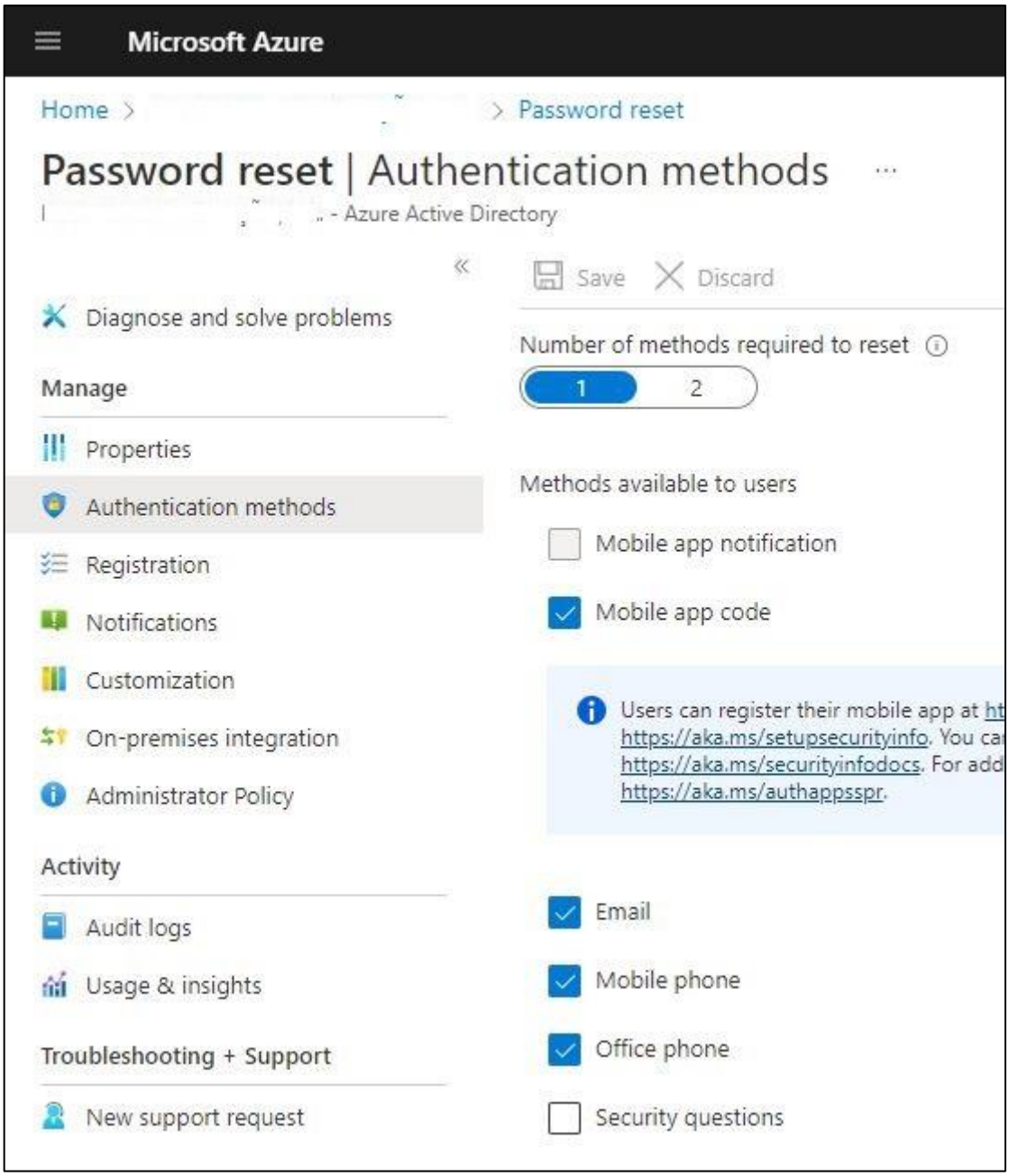

FIGURA 5.21 - MICROSOFT AZURE AD (*PASSWORD RESET*)

Por último, é criada a regra que aplica os parâmetros definidos ao grupo de segurança criado inicialmente. Nesta regra, criada na secção "Condicional Access", do portal Azure, conseguimos aplicar um conjunto de acções e condições que irão balizar o comportamento da regra propriamente dita. Por exemplo, qual o grupo a quem será aplicada, o que sucede se o utilizador falhar a autenticação um número de vezes, se tem permissões para aceder a determinadas *web apps*, etc. Outra possibilidade é a de criar zonas de exclusão, ou seja, podem ser adicionados os IP públicos da empresa, por exemplo, para que não seja solicitado

um segundo ou terceiro método de autenticação caso o acesso seja feito a partir dessa localização. Este é um método de tornar a segurança menos intrusiva, não requerendo aos utilizadores que executem o processo de MFA de todas as vezes que se autenticam ao longo do dia, desde que se encontrem nas instalações da empresa. Foi implementado exatamente nestes moldes, no nosso caso prático (Figuras 5.22, 5.23, 5.24 e 5.25).

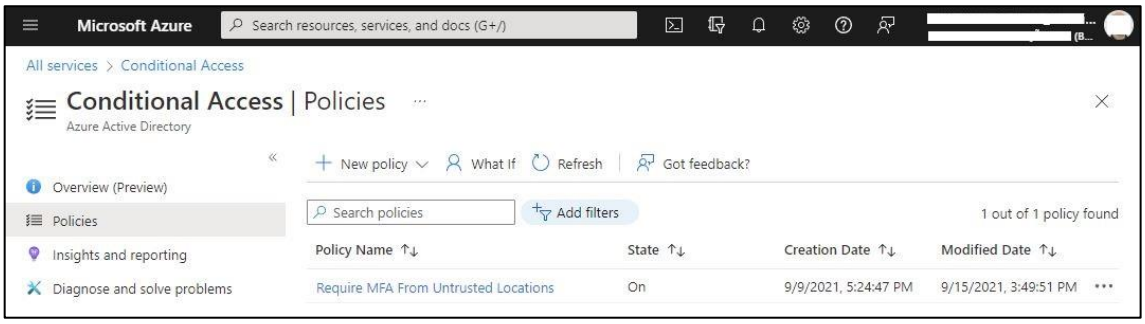

FIGURA 5.22 - MICROSOFT AZURE AD (CRIAÇÃO DE REGRA DE APLICAÇÃO)

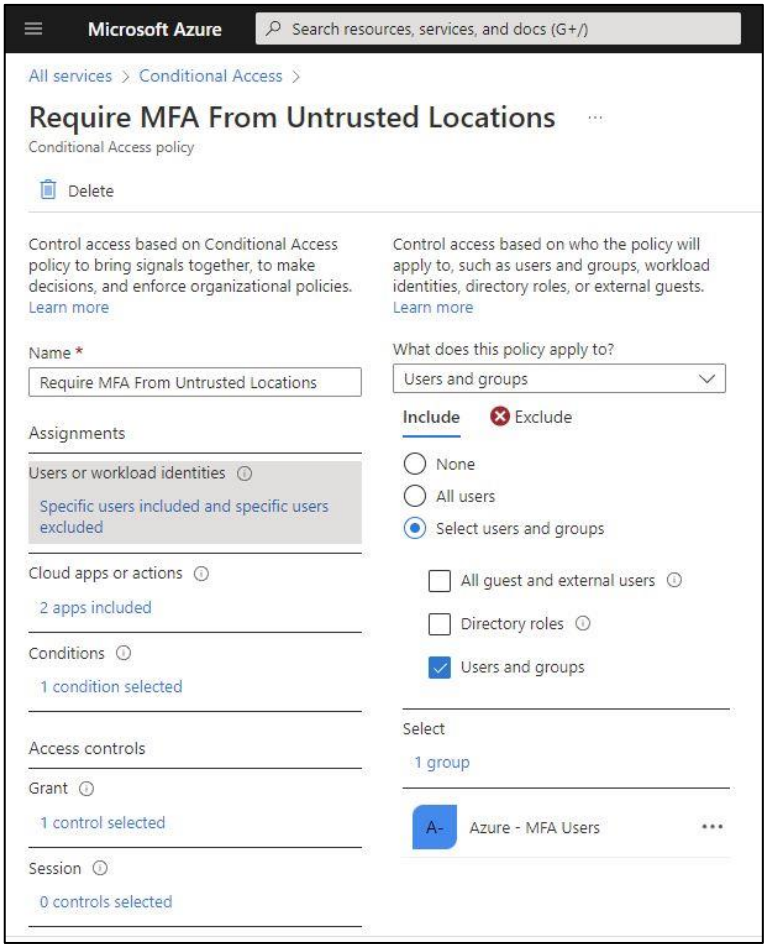

FIGURA 5.23 - MICROSOFT AZURE AD (PARAMETRIZAÇÃO DE REGRA DE APLICAÇÃO), 1/2

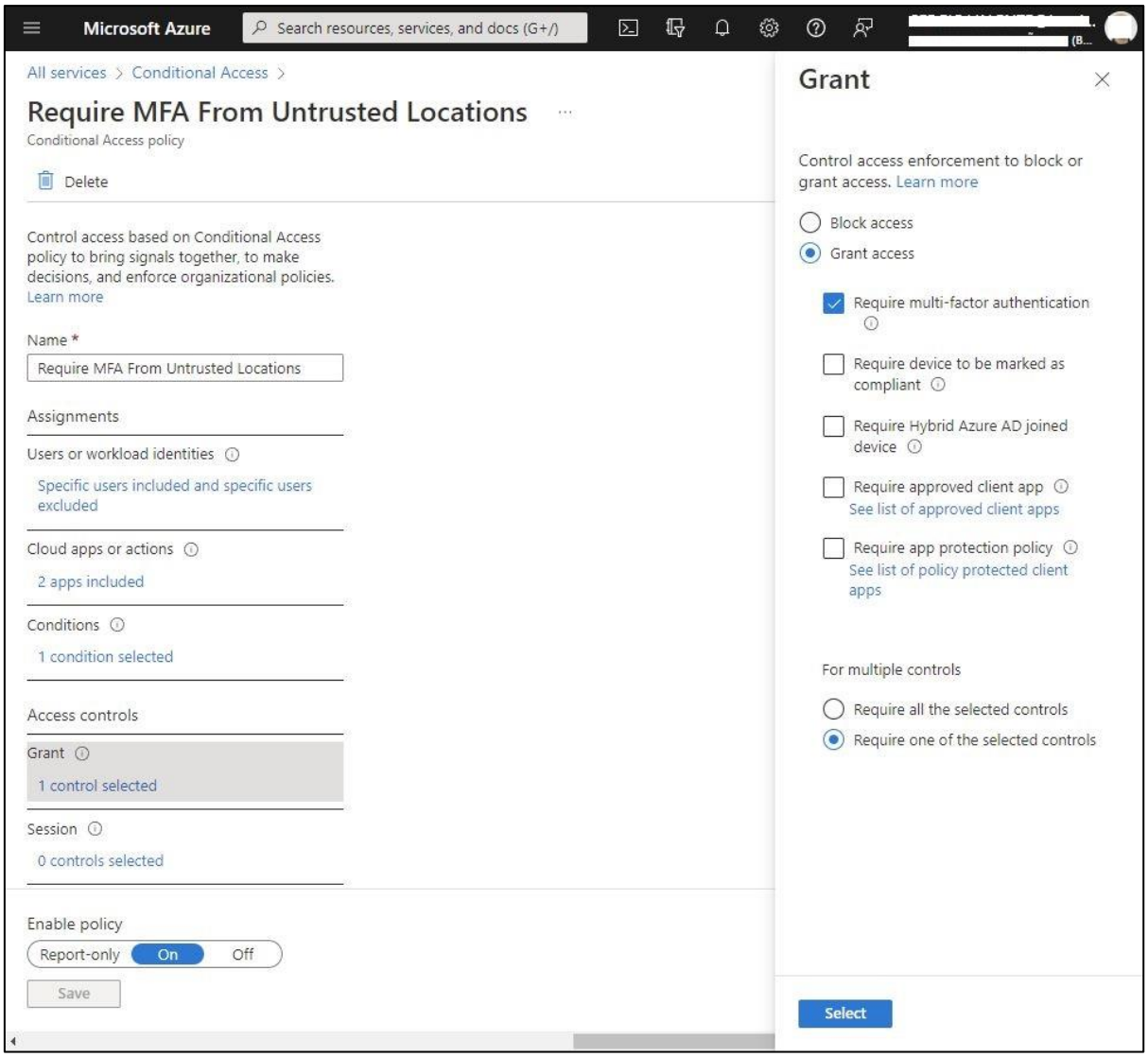

FIGURA 5.24 - MICROSOFT AZURE AD (PARAMETRIZAÇÃO DE REGRA DE APLICAÇÃO), 2/2

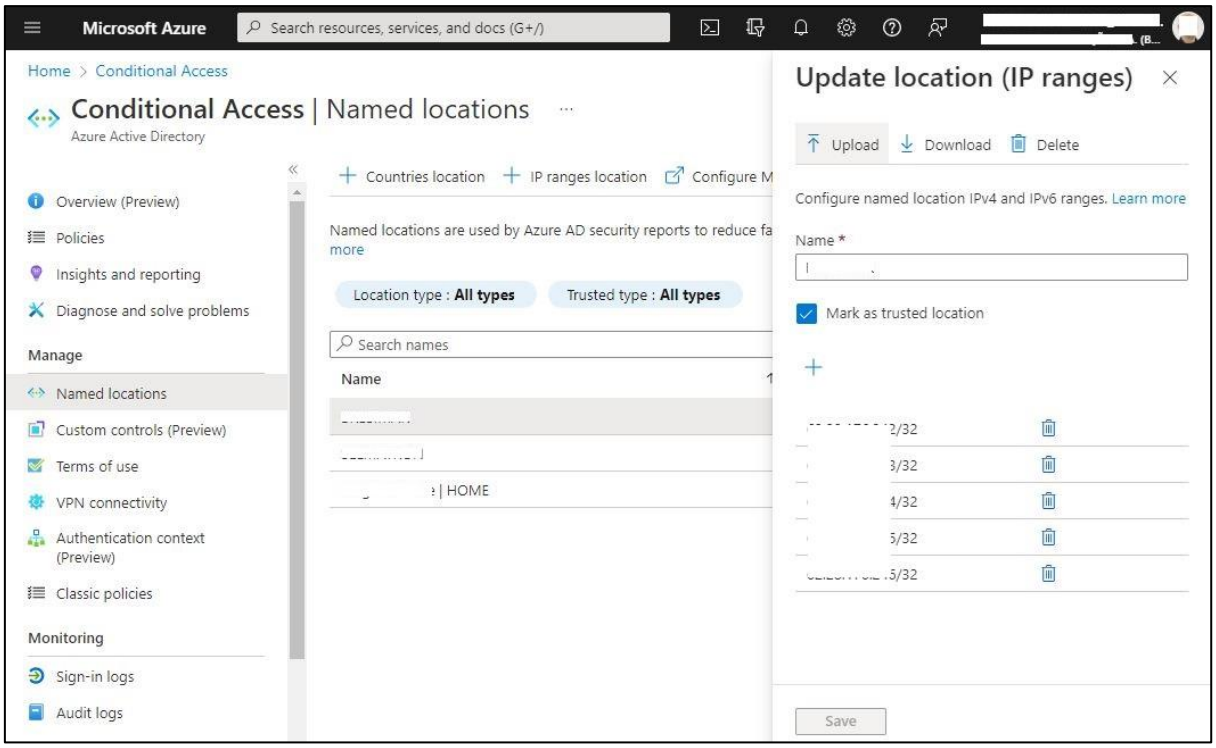

FIGURA 5.25 - MICROSOFT AZURE AD (*TRUSTED LOCATIONS*)

5.1.4. Microsoft Intune: Bitlocker e ATP

Uma outra implementação recomendada é a encriptação dos discos dos dispositivos das PME. Se considerarmos que apenas 23% dos inquiridos no nosso questionário indicam que os dados da empresa são menos valiosos do que o que custa protegê-los, conseguimos perceber que, apesar de estes terem muito valor para as empresas, o investimento necessário é um claro obstáculo a fazê-lo. A encriptação dos dados é, provavelmente, uma das formas menos dispendiosas e mais simples de acrescentar alguma protecção aos dados das organizações. Desta forma, implementou-se a encriptação dos discos dos computadores portáteis, grupo mais vulnerável por via da mobilidade inerente, através da plataforma Microsoft Intune (*Cloud*), uma forma de rentabilizar, para a organização, o investimento já existente no licenciamento Microsoft 365. Simultaneamente, foi também implementada uma solução antivirus baseada na *Cloud*, o Microsoft ATP. Este é outro modo de optimizar recursos financeiros de investimento, outro indicador relevante que podemos retirar do nosso questionário, visto que a subscrição engloba o licenciamento necessário para a utilização desta tecnologia.

Mais uma vez, para que as regras que são criadas na *Cloud*, neste caso no portal do Microsoft Intune (https://endpoint.microsoft.com/), é necessário acrescentar as máquinas

que queremos que tenham os discos encriptados com Bitlocker a um grupo de segurança da Active Directory. Assim como para que sejam aplicadas nas máquinas as regras de segurança do Microsoft ATP, também é necessário que seja adicionado o grupo de segurança ao respectivo objecto da AD. Para o nosso caso, adicionámos as máquinas pretendidas aos dois grupos: “Intune - Bitlocker Computers” e “Intune - Windows Defender Regular Profile”. Relembramos que, caso estas alterações sejam feitas na versão on-premises da AD, é necessário que esta seja sincronizada com a Azure Active Directory, o que ocorre com regularidade de forma automática, mas pode ser forçado, da forma que vimos anteriormente, com o respectivo comando *PowerShell* (Figura 5.36).

