					Insira aqui a designação da entidade jurídica registada							
Número do documento: P27					Título do documento: **Política de Utilização da Cloud**							
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	Requisitos de planeamento e controlo operacional em ambiente cloud.
ISO/IEC 27002:2022	Controlos 5.23–5.25	Requisitos relativos à utilização, política e segurança dos serviços cloud.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12–SC-28, SR-5	Utilização de sistemas externos, requisitos contratuais e técnicos, proteções criptográficas e proteção da cadeia de abastecimento.
RGPD da UE	Artigos 28, 32, Capítulo V	Requisitos aplicáveis a subcontratantes cloud, segurança do tratamento e transferências de dados.
Diretiva NIS2 da UE	Artigo 21(2)(f, i)	Requisitos relativos ao risco de terceiros e à cadeia de abastecimento.
DORA da UE	Artigos 5(2), 28	Governação das TIC e supervisão de terceiros cloud para entidades financeiras.
COBIT 2019	BAI04, DSS01, DSS05	Disponibilidade cloud, operações e gestão da segurança.

1. Finalidade

1.1 A presente política estabelece os requisitos obrigatórios da organização para a utilização segura, conforme e responsável de serviços de computação em cloud nos modelos de prestação Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) e Software-as-a-Service (SaaS).

1.2 A política visa assegurar que os serviços cloud são adotados e governados de forma a proteger a confidencialidade, integridade e disponibilidade dos ativos de informação, cumprindo simultaneamente as obrigações regulamentares, legais e contratuais.

1.3 Define controlos para gerir o risco associado à cloud, proteger os dados, monitorizar o cumprimento por parte dos fornecedores e eliminar utilizações não autorizadas. Apoia igualmente a inovação do negócio através de plataformas cloud, alinhando segurança, fiabilidade operacional e eficiência de custos.

2. Âmbito

2.1 A presente política aplica-se a todos os colaboradores, prestadores de serviços, fornecedores terceiros e consultores externos que aprovisionem, configurem, acedam, administrem ou utilizem serviços cloud em nome da organização.

2.2 Aplica-se a todos os ambientes em que os dados ou cargas de trabalho da organização sejam tratados, incluindo:

2.2.1 Implementações de cloud pública, privada, híbrida e comunitária

2.2.2 Todos os modelos de serviço cloud (IaaS, PaaS, SaaS)

2.2.3 Arquiteturas multicloud e federadas

2.2.4 Utilização de shadow IT ou de contas cloud pessoais para fins profissionais

2.3 Abrange todas as classificações de dados e aplica-se tanto a sistemas internos como a plataformas alojadas por fornecedores nas quais sejam armazenados ou tratados dados da organização ou dados sujeitos a regulação.

3. Objetivos

3.1 Assegurar uma utilização segura e consistente das tecnologias cloud através de orientações de utilização claramente definidas, referenciais de segurança e papéis de governação.

3.2 Minimizar os riscos operacionais e regulamentares associados à computação em cloud, incluindo acesso não autorizado, violações de dados, configurações incorretas, incumprimento e interrupção de serviço.

3.3 Impor requisitos de segurança e privacidade a todos os fornecedores cloud e verificar o respetivo cumprimento através de cláusulas contratuais, avaliações e direitos de auditoria.

3.4 Permitir uma adoção da cloud escalável e resiliente sem comprometer a postura de segurança, os requisitos legais ou a continuidade do negócio.

3.5 Alinhar a governação e a utilização da cloud com o SGSI da organização, as obrigações legais (por exemplo, RGPD, DORA), orientações setoriais e boas práticas reconhecidas no setor (por exemplo, NIST, COBIT).

4. Papéis e responsabilidades

4.1 Gestão Executiva

4.1.1 Aprova a Política de Utilização da Cloud e o roteiro estratégico de adoção da cloud.

4.1.2 Revê e valida exceções de risco elevado aos requisitos normais de governação da cloud.

4.1.3 Assegura que as iniciativas cloud dispõem de financiamento, supervisão e integração adequados com os referenciais de risco empresariais.

4.2 Chief Information Security Officer (CISO)

4.2.1 É responsável pela presente política e pelo Registo de Serviços Cloud da organização.

4.2.2 Aprova a integração de novos fornecedores cloud com base em diligência prévia e avaliação de risco.

4.2.3 Revê a documentação de conformidade dos fornecedores e valida o alinhamento 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 A presente política deve ser revista pelo menos anualmente e atualizada sempre que necessário para assegurar o alinhamento contínuo com:

9.1.1 A evolução dos requisitos legais e regulamentares (por exemplo, RGPD, NIS2, DORA)

9.1.2 Alterações às normas ISO/IEC 27001 ou ISO/IEC 27002

9.1.3 Atualizações da arquitetura cloud, do panorama de risco ou do portefólio de serviços da organização

9.1.4 Investigações de incidentes, resultados de auditoria ou lições aprendidas com a utilização operacional

9.2 O CISO é responsável por iniciar a revisão e reunir as partes interessadas relevantes, incluindo:

9.2.1 Arquiteto de Segurança Cloud

9.2.2 Equipa Jurídica e de Compliance

9.2.3 Compras e Gestores de Fornecedores

9.2.4 Proprietários de Serviço e Operações de TI

9.3 Todas as atualizações devem ser:

9.3.1 Sujeitas a controlo de versões e datadas

9.3.2 Aprovadas pela Gestão Executiva

9.3.3 Comunicadas às partes afetadas, incluindo colaboradores, prestadores de serviços e terceiros

9.3.4 Arquivadas em conformidade com as políticas internas de documentação

9.4 Revisões intercalares podem ser desencadeadas por:

9.4.1 Novas contratações de CSP ou migrações de grande dimensão

9.4.2 Ameaças emergentes à infraestrutura cloud

9.4.3 Alterações materiais nas obrigações contratuais, legais ou setoriais

10. Políticas relacionadas e ligações

10.1 A presente política está estreitamente ligada e dependente das seguintes políticas internas:

10.1.1 P1 – Política de Segurança da Informação: Estabelece os princípios gerais que regem a operação segura de sistemas e serviços, aplicados pela presente política ao contexto cloud.

