					Insira aqui a designação da entidade jurídica registada							
Número do documento: P26					Título do documento: **Política de Segurança de Terceiros e 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	Cláusula 8	Planeamento e controlo operacional: requer controlos formais sobre serviços de terceiros com impacto no SGSI
ISO/IEC 27002:2022	Controlos 5.19–5.22	Políticas e procedimentos para relações com fornecedores; gestão do risco de fornecedores; gestão da prestação de serviços de fornecedores; monitorização e revisão de fornecedores
NIST SP 800-53 Rev. 5	SA-9, SA-10, CA-3, PS-7	Serviços de sistemas externos; gestão da configuração do fornecedor; interligações de sistemas; segurança do pessoal de terceiros
RGPD da UE	Artigos 28, 32, 33	Obrigações dos subcontratantes no tratamento de dados, segurança do tratamento, notificação de uma violação de dados pessoais
Diretiva NIS2 da UE	Artigo 21(2)(e–f)	gestão de fornecedores baseada no risco e supervisão da segurança
DORA da UE	Artigos 28, 30	Risco de terceiros em TIC, supervisão de prestadores terceiros críticos de TIC
COBIT 2019	BAI05, DSS02, MEA03	Gerir a capacitação para a mudança organizacional; gerir pedidos de serviço e incidentes; monitorizar, avaliar e analisar o cumprimento

1. Finalidade

1.1 Esta política define os requisitos de segurança da informação para estabelecer, gerir e manter relações seguras com fornecedores e prestadores de serviços terceiros.

1.2 Assegura que todos os fornecedores com acesso aos dados, sistemas ou infraestruturas da organização ficam sujeitos a controlos de segurança rigorosos, salvaguardas contratuais e supervisão contínua ao longo de todo o ciclo de vida do serviço.

1.3 A política suporta os controlos 5.19 a 5.22 do Anexo A da ISO/IEC 27001, incorporando requisitos de segurança nos processos de aquisição, integração de fornecedores, diligência prévia de fornecedores, gestão contratual, monitorização do serviço e cessação.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os fornecedores terceiros, contratados, prestadores de serviços na cloud e organizações prestadoras de serviços que tratem ou acedam aos ativos de informação da organização

2.1.2 Todas as funções internas envolvidas na avaliação de fornecedores, integração de fornecedores, contratação, gestão de riscos, monitorização ou cessação

2.1.3 Todas as relações com fornecedores que incluam acesso a dados sensíveis, integração com serviços em produção ou suporte a funções críticas do negócio

2.2 Abrange tanto fornecedores diretos como os respetivos subcontratantes, quando aplicável, e inclui software de terceiros, infraestrutura, suporte e serviços geridos.

3. Objetivos

3.1 Assegurar que os riscos de segurança associados a fornecedores são identificados, avaliados e mitigados de forma consistente ao longo do ciclo de vida da relação.

3.2 Incorporar requisitos de segurança normalizados em todos os contratos com fornecedores, incluindo obrigações de notificação de violações, cláusulas de direito de auditoria e responsabilidades de proteção de dados.

3.3 Exigir diligência prévia formal e avaliações de risco documentadas antes da contratação de novos fornecedores ou da renovação de acordos de serviço de alto risco.

3.4 Estabelecer mecanismos de monitorização contínua do cumprimento dos fornecedores, incluindo avaliações de desempenho, auditorias e escalonamento de incidentes.

3.5 Gerir alterações aos serviços dos fornecedores e impor um processo de cessação seguro, bem como a devolução ou destruição de dados aquando da cessação.

3.6 Alinhar os controlos de segurança de terceiros com as obrigações regulatórias e contratuais aplicáveis, incluindo o RGPD da UE, a Diretiva NIS2 da UE, a DORA da UE e as normas ISO/IEC 27001.

4. Papéis e responsabilidades

4.1 Diretor de Segurança da Informação (CISO)

4.1.1 É o responsável por esta política e assegura o seu alinhamento com o SGSI global, a gestão de riscos e a estratégia de conformidade.

4.1.2 Aprova os níveis de classificação de fornecedores, os resultados das revisões de segurança e as exceções de alto risco.

4.1.3 Participa no escalonamento de incidentes graves relacionados com fornecedores e nas negociações contratuais relativas a serviços críticos.

4.2 Aquisição e gestão de fornecedores

4.2.1 Assegura que todos os contratos novos e renovados com fornecedores incorporam cláusulas aprovadas de segurança e proteção de dados.

4.2.2 Mantém o registo centralizado de fornecedores e coordena-se com Recursos Humanos e com o Jurídico em matéria de documentação do risco de terceiros.

4.2.3 Inicia os processos de integração de fornecedores e assegura o alinhamento com as avaliações de segurança pré-contratuais.

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

9. Requisitos de revisão e atualização

9.1 Esta política deve ser revista, pelo menos, anualmente, ou antes disso em caso de:

9.1.1 Alterações materiais à estratégia de aquisição ou ao ecossistema de fornecedores

9.1.2 Atualizações dos quadros legais ou regulatórios (por exemplo, DORA da UE, RGPD da UE)

9.1.3 Incidentes relevantes de terceiros, violações de dados ou falhas de auditoria

9.1.4 Constatações provenientes de avaliações de risco ou de organismos externos de certificação

9.2 O processo de revisão é da responsabilidade conjunta do CISO e das funções de Aquisição, Jurídico e gestão de riscos.

