Guia Prático para PMEs Portuguesas:

Preparação para a Diretiva NIS2

highdome
closing the cyber gap

Introdução

A cibersegurança deixou de ser uma preocupação exclusiva das grandes corporações e infraestruturas críticas. Com a transposição da Diretiva (UE) 2022/2555, conhecida como NIS2, para o ordenamento jurídico português através do Decreto-Lei n.º 125/2025, de 4 de dezembro, o panorama regulatório da cibersegurança em Portugal sofreu uma alteração significativa [1]. Este novo regime, que entrará em vigor a 3 de abril de 2026, alarga o seu âmbito de aplicação a um vasto conjunto de entidades, incluindo muitas Pequenas e Médias Empresas (PMEs) que, até então, não estavam sujeitas a obrigações regulamentares tão rigorosas [1].

O presente guia prático visa fornecer às PMEs portuguesas, em particular às micro e pequenas empresas, uma orientação clara e objetiva sobre como se preparar para cumprir as novas exigências da NIS2. O foco reside na contextualização da realidade empresarial portuguesa e na apresentação de medidas concretas, divididas em aspetos de Governança e Técnicos, essenciais para a gestão eficaz dos riscos de cibersegurança.

highdome
closing the cyber gap

1. Contextualização: O Cenário Português e a Ameaça Cibernética

1.1. A Diretiva NIS2 e a Realidade Portuguesa

A NIS2 estabelece um quadro harmonizado de medidas de cibersegurança e notificação de incidentes em toda a União Europeia, visando aumentar a resiliência cibernética dos Estados-Membros [1]. Em Portugal, a transposição da Diretiva reconhece a importância de setores críticos e de outros setores essenciais para a economia e sociedade.

A classificação das entidades como Essenciais ou Importantes baseia-se, em grande parte, no seu setor de atividade e na sua dimensão, utilizando os limiares de PME (menos de 250 trabalhadores e volume de negócios anual não superior a 50 milhões de euros ou balanço total anual não superior a 43 milhões de euros) como critério de exclusão para as micro e pequenas empresas, exceto em casos específicos [1]. No entanto, a esmagadora maioria do tecido empresarial português é composta por PMEs, com uma forte predominância de microempresas [2]. Mesmo que muitas PMEs não sejam diretamente abrangidas, a sua inclusão na cadeia de abastecimento de entidades Essenciais ou Importantes significa que a sua ciber-resiliência é crucial para o cumprimento da NIS2 por parte dos seus parceiros de negócio [1].

1.2. PMEs como Alvo Prioritário

Contrariamente à perceção comum, as PMEs são alvos cada vez mais frequentes e lucrativos para os cibercriminosos. Os atacantes exploram a menor sofisticação dos seus sistemas de segurança e a falta de recursos dedicados, transformando-as em "elos fracos" [3].

As estatísticas recentes sublinham a gravidade da situação em Portugal:

Indicador	2025	Fonte
PMEs alvo de ciberataques	54%	Relatório de Ciberpreparação Hiscox [3]
Aumento de incidentes	Significativo	CNCS [4]
Principais Vetores de Ataque	Phishing/Smishing	CNCS [4]

O impacto de um ciberataque numa PME pode ser devastador, resultando em perdas financeiras, interrupção operacional e danos reputacionais. Com a NIS2, o risco é agravado pela possibilidade de aplicação de coimas elevadas (até 10 milhões de euros ou 2% do volume de negócios mundial, o que for superior) por incumprimento das obrigações de gestão de risco [1].

2. Orientações Práticas para a Conformidade NIS2

A NIS2 exige que as entidades abrangidas implementem medidas de gestão de risco de cibersegurança que incluam, pelo menos, dez elementos fundamentais. Para as PMEs, estas medidas devem ser proporcionais ao seu risco e dimensão. Apresentamos as orientações divididas em aspetos de Governança e Técnicos.

2.1. Dicas de Governança e Organização

As medidas de governança estabelecem o quadro de responsabilidade e as políticas que orientam a cibersegurança na empresa. O envolvimento da gestão de topo é um requisito explícito da NIS2.

Foco	Dica de Governança	Justificação (NIS2)
Responsabilidade da Gestão	O órgão de gestão (administração/ direção) deve aprovar as medidas de gestão de risco e supervisionar a sua aplicação.	A NIS2 responsabiliza diretamente os órgãos de gestão pelo incumprimento, podendo responder por ação ou omissão [1].
Formação e Sensibilização	Implementar um programa de formação regular em ciber-higiene para todos os colaboradores, incluindo a gestão.	Requisito de "Práticas básicas de ciber-higiene e formação em cibersegurança" [1]. É a primeira linha de defesa contra Phishing/Smishing.t
Gestão de Fornecedores	Mapear e avaliar o risco de cibersegurança dos fornecedores e prestadores de serviços críticos (a cadeia de abastecimento).	Requisito de "Segurança da cadeia de abastecimento" [1]. A PME deve garantir que os seus fornecedores também são resilientes.
Documentação de Políticas	Criar e manter políticas e procedimentos simples e documentados para a gestão de risco, uso aceitável de recursos e resposta a incidentes.	Requisito de "Políticas e procedimentos para avaliar a eficácia das medidas de gestão de risco de cibersegurança" [1].
Continuidade de Negócio	Desenvolver um Plano de Continuidade de Atividades e um Plano de Resposta a Incidentes testado, garantindo que a empresa pode recuperar rapidamente após um ataque.	Requisito de "Continuidade de atividades" e "Tratamento de incidentes" [1].