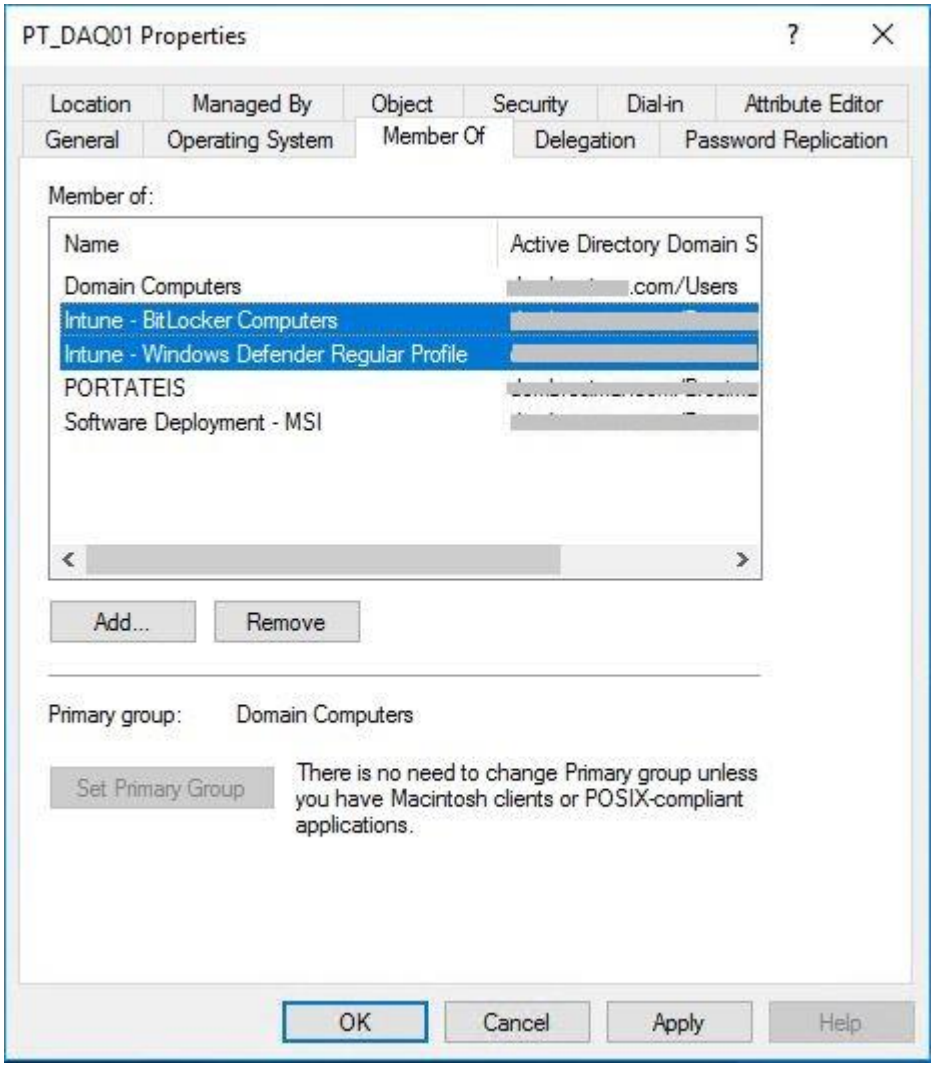

FIGURA 5.26 - ATRIBUIÇÃO DE GRUPOS DE SEGURANÇA A OBJECTOS DA AD (BITLOCKER E ATP)

À semelhança do procedimento para implementar MFA, também no caso do Bitlocker, é necessário criar uma regra que defina as condições a aplicar nas máquinas. É aqui que é parametrizado o tipo de encriptação, quais os discos e qual o grupo de segurança da AD onde a regra irá actuar. Depois de implementada e os discos serem efectivamente encriptados com Bitlocker, na página dos dispositivos conseguimos ver as respectivas chaves de identificação e chaves de recuperação (Figuras 5.27, 5.28 e 5.29).

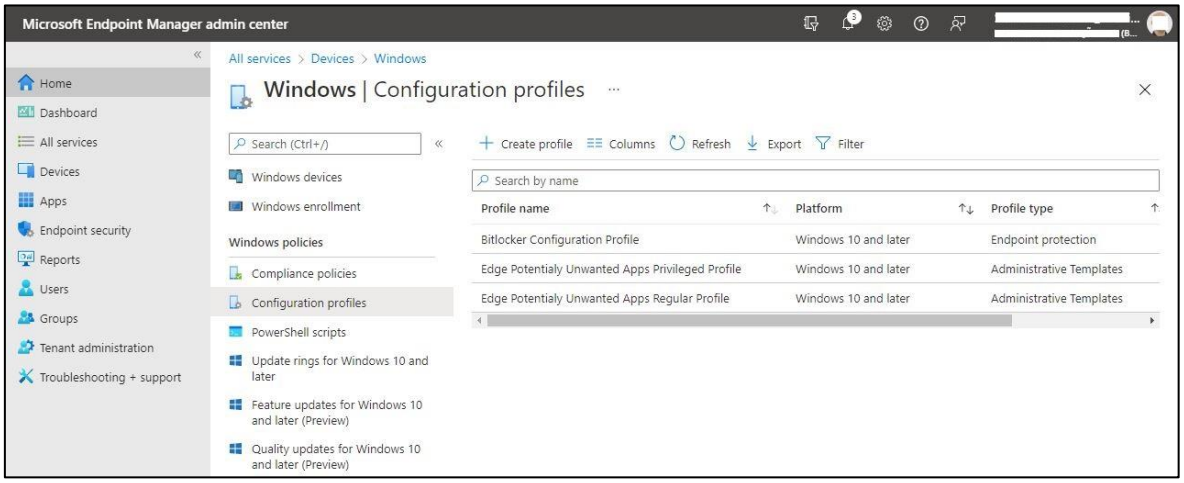

FIGURA 5.27 - CRIAÇÃO DE PERFIS PARA UTILIZAÇÃO NA REGRA DE BITLOCKER (MICROSOFT AZURE)

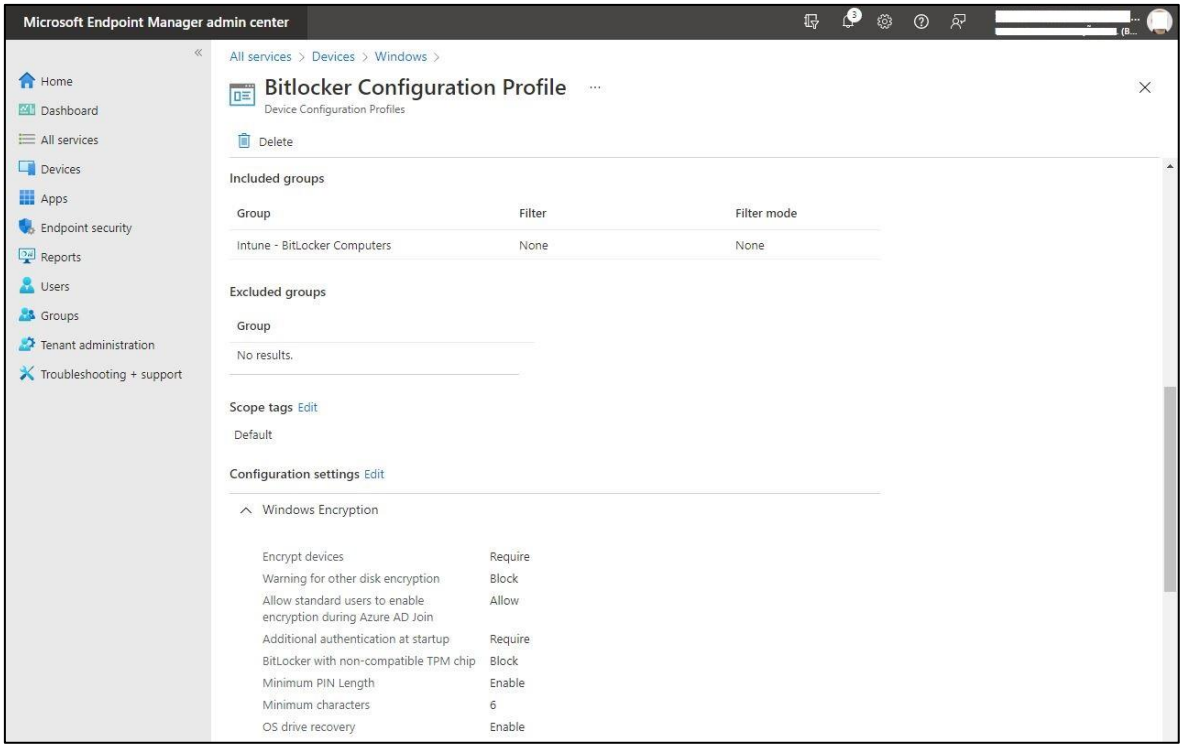

FIGURA 5.28 - PARÂMETROS DA REGRA DE APLICAÇÃO DO BITLOCKER (MICROSOFT AZURE)

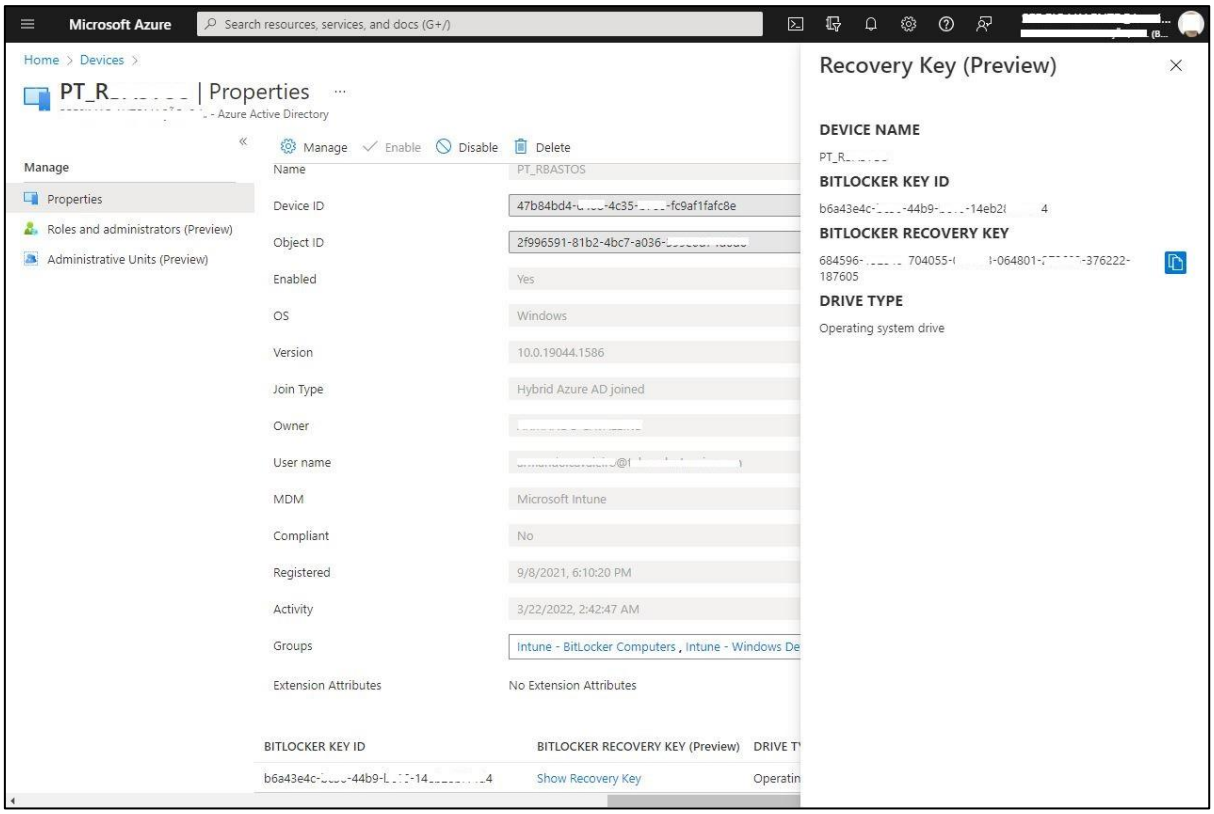

FIGURA 5.29 - CHAVES DO BITLOCKER NO PAINEL DO DISPOSITIVO (MICROSOFT AZURE)

Mais uma vez, aplica-se o mesmo conceito de aplicação de regras a grupos de segurança, relativamente à implementação do Microsoft ATP. Depois de atribuídos os grupos aos utilizadores que queremos que sejam protegidos pela regra do ATP, é necessário criá-la, no portal do Intune. Na secção de "Antivirus" configuramos a regra que permite parametrizar várias propriedades, como a exclusão de directorias, ficheiros ou extensões, o nível de criticidade ou o grupo de segurança da AD a que se aplica, por exemplo. Depois de a regra ser aplicada nos terminais, é possível gerar relatórios e configurar alarmística, o que permite ter um nível de controlo elevado sobre o grau de exposição que existe na empresa, ao nível dos vírus informáticos, assim como permite identificar, por exemplo, quais os utilizadores que têm comportamentos de risco (Figuras 5.30, 5.31 e 5.32).

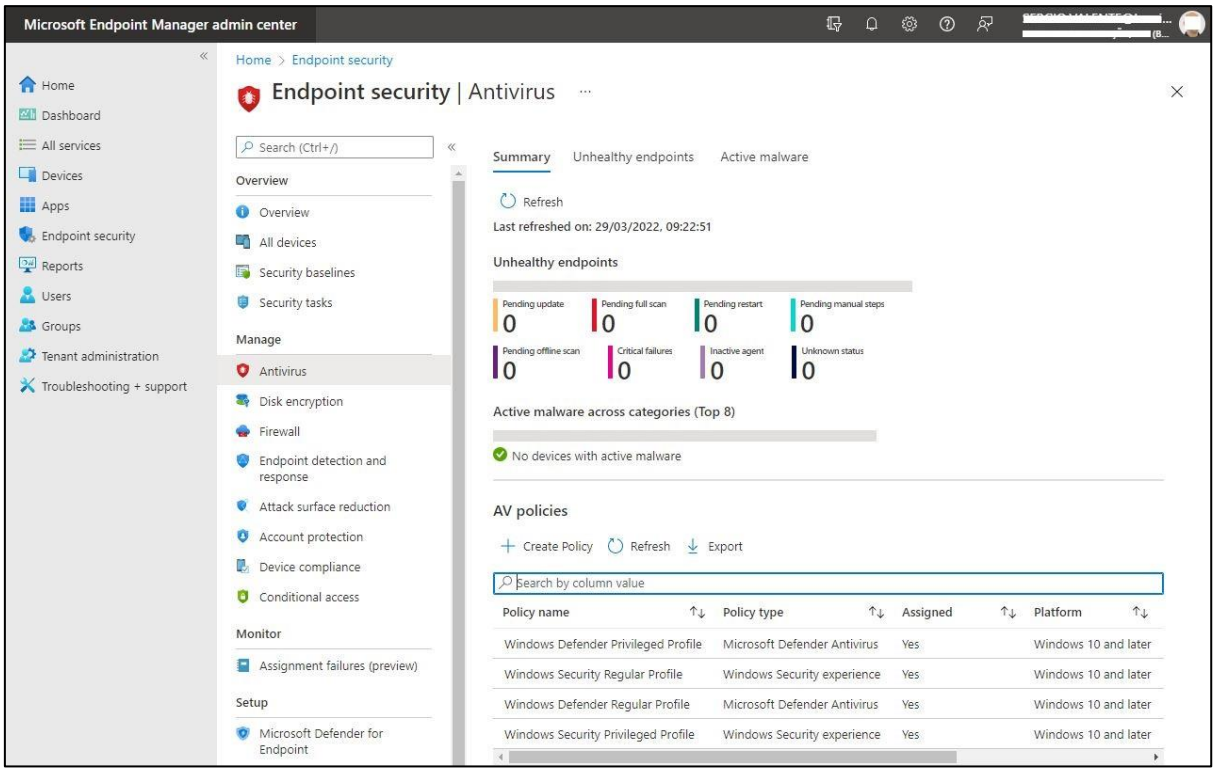

FIGURA 5.30 - CRIAÇÃO DE PERFIS PARA APLICAÇÃO DE MICROSOFT ATP (MICROSOFT AZURE)

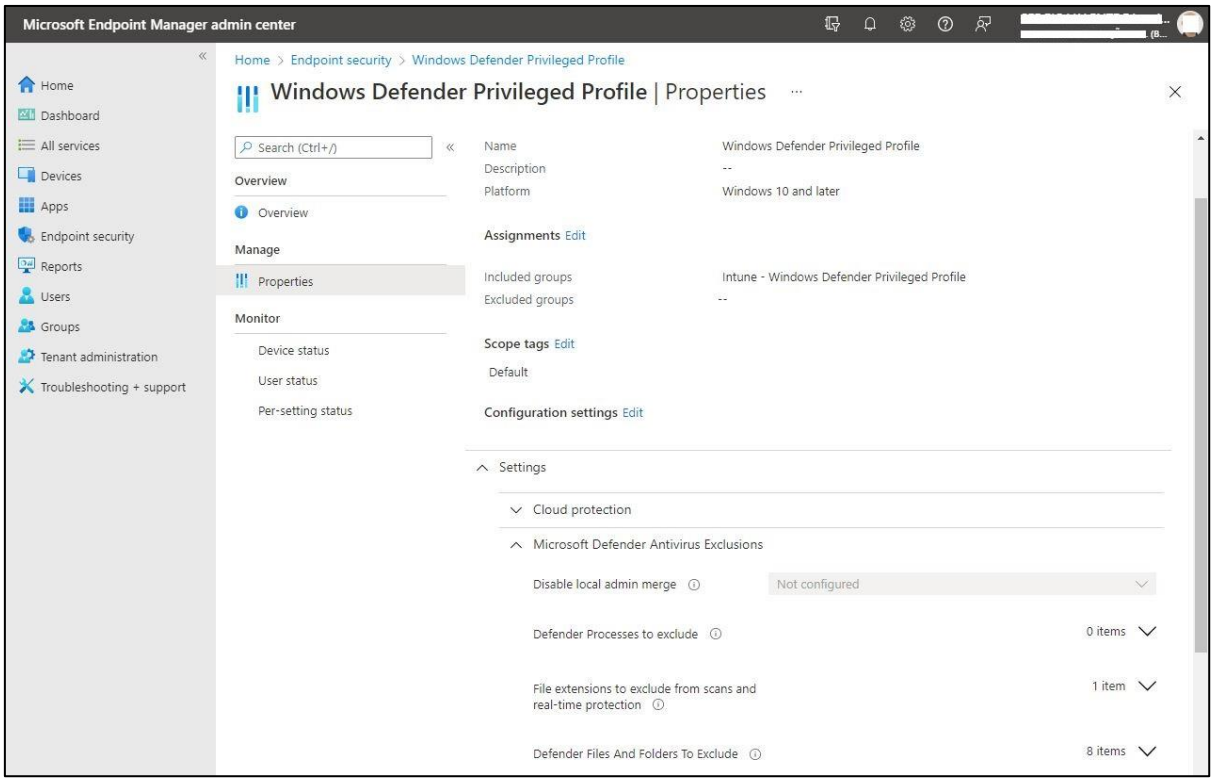

FIGURA 5.31 - PARÂMETROS DA REGRA DE APLICAÇÃO DE MICROSOFT ATP (MICROSOFT AZURE)

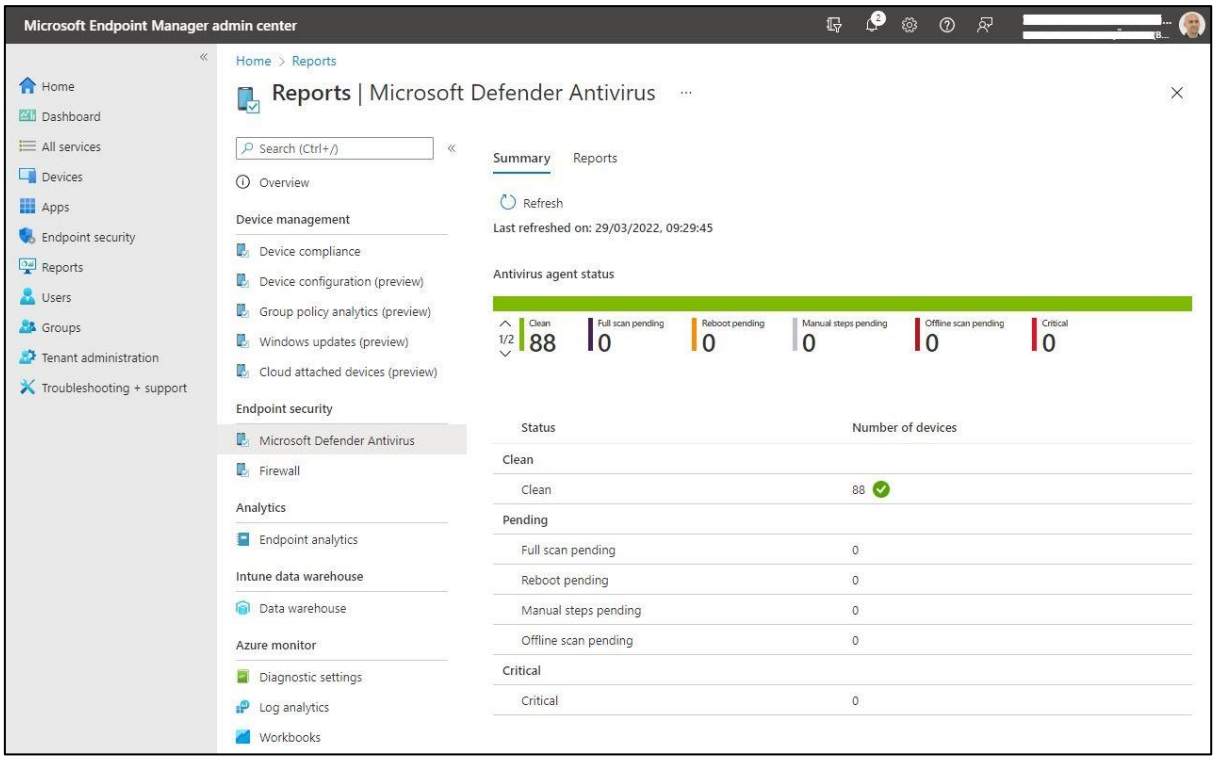

FIGURA 5.32 - RELATÓRIOS DO MICROSOFT DEFENDER ANTIVIRUS (MICROSOFT AZURE)

Uma questão muito relevante, que importa salientar ainda neste ponto, é a efectividade comprovada desta implementação, ilustrada com muita clareza nos dois exemplos seguintes, onde o facto de existirem estas tecnologias implementadas foi decisivo na protecção de dados sensíveis da empresa e potencialmente na continuidade do negócio.

O primeiro caso, refere-se ao furto do computador portátil de um funcionário da empresa, com responsabilidades de direcção, cujos dados não foram extraviados pois a encriptação do disco rígido dessa máquina eliminou esse risco. No segundo caso, um colaborador da empresa conectou o seu computador portátil numa rede empresarial de um cliente, tendo sido alvo de tentativas de intrusão que geraram alertas imediatos para o administrador de sistemas (Figura 5.33), tendo sido assim possível actuar com celeridade e mitigar o risco.

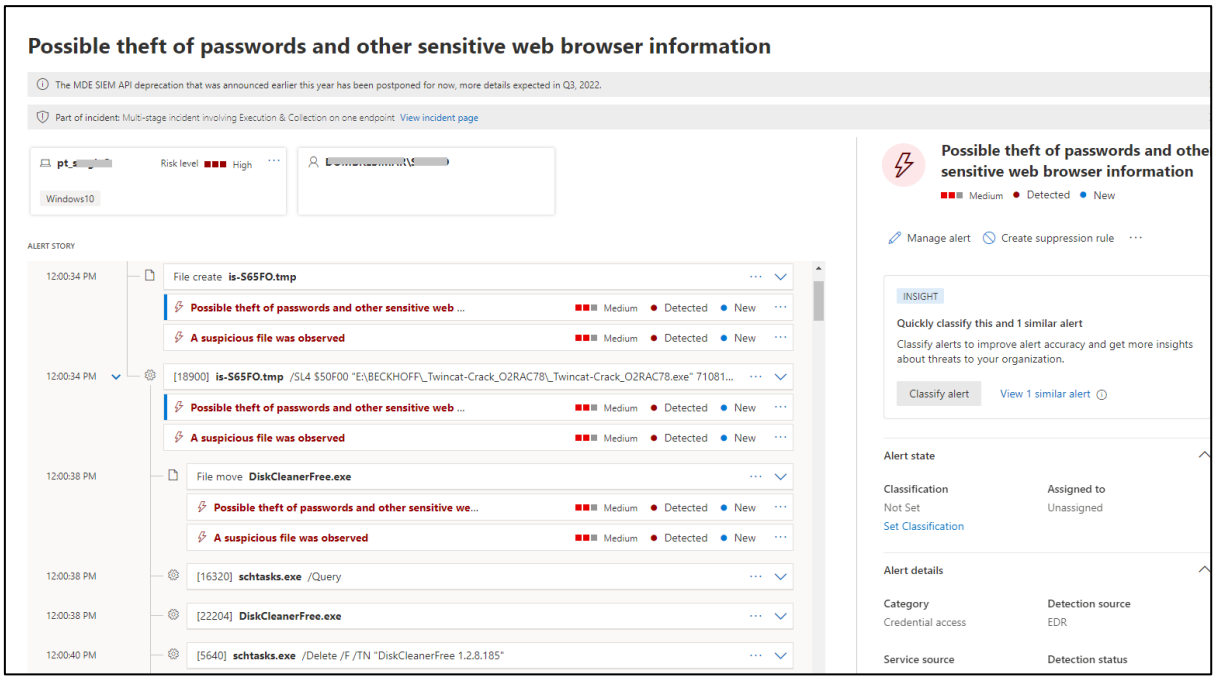

FIGURA 5.33 – ALERTAS MICROSOFT ATP

5.1.5. Formação aos utilizadores sobre Cibersegurança

Por último, e em grande alinhamento com as respostas obtidas no questionário, apresenta-se um plano de formação simples, para os colaboradores das PME tomarem consciência das envolvências da Cibersegurança. Relembrando, 47,04% dos inquiridos, considera que o principal vector de entrada de ataques informáticos nas empresas, são as pessoas. Este número é bastante impressionante, quando olhamos apenas para as respostas dos profissionais de TI das PME, em Portugal. Neste caso, 78,95% afirma que são as pessoas os principais alvos destes ataques.

Posto isto, torna-se evidente a necessidade de trabalhar na consciencialização para as temáticas da Cibersegurança e da mitigação do cibercrime dos profissionais destas empresas. Foi, por este motivo, desenhado um plano de formação que consiste na elaboração de um manual de boas-práticas, incluído como anexo neste documento (Anexo I), que servirá dois propósitos. Primeiramente, passará a fazer parte da documentação entregue a todos os novos colaboradores da empresa do nosso caso particular de estudo, juntamente com o manual de boas-vindas, regulamento interno, etc.; E, em segundo lugar, servirá de suporte a uma sessão de formação e esclarecimento anual, com duração de uma a duas horas, e cuja implementação será proposta à empresa como parte integrante do plano de formação anual dos seus colaboradores.

6. Conclusão

Considerando que o tecido empresarial português é constituído em 99,9% por PME (PORDATA, 2022), e que, numa sociedade cada vez mais digitalizada, onde os negócios são feitos a cada minuto, com base em sistemas de comunicação altamente informatizados, é fundamental perceber qual o grau de consciencialização para as matérias da Cibersegurança e qual a capacidade de mitigação do cibercrime existentes nestas empresas. É imperativo, portanto, de modo a garantir que as empresas portuguesas têm capacidade para assegurar a continuidade do negócio, avaliar se elas estão preparadas para acompanhar esta transformação global das últimas décadas, onde a exposição a factores de ameaça à segurança digital ditam novos paradigmas. Desde logo, a necessidade de investimentos orientados especificamente para a Cibersegurança e a sua viabilidade no contexto destas empresas. A implementação de práticas procedimentais mais adequadas, assim como a aposta em tecnologias mais modernas e robustas do ponto de vista da segurança, e a reavaliação do próprio perfil técnico dos seus colaboradores.

Os resultados do questionário elaborado revelam que a literacia dos profissionais das PME em Portugal, no âmbito das questões da Cibersegurança, é insuficiente. Apesar de haver familiarização com alguns dos tipos mais frequentes de ataques, como é o caso do *Ransomware*, por exemplo, ou com tipos de software malicioso mais comuns, como os *vírus* ou o *spyware*, a verdade é que existe um elevado grau de desconhecimento acerca de vários tipos de ataque que têm altos níveis de incidência, como são disso exemplo os casos dos ataques de *DDoS* ou *Zero-day-Exploit*. Este desconhecimento, necessariamente, acaba por remeter estas empresas para um elevado grau de exposição ao cibercrime, especialmente se considerarmos que, de acordo com os resultados obtidos, o principal vector de entrada dos ciberataques nas empresas são as pessoas.

No entanto, não devemos precipitar-nos na atribuição das responsabilidades pelas consequências deste tipo de ameaças. Seria redutor excluir deste contexto a baixa capacidade – ou disponibilidade – de investimento na área da Cibersegurança que existe, de forma generalizada, nas PME portuguesas. Investimento este que se manifesta quer ao nível da contratação e/ou requalificação de quadros, quer ao nível da aquisição de tecnologia específica de mitigação do cibercrime, seja em equipamentos ou serviços. Este fenómeno é particularmente visível na ausência de implementação de tecnologias MFA, combinada com uma estratégia de não regulamentação ou controlo, quer dos dispositivos, quer dos acessos aos sistemas e plataformas informáticas destas empresas. Ainda assim, existe uma clara noção da importância que a Cibersegurança representa para a continuidade do negócio, o

que parece comprovar a teoria de que será efectivamente uma questão de incapacidade financeira a estar na origem desta baixa propensão para estes investimentos.

Apesar do exposto, existe uma área tecnológica onde o investimento futuro parece ser mais consensual. Falamos da *Cloud*. Cerca de dois terços das respostas ao nosso questionário apontam no sentido da existência de investimentos em tecnologias na *Cloud*, o que, dada a tendência para os fabricantes deste tipo de plataformas ou sistemas embeberem cada vez mais metodologias de segurança nos seus produtos, poderá ser um indicador de que, naturalmente, estas empresas possam acabar por estar mais protegidas. Se a isto juntarmos a maior facilidade de implementações específicas de segurança, potencialmente com custos de aquisição e manutenção menores, podemos estar perante uma boa solução para aumentar os níveis de segurança digital das PME, no médio e longo prazo. Isto acaba por ser um bom indício, em particular, quando consideramos que uma larga maioria dos profissionais de PME, em Portugal, considera que o custo financeiro de proteger os dados das empresas é, pelo menos semelhante, mas muitas vezes inferior ao valor que os próprios dados têm para a empresa.

Maximizar a probabilidade dos colaboradores adoptarem boas-práticas de Cibersegurança, pode reduzir o risco e os custos associados a violações de dados ou intrusões. Muitas vezes estes profissionais, ocupados com as suas próprias responsabilidades, assumem que existem medidas adequadas de protecção, capazes de mitigar as consequências de qualquer erro de segurança seu. Além de poderem ver algumas restrições ou regras como um obstáculo ao seu trabalho, o que pode levá-los a um caminho de facilitismo (Craw et al., 2020). Desta forma, torna-se fulcral aumentar o nível de literacia dos profissionais das PME, para conseguir elevar o grau de consciencialização para a Cibersegurança. Uma boa estratégia para o alcançar poderá passar por fazer os colaboradores sentir que são parte da solução e que têm um papel não só activo, como também determinante neste processo. Para que interiorizem que, independentemente do investimento que as empresas façam em tecnologia, produtos ou serviços, o factor humano continua a existir e a ser decisivo. E apenas investindo no seu esclarecimento e na sua formação, será possível alcançá-lo. Pois a segurança de todos, neste contexto, depende absolutamente de cada acção individual.

6.1. Trabalho futuro

Nos dias de hoje, cada vez é mais incomum depararmo-nos com ambientes ou sistemas estanques. Vivemos num mundo em constante mutação, característica intrínseca a

uma globalidade altamente tecnológica. Isto significa que o trabalho de manter os sistemas informáticos seguros, em teoria, nunca está verdadeiramente terminado. Assim, enquanto proposta de continuidade para este estudo, a abrangência de possibilidades é enorme, ainda que a monitorização das tecnologias implementadas seja das mais imediatas. No fundo, avaliar em que medida, preferencialmente de forma quantificável, a tecnologia implementada contribui efectivamente para mitigar ataques. Da mesma forma que validar o grau de autonomia e capacidade dos colaboradores para avaliar quando se encontram perante uma ameaça e como agir em conformidade.

Um bom exemplo de um meio de avaliar a robustez dos sistemas, quer ao nível tecnológico, quer no que concerne à literacia e consciencialização dos colaboradores, pode ser a implementação de "*Pen tests*" periódicos. Ou seja, testes de penetração, também conhecido como *hacking* ético. São ciberataques simulados e autorizados num sistema, realizados para avaliar a segurança desse sistema.

Outra possível continuidade a este trabalho poderá passar pela elaboração de um estudo comparativo com a realidade vivida noutras geografias e que se encontre devidamente documentada em estudos semelhantes a este. Ou seja, poderia ser pertinente avaliar em que difere a realidade portuguesa daquela que está presente em países tecnologicamente e economicamente mais avançados, como os Estados Unidos da América, por exemplo, assim como comparar também com países com menos desenvolvimento tecnológico presente no seu tecido empresarial, como alguns países africanos ou sul americanos, por exemplo. Neste estudo, seria também pertinente avaliar quais as causas para as divergências, no caso de existirem e de ser possível identificá-las.

7. Referências Bibliográficas

Bada, M. & Nurse, J. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security, 27* (83), 393-410. https://doi.org/10.1108/ICS-07-2018-0080

Bunker, G. (2020). Targeted cyber attacks: how to mitigate the increasing risk. *Network Security*, 2020(1), 17-19. https://doi.org/10.1016/S1353-4858(20)30010-6

Caravelli, J., & Jones, N. (2019). *Cyber security: Threats and responses for government and business*. ABC-CLIO.

Emer, A., Unterhofer, M. & Rauch, E. (2021). A cybersecurity assessment model for small and medium-sized enterprises. *IEE Engineering Management Review, 49* (2) 98-109. https://doi.org/10.1109/EMR.2021.3078077

Goethals, P. L., & Hunt, M. E. (2019). A review of scientific research in defensive cyberspace operation tools and technologies. Journal of Cyber Security Technology, 3(1), 1-46. https://doi.org/10.1080/23742917.2019.1601889

Lessig, L. (2009). *Code: And other laws of cyberspace*. Basic Books, Inc.

Manns, G. (2021). The Adoption of Cybersecurity in Small - to Medium-Sized Businesses: A correlation Study. A Dissertation Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy. Capella University, USA.

Miaoui, Y., & Boudriga, N. (2019). Enterprise security economics: A self-defense versus cyber-insurance dilemma. *Applied Stochastic Models in Business and Industry*, 35(3), 448-478. https://doi.org/10.1002/asmb.2451

Phan, K. (2018). Implementing Resiliency of Adaptive Multi-Factor. *Culminating Projects in Information Assurance*, 65, 1-95. Disponível em: https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1095&context=msia_etds

PORDATA - Base de Dados Portugal Contemporâneo (acedido em 30/03/2022). Disponível em: https://www.pordata.pt

Rashid, A., Chievers, H., Denezis, G., Lupu, E., & Martin, A. (Eds., 2019). *CyBOK - The Cyber Security Body of Knowledge*. Crown Copyright - The National Cyber Security Centre.

Santos, S. I. D. S. (2018). *Estudo das perceções de cibersegurança e cibercrime e das implicações na formulação de Políticas Públicas-estudo exploratório do caso português*. Dissertação de Doutoramento não publicada. Instituto Superior de Ciências Sociais e Políticas.

Sistema de Segurança Interna (2020). *Relatório Anual de Segurança Interna 2020*. Acedido em 29 de Janeiro, 2022, em https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3D%3DBQAAAB%2BLCAAAAAAABAAzNDQ1NAUABR26oAUAAAA%3D

Scholtz, T. (Ed., 2021). *Rethink the Security & Risk Strategy*. Gartner Inc. Acedido em 31 de Janeiro, 2022, em https://emtemp.gcom.cloud/ngw/globalassets/en/publications/documents/rethink-security-risk-strategy-ebook.pdf

8. Anexos

Anexo I: Cibersegurança, Consciencialização e mitigação do cibercrime - Guia Pedagógico

FIGURA 8.1 - GUIA PEDAGÓGICO, DIAPOSITIVO 1

O que é a Cibersegurança?

Microsoft

"A Cibersegurança, ou segurança digital, é a prática de proteger as suas informações digitais, dispositivos e recursos. O que inclui informações pessoais, contas, ficheiros, fotografias e até dinheiro."

Kaspersky

"Cibersegurança é o ato de proteger computadores e servidores, dispositivos móveis, sistemas eletrónicos, redes e dados contra ataques maliciosos."

FIGURA 8.2 - GUIA PEDAGÓGICO, DIAPOSITIVO 2

O que é o cibercrime?

O cibercrime é qualquer tipo de crime cometido eletronicamente.

Pode incluir:

- Roubo;
- Fraude;
- Tráfico, etc.

Exemplos

- roubo de identidade
- pedofilia
- crimes económicos
- violação de propriedade intelectual
- Malware
- engenharia social maliciosa

FIGURA 8.3 - GUIA PEDAGÓGICO, DIAPOSITIVO 3

Malware (software malicioso)

O que é?

Malware, ou software malicioso, é um termo genérico que descreve qualquer programa ou código malicioso que seja prejudicial para os sistemas.

Intencionalmente maldoso, tenta invadir, danificar ou incapacitar computadores, sistemas, redes, tablets e dispositivos móveis, assumindo, frequentemente, o controlo parcial das operações de um dispositivo.

Exemplos

- Ransomware
- Adware
- Botnets
- Rootkits
- Spyware
- Vírus
- Worms

FIGURA 8.4 - GUIA PEDAGÓGICO, DIAPOSITIVO 4

Ransomware, Spyware e Vírus

Ransomware

Um tipo de malware que impede os utilizadores de aceder ao seu sistema ou ficheiros pessoais e exige-lhes o pagamento de um resgate para devolver o acesso. Um dos métodos de infeção mais comuns é através de spam malicioso, que consiste em emails não solicitados, utilizados para enviar malware.

Spyware

Software malicioso que infeta o seu PC ou dispositivo móvel e que recolhe informações sobre si, os seus hábitos de navegação, de uso da internet e outros dados. Entra num computador sem que tenhamos conhecimento ou seja dada autorização, anexando-se ao sistema operativo.

Vírus

Um software malicioso, ou um pedaço de código executável, que infeta ficheiros e programas num computador. Abrir um ficheiro infetado faz com que o código do vírus seja executado, resultando em danos nos ficheiros, na máquina, e podendo comprometer a segurança na Internet.

FIGURA 8.5 - GUIA PEDAGÓGICO, DIAPOSITIVO 5

BOTs

O que são?

Um bot é uma aplicação de software programada para realizar determinadas tarefas. Os bots são automatizados e geralmente imitam ou substituem o comportamento de um utilizador humano. Normalmente, eles realizam tarefas repetitivas e podem fazê-las muito mais rápido do que os humanos.

Nem todos os bots são maus…

Nem todos os bots são maus. Quando usamos um motor de busca, esses resultados são possíveis, de forma tão rápida, pela ajuda de bots que percorrem a internet a indexar os conteúdos. Os "chatbots", como a Siri e Alexa, são outro tipo comum de bot "bom".

Bots maliciosos:

- Tentam adivinhar passwords
- Registam teclas pressionadas
- Obtêm informações financeiras
- Usam o nosso e-mail para enviar spam
- Abrem "backdoors" em dispositivos infetados

FIGURA 8.6 - GUIA PEDAGÓGICO, DIAPOSITIVO 6

Engenharia Social

Em que consiste?

Cibercriminosos tentam enganar-nos, usando informações comumente disponíveis em…

- Redes sociais
- Partilha de localização (GPS)
- Conversas pessoais
- Relações profissionais existentes ou comuns

Exemplos

- Phishing
- Pretexting
- Baiting
- Quid pro quo
- Tailgating
- Inside job
- Swatting

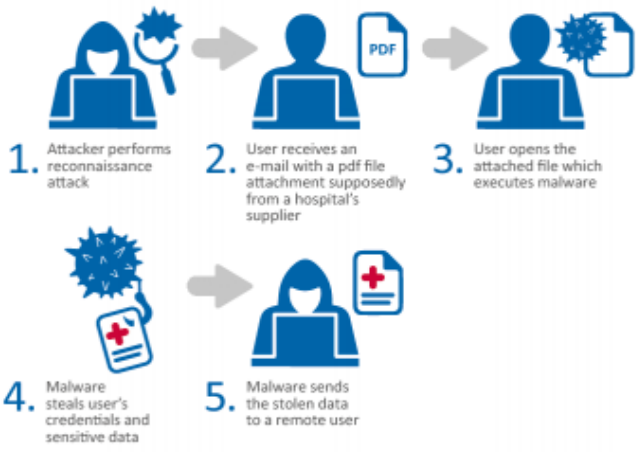

FIGURA 8.7 - GUIA PEDAGÓGICO, DIAPOSITIVO 7

Phishing

O que é?

Mensagens falsas de uma fonte aparentemente confiável ou respeitável projetada para convencer-nos a…

- Revelar informações
- Dar acesso não autorizado a um sistema
- Clicar num link
- Comprometer-se com uma transação financeira

Exemplos

- Emails
- Mensagens de texto
- Chamadas telefónicas
- Mensagens e posts em redes sociais
- Links suspeitos

FIGURA 8.8 - GUIA PEDAGÓGICO, DIAPOSITIVO 8

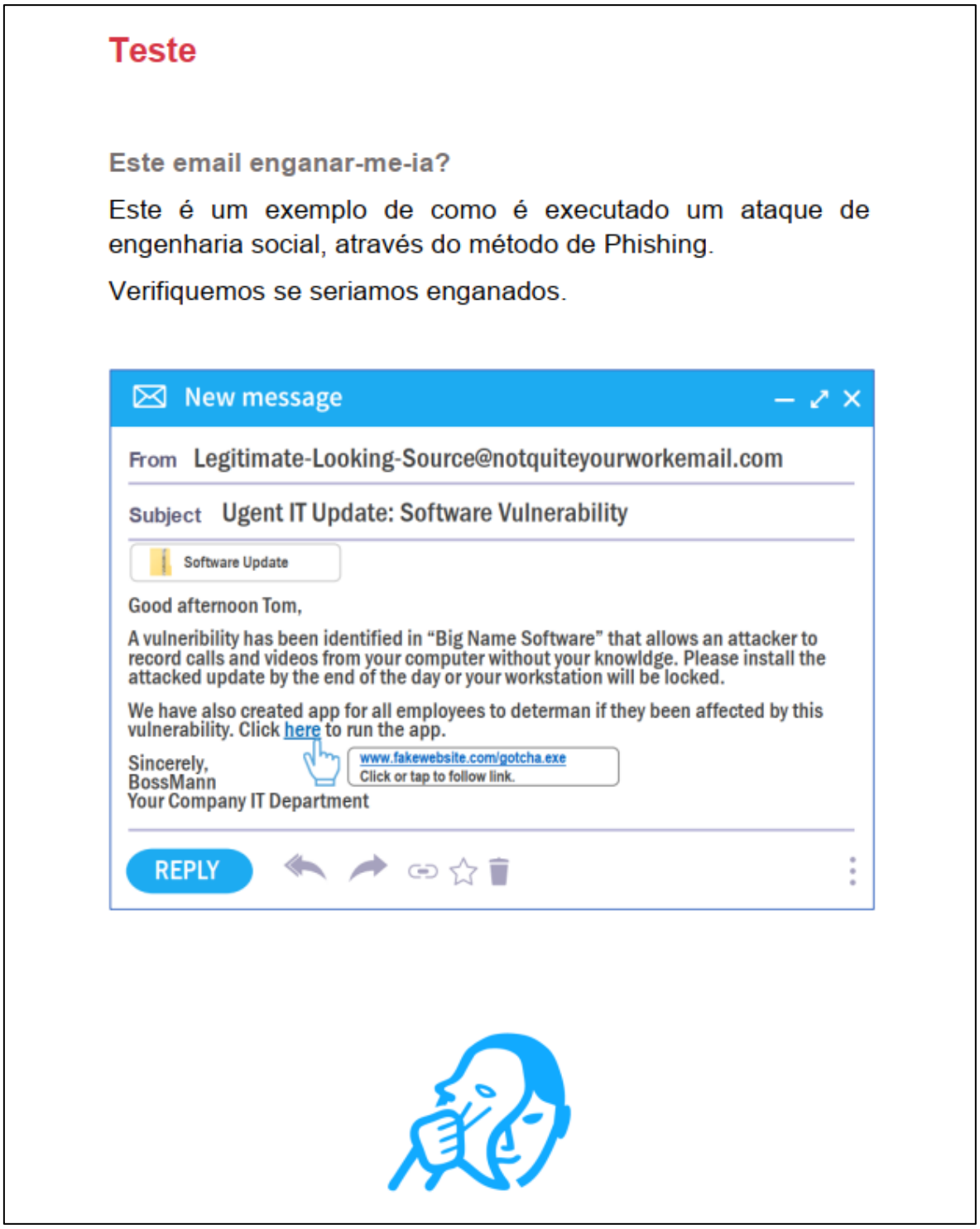

FIGURA 8.9 - GUIA PEDAGÓGICO, DIAPOSITIVO 9

Outras vias de ataque

Exemplos de vias usadas para ataques

- Internet de tudo (internet das coisas)
- Qualquer dispositivo conectado à rede
- Acesso remoto
- Bluetooth
- Portas abertas (firewall)

Porque nos devemos preocupar

- A rede pode ser usada para atacar outra pessoa
- Qualquer dispositivo que armazene informações ou esteja conectado à internet pode ser uma vulnerabilidade
- Assuma que é vulnerável e tome medidas para entender e mitigar o risco

Exemplos de dispositivos atacados

- Dispositivos inteligentes
- Telemóveis
- Termostatos
- Veículos
- Consolas de jogos
- Impressoras
- Equipamentos médicos
- Sistemas Industriais

FIGURA 8.10 - GUIA PEDAGÓGICO, DIAPOSITIVO 10

Como nos podemos proteger online?

Tornar as nossas redes seguras

Os routers wireless são uma maneira de os cibercriminosos acederem a dispositivos online. E as redes abertas são um alvo fácil para ataques.

Manter os dispositivos atualizados

Mantenha o software atualizado para as versões mais recentes e configure o software de segurança para executar verificações regulares.

Se é ligado, é protegido

Uma defesa comprovada contra invasões é a atualização para o software de proteção antivírus mais recente. Qualquer dispositivo que se liga à Internet deve estar protegido.

Dupla proteção na autenticação

Ativar a autenticação multifator (MFA), para garantir que a única pessoa quem tem acesso à sua conta é você. Usar pelo menos dois dos três tipos de elementos: algo que sabe (password), algo que possui (código via telemóvel), algo que é (biométricos).

FIGURA 8.11 - GUIA PEDAGÓGICO, DIAPOSITIVO 11

Passwords

Sabia que…?

Password Stuffing é um ataque que tenta "preencher" (stuffing) um nome de utilizador e password comprometidos, de um site para outro, na esperança de que os dados de autenticação usados, sejam os mesmos em várias plataformas.

Dicas para manter as suas passwords seguras

- Utilize passwords diferentes, em sistemas e contas diferentes
- Utilize o máximo de caracteres possível
- Utilize uma mistura de maiúsculas, minúsculas, algarismos e símbolos
- Reponha a sua password com frequência
- Utilize um software de gestão de passwords

FIGURA 8.12 - GUIA PEDAGÓGICO, DIAPOSITIVO 12

Anexo II: A Cibersegurança no contexto das pequenas e médias empresas portuguesas – Questionário

Secção: Identificação da Empresa

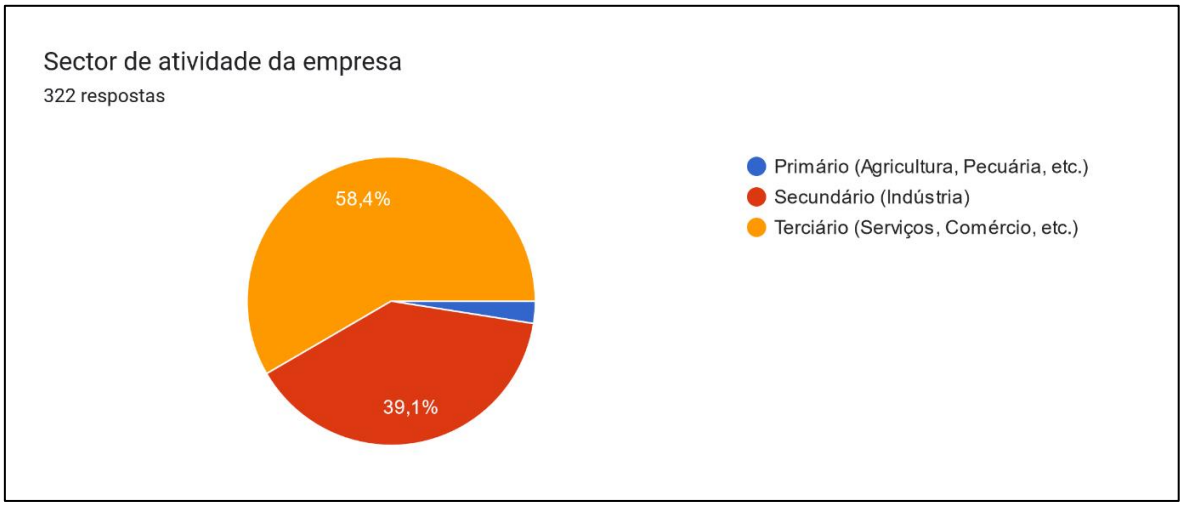

FIGURA 8.13 - QUESTIONÁRIO: SECTOR DE ACTIVIDADE DA EMPRESA

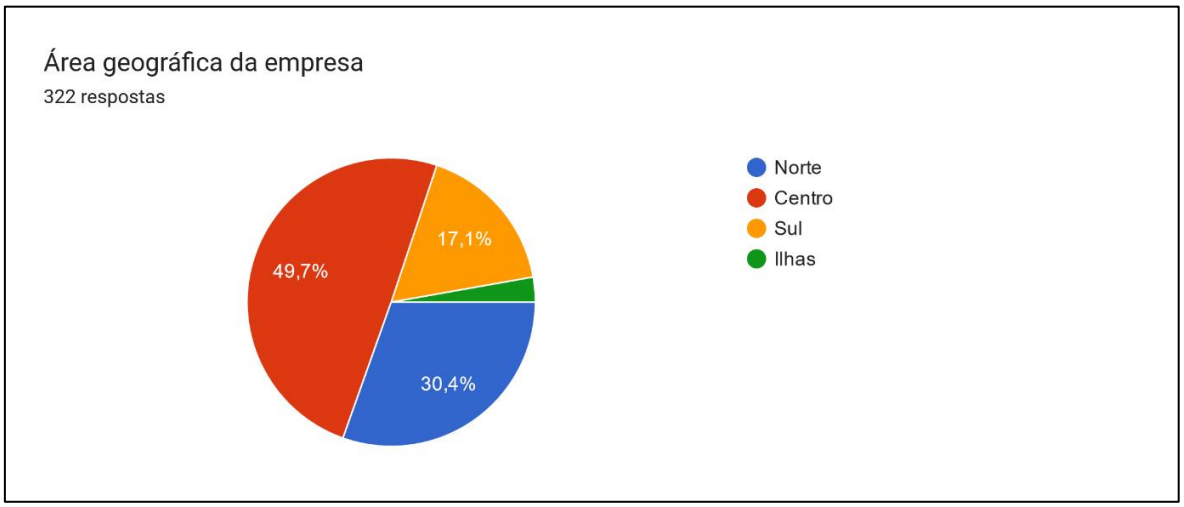

FIGURA 8.14 - QUESTIONÁRIO: ÁREA GEOGRÁFICA DA EMPRESA

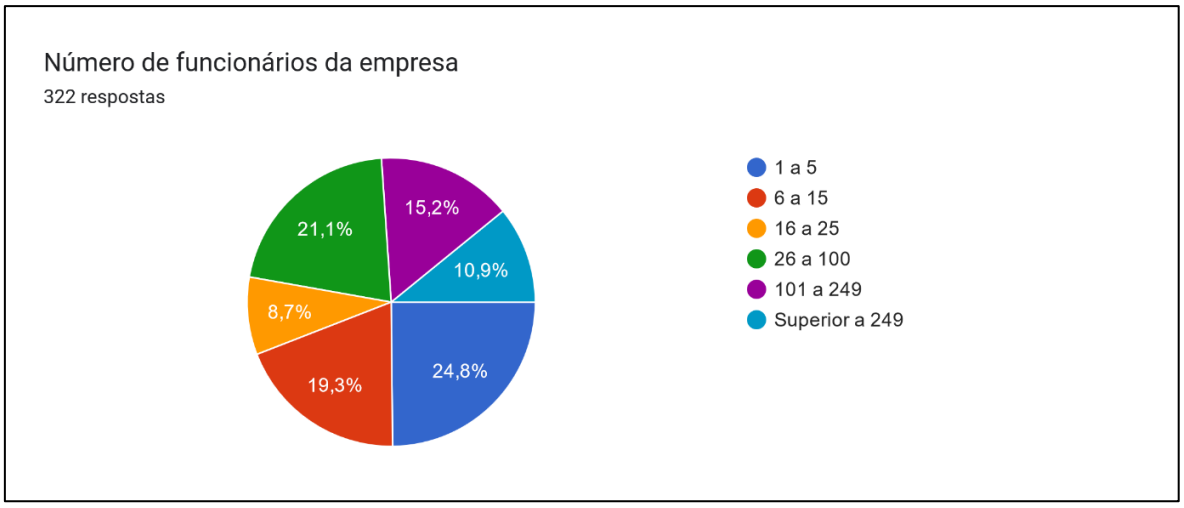

FIGURA 8.15 - QUESTIONÁRIO: NÚMERO DE FUNCIONÁRIOS DA EMPRESA

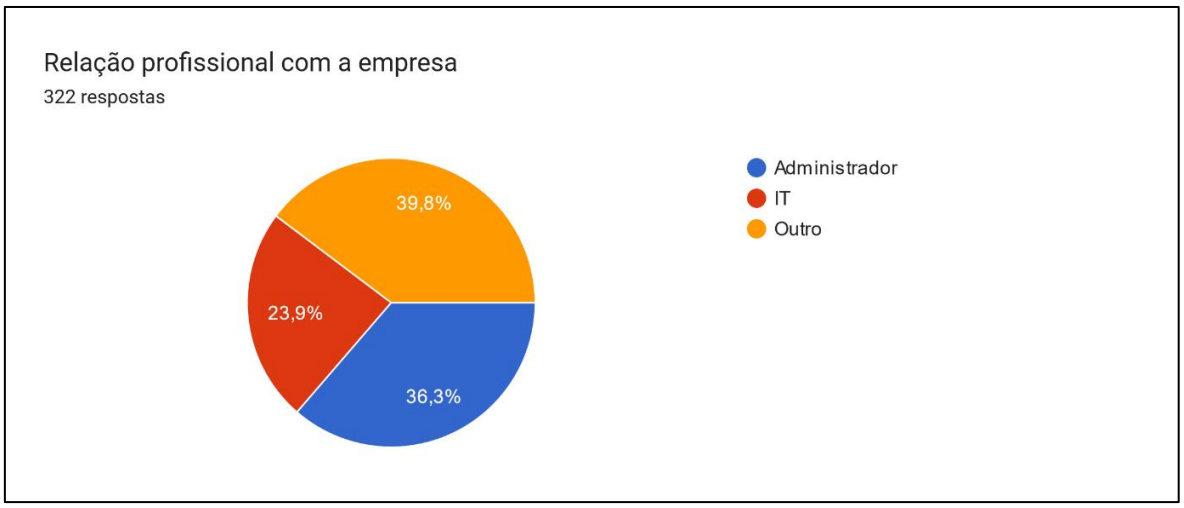

FIGURA 8.16 - QUESTIONÁRIO: RELAÇÃO PROFISSIONAL COM A EMPRESA

Secção: Consciencialização para os perigos

FIGURA 8.17 - QUESTIONÁRIO: JÁ FOI ALVO, OU TEM CONHECIMENTO DE ALGUMA EMPRESA QUE TENHA SIDO ALVO, DE UM ATAQUE INFORMÁTICO?

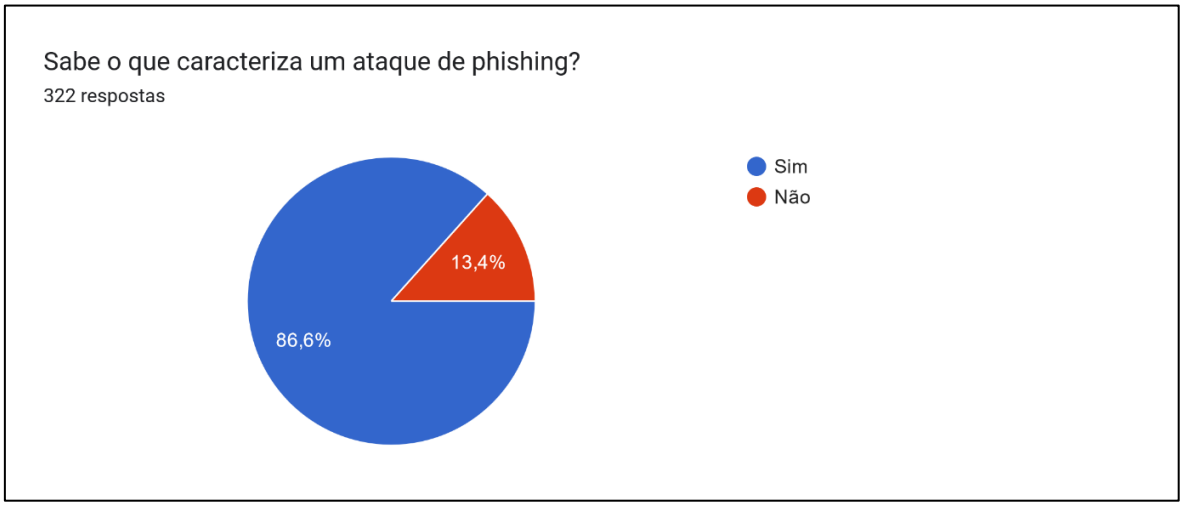

FIGURA 8.18 - QUESTIONÁRIO: SABE O QUE CARACTERIZA UM ATAQUE DE PHISHING?

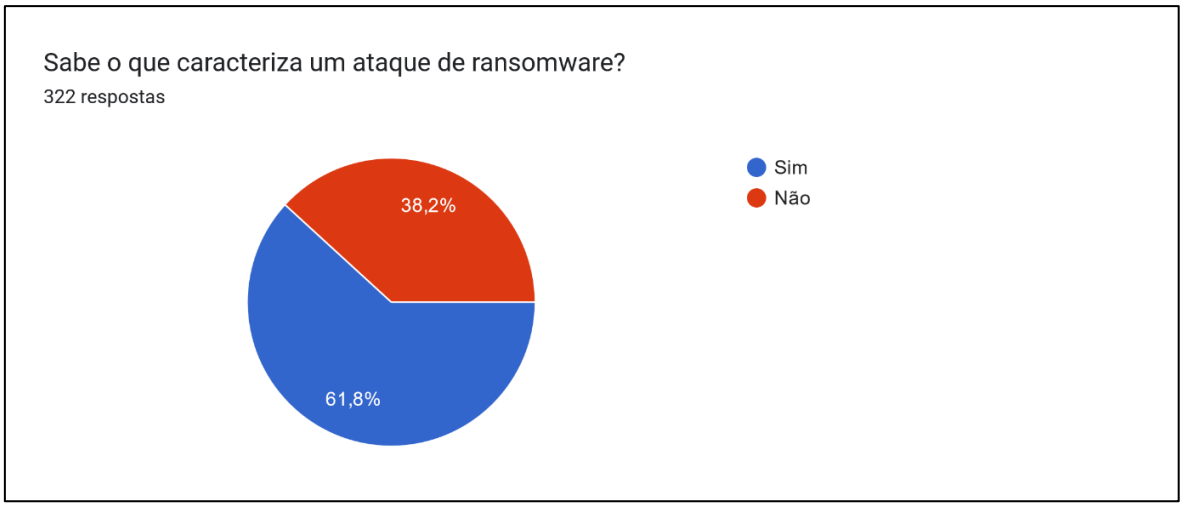

FIGURA 8.19 - QUESTIONÁRIO: SABE O QUE CARACTERIZA UM ATAQUE DE RANSOMEWARE?

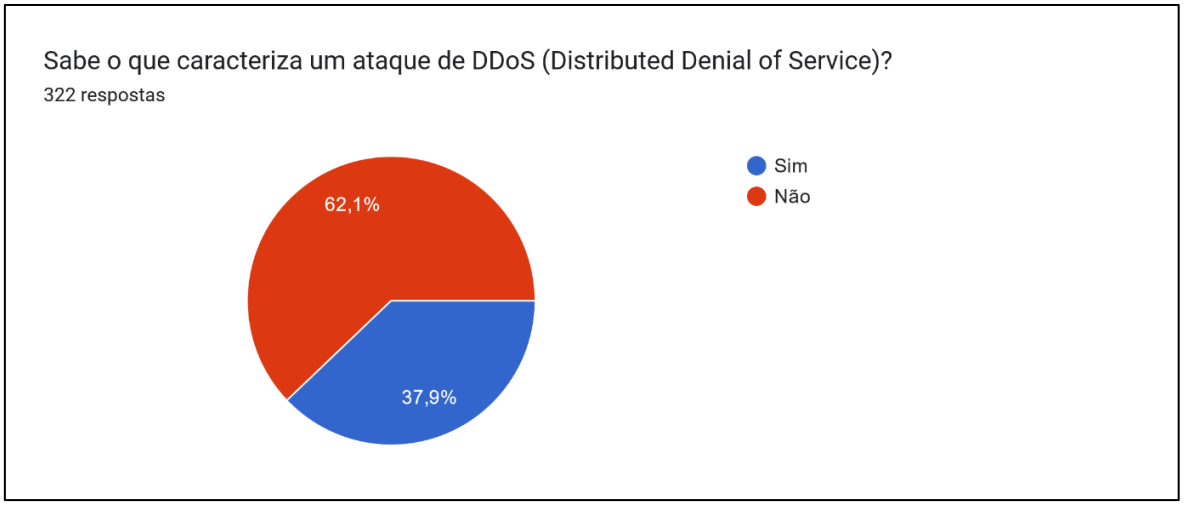

FIGURA 8.20 - QUESTIONÁRIO: SABE O QUE CARACTERIZA UM ATAQUE DE DDOS (DISTRIBUTED DENIAL OF SERVICE)?

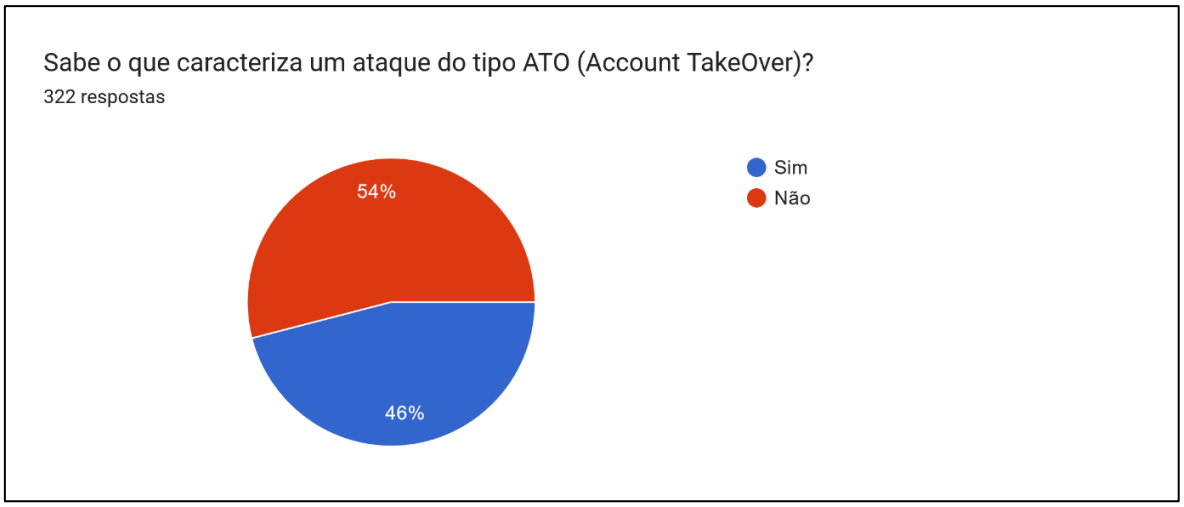

FIGURA 8.21 - QUESTIONÁRIO: SABE O QUE CARACTERIZA UM ATAQUE DO TIPO ATO (ACCOUNT TAKEOVER)?

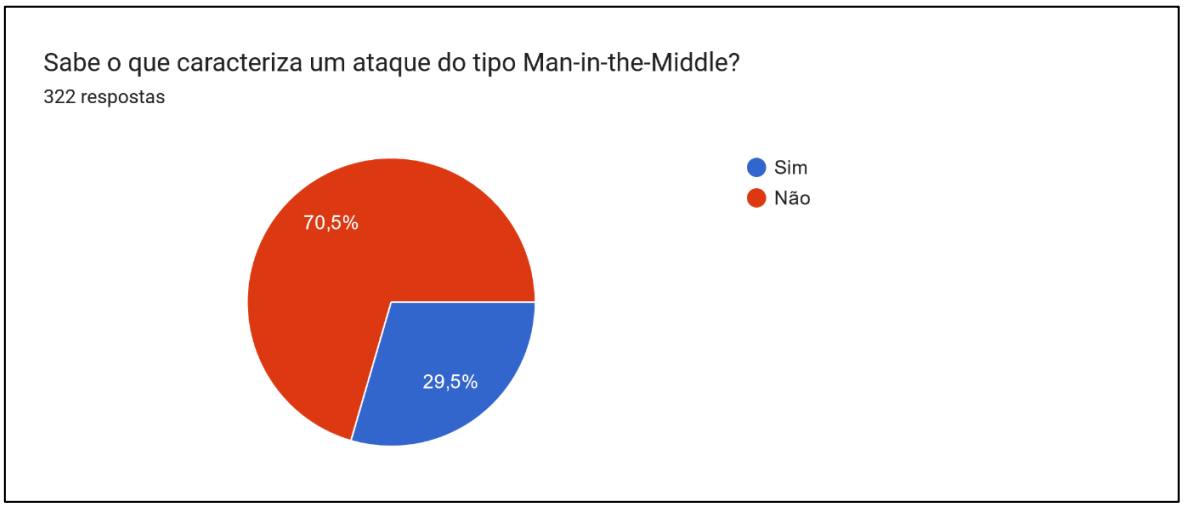

FIGURA 8.22 - QUESTIONÁRIO: SABE O QUE CARACTERIZA UM ATAQUE DO TIPO MAN-IN-THE-MIDDLE?

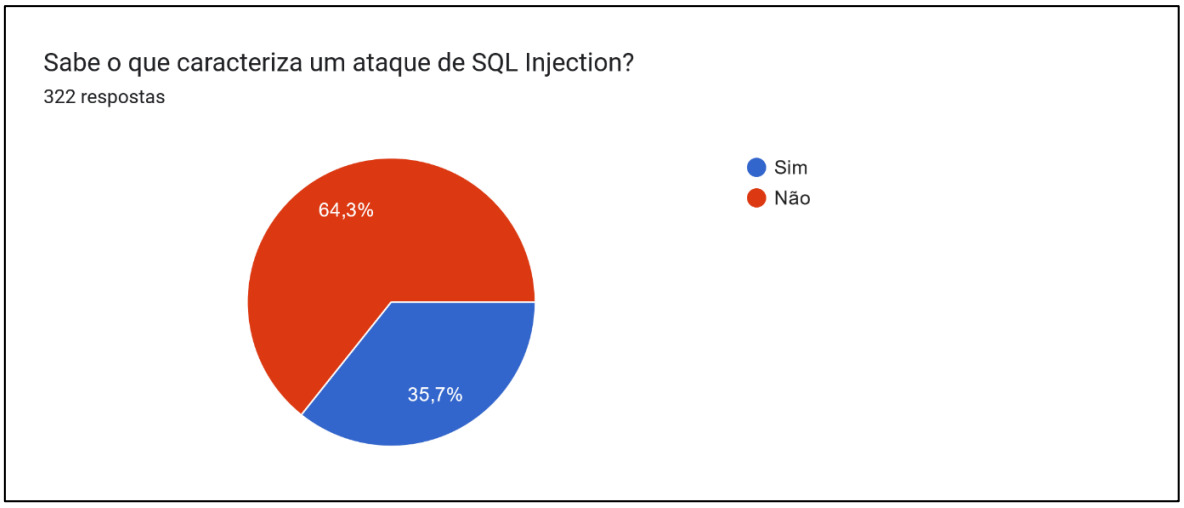

FIGURA 8.23 - QUESTIONÁRIO: SABE O QUE CARACTERIZA UM ATAQUE DE SQL INJECTION?

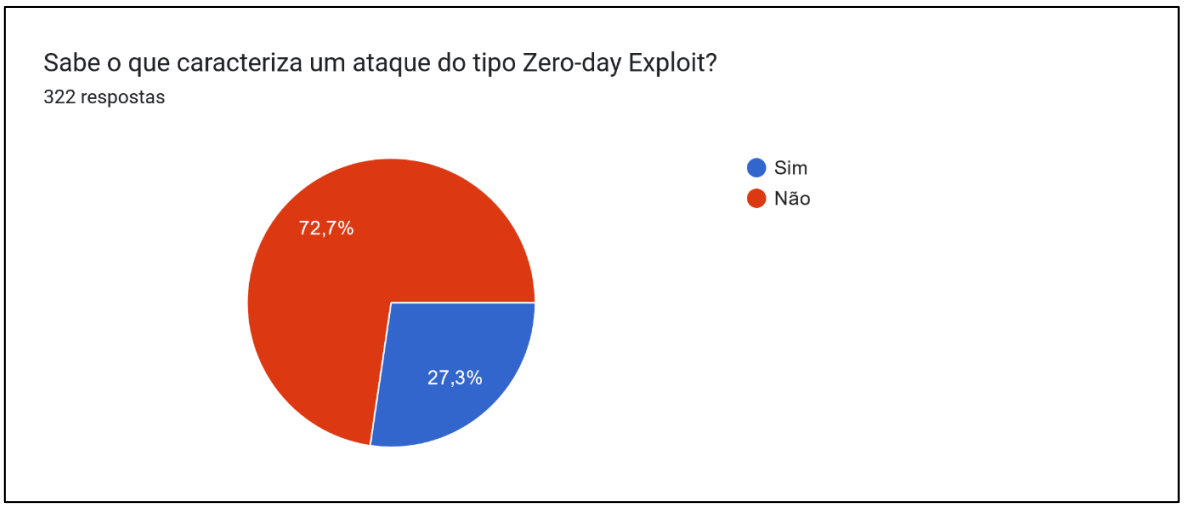

FIGURA 8.24 - QUESTIONÁRIO: SABE O QUE CARACTERIZA UM ATAQUE DO TIPO ZERO-DAY EXPLOIT?

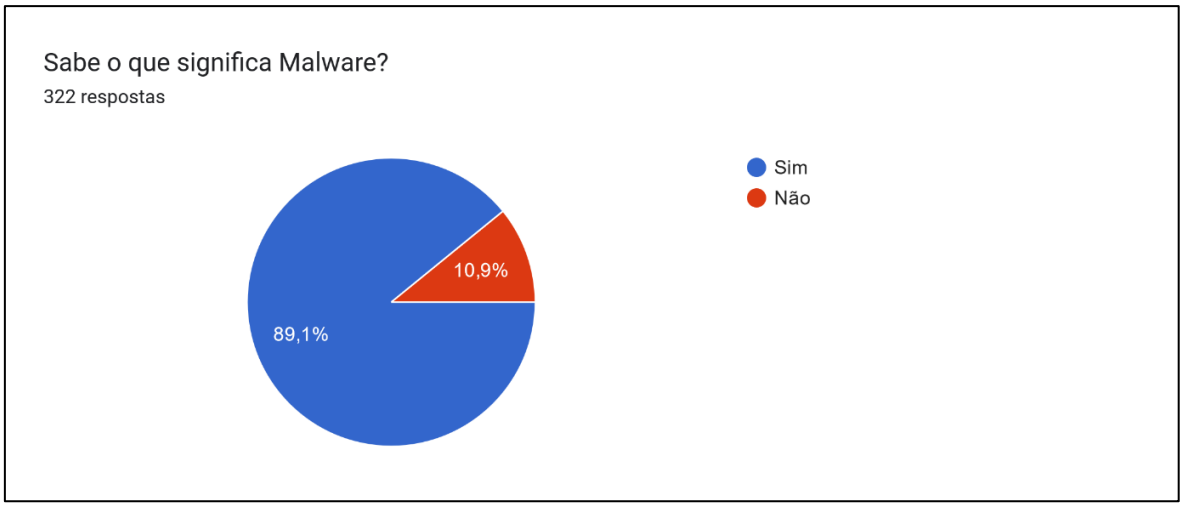

FIGURA 8.25 - QUESTIONÁRIO: SABE O QUE SIGNIFICA MALWARE?

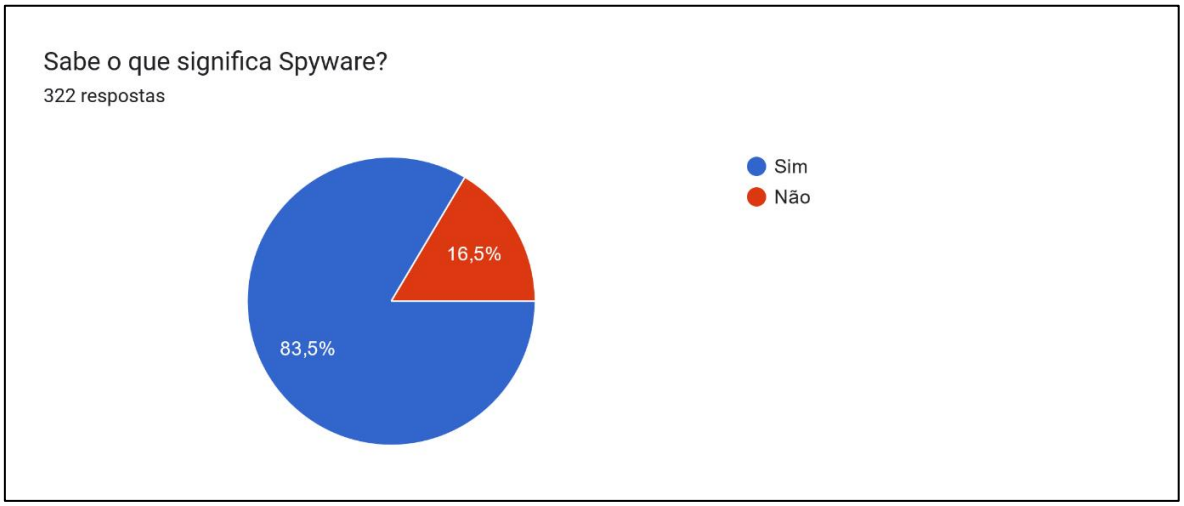

FIGURA 8.26 - QUESTIONÁRIO: SABE O QUE SIGNIFICA SPYWARE?

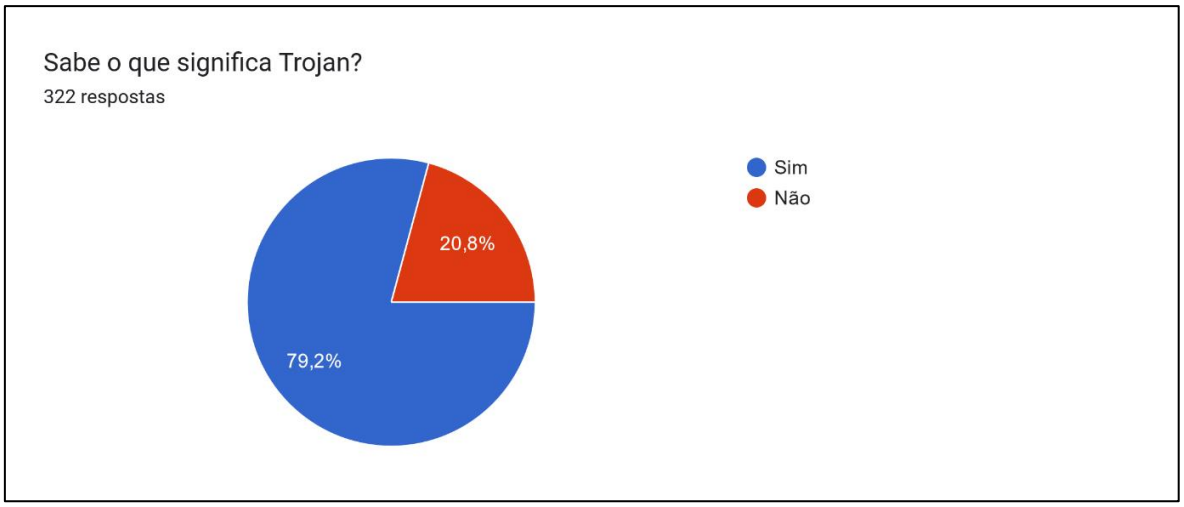

FIGURA 8.27 - QUESTIONÁRIO: SABE O QUE SIGNIFICA TROJAN?

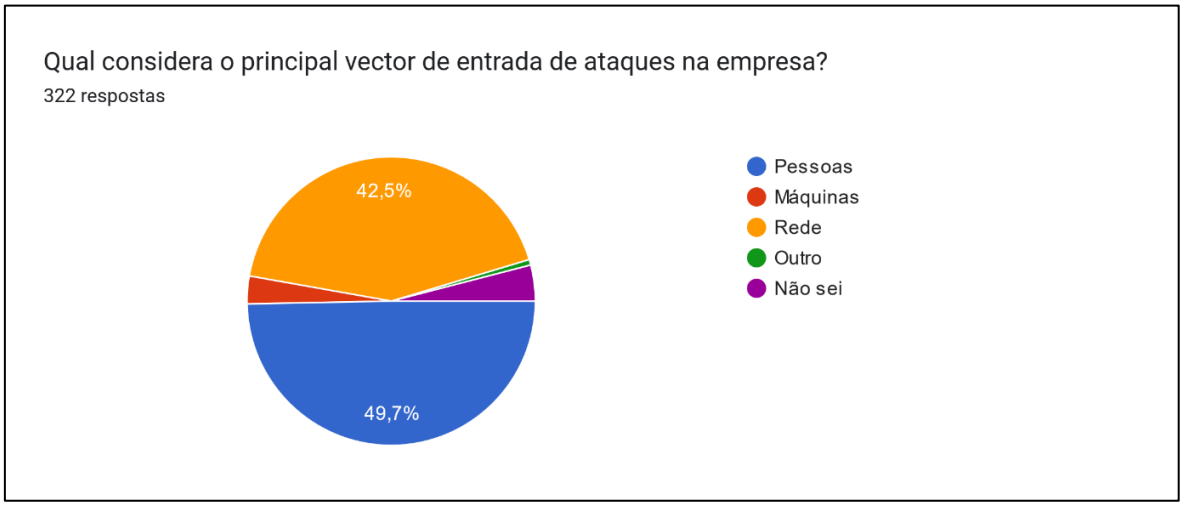

FIGURA 8.28 - QUESTIONÁRIO: QUAL O PRINCIPAL VECTOR DE ENTRADA DE ATAQUES NA EMPRESA?

Secção: Protecção e resiliência

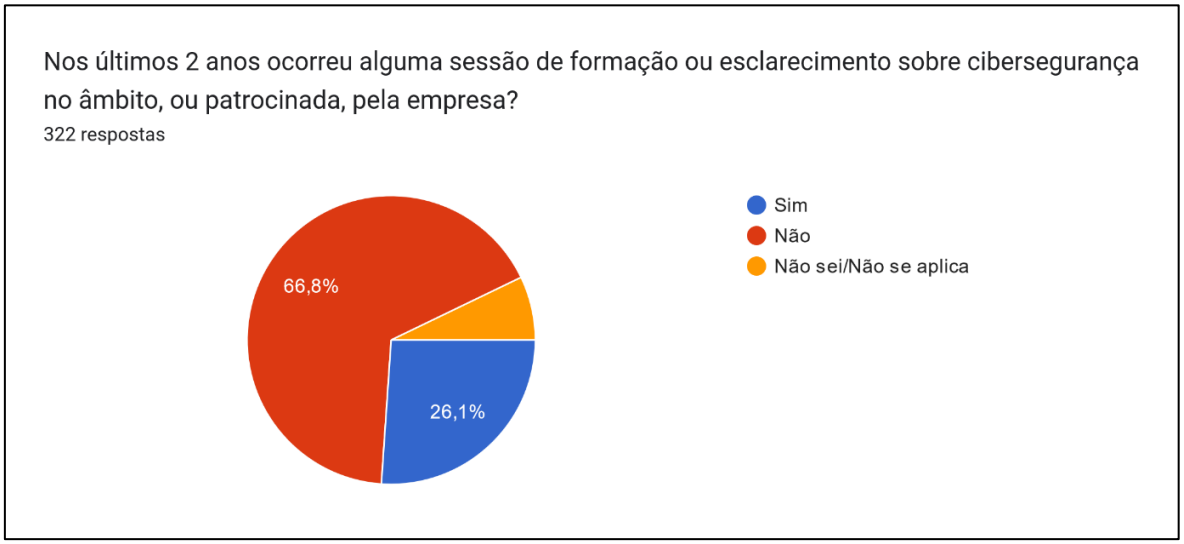

FIGURA 8.29 - QUESTIONÁRIO: NOS ÚLTIMOS 2 ANOS OCORREU ALGUMA SESSÃO DE FORMAÇÃO OU ESCLARECIMENTO SOBRE CIBERSEGURANÇA NO ÂMBITO, OU PATROCINADA, PELA EMPRESA?

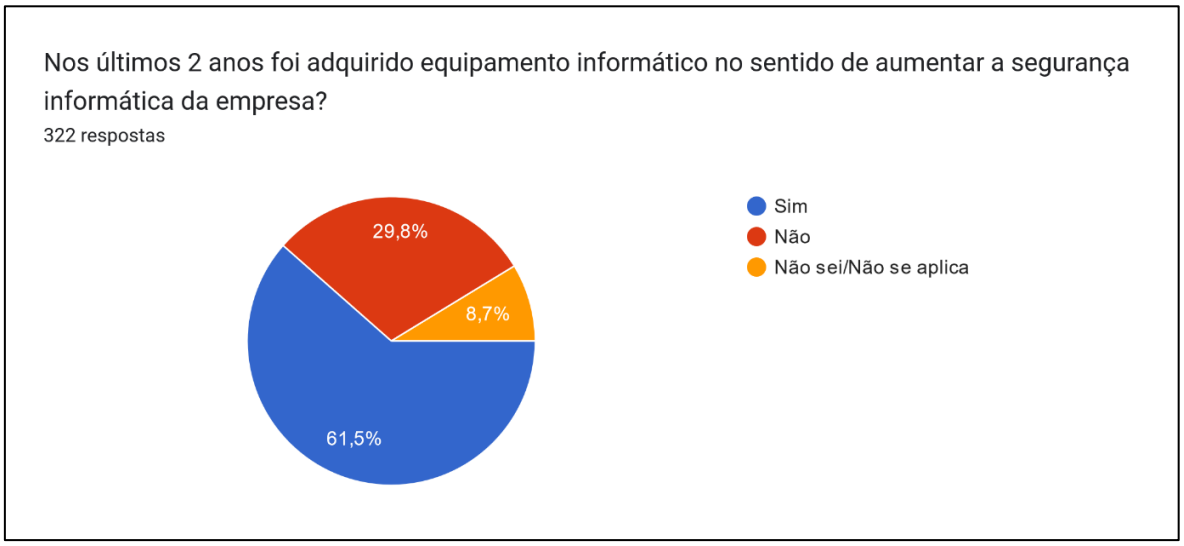

FIGURA 8.30 - QUESTIONÁRIO: NOS ÚLTIMOS 2 ANOS FOI ADQUIRIDO EQUIPAMENTO INFORMÁTICO NO SENTIDO DE AUMENTAR A SEGURANÇA INFORMÁTICA DA EMPRESA?

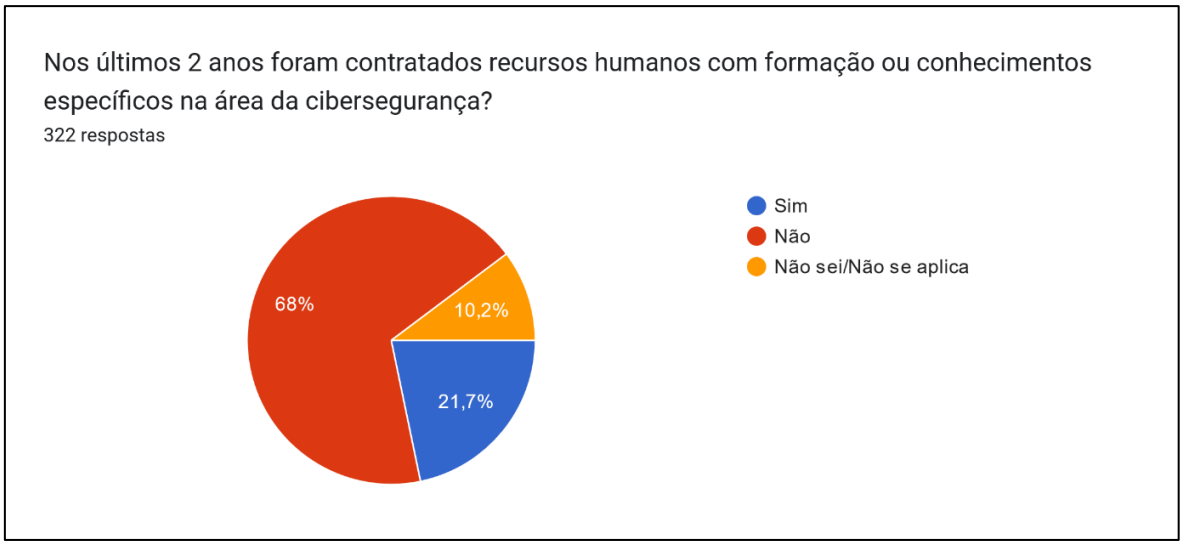

FIGURA 8.31 - QUESTIONÁRIO: NOS ÚLTIMOS 2 ANOS FORAM CONTRATADOS RECURSOS HUMANOS COM FORMAÇÃO OU CONHECIMENTOS ESPCÍFICOS NA ÁREA DA CIBERSEGURANÇA?

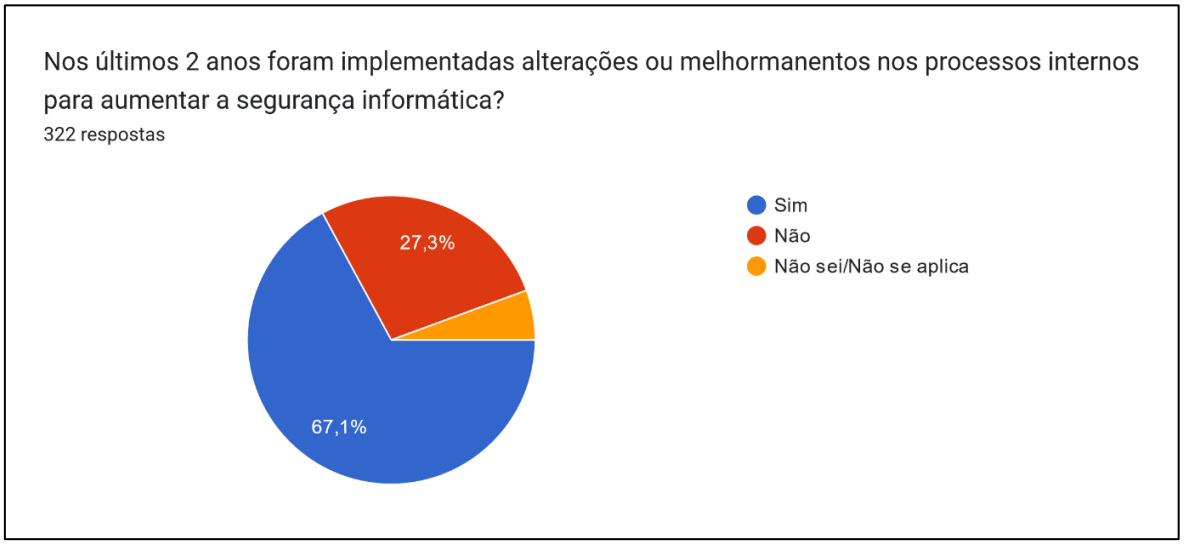

FIGURA 8.32 - QUESTIONÁRIO: NOS ÚLTIMOS 2 ANOS FORAM IMPLEMENTADAS ALTERAÇÕES OU MELHORAMENTOS NOS PROCESSOS INTERNOS PARA AUMENTAR A SEGURANÇA INFORMÁTICA?

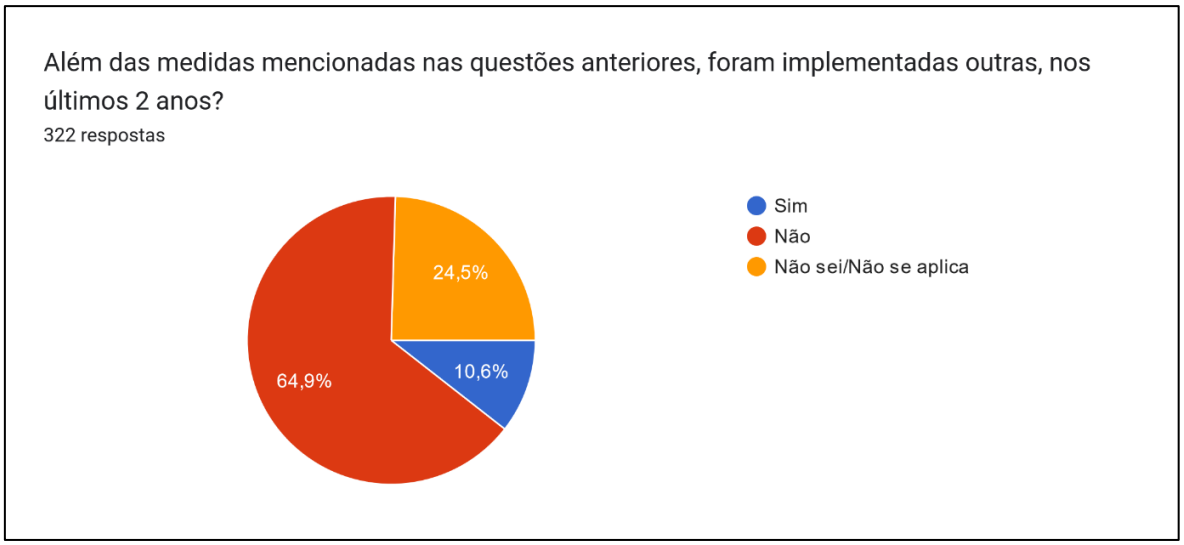

FIGURA 8.33 - QUESTIONÁRIO: ALÉM DAS MEDIDAS MENCIONADAS NAS QUESTÕES ANTERIORES, FORAM IMPLEMENTADAS OUTRAS, NOS ÚLTIMOS 2 ANOS?

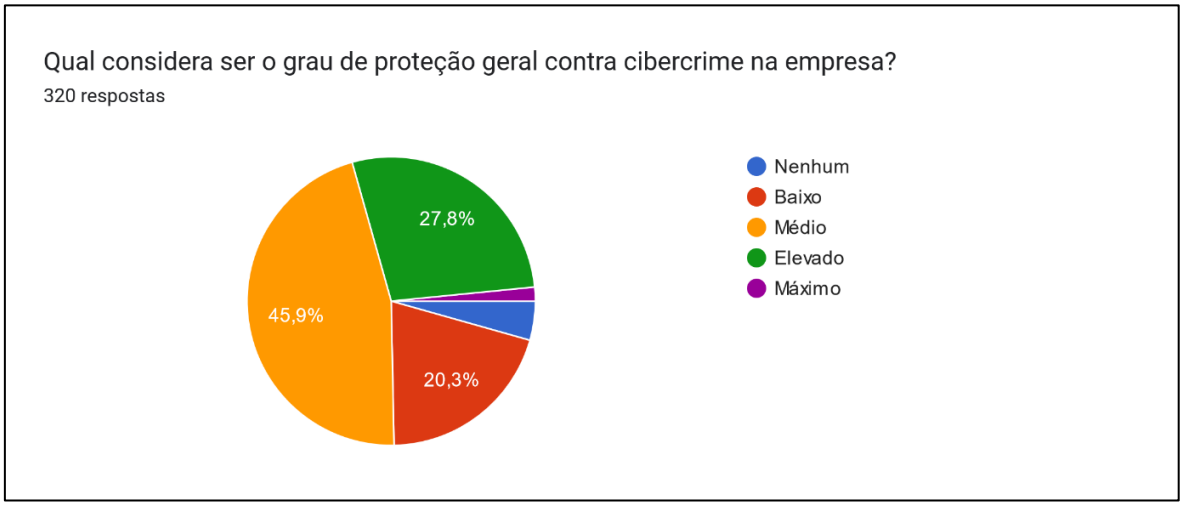

FIGURA 8.34 - QUESTIONÁRIO: QUAL CONSIDERA SER O GRAU DE PROTECÇÃO GERAL CONTRA O CIBERCRIME NA EMPRESA?