9.3 Todas as revisões da política devem ser documentadas no registo de controlo documental do SGSI, sujeitas a controlo de versões e comunicadas às partes interessadas relevantes através dos canais de governação de fornecedores e dos programas de sensibilização dos trabalhadores.

9.4 As versões substituídas devem ser arquivadas por um período mínimo de três anos para efeitos de rastreabilidade e cumprimento legal.

10. Políticas relacionadas e ligações

10.1 P1 – Política de Segurança da Informação. Estabelece o compromisso global de proteger todas as operações da organização, incluindo a dependência de fornecedores terceiros e prestadores externos de serviços de TI.

10.2 P6 – Política de Gestão de Riscos. Orienta a identificação, avaliação e mitigação de riscos associados a relações com terceiros, incluindo riscos herdados ou sistémicos decorrentes do ecossistema de fornecedores.

10.3 P17 – Política de Proteção de Dados e Privacidade. Aplica-se a todos os fornecedores que tratem dados pessoais, exigindo termos contratuais adequados, salvaguardas de transferência e princípios de privacidade desde a conceção.

10.4 P4 – Política de Controlo de Acesso. Controla a forma como o pessoal de terceiros obtém acesso aos sistemas da organização, impondo permissões baseadas em funções, controlos de sessão e procedimentos de revogação.

10.5 P22 – Política de Registo e Monitorização. Exige que o acesso de fornecedores aos sistemas seja monitorizado, registado e revisto, em particular em ambientes onde ocorram atividades privilegiadas ou centradas em dados.

10.6 P30 – Política de Resposta a Incidentes (P30). Define os procedimentos de escalonamento e os requisitos de notificação de violações para eventos de segurança com origem em fornecedores ou investigações conjuntas que envolvam sistemas de terceiros.

11. Normas e quadros de referência

11.1 ISO/IEC 27001: Cláusula 8.1 – Planeamento e controlo operacional: requer controlos formais sobre serviços de terceiros com impacto no SGSI.

11.2 ISO/IEC 27002:2022 – Controlos 5.19 a 5.22:

11.2.1 Controlo do Anexo A 5.19 – Políticas e procedimentos para relações com fornecedores: impõe controlos para gerir as interações com fornecedores.

11.2.2 Controlo do Anexo A 5.20 – Gestão do risco de fornecedores: centra-se na identificação, avaliação e supervisão contínua da postura de segurança dos fornecedores.

11.2.3 Controlo do Anexo A 5.21 – Gestão da prestação de serviços de fornecedores: requer alinhamento do desempenho e da segurança com as expectativas contratuais.

11.2.4 Controlo do Anexo A 5.22 – Monitorização e revisão de fornecedores: reforça a necessidade de validação contínua e reavaliação do cumprimento por parte de terceiros.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 SA-9 – Serviços de sistemas externos: define requisitos de segurança e de risco para sistemas operados por entidades externas.

11.3.2 SA-10 – Gestão da configuração do fornecedor: aplica-se quando terceiros fornecem software ou ambientes.

11.3.3 CA-3 – Interligações de sistemas: requer supervisão e acordo sobre os fluxos de dados entre sistemas de diferentes entidades.

11.3.4 PS-7 – Segurança do pessoal de terceiros: assegura que contratados e pessoal de fornecedores são adequadamente verificados e monitorizados.

11.4 RGPD da UE (2016/679):

11.4.1 Artigo 28 – Obrigações dos subcontratantes no tratamento de dados: requer acordos escritos com subcontratantes no tratamento de dados, incluindo medidas técnicas e organizativas (TOMs).

11.4.2 Artigo 32 – Segurança do tratamento: impõe salvaguardas adequadas tanto aos responsáveis pelo tratamento como aos subcontratantes.

11.4.3 Artigo 33 – Notificação de uma violação de dados pessoais: exige notificação célere por parte dos fornecedores em caso de violação.

11.5 Diretiva NIS2 da UE (2022/2555):

11.5.1 Artigo 21(2)(e–f): exige gestão de fornecedores baseada no risco e supervisão da segurança, em especial nas cadeias de fornecimento digitais de entidades essenciais e importantes.

11.6 DORA da UE (2022/2554):

11.6.1 Artigo 28 – Risco de terceiros em TIC: impõe obrigações de avaliação de risco, termos contratuais de segurança e estratégias de saída para prestadores de serviços financeiros.

11.6.2 Artigo 30 – Supervisão de prestadores terceiros críticos de TIC: estabelece expectativas reforçadas de monitorização e supervisão para fornecedores-chave.

11.7 COBIT 2019:

11.7.1 BAI05 – Gerir a capacitação para a mudança organizacional: assegura que as transições de fornecedores são governadas de forma segura.

11.7.2 DSS02 – Gerir pedidos de serviço e incidentes: aplica-se a questões comunicadas por fornecedores e à integração do tratamento de incidentes.

11.7.3 MEA03 – Monitorizar, avaliar e analisar o cumprimento: reforça a medição do desempenho dos fornecedores e a monitorização do cumprimento.