2.2. Dicas Técnicas Essenciais

As medidas técnicas são a implementação prática das políticas de governança, focando na proteção dos sistemas e dados.

Quick Wins - Ações Imediatas (1 dia)

Medidas simples que dão proteção imediata:

- Bloqueio automático de ecrã após 10-15 minutos
- Firewall ativo em todos os dispositivos
- Desativar macros por defeito no Microsoft Office
- Desativar acesso RDP direto da Internet e usar VPN ou Gateway de Área de Trabalho Remota
- Criar inventário básico de ativos críticos (servidores, sistemas, dados sensíveis)
- Desativar contas de utilizadores inativos há mais de 90 dias

Medidas Técnicas Prioritárias

Foco	Dica Técnica	Justificação (NIS2)
Acesso e Identidade	Implementar Autenticação Multifator (MFA) em todos os serviços críticos (e-mail, VPN, sistemas de gestão). **Ferramentas:** Microsoft Authenticator, Google Authenticator (gratuitas), Duo Security, Azure MFA (pagas) **Como fazer:** Ativar no Microsoft 365/Google Workspace e guardar backup codes. Começar pelos utilizadores com privilégios de administrador.	Requisito explícito de "Utilização de autenticação multifator" [1]. É a defesa mais eficaz contra roubo de credenciais.
Proteção de Dados	Encriptar dados sensíveis em trânsito (HTTPS) e em repouso (discos encriptados). **Ferramentas:** BitLocker (Windows Pro), FileVault (macOS), VeraCrypt (gratuito) **Como fazer:** Encriptar discos de todos os portáteis e usar VPN para trabalho remoto (WireGuard, OpenVPN). Garantir que sites internos usam HTTPS.	Requisito de "Políticas e procedimentos relativos à utilização de criptografia e de cifragem" [1].

highdome
closing the cyber gap

Foco	Dica Técnica	Justificação (NIS2)
Gestão de Vulnerabilidades	Manter sistemas, aplicações e firmware atualizados. **Ferramentas:** Windows Update (nativo), WSUS (gratuito), ManageEngine, Heimdal (pagas) **Como fazer:** Ativar atualizações automáticas. Como melhor prática de mercado, aplicar patches críticos em 7 dias e restantes em 30 dias.	Requisito de "Gestão de vulnerabilidades" [1]. A maioria dos ataques de ransomware explora falhas já corrigidas.
Backup	**Regra 3-2-1:** 3 cópias, 2 tipos de media, 1 offline. **Ferramentas:** Veeam Community Edition (gratuito até 10 VMs), Acronis, Backblaze, Synology/QNAP **Como fazer:** Backup diário dos dados críticos. Testar restore todos os meses. Garantir que pelo menos uma cópia está offline (desconectada da rede) ou imutável.	Requisito de "Continuidade de atividades" [1]. Sem backup offline, o ransomware apaga tudo.
Monitorização	Detetar e responder a atividades suspeitas nos endpoints e rede. **Ferramentas:** Microsoft Defender for Business, Bitdefender GravityZone (EDR), soluções de Log Management básico **Como fazer:** Instalar EDR em todos os dispositivos, configurar alertas para atividades suspeitas e rever logs semanalmente.	Requisito de "Segurança dos sistemas de rede" e "Tratamento de incidentes" [1].
Gestão de Passwords	Passwords únicas e complexas em cada serviço. Esta é uma medida de ciber-higiene obrigatória. **Ferramentas:** Bitwarden (gratuito/pago), 1Password, Keeper **Como fazer:** Mínimo 12 caracteres, nunca reutilizar passwords. Implementar política de alteração de passwords comprometidas.	Requisito de "Práticas básicas de ciber-higiene" [1]. A gestão adequada de passwords é um elemento central da ciber-higiene.
Gestão de Acessos	Implementar o princípio de privilégio mínimo. **Como fazer:** Remover direitos de administrador local dos utilizadores comuns. Criar contas de administrador separadas apenas para tarefas que o exijam. Rever permissões trimestralmente.	Requisito de "Políticas e procedimentos relativos ao controlo de acesso" [1]. A implementação do Princípio do Privilégio Mínimo (PPM)

highdome
closing the cyber gap

Como Validar a Implementação

Medidas	O que verificar
MFA	100% dos utilizadores com privilégios têm MFA ativo
Backup	Teste de restore mensal bem-sucedido (simular recuperação real)
Patches	95% dos sistemas críticos atualizados em 30 dias
EDR/Antivírus	100% dos endpoints com proteção ativa e atualizada
Passwords	100% dos utilizadores usam gestor de passwords
Inventário	Lista atualizada de todos os ativos críticos