Secção: Tecnologias implementadas

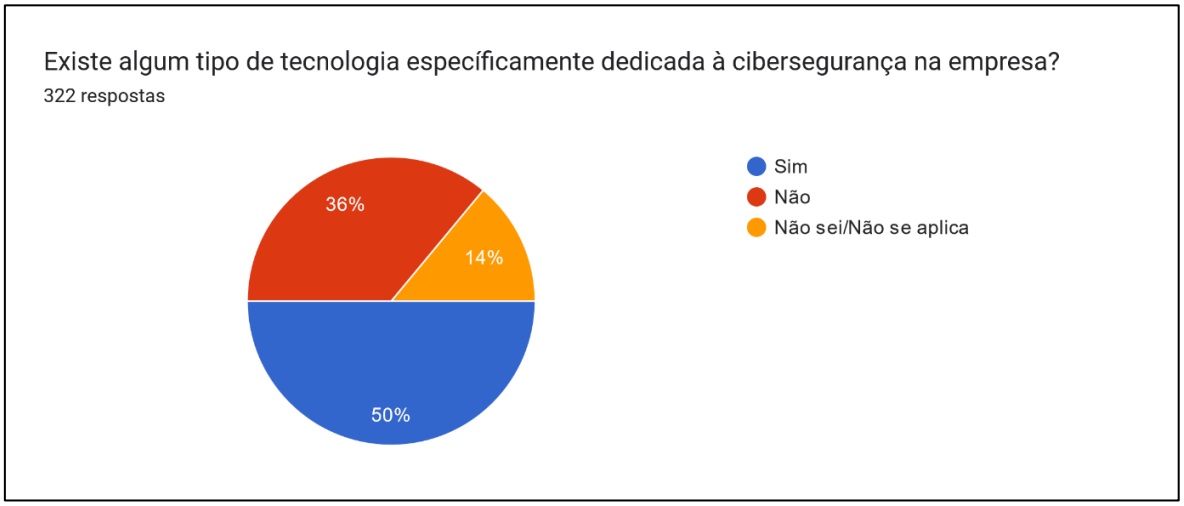

FIGURA 8.35 - QUESTIONÁRIO: EXISTE ALGUM TIPO DE TECNOLOGIA ESPECIFICAMENTE DEDICADA À CIBERSEGURANÇA NA EMPRESA?

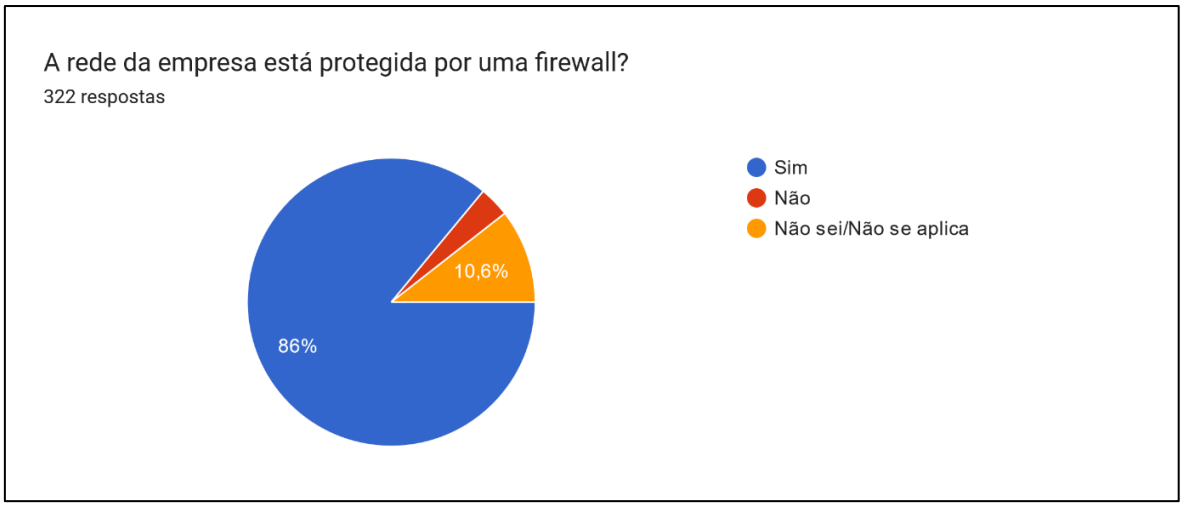

FIGURA 8.36 - QUESTIONÁRIO: A REDE DA EMPRESA ESTÁ PROTEGIDA POR UMA FIREWALL?

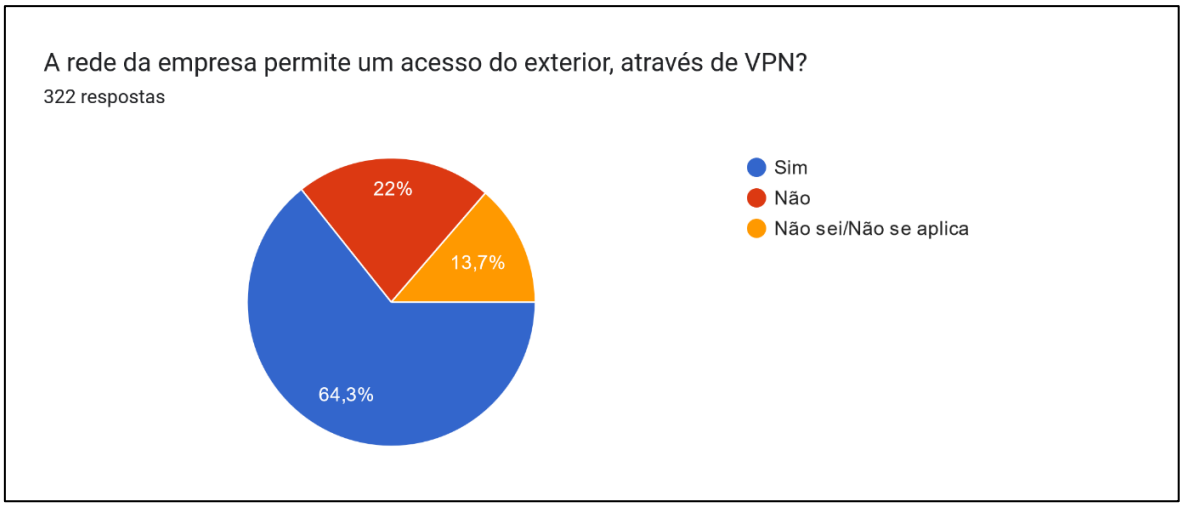

FIGURA 8.37 - QUESTIONÁRIO: A REDE DA EMPRESA PERMITE UM ACESSO DO EXTERIOR, ATRAVÉS DE VPN?

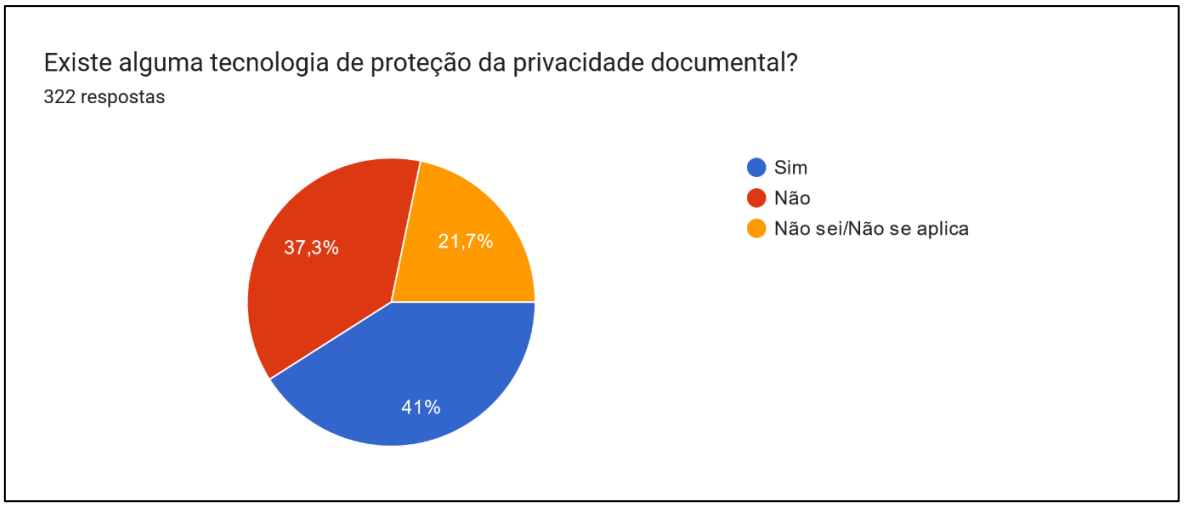

FIGURA 8.38 - QUESTIONÁRIO: EXISTE ALGUMA TECNOLOGIA DE PROTECÇÃO DA PRIVACIDADE DOCUMENTAL?

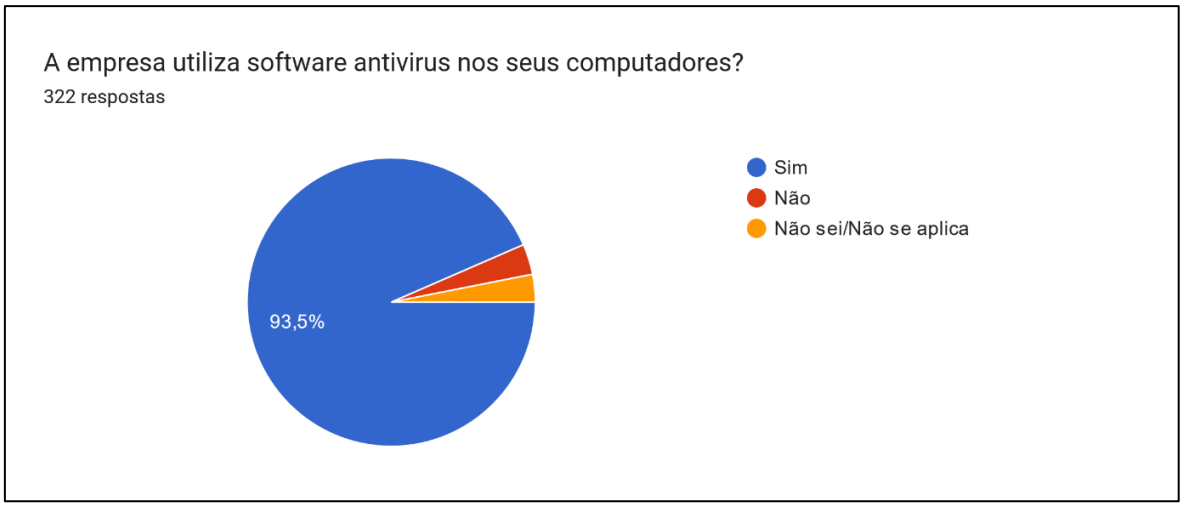

FIGURA 8.39 - QUESTIONÁRIO: A EMPRESA UTILIZA SOFTWARE ANTIVIRUS NOS SEUS COMPUTADORES?

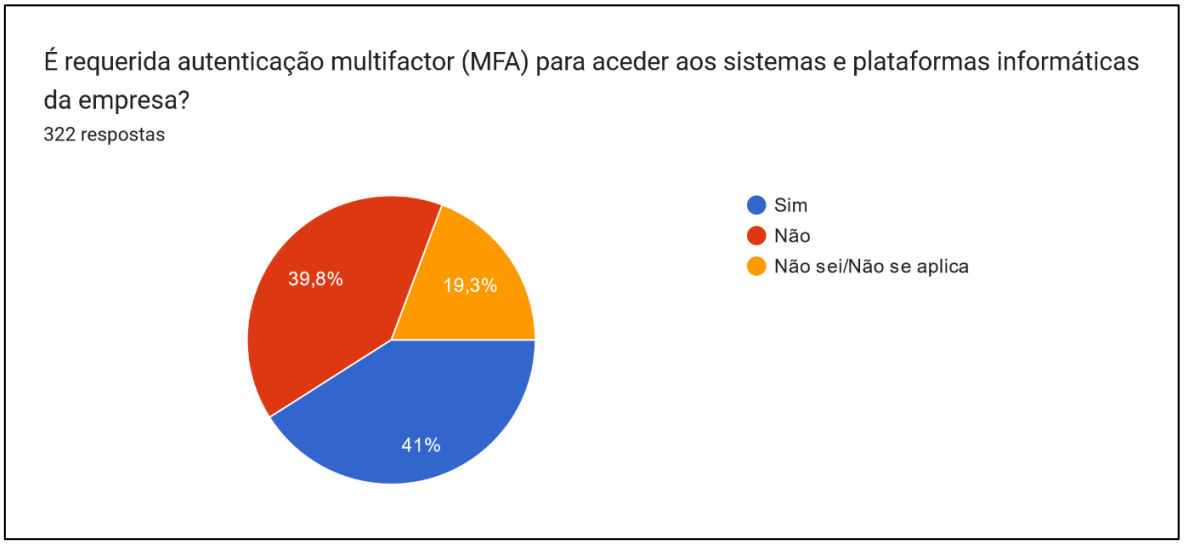

FIGURA 8.40 - QUESTIONÁRIO: É REQUERIDA AUTENTICAÇÃO MULTIFACTOR (MFA) PARA ACEDER AOS SISTEMAS E PLATAFORMAS INFORMÁTICAS DA EMPRESA?

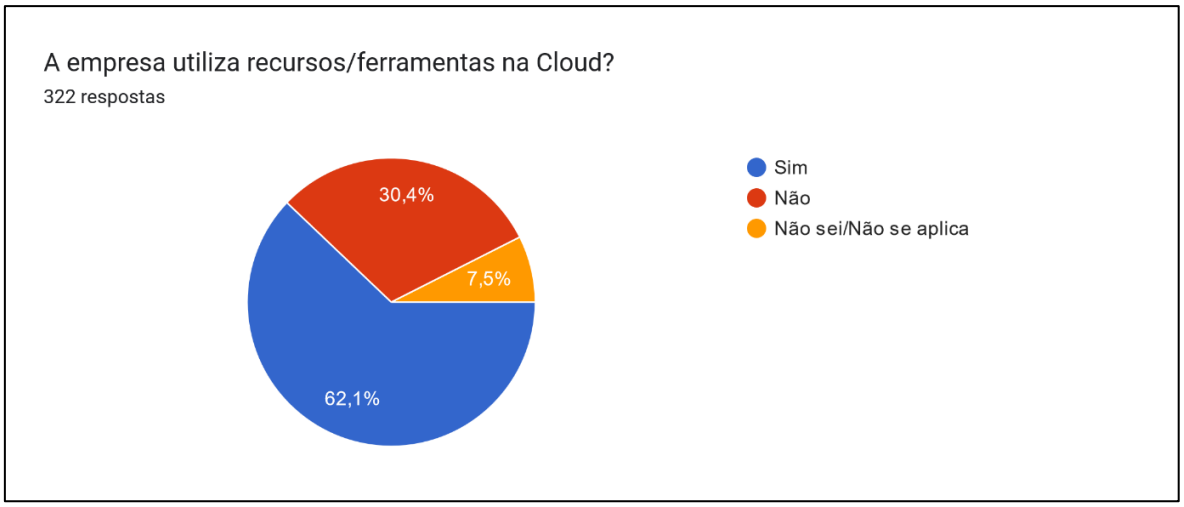

FIGURA 8.41 - QUESTIONÁRIO: A EMPRESA UTILIZA RECURSOS/FERRAMENTAS NA *CLOUD*?

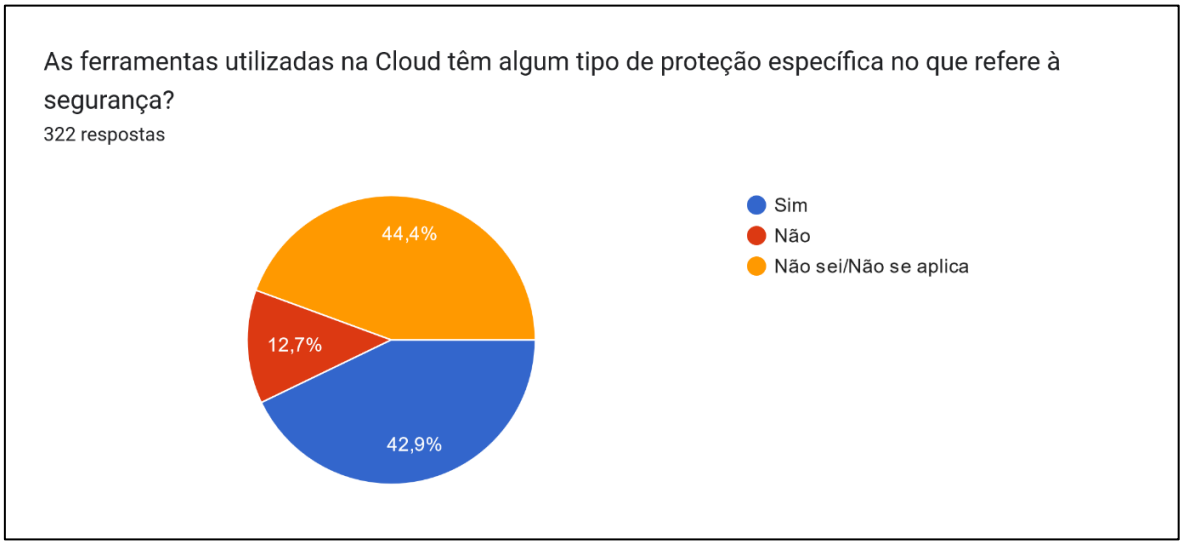

FIGURA 8.42 - QUESTIONÁRIO: AS FERRAMENTAS UTILIZADAS NA *CLOUD* TÊM ALGUM TIPO DE PROTECÇÃO ESPECÍFICA NO QUE REFERE À SEGURANÇA?

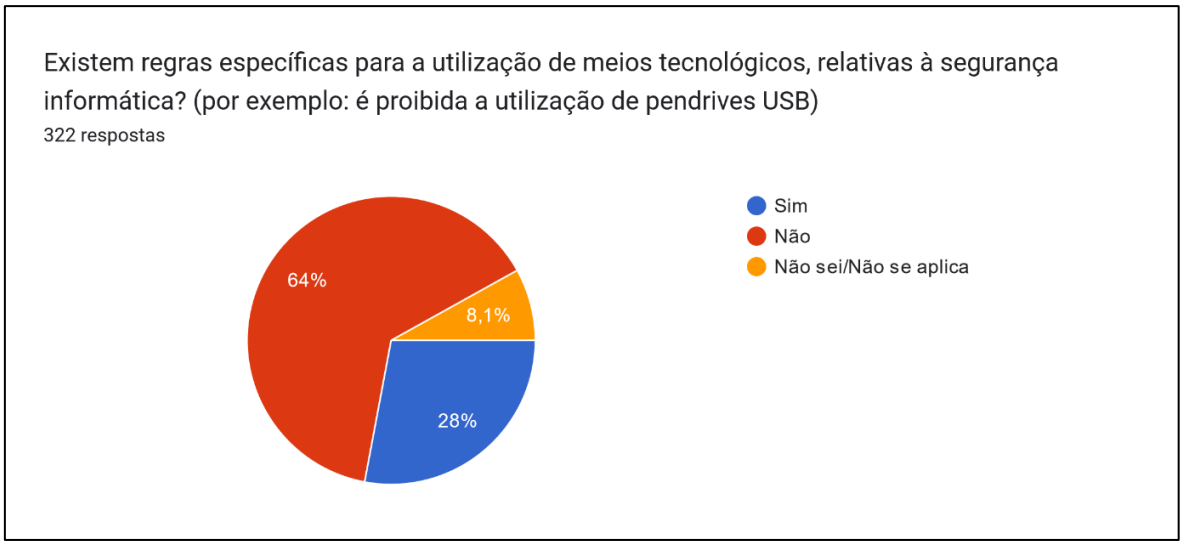

FIGURA 8.43 - QUESTIONÁRIO: EXISTEM REGRAS ESPECÍFICAS PARA A UTILIZAÇÃO DE MEIOS TENOLÓGICOS, RELATIVAS À SEGURANÇA INFORMÁTICA? (POR EXEMPLO: É PROIBIDA A UTILIZAÇÃO DE *PENDRIVES* USB)

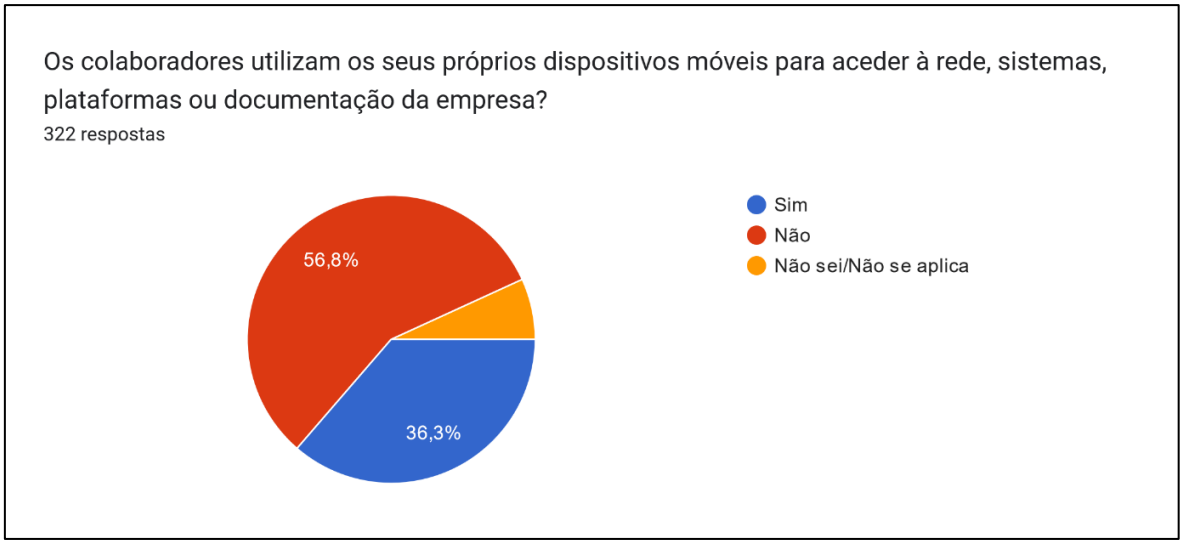

FIGURA 8.44 - QUESTIONÁRIO: OS COLABORADORES UTILIZAMOS SEUS PRÓPRIOS DISPOSITIVOS MÓVEIS PARA ACEDER À REDE, SISTEMAS, PLATAFORMAS OU DOCUMENTAÇÃO DA EMPRESA?

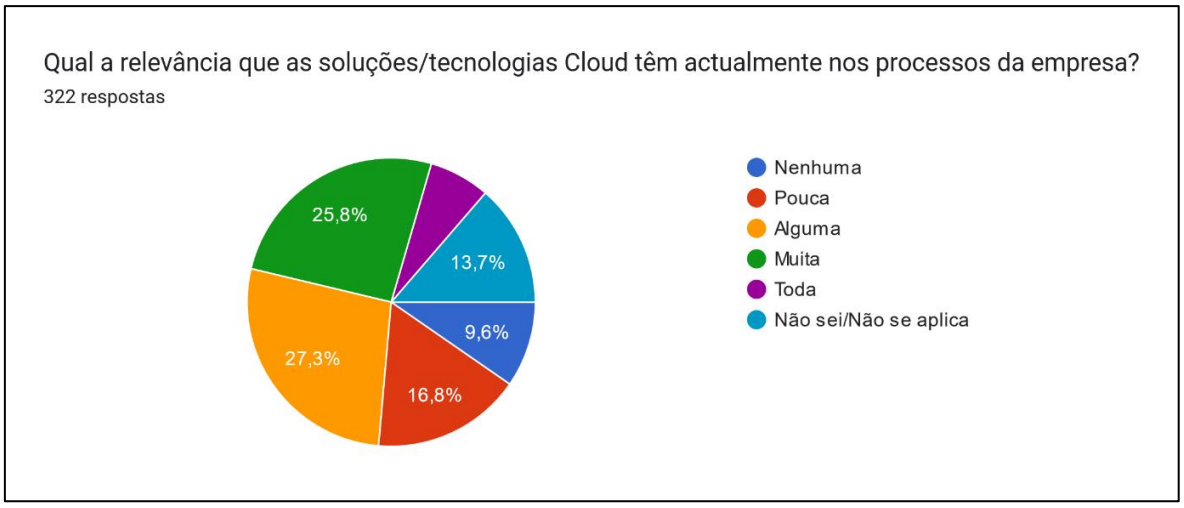

FIGURA 8.45 - QUESTIONÁRIO: QUAL A RELEVÂNCIA QUE AS SOLUÇÕES/TECNOLOGIAS CLOUD TÊM ACTUALMENTE NOS PROCESSOS DA EMPRESA?

Secção: Investimento em Cibersegurança

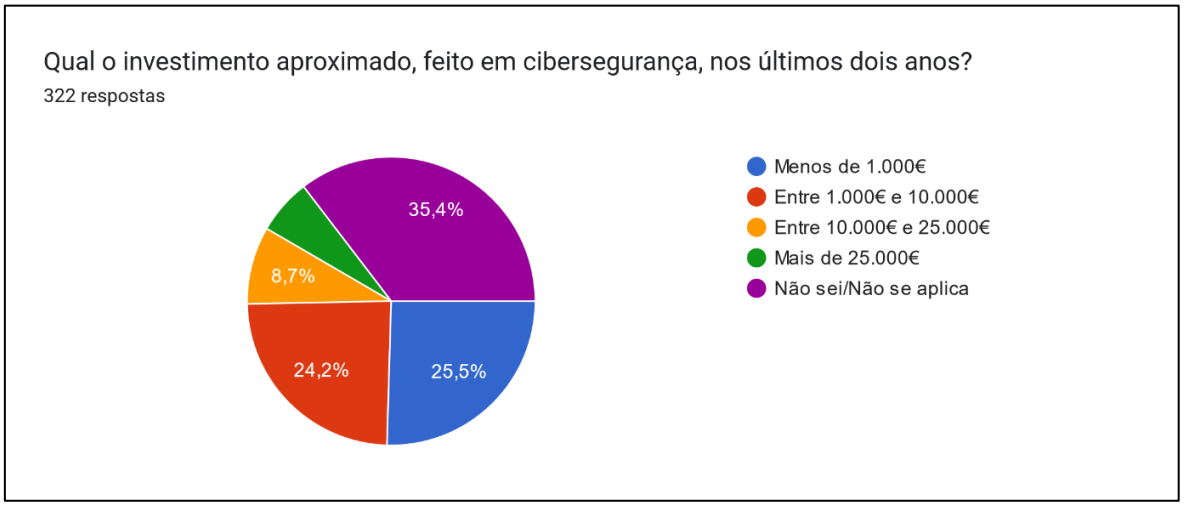

FIGURA 8.46 - QUESTIONÁRIO: QUAL O INVESTIMENTO APROXIMADO, FEITO EM CIBERSEGURANÇA, NOS ÚLTIMOS DOIS ANOS?

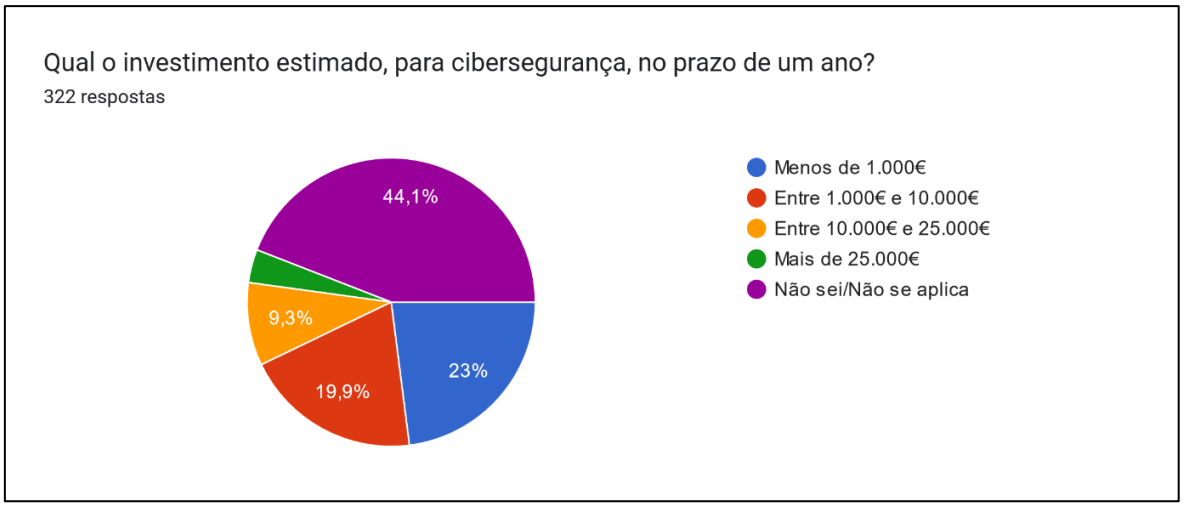

FIGURA 8.47 - QUESTIONÁRIO: QUAL O INVESTIMENTO ESTIMADO, PARA CIBERSEGURANÇA, NO PRAZO DE UM ANO?

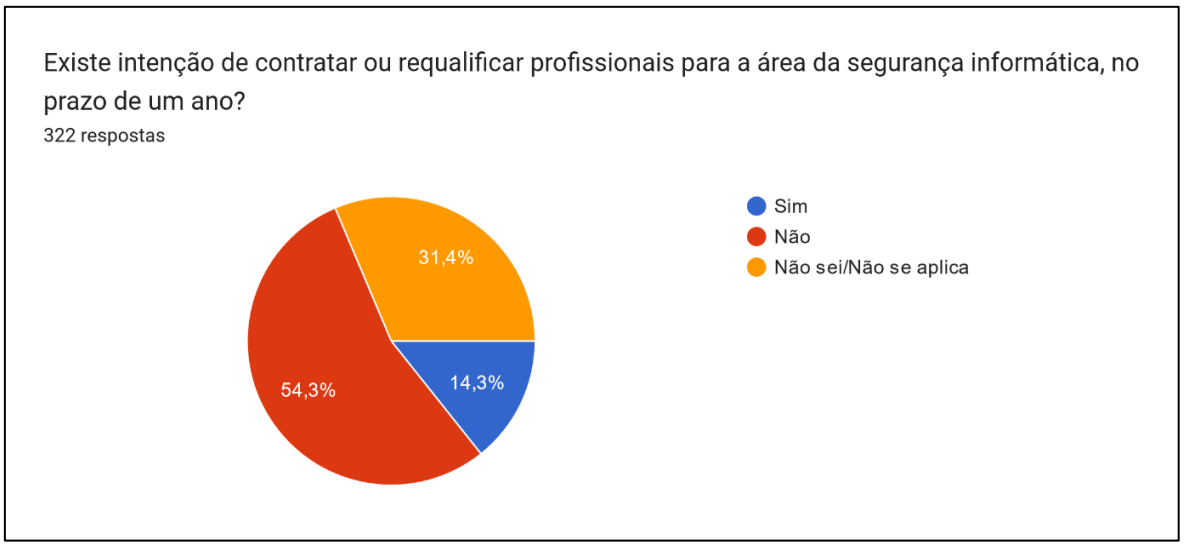

FIGURA 8.48 - QUESTIONÁRIO: EXISTE INTENÇÃO DE CONTRATAR OU REQUALIFICAR PROFISSIONAIS PARA A ÁREA DA SEGURANÇA INFORMÁTICA, NO PRAZO DE UM ANO?

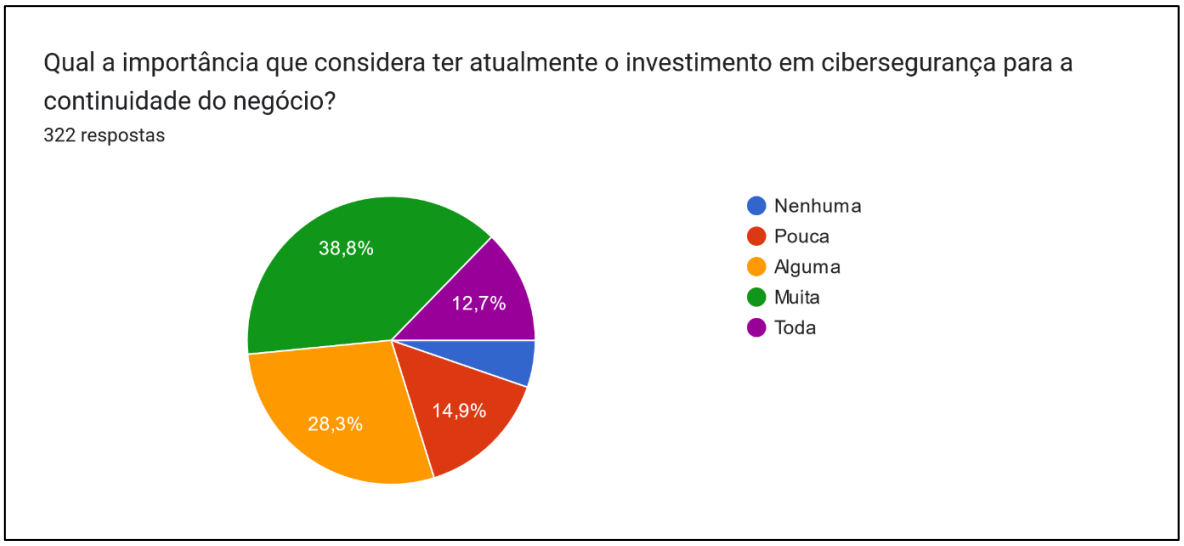

FIGURA 8.49 - QUESTIONÁRIO: QUAL A IMPORTÂNCIA QUE CONSIDERA TER ACTUALMENTE O INVESTIMENTO EM CIBERSEGURANÇA PARA A CONTINUIDADE DO NEGÓCIO?

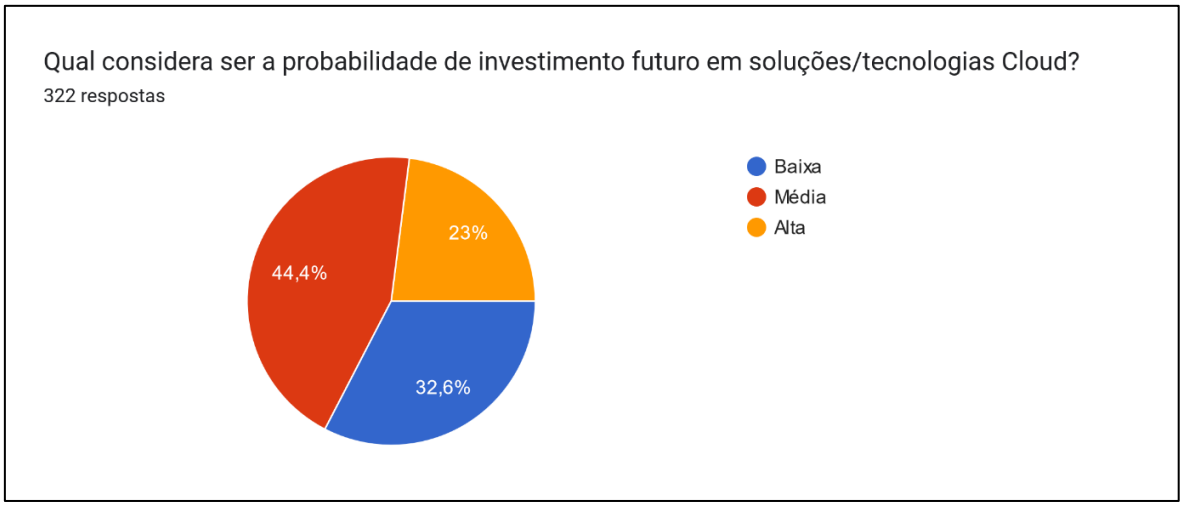

FIGURA 8.50 - QUESTIONÁRIO: QUAL CONSIDERA SER A PROBABILIDADE DE INVESTIMENTO FUTURO EM SOLUÇÕES/TECNOLOGIAS *CLOUD*?

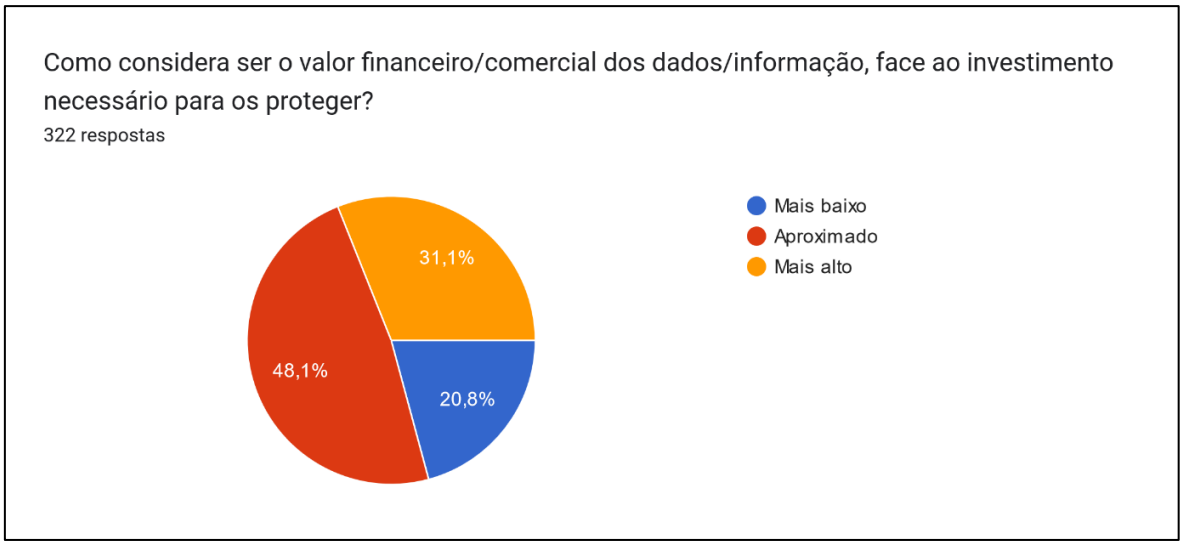

FIGURA 8.51 - QUESTIONÁRIO: COMO CONSIDERA SER O VALOR FINANCEIRO/COMERCIAL DOS DADOS/INFORMAÇÃO, FACE AO INVESTIMENTO NECESSÁRIO PARA OS PROTEGER?