					Insira aqui a designação da entidade jurídica registada							
Número do documento: P41					Título do documento: **Política de Gestão do Risco de Dependência de Fornecedores**							
Versão: 1.0		Data de entrada em vigor: 01.01.2025			Proprietário do documento:							
X	Política		Norma		Procedimento		Formulário		Registo		Outro	

Histórico de revisões				
Número da revisão	**Data da revisão**	**Alterações**	**Revisto por**	**Proprietário do processo**

Aprovações			
Nome	**Cargo**	**Data**	**Assinatura**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	6.1.3, 8.1, 9.1	
ISO/IEC 27002:2022	5.20, 5.21, 5.22, 5.23, 5.30	
NIST SP 800-53 Rev.5	SR-2, SR-3, SR-5, SR-6, SR-11, RA-3	
RGPD da UE	Art. 28, Art. 32(1)(d)	
Diretiva NIS2 da UE	Art. 21(2)(d), Art. 21(3), Art. 22	
DORA da UE	Art. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Finalidade

1.1 Reforçar as práticas de segurança da cadeia de fornecimento da organização através da implementação de um processo para identificar e gerir dependências críticas de fornecedores e prestadores de serviços, em conformidade com o artigo 21.º, n.º 3, da Diretiva NIS2 da UE e com as avaliações de risco da cadeia de fornecimento realizadas ao nível da União.

1.2 Assegurar que os riscos decorrentes da concentração ou da dependência de um único fornecedor são compreendidos e mitigados, e que quaisquer riscos da cadeia de fornecimento específicos do setor, sinalizados pelas autoridades ao abrigo do artigo 22.º da NIS2, são incorporados na nossa gestão de riscos e no planeamento da continuidade do negócio.

2. Âmbito

2.1 Esta política aplica-se a todos os fornecedores e prestadores de serviços essenciais dos quais a organização depende para operações críticas, em especial os integrados na cadeia de fornecimento das TIC (hardware, software, serviços na nuvem, telecomunicações e serviços geridos).

2.2 Abrange funções internas, incluindo compras, gestão de fornecedores, gestão de riscos e departamentos operacionais relevantes. Abrange igualmente esses fornecedores, na medida necessária à recolha de informação de risco. Consideram-se “fornecedores críticos” aqueles cuja falha ou comprometimento possa afetar significativamente a nossa capacidade de prestar serviços ou cumprir obrigações legais.

3. Objetivos

3.1 Obter visibilidade sobre as dependências da cadeia de fornecimento, nomeadamente através da identificação de pontos únicos de falha ou de risco elevado de concentração na nossa base de fornecedores (por exemplo, dependência de um único prestador de serviços na nuvem para todos os serviços).

3.2 Implementar medidas para reduzir e gerir riscos relacionados com fornecedores, tais como diversificação, planos de contingência ou exigência de reforço dos controlos do fornecedor, reforçando assim a resiliência face a falhas de fornecedores ou a ataques com origem na cadeia de fornecimento.

3.3 Assegurar o alinhamento com os requisitos da NIS2 através da integração, nas decisões de risco da organização, dos resultados de quaisquer avaliações coordenadas de risco de segurança sobre

cadeias de fornecimento críticas (nos termos do artigo 22.º), garantindo que a nossa abordagem ao risco da cadeia de fornecimento se encontra documentada e é demonstrável.

4. Papéis e responsabilidades

4.1 Gabinete de Gestão de Fornecedores (VMO): é responsável pelo registo das dependências de fornecedores e coordena as avaliações de risco. Assegura que, durante a integração de fornecedores e periodicamente daí em diante, cada fornecedor-chave é avaliado quanto à sua criticidade e ao nível de dependência.

4.2 Gestão de Riscos (Comité de Risco Empresarial): revê o risco de concentração e as análises de dependência, e valida as estratégias de tratamento do risco (por exemplo, aprovar a introdução de um fornecedor alternativo ou manter inventário adicional para componentes críticos). Incorpora o risco da cadeia de fornecimento no Registo de Riscos global e reporta à direção de topo.

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Monitorização e auditoria

9.1 O registo de dependências e as avaliações de risco serão sujeitos a auditoria interna numa base anual. A Auditoria Interna verificará se todos os fornecedores críticos estão registados, se as suas classificações de risco estão atualizadas e se existem planos de mitigação definidos e em execução. Verificará igualmente se os contributos externos para avaliação de risco (relatórios ao abrigo do artigo 22.º, etc.) foram devidamente considerados.