10.1.2 P5 – Política de Gestão da Mudança: Todas as alterações de configuração cloud devem seguir os procedimentos de controlo de alterações definidos na P5.

10.1.3 P13 – Política de Classificação e Rotulagem da Informação: Determina como os dados são avaliados antes da transferência para a cloud e como são aplicados controlos como cifragem e residência.

10.1.4 P18 – Política de Controlos Criptográficos: Define normas para cifragem, gestão de chaves e utilização de algoritmos criptográficos, aplicadas diretamente nas configurações dos serviços cloud.

10.1.5 P22 – Política de Registo de Eventos e Monitorização: Especifica os requisitos para recolha, retenção e análise de registos, que devem ser aplicados em ambientes cloud.

10.1.6 P30 – Política de Resposta a Incidentes: Define os procedimentos de escalonamento, contenção e remediação para eventos de segurança relacionados com a cloud.

10.1.7 P33 – Política de Monitorização de Auditoria e Conformidade: Apoia a preparação para auditoria e a garantia contínua de que os controlos cloud são aplicados e monitorizados.

11. Normas e referenciais de referência

11.1 ISO/IEC 27001: Cláusula 8.1 – Planeamento e controlo operacional: Exige que as organizações implementem e controlem os processos necessários para cumprir os requisitos de segurança da informação, incluindo os que envolvem ambientes cloud.

11.2 ISO/IEC 27002:2022 – Controlos 5.23 a 5.25:

11.2.1 Anexo A Controlo 5.23 – Utilização de serviços cloud: Exige avaliação baseada no risco, autorização formal e documentação da utilização de serviços cloud.

11.2.2 Anexo A Controlo 5.24 – Política de utilização da cloud: Exige o estabelecimento e a aplicação de políticas formais de utilização da cloud alinhadas com as necessidades e os riscos da organização.

11.2.3 Anexo A Controlo 5.25 – Segurança em serviços cloud: Exige a integração da segurança, proteções contratuais e monitorização de cargas de trabalho e dados alojados na cloud.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Utilização de sistemas externos: Exige regras e condições definidas para o acesso a recursos da organização a partir de sistemas externos ou baseados em cloud.

11.3.2 SA-9(5) – Serviços de sistemas de informação externos: Exige requisitos contratuais de segurança, supervisão e monitorização contínua para sistemas cloud de terceiros.

11.3.3 SC-12 a SC-28 – Proteções criptográficas, defesa de perímetro e integridade da transmissão: Alinham-se com os requisitos de cifragem, identidade e acesso para serviços alojados na cloud e dados em trânsito.

11.3.4 SR-5 – Proteção da cadeia de abastecimento: Suporta a avaliação e o controlo contratual sobre CSP envolvidos na prestação do serviço.

11.4 RGPD da UE (2016/679):

11.4.1 Artigo 28.º – Obrigações do subcontratante: Exige contratos formais com fornecedores cloud para assegurar a segurança, confidencialidade e auditabilidade do tratamento de dados pessoais.

11.4.2 Artigo 32.º – Segurança do tratamento: Sustenta a aplicação de cifragem, controlos de acesso, registo de eventos e outras salvaguardas em ambientes cloud.

11.4.3 Capítulo V – Transferências internacionais de dados: Exige a transferência lícita de dados para fora da UE/EEE com recurso a salvaguardas como SCC ou decisões de adequação.

11.5 Diretiva NIS2 da UE (2022/2555):

11.5.1 Artigo 21(2)(f, i): Exige que as entidades gerem os riscos decorrentes de fornecedores terceiros de serviços cloud e assegurem a integridade da cadeia de abastecimento digital através de medidas contratuais e técnicas.

11.6 DORA da UE (2022/2554):

11.6.1 Artigo 5(2) – Governação dos riscos de TIC: Exige a integração do risco de terceiros de TIC, incluindo serviços cloud, na governação global do risco.

11.6.2 Artigo 28.º – Supervisão de prestadores terceiros críticos de serviços de TIC: Exige que as entidades financeiras monitorizem, controlem e reportem dependências de fornecedores cloud, postura de segurança e resiliência.

11.7 COBIT 2019:

11.7.1 BAI04 – Gerir a disponibilidade e a capacidade: Assegura que os serviços cloud são resilientes, monitorizados e cumprem critérios de desempenho definidos.

11.7.2 DSS01 – Gerir operações: Suporta a integração operacional, o tratamento de incidentes e os referenciais de configuração em plataformas alojadas na cloud.

11.7.3 DSS05 – Gerir serviços de segurança: Orienta a implementação de controlos de segurança específicos para cloud, monitorização e prevenção de incidentes nos serviços digitais.