Cenário Mínimo Viável:

- MFA com soluções gratuitas ou básicas
- Backup cloud básico
- EDR/Antivírus de endpoint
- Gestor de passwords
- Patch management básico (soluções nativas)

Cenário Recomendado:

- MFA empresarial com suporte
- Backup profissional com retenção alargada e testes automáticos
- EDR avançado com deteção comportamental e Log Management
- Firewall dedicado com subscrições de segurança
- Patch management automatizado
- Programa de formação em cibersegurança (anual)
- Consultoria/auditoria externa (trimestral)

highdome
closing the cyber gap

Investimento inicial em hardware: (Firewall empresarial, NAS para backup local, Switch gerido com suporte VLAN)

Roadmap de Implementação Sugerido

Fase 1 - Fundações (Meses 1-3):

- Implementar Quick Wins
- Ativar MFA em serviços críticos (começar por administradores)
- Configurar backup básico (3-2-1) com testes mensais
- Criar inventário de ativos e sistemas críticos
- Designar responsável de cibersegurança e ponto de contacto

Fase 2 - Proteção e Monitorização (Meses 4-6):

- Implementar EDR em todos os endpoints
- Configurar patch management com calendário definido
- Documentar políticas de gestão de acessos
- Realizar primeira formação de ciber-higiene para todos os colaboradores

Fase 3 - Maturidade (Meses 7-12):

- Implementar segmentação básica de rede
- Configurar solução de Log Management
- Realizar primeiro exercício de resposta a incidentes (tabletop exercise)
- Documentar todos os procedimentos e políticas
- Preparar relatório anual para o CNCS

Nota sobre o prazo:

O Decreto-Lei n.º 125/2025 entra em vigor a 3 de abril de 2026, mas prevê um período de carência de 12 meses para aplicação de coimas (até 3 de abril de 2027), desde que a entidade demonstre ter um procedimento interno de adaptação em curso [1]. Isto significa que as PMEs devem iniciar o processo imediatamente, mas têm margem para implementação faseada até 2027.

highdome
closing the cyber gap

Conclusão

A NIS2 representa uma oportunidade para as PMEs portuguesas elevarem o seu nível de ciber-resiliência, protegendo-se contra ameaças que se tornam cada vez mais sofisticadas. A preparação para o Decreto-Lei n.º 125/2025 não deve ser vista apenas como um encargo regulatório, mas sim como um investimento estratégico na continuidade e na confiança do negócio. Ao focar-se nas orientações de Governança (responsabilidade e políticas) e nas medidas Técnicas essenciais (MFA, backups, atualizações), a PME garante que está a dar passos firmes para a conformidade e, mais importante, para a sua sobrevivência no ecossistema digital.

highdome
closing the cyber gap

A **Highdome** é a unidade de cibersegurança da Agap2IT, uma empresa portuguesa, com 20 anos de tradição, presente em 13 países na Europa e estamos comprometidos em apoiar PMEs na gestão prática e proporcional do risco cibernético e na preparação para requisitos regulatórios como a Diretiva NIS2. Atuamos como parceiro estratégico, combinando **serviços de consultoria, avaliações de risco, apoio à implementação de controlos técnicos e governança**, com uma **plataforma própria e simplificada de consciencialização em cibersegurança**, desenhada para capacitar colaboradores de forma contínua, acessível e alinhada com as exigências da NIS2 e de frameworks como NIST e ISO 27001. O nosso foco é transformar a conformidade regulatória em **resiliência real**, ajudando as empresas a reduzirem riscos, fortalecer a sua cadeia de abastecimento e demonstrar maturidade em cibersegurança de forma clara, pragmática e sustentável. Estamos prontos para realizar uma demonstração não só da nossa plataforma mas também de todo o nosso portfólio em cibersegurança.

Referências

[1] Decreto-Lei n.º 125/2025, de 4 de dezembro. Aprova o regime jurídico da cibersegurança, transpondo a Diretiva (UE) 2022/2555 (NIS 2). Diário da República, 1.ª série. Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/125-2025-962603401

[2] Comissão Europeia. Portugal - SME Fact Sheet 2025. Disponível em: https://single-market-economy.ec.europa.eu/document/download/97a81ff7-0461-4de6-bc6d-a45d36e0dd42_en?filename=Portugal%20-%20SME%20Fact%20Sheet%202025.pdf

[3] Hiscox. Relatório de Ciberpreparação Hiscox 2025. Hiscox Group. Disponível em: https://www.hiscoxgroup.com/sites/group/files/documents/2025-10/HSX374%20%E2%80%93%202025%20CRR%20Report%20Final.pdf

[4] Centro Nacional de Cibersegurança (CNCS). Cibersegurança em Portugal: Riscos e Conflitos - 6.ª Edição (Relatório Anual 2024). CNCS, setembro de 2025.

highdome
closing the cyber gap