9.2 A eficácia das medidas de diversificação e de contingência será testada periodicamente. Por exemplo, poderá ser realizada uma simulação planeada em que se assume a falha de um fornecedor principal, com o objetivo de testar os nossos planos de continuidade e os mecanismos alternativos (de forma semelhante a um exercício de recuperação de desastre, mas para indisponibilidade de fornecedor). Os resultados destes testes serão documentados e quaisquer deficiências serão corrigidas.

9.3 Métricas: a função de Gestão de Riscos acompanhará métricas como “% de serviços críticos com pelo menos um fornecedor ou solução alternativa disponível” ou “Top 5 dependências de fornecedores e respetiva tendência de risco”. Estas métricas serão incluídas em painéis de risco dirigidos à gestão de topo. Uma tendência decrescente do risco de dependência ao longo do tempo é um objetivo; se as métricas indicarem aumento da dependência, tal deve desencadear discussão pela gestão.

10. Revisão e manutenção

10.1 Esta política será revista pelo menos anualmente pelas equipas de gestão de fornecedores e de gestão de riscos. A revisão incorporará quaisquer alterações no panorama de fornecedores (por exemplo, se um novo fornecedor se tornar crítico ou se um fornecedor anterior for descontinuado progressivamente) e quaisquer novos requisitos regulamentares relativos a outsourcing ou risco de terceiros.

10.2 Se autoridades setoriais emitirem orientações atualizadas ou se um incidente revelar lacunas (por exemplo, se a indisponibilidade de um fornecedor tiver tido impacto superior ao previsto, indicando que a nossa avaliação de risco subestimou a dependência), a política será atualizada para aperfeiçoar critérios ou estratégias de mitigação.

10.3 As versões revistas da política devem ser aprovadas pela direção de topo. Alterações significativas serão comunicadas a todos os departamentos relevantes, e os materiais de formação serão atualizados em conformidade para refletir novos procedimentos ou normas.

11. Políticas relacionadas e ligações

11.1 P01 – Política de Segurança da Informação. Atribui responsabilidade pela governação da dependência de fornecedores.

11.2 P02 – Política de Papéis e Responsabilidades de Governação. Clarifica a titularidade das decisões sobre risco de fornecedores.

11.3 P06 – Política de Gestão de Riscos. Integra o risco de concentração nos registos de risco empresariais.

11.4 P26 – Política de Segurança de Terceiros e Fornecedores. Estabelece a linha de base de segurança; a P41 acrescenta controlos de dependência/concentração.

11.5 P27 – Política de Utilização da Cloud. Aplica critérios de dependência à adoção de serviços cloud e aos planos de saída.

11.6 P28 – Política de Desenvolvimento Externalizado. Abrange riscos de dependência na engenharia externa.

11.7 P32 – Política de Continuidade do Negócio e Recuperação de Desastre. Planeia cenários de indisponibilidade/substituição de fornecedores.

11.8 P37 – Política de Cumprimento Jurídico e Regulatório. Assegura que contratos/obrigações refletem controlos de dependência.

12. Referências

12.1 Diretiva NIS2 (UE 2022/2555), artigo 21.º, n.º 3 (exige a consideração das vulnerabilidades específicas de cada fornecedor direto/prestador de serviços e da qualidade da sua cibersegurança, incluindo os resultados de avaliações coordenadas de risco da cadeia de fornecimento)

12.2 Diretiva NIS2, artigo 22.º, n.º 1 (avaliações coordenadas de risco de segurança ao nível da União sobre cadeias de fornecimento críticas — informa as entidades sobre riscos de fornecedores à escala setorial)

12.3 Regulamento de Execução da Comissão (UE) 2024/2690, Anexo, secção 5 (requisitos de segurança da cadeia de fornecimento para entidades, incluindo critérios para seleção de fornecedores, diversificação e obrigações contratuais)

12.4 Boas práticas da ENISA para a cibersegurança da cadeia de fornecimento (2022) — recomendações sobre identificação de fornecedores críticos e gestão dos riscos associados

12.5 ISO/IEC 27001:2022 / ISO/IEC 27002:2022