					Insira aqui a designação da entidade jurídica registada							
Número do documento: P27S					Título do documento: **Política de Utilização de Serviços Cloud P27S**							
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**

Alinhada com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 8	
ISO/IEC 27002:2022	Controlos 5.23–5.25	
NIST SP 800-53 Rev. 5	AC-20, SC-12, SC-13, SR-5	
RGPD da UE	Artigo 28, 32 e Capítulo V	
Diretiva NIS2 da UE	Artigos 21(2)(f), (i)	
DORA da UE	Artigos 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI04	

1. Finalidade

1.1 A presente política define de que forma os serviços cloud podem ser utilizados de forma segura na organização. Assegura que os dados tratados ou armazenados na cloud estão protegidos, que os acessos são controlados e que os riscos são geridos de forma responsável.

1.2 Esta política ajuda as PME a cumprir obrigações legais e expectativas dos clientes relativas à proteção de informação sensível, à prevenção de fugas de dados e à gestão eficaz dos riscos associados à utilização da cloud, sem exigir infraestruturas de escala empresarial.

1.3 Esta política apoia a certificação ISO/IEC 27001, o cumprimento do RGPD e a segurança da cadeia de fornecimento através de uma governação consistente de todos os serviços cloud de terceiros.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Qualquer serviço cloud utilizado para armazenar, tratar ou transmitir dados da organização

2.1.2 Todos os colaboradores, prestadores de serviços ou fornecedores que utilizem ferramentas cloud em nome da organização

2.1.3 Soluções cloud gratuitas e pagas, incluindo plataformas de correio eletrónico, partilha de documentos, ferramentas SaaS, plataformas de cópia de segurança, videoconferência e plataformas de gestão de clientes

2.1.4 Qualquer dispositivo (computador, dispositivo móvel, tablet) que aceda a informação da organização através de aplicações cloud

2.2 Isto inclui, sem caráter limitativo:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business

2.2.2 Zoom, Microsoft Teams, Google Meet

2.2.3 AWS, Azure, GCP

2.2.4 Ferramentas cloud de cópia de segurança e recuperação de desastre

2.2.5 Pastas partilhadas ou aplicações utilizadas para faturação, gestão de projetos ou comunicação com clientes

3. Objetivos

3.1 Prevenir a utilização não autorizada ou de risco elevado de serviços cloud não aprovados.

3.2 Assegurar que os dados sensíveis ou regulamentados armazenados na cloud são protegidos através de controlos técnicos e organizativos adequados.

3.3 Definir responsabilidades claras para a aprovação, configuração, monitorização e desativação de serviços cloud.

3.4 Controlar os fluxos de dados e assegurar o cumprimento das obrigações de retenção, eliminação e privacidade aplicáveis à informação armazenada na cloud.

3.5 Reduzir a dependência de contas pessoais ou ferramentas não controladas, exigindo a aprovação de todos os sistemas cloud utilizados para fins empresariais.

3.6 Cumprir os requisitos da ISO/IEC 27001:2022, do RGPD, da NIS2 e do DORA para a gestão de dependências externas de serviços cloud.

4. Papéis e responsabilidades

4.1 Diretor-Geral (DG)

4.1.1 Aprova a utilização de todos os novos serviços cloud

4.1.2 Revê os riscos associados aos fornecedores cloud e aos tipos de serviço

4.1.3 Assegura a aplicação da política e supervisiona as decisões de exceção

4.2 Prestador de serviços de TI ou suporte técnico

4.2.1 Avalia e implementa a configuração segura dos serviços cloud

4.2.2 Configura contas, controlos de acesso e cópias de segurança

4.2.3 Monitoriza o cumprimento dos requisitos de palavra-passe, MFA e definições de segurança

[... 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 pelo Diretor-Geral, em coordenação com o prestador de serviços de TI.

9.2 Deve igualmente ocorrer uma revisão formal:

9.2.1 Após um incidente de segurança relacionado com a cloud (por exemplo, violação de dados, perda de dados)

9.2.2 Quando for introduzida uma nova plataforma cloud de maior relevância

9.2.3 Se os requisitos legais ou regulamentares forem alterados (por exemplo, atualizações ao RGPD, NIS2 ou DORA)

9.2.4 Se as atividades de monitorização revelarem utilização indevida ou novos riscos

9.3 O DG deve assegurar que:

9.3.1 O Registo de Serviços Cloud é atualizado com serviços novos ou descontinuados

9.3.2 Os requisitos legais e de privacidade continuam a ser cumpridos

9.3.3 Todas as alterações são comunicadas aos utilizadores e às partes interessadas relevantes

9.4 As versões arquivadas devem ser armazenadas de forma segura, e as versões antigas da política devem ser tratadas de acordo com a política P14S – Política de Retenção e Eliminação de Dados da organização.

10. Políticas relacionadas e articulações

10.1 Esta política deve ser utilizada em articulação com as seguintes políticas de segurança da informação alinhadas para PME:

10.1.1 P2S – Política de Papéis e Responsabilidades de Governação: define a responsabilização pela aprovação de serviços cloud e pela gestão das relações com fornecedores.

10.1.2 P4S – Política de Controlo de Acessos: suporta as práticas de início de sessão seguro, gestão de sessões e revogação de acessos exigidas para plataformas cloud.

10.1.3 P14S – Política de Retenção e Eliminação de Dados: regula a forma como os dados na cloud são objeto de cópia de segurança, retenção e eliminação em conformidade com as obrigações legais.

10.1.4 P17S – Política de Proteção de Dados e Privacidade: assegura que quaisquer dados pessoais armazenados em serviços cloud são tratados de acordo com os princípios do RGPD.

10.1.5 P30S – Política de Resposta a Incidentes: estabelece procedimentos estruturados para responder a incidentes de segurança na cloud, incluindo recolha de evidência e notificação externa.

10.2 Em conjunto, estas políticas asseguram que a utilização da cloud é segura, conforme e operacionalmente resiliente.

11. Normas e referenciais

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Exige que as organizações implementem controlos operacionais para o tratamento de dados, incluindo os relacionados com sistemas cloud.

11.2 ISO/IEC 27002

11.2.1 Controlo 5.23 – Exige governação sobre a utilização de serviços cloud e ferramentas SaaS de terceiros.

11.2.2 Controlo 5.24 – Exige uma política definida para a utilização da cloud, alinhada com os riscos e os requisitos regulamentares.

11.2.3 Controlo 5.25 – Exige que as organizações assegurem que os controlos de segurança em ambientes cloud satisfazem as necessidades da organização.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – Exige políticas formais de utilização para sistemas externos, tais como serviços cloud.

11.3.2 SC-12, SC-13 – Abordam a cifragem de dados em trânsito e em repouso em ambientes cloud.

11.3.3 SR-5 – Abrange controlos de risco cloud e de terceiros no âmbito da cadeia de fornecimento.

11.4 RGPD da UE (2016/679)

11.4.1 Artigo 28 – Exige que os prestadores cloud que atuem como subcontratantes cumpram obrigações contratuais vinculativas.

11.4.2 Artigo 32 – Exige controlos técnicos e organizativos para o tratamento de dados em ambientes cloud.

11.4.3 Capítulo V – Proíbe transferências internacionais não autorizadas de dados pessoais armazenados na cloud.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(f), (i) – Exige que as entidades essenciais e importantes implementem políticas adequadas para a segurança dos serviços cloud e o controlo da cadeia de fornecimento.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 5(2) – Exige que as PME financeiras integrem a segurança cloud nos seus quadros de gestão do risco das TIC.

11.6.2 Artigo 28 – Estabelece regras de supervisão para prestadores terceiros críticos de serviços TIC, incluindo fornecedores cloud.

11.7 COBIT 2019

11.7.1 DSS01 – “Gerir Operações” aborda a integridade operacional dos serviços cloud.

11.7.2 DSS05 – “Gerir Serviços de Segurança” inclui proteções e monitorização específicas para cloud.

11.7.3 BAI04 – “Gerir Disponibilidade e Capacidade” assegura a continuidade do negócio e o desempenho em ambientes cloud.