Política de Fornecedores

Data Criação:	20 de Junho de 2025
Data Aprovação:	30 de Setembro de 2025
Versão:	4
Proprietário:	Conselho de Administração
Classificação da Informação:	PÚBLICA
Lista de Distribuição:	Público em Geral

Histórico de Alterações

Versão	Data Aprovação	Descrição das Alterações	Responsável:	Revisto por:	Aprovado por:
1	17-05-2022	-	DEO-UEO	DdC e CE	CA
2	19-09-2022	Alteração da classificação da informação, de "Uso Interno" para "Pública"; Introdução do conceito de Fornecedor Crítico e respectivas orientações; e Reorganização da informação ao nível dos requisitos da Segurança da Informação.	DEO-UEO	DdC e FSI	CA
3	20-01-2023	Introdução da aplicabilidade de presente Política para compras ou fornecimento de serviços de montante igual ou superior a 5.000 EUR e clarificação dos documentos a apresentar aos fornecedores não críticos.	DEO-UEO	DdC	CA
4	30-09-2025	Incorporação dos requisitos do Regulamento DORA conforme *gap assessment.*	DdC	CF	CA

Índice

1. Âmbito e Objectivo 5

2. Glossário 5

3. Intervenientes e Responsabilidades 7

4. Destinatários 11

5. Princípios Orientadores 11

6. Política de fornecedores 12

6.1. Compromissos de âmbito Ético, Social, Ambiental, Continuidade do Negócio e Saúde e Segurança no Trabalho 12

6.2. Selecção, Aprovação e Adjudicação 14

6.3. Orientações Específicas – Serviços de TIC 15

6.3.1. Análise Prévia 15

6.3.2. Disposições Contratuais 16

6.3.3. Monitorização Contínua 20

6.3.4. Registo de Informação 20

6.3.5. Deveres de Reporte 21

6.3.6. Estratégias de Saída 22

6.4. Orientações Específicas de Segurança da Informação 23

6.4.1. Requisitos gerais 23

6.4.2. Disposições Contratuais 24

6.5. Monitorização e Avaliação 26

6.5.1. Monitorização e Avaliação dos Serviços 26

6.5.2. Gestão da Mudança 27

7. Incumprimento 27

8. Monitorização (registo e documentação) 28

8.1. Registo 28

8.2. Documentação 28

9. Revisão, Aprovação e Divulgação 29

10. Enquadramento legal e regulamentar 29

11. Relação com outros documentos 30

Copyright

1. Âmbito e Objectivo

Assegurar a confiança e integridade dos fornecedores ou prestadores de serviços do Banco é fundamental para o seu negócio e para a segurança dos seus activos. A Política de Fornecedores visa os seguintes principais objectivos:

- Instituir um modelo de gestão e de governo interno associado ao estabelecimento, manutenção e cessação de relações de contratação, de modo a manter um nível adequado de controlo sobre as mesmas e gerir adequadamente os riscos que lhe estão associados;
- Encorajar os prestadores de serviços na adopção de uma conduta responsável idêntica à do BAIE, designadamente compromissos de índole ambiental, ética e social, bem como da adesão aos princípios gerais através do conhecimento do Código de Conduta do Banco;
- Assegurar que os acordos com fornecedores consideram a segurança da informação na prestação de serviços, sempre que aplicável;
- Garantir a protecção dos activos do Banco acessíveis por fornecedores e prestadores de serviços, sempre que aplicável; e
- Atribuir responsabilidades pela execução dos diversos procedimentos associados à contratação de serviços;

A presenta Política deve ser lida em conjunto com o Manual de Processo – Pedidos de Compras e o Manual de Processo - Gestão de Fornecedores TIC, Críticos e Subcontratantes.

2. Glossário

Activo - Qualquer componente (seja humano, tecnológico, *software*, entre outros) que suporte um ou mais processos de negócio de uma unidade ou área de negócio.

Contratação - Acordo que, independentemente da sua forma, seja celebrado entre o Banco e terceiros para prestação de serviços ou actividades que, sem esse acordo, não podem ser realizados pelo Banco.

Factores de sustentabilidade – As questões ambientais, sociais e laborais, o respeito dos direitos humanos, a luta contra a corrupção e o suborno.

Fornecedores - Entidades físicas ou jurídicas que produzem, montam, criam, constroem, transformam, importam, exportam, distribuem ou comercializam produtos ou serviços.

Fornecedores TIC – Entidade terceira que presta serviços TIC.

Fornecedores críticos – Fornecedor que dadas as suas especificidades e importância na actividade do Banco, a interrupção da prestação dos seus serviços colocaria em causa o desempenho operacional do Banco e, consequentemente, a sua estabilidade financeira.

Função crítica ou importante (CIF) – Função cuja perturbação compromete significativamente i) o desempenho financeiro de uma entidade financeira ou a solidez ou continuidade dos seus serviços e das suas actividades, ii) ou a interrupção, anomalia ou falha dessa função compromete significativamente o contínuo cumprimento das condições e obrigações decorrentes da autorização da entidade financeira, iii) ou das suas restantes obrigações ao abrigo do direito dos serviços financeiros aplicável.

Investimentos sustentáveis - correspondem a investimentos em actividades económicas com objectivos de natureza ambiental e/ou social, e/ou aqueles que não prejudiquem significativamente quaisquer objectivos de natureza sustentável e desde que as empresas beneficiárias empreguem práticas de boa governação, no que respeita a estruturas de gestão, relações laborais, práticas de remuneração e cumprimento das obrigações fiscais.

Prestador de serviços - Entidade terceira que realiza, no todo ou em parte, uma actividade, um processo ou um serviço ao abrigo de um acordo de (sub)contratação.

Serviços de TIC - Serviços digitais e de dados prestados por meio de sistemas de TIC a um ou mais utilizadores internos ou externos, de forma contínua incluindo equipamentos informáticos enquanto serviço e serviços de equipamento informático, o que inclui a prestação de apoio técnico através de actualizações de programas informáticos ou microprogramas pelo fornecedor de equipamentos informáticos, com exclusão dos serviços telefónicos analógicos tradicionais.

Subcontratação - Acordo que, independentemente da sua forma, seja celebrado entre o Banco e terceiros para prestação de serviços ou actividades que, sem esse acordo, seriam realizados pelo Banco.

Terceiros - Quaisquer pessoas externas ao Banco, incluindo entidades do Grupo BAI.

3. Intervenientes e Responsabilidades

Conselho de Administração (CA) - Órgão responsável, no âmbito das suas funções de gestão, por:

- Definir e aprovar a Política de Fornecedores;
- Garantir o alinhamento dos procedimentos de contratação com os objectivos estratégicos, cultura e valores do Banco, bem como com a legislação, regulamentação, orientações e boas práticas em vigor em matéria de contratação.

Comissão Executiva (CE) – Órgão responsável, no âmbito das suas funções de gestão, por:

- Garantir o alinhamento dos procedimentos de contratação com os objectivos estratégicos, cultura e valores do Banco, bem como com a legislação, regulamentação, orientações e boas práticas em vigor em matéria de contratação;
- Definir as responsabilidades das áreas de negócio e de suporte no âmbito da contratação;
- Assegurar a implementação dos procedimentos de controlo e de gestão de riscos associados à contratação;
- Garantir que o recurso à contratação não prejudica:
  - ✓ A manutenção, em permanência, das condições necessárias à manutenção da licença bancária;
  - ✓ A capacidade do Banco para respeitar as suas obrigações legais e regulamentares, bem como quaisquer condições impostas pelas autoridades competentes;
  - ✓ O controlo adequado da gestão corrente e da organização interna;
  - ✓ A identificação, avaliação e gestão de conflitos de interesses.
- Aprovar a celebração ou manutenção de todos os tipos de acordos de contratação;
- Apreciar os relatórios anuais de avaliação de riscos de contratação de serviços de TIC;
- Assegurar a divulgação da Política de Fornecedores a todos os colaboradores.

Conselho de Fiscal (CF) - Órgão responsável, no âmbito das suas funções de fiscalização, por:

- Apreciar e emitir parecer prévio sobre a Política de Fornecedores e sucessivas revisões;
- Fiscalizar e acompanhar a implementação da Política de Fornecedores;
- Avaliar a efectiva aplicação do sistema de gestão de riscos de contratação;
- Emitir um parecer prévio i) à aprovação da contratação de serviços de TIC que suportem funções críticas ou importantes (CIF) ou ii) nas situações em que o risco residual estimado é superior ao risco residual pretendido para a contratação;
- Realizar acções de controlo dentro das suas competências legais e regulamentares, no âmbito do processo de monitorização da cultura organizacional e dos sistemas de governo e controlo interno;
- Assegurar que o Banco avalia a adequação e eficácia da cultura organizacional, dos sistemas de governo e do controlo interno.

Comité de Acompanhamento da Gestão de Riscos (CAGR) - Comité responsável por assegurar o acompanhamento permanente do sistema de gestão dos riscos do Banco, bem como da adequação e da eficácia das medidas tomadas para corrigir eventuais deficiências desse sistema. No âmbito da monitorização, o CAGR é responsável por:

- Acompanhar, analisar e monitorizar, em sede de comité, os riscos de contratação de serviços de TIC;
- Apreciar medidas de mitigação e redução dos riscos de contratação de serviços de TIC;
- Apreciar os relatórios anuais de avaliação de riscos de contratação de serviços excepto fornecedores correntes, ou seja, fornecedores não TIC e não críticos e apresentação dos resultados dos mesmos ao Conselho de Administração, caso sejam identificados riscos materiais.

Departamento de *Compliance* (DdC) - Departamento responsável, no âmbito dos procedimentos de contratação, pela gestão global da contratação de terceiros no Banco. Em específico, é responsável:

- Pela revisão da Política de Fornecedores e sucessivas actualizações;
- Pelo controlo e acompanhamento da implementação e actualização dos procedimentos de contratação;
- Pela análise do risco de conformidade do prestador de serviços, com identificação do seguinte:
  - ✓ Eventuais situações de conflitos de interesse e indicação de medidas mitigatórias, caso aplicável, em conformidade com a Política de Conflito de Interesses e a Política de Partes Relacionadas em vigor no Banco;
  - ✓ Eventuais riscos em matéria reputacional ou de branqueamento de capitais e financiamento do terrorismo e indicação de medidas mitigadoras, caso aplicável;
  - ✓ Verificação de existência de autorizações legais e regulatórias, caso estejam em causa serviços de pagamento ou actividades bancárias que, pela sua natureza, necessitem de autorização de uma autoridade de supervisão competente, bem como as demais exigências regulamentares.
- Por garantir, em articulação com as respectivas áreas de negócio, o preenchimento inicial e a actualização contínua das avaliações de risco associados à contratação de serviços de TIC;
- Pelos deveres de reporte ao Banco de Portugal mencionados na presente Política; e

Função de Gestão de Riscos (FGR) - Função responsável por assegurar a aplicação efectiva do sistema de gestão de riscos do Banco de acordo com a respectiva política interna, através do acompanhamento constante da sua adequação e eficácia, bem como da adequação e da eficácia das medidas tomadas para corrigir eventuais deficiências desse sistema. No âmbito da contratação, a FGR é responsável:

- Pela prestação de aconselhamento ao CAGR em matéria de contratação de serviços de TIC;
- Pelo acompanhamento e supervisão dos riscos associados à contratação de serviços de TIC, com o apoio da FSI;
- Por validar as avaliações dos riscos decorrentes da contratação de serviços de TIC, com o apoio da FSI, incluindo os indicadores associados ao desempenho, a estimativa do impacto que o acordo de assume em

matéria de aumento ou diminuição do risco operacional e de concentração do Banco, bem como as medidas mitigatórias a adoptar, caso necessário;

- Por submeter à apreciação do CAGR os resultados das avaliações de riscos de contratação de serviços de TIC.

Função da Segurança da Informação (FSI) - Estrutura responsável, no âmbito das suas funções, pela definição, actualização e monitorização das políticas, normas, planos e processos respeitantes à segurança da informação. No âmbito da contratação, sempre que exista ligação de sistemas entre o Banco e fornecedor, tratamento e transferência de dados ou informação, a FSI tem a responsabilidade de:

- Definir os requisitos de segurança da informação a integrar no NDA do fornecedor;
- Identificar, analisar e avaliar os riscos de segurança da informação e definir a estratégia de tratamento dos mesmos (e.g., mitigação);
- Garantir que as actividades de terceiros são realizadas em conformidade com as Políticas e Normas de Segurança de Informação do Banco, definindo os controlos necessários para o efeito, em coordenação com a 1ª linha de defesa (e.g., DSI) e promover, caso necessário, auditorias de segurança;
- Gerir a segurança da informação de forma a assegurar a adequada protecção dos activos do Banco em termos de salvaguarda da confidencialidade, integridade e disponibilidade.

Unidade de Eficiência Operacional (UEO) – Estrutura integrada no Departamento de Eficiência e Operações (DEO), no âmbito das suas funções, responsável pelo acompanhamento dos fornecedores correntes.

Encarregado de Protecção de Dados (EPD) - Função responsável por controlar o cumprimento das obrigações em matéria de protecção de dados pessoais, cooperando com a Comissão Nacional de Protecção de Dados (CNPD) e servindo como ponto de contacto entre o Banco e a autoridade de controlo e para os titulares dos dados pessoais.
O EPD é responsável por emitir parecer sobre o impacto da contratação de serviços críticos em matéria de protecção de dados pessoais, caso esteja previsto a transferência ou tratamento de dados pessoais.

Estruturas Proponentes/ Contratantes - As áreas de negócio, funções de suporte ou de controlo que pretendam celebrar ou manter acordos de contratação relacionados com as suas áreas funcionais são responsáveis por:

- Obter informação respeitante aos prestadores de serviços que permita garantir a aplicação dos procedimentos de análise e de avaliação que se encontram definidos na presente Política;
- Identificar o tipo de contratação, através do correcto preenchimento dos *templates* de contratação, e cumprir os procedimentos previstos na presente Política;
- Assegurar a elaboração das estratégias de saída e/ou transição de acordos contratuais para a utilização de serviços de TIC prestados por terceiros que suportem funções críticas ou importantes (CIF);

- Analisar, em colaboração com o Responsável do Plano de Continuidade de Negócio, a capacidade dessa continuidade, nomeadamente no que diz respeito a estratégias de saída e planos de contingência, caso aplicável;
- Assegurar, em articulação com o Encarregado de Protecção de Dados, eventuais temas relacionados com a protecção de dados;
- Identificar, em colaboração com o Departamento de *Compliance*, eventuais situações de conflitos de interesses;
- Apresentar propostas de contratação para aprovação do Administrador de Pelouro (fornecedores não-TIC);
- Apresentar propostas de contratação de serviços de TIC para aprovação de pelo menos 2 Administradores (não críticos) e da Comissão Executiva, mediante parecer prévio da Conselho Fiscal (fornecedores TIC críticos);
- Assegurar, em coordenação com a Unidade de Apoio Jurídico, a inclusão nos acordos contratuais para a utilização de serviços de TIC prestados por terceiros de todas as cláusulas contratuais relevantes de acordo com a presente Política;
- Pelo registo e manutenção dos acordos/ contratos estabelecidos com prestadores de serviços (incluindo fornecedores TIC);
- Proceder às respectivas avaliações anuais, em função do tipo de contratação, dando informação de resultados finais à DdC e FGR, para efeitos de elaboração das avaliações anuais.

Departamento de Auditoria Interna (DAI) - Departamento responsável pela execução de auditorias periódicas, de modo a avaliar a adequação e eficácia da cultura organizacional e dos sistemas de governo e controlo interno do Banco. No âmbito da contratação, o DAI é responsável por:

- Incluir no plano de auditoria os procedimentos de contratação, em especial, os acordos contratuais relativos à utilização de serviços de TIC prestados por terceiros que suportem funções críticas ou importantes (CIF);
- Avaliar se os procedimentos de contratação adoptados cumprem a legislação e a regulamentação aplicáveis, a estratégia de risco e as decisões do CA/CE;
- Avaliar a implementação correcta e efectiva dos procedimentos de contratação de serviços de TIC, nomeadamente em termos de:
  - ✓ Adequação, qualidade e eficácia da avaliação de criticidade do serviço;
  - ✓ Adequação, qualidade e eficácia da avaliação dos riscos decorrentes dos acordos de contratação, e se os riscos se mantêm em consonância com a estratégia de risco do Banco;
  - ✓ Adequação do acompanhamento e gestão dos acordos de contratação; e
  - ✓ Envolvimento adequado dos órgãos de governo intervenientes nos procedimentos de contratação.

Unidade de Apoio Jurídico (UAJ) - Unidade responsável, no âmbito das suas funções, pela elaboração de minutas contratuais para aplicação consistente do clausulado base estabelecido na presente Política e pelo apoio às Estruturas Contratantes na elaboração da proposta de contracto e respectiva negociação contractual com os fornecedores.

4. Destinatários

A presente Política destina-se a todos os colaboradores do Banco que tenham intervenção, directa ou indirecta, no estabelecimento, manutenção ou cessação na contratação de serviços.

5. Princípios Orientadores

Para garantir uma adequada e continuada relação com os seus fornecedores o BAIE define os seguintes princípios gerais:

- Cumprimento das obrigações legais e regulamentares, garantindo que os acordos contratuais não exoneram o BAIE nem o seu órgão de administração das suas responsabilidades;
- Garantia de que os acordos não impedem a supervisão eficaz por parte das autoridades competentes nem violam quaisquer restrições de supervisão em matéria de serviços e actividades;
- Equidade de acesso, tratamento e transparência;
- Práticas de negócio com elevados padrões sociais, éticos e ambientais;
- Observância de elevados padrões de qualidade;
- Cooperação na monitorização e cumprimento dos princípios descritos na presente Política e demais requisitos regulamentares relevantes; e
- Aplicação dos princípios na contratação de serviços de terceiros.

6. Política de fornecedores

O relacionamento com os fornecedores é uma componente relevante na actividade do BAIE, nomeadamente para assegurar a comercialização dos seus produtos e serviços de uma forma equilibrada e responsável, de acordo com a sua estratégia de sustentabilidade.

Nesse sentido, com o objectivo de reforçar os seus valores de exigência, rigor, agilidade, respeito e ética, o BAIE pretende promover junto dos seus fornecedores a adopção de uma conduta responsável equiparável.

A presenta Política deve ser lida em conjunto com o Manual de Processo – Pedidos de Compras e Manual de Processo - Gestão de Fornecedores TIC, Críticos e Subcontratantes.

6.1. Compromissos de âmbito Ético, Social, Ambiental, Continuidade do Negócio e Saúde e Segurança no Trabalho

Visando a promoção da consciência ESG (*Environment, Social and Governance*) dos colaboradores do Banco e dos interlocutores externos (prestadores de serviços), espera-se que ambos:

- **No âmbito Ético:**
  - Promovam práticas comerciais justas, razoáveis e éticas;
  - Previnam tentativas de fraude, suborno, conflitos de interesse, ofertas, pagamentos ou benefícios indevidos para influenciar a decisão;
  - Respeitam a confidencialidade e asseguram a protecção da informação.

- **No âmbito Social:**
  - Adoptam os princípios consagrados na Declaração Universal dos Direitos Humanos e que cumpram as oito convenções fundamentais da Organização Internacional do Trabalho;
  - Sejam tratados com respeito e dignidade;
  - Garantam a igualdade de remuneração de homens e mulheres por trabalho de igual valor;
  - Previnam a discriminação sob qualquer forma (nacionalidade, raça, cor, género, religião, orientação sexual, opção política, idade, condições de saúde e deficiência);
  - Proíbam o abuso físico ou verbal, ameaças, actos de violência ou intimidação e o assédio moral ou sexual dos colaboradores;
  - Asseguram o cumprimento da idade mínima legal de emprego;
  - Garantam o cumprimento dos horários de trabalho de acordo com as leis nacionais e as especificidades de cada sector;
  - Proíbam o trabalho forçado e permitam que os colaboradores sejam livres de rescindir o seu contrato após aviso prévio;

- Tenham a liberdade de aderir ou não a um órgão de representação de trabalhadores.

- **No âmbito Ambiental:**
  - Cumpram a legislação ambiental em vigor;
  - Tenham práticas de identificação e mitigação dos riscos ambientais na sua actividade;
  - Favoreçam a implementação de tecnologias e instrumentos favoráveis ao ambiente;
  - Promovam a utilização sustentada de recursos naturais;
  - Promovam a reutilização e, se não for possível, a reciclagem dos seus produtos ou serviços;
  - Introduzam sistemas de gestão de resíduos perigosos e não perigosos;
  - Introduzam medidas de gestão carbónica e de outros gases relacionados com as alterações climáticas e implementem objectivos de redução de emissões;
  - Promovam a gestão das áreas florestais com foco na preservação da natureza e biodiversidade.

- **No âmbito da Continuidade de Negócio:**

  Estejam preparados para eventuais cenários de contingência que possam colocar em causa o funcionamento do negócio (por exemplo: pandemia, terrorismo, desastres naturais, ataques de cibersegurança, entre outros), com a existência de planos de continuidade de negócio, assegurando a prestação do serviço, a protecção e segurança dos colaboradores e o controlo de efeitos inesperados no âmbito das operações.

- **No âmbito da Saúde e Segurança no Trabalho (SST):**
  - Cumpram a legislação em vigor nesta matéria;
  - Garantam as condições de segurança de trabalho em conformidade com a legislação em vigor;
  - Tenham práticas de identificação, minimização e controlo dos riscos de saúde e de segurança;
  - Promovam acções de formação no âmbito da SST;
  - Identificam e implementam oportunidades de melhoria no desempenho da SST.

- **No âmbito da Segurança da Informação e Cibersegurança:**
  - Cumpram com a legislação a que estão obrigados, podendo ser exigido que façam prova do seu cumprimento (ex. NIS 2);
  - Assegurem o cumprimento das boas práticas de segurança definidas pelo Banco no contrato, SLA ou NDA;
  - Assegurem o cumprimento dos requisitos de segurança da informação no contrato, SLA ou NDA;
  - Informem o Banco de acordo com o contrato ou SLA em vigor de quaisquer incidentes de segurança da informação, que envolva dados ou informação partilhada pelo Banco.

Os compromissos acima descritos são, também, aplicáveis aos prestadores de serviços subcontratados pelo Banco.

6.2. Selecção, Aprovação e Adjudicação

Na selecção dos seus fornecedores ou prestadores de serviços, o BAIE observará os princípios de equidade de acesso, tratamento e transparência, cumprindo com as seguintes condições:

Fornecedores ou prestadores de serviço		Não TIC	TIC Não críticos	TIC Críticos
Análise e selecção	Definidos os critérios e necessidades para a prestação de um serviço externo, inicia-se o processo de selecção respectivo. Neste processo devem ser analisadas e registadas, sempre que possível, 3 (três) propostas de entidades diferentes, sujeitando o candidato elegível a uma análise do risco de BC/FT, conformidade e reputacional.	X	X	X
Aprovação	A decisão pela aprovação do serviço será delegada no Administrador de Pelouro	X		
	A decisão pela aprovação do serviço será efectuada por 2 Administradores.		X	
	O órgão de decisão pela aprovação dos serviços contratados reside na Comissão Executiva. Tratando-se de uma contratação de fornecedores críticos é, ainda, necessário a emissão de um parecer prévio pelo órgão de fiscalização do Banco.			X
Adjudicação	A adjudicação destes serviços poderá ser realizada via digital ou formalizada por contrato escrito. No *onboarding* do fornecedor/prestação de serviço pode ser necessário a tomada de conhecimento do Código de Conduta em função do serviço a ser contratualizado; neste sentido, recomenda-se que a Unidade de Apoio Jurídico seja contactada no sentido de clarificar a aplicabilidade da tomada de conhecimento do Código de Conduta do BAIE ao fornecedor/prestador de serviço em causa.	X	X	
	Após a adjudicação, a subcontratação é sempre formalizada através de contrato escrito, existindo determinadas especificidades para acordos de subcontratação de funções essenciais ou importantes e para outros acordos de subcontratação de serviços.[1]".			X

Nota[1]: Para mais informações, consultar o ponto "Orientações Específicas – Disposições Contratuais".

6.3. Orientações Específicas – Serviços de TIC

Sempre que o acordo contratual diga respeito à utilização de serviços de TIC prestados por terceiros, devem ser observados os seguintes requisitos específicos, em alinhamento com o quadro regulamentar aplicável.

6.3.1. Análise Prévia

Antes da celebração de qualquer acordo contratual com terceiros prestadores de serviços de TIC, o BAIE assegura a adopção de um conjunto de diligências destinadas a avaliar, mitigar e documentar os riscos associados à contratação. Esta fase é essencial para garantir que a decisão de contratar um determinado prestador é tomada de forma sustentada e informada e reveste a forma de condição indispensável para a celebração de qualquer acordo contratual para a utilização de serviços de TIC prestados por terceiros.

Neste âmbito, a Avaliação Pré-Contratual compreende os seguintes três (3) elementos:

- **Avaliação da criticidade:** Determinação da relevância dos serviços de TIC a contratar, através do seu suporte ou não a funções críticas ou importantes (CIF) e o impacto potencial na continuidade e na disponibilidade dos serviços e actividades financeiros do BAIE;
- **Análise da adequabilidade:** Realização de diligências que permitam avaliar a capacidade técnica, financeira, operacional e reputacional do prestador para fornecer o serviço de TIC em conformidade com os objectivos e necessidades do BAIE; e
- **Avaliação do risco:** Identificação e avaliação de todos os riscos relevantes que possam surgir em resultado da relação contratual para a utilização de determinado serviço de TIC prestado por um terceiro.

Não obstante da Análise de Adequabilidade supramencionada, o BAIE apenas poderá utilizar serviços de TIC prestados por um terceiro prestador de serviços de TIC estabelecido num país terceiro e que tenha sido designado como crítico nos termos do Artigo 31.º do Regulamento DORA, caso este último tenha estabelecido uma filial na União Europeia no prazo de 12 meses após a referida designação pelas ESA (*European Supervisory Authorities*).

Por outro lado, no âmbito da Avaliação do Risco, o BAIE deve assegurar obrigatoriamente:

- A identificação e avaliação dos conflitos de interesses que possam decorrer do acordo contratual; e
- A identificação e avaliação do risco de concentração no domínio das TIC, ponderando os benefícios e os custos de soluções alternativas como a utilização de terceiros prestadores de serviços de TIC diferentes, tendo em conta se e como as soluções previstas satisfazem as necessidades operacionais e os objectivos definidos na sua estratégia de resiliência digital.

Em adição ao supramencionado, para os acordos contratuais relativos à utilização de serviços de TIC prestados por terceiros que suportem funções críticas ou importantes (CIF) a Avaliação de Risco deve incluir ainda:

- A identificação e avaliação do risco de concentração no domínio das TIC, nomeadamente através da celebração de:
  - um contrato com um terceiro prestador de serviços de TIC que não seja facilmente substituível;
  - vários acordos contratuais em relação à prestação de serviços de TIC que apoiem funções críticas ou importantes (CIF) com o mesmo terceiro prestador de serviços de TIC ou com terceiros prestadores de serviços de TIC com ligações estreitas entre si;
- A identificação e avaliação do risco relativo à eventual permissibilidade de subcontratação em cadeia:
  - tendo em consideração os benefícios e os riscos que podem surgir associados a essa possível subcontratação, em especial perante a localização de um subcontratante de TIC num país terceiro e, consequentemente, o cumprimento das regras da União em matéria de protecção de dados e a aplicação efectiva da lei nesse país terceiro;
  - nomeadamente no que diz respeito ao facto de cadeias de subcontratação potencialmente longas e complexas poderem afectar a sua capacidade de monitorizar cabalmente as funções subcontratadas e a capacidade de o Banco de Portugal supervisionar eficazmente o BAIE nesse aspecto.

6.3.2. Disposições Contratuais

Os acordos contratuais para a utilização de serviços de TIC prestados por terceiros devem revestir a forma de contracto escrito, identificando claramente os direitos e obrigações do BAIE e do terceiro prestador de serviços de TIC. Após a sua assinatura nos termos legalmente exigidos, este contrato deverá ser disponibilizado a ambas as partes em papel ou num documento com outro formato descarregável, duradouro e acessível.

Em conformidade com o princípio da proporcionalidade, as disposições mínimas a incluir nos acordos contratuais relativos à utilização de serviços de TIC prestados por terceiros são definidas em função de suportarem ou não funções críticas ou importantes (CIF), sendo aplicados requisitos mais exigentes sempre que estejam em causa serviços que suportem tais funções.

Desta forma, todos os acordos contratuais para a utilização de serviços de TIC devem conter obrigatoriamente os seguintes elementos mínimos:

- Descrição clara e completa de todas as funções e serviços de TIC a prestar pelo terceiro;
- Data de início e a data de término da prestação do serviço;
- Identificação da lei aplicável ao acordo contratual;

- Identificação dos locais, nomeadamente as regiões ou os países, onde as funções e os serviços de TIC objecto de contratação devem ser prestados e onde devem ser tratados os dados, nomeadamente o local de conservação dos dados, bem como o requisito, aplicável ao terceiro prestador de serviços de TIC, de notificar antecipadamente o BAIE se planear mudar de locais;
- Descrições do nível de serviço, incluindo os moldes para a respectiva actualização e revisão;
- Disposições sobre a disponibilidade, autenticidade, integridade e confidencialidade em relação à protecção de dados, incluindo dados pessoais;
- Obrigação de o terceiro prestador de serviços de TIC implementar e manter controlos técnicos e organizacionais adequados à protecção da confidencialidade, integridade e disponibilidade dos sistemas, dados e/ou serviços contratados;
- Obrigação de o terceiro prestador de serviços de TIC notificar imediatamente, e sem demora injustificada, a ocorrência de qualquer incidente, falha, disrupção ou qualquer evento de segurança que possa comprometer, total ou parcialmente, a prestação dos serviços contratados bem como a confidencialidade, integridade e disponibilidade dos dados ou sistemas do BAIE;
- Disposições sobre a garantia de acesso, recuperação e devolução, num formato facilmente acessível, dos dados pessoais e dos dados não pessoais tratados pela entidade financeira em caso de insolvência, resolução ou descontinuação das operações comerciais do terceiro prestador de serviços de TIC, ou em caso de rescisão dos acordos contratuais
- Obrigação de o terceiro prestador de serviços de TIC prestar assistência ao BAIE sem custos adicionais, ou a um custo previamente determinado, caso ocorra um incidente relacionado com as TIC que envolve o serviço de TIC prestado;
- Obrigação de o terceiro prestador de serviços de TIC cooperar plenamente com as autoridades competentes e as autoridades de resolução do BAIE, e, nomeadamente, com pessoas designadas por essas autoridades;
- Condições aplicáveis à participação de terceiros prestadores de serviços de TIC nos programas de sensibilização para a segurança das TIC e na formação em matéria de resiliência operacional digital das entidades financeiras, nos termos do n. º 6 do Artigo 13.º do Regulamento (UE) 2022/2554 (DORA);
- Direitos de rescisão que correspondam às expectativas das autoridades competentes e das autoridades de resolução e, nomeadamente, em qualquer uma das seguintes situações:
    - Violação significativa pelo terceiro prestador de serviços de TIC da legislação, regulamentação ou das condições contratuais aplicáveis;
    - Circunstâncias identificadas aquando da monitorização do risco associado às TIC devido a terceiros que sejam consideradas como passíveis de alterar o desempenho das funções realizadas através do acordo contratual, nomeadamente alterações materiais que afectem o acordo contratual ou a situação do terceiro prestador de serviços de TIC;

- Debilidades comprovadas do terceiro prestador de serviços de TIC que se prendem com a sua gestão global do risco associado às TIC e, em particular, qualquer deficiência na forma como garante a disponibilidade, autenticidade, integridade e confidencialidade dos dados, pessoais ou sensíveis ou dos dados não pessoais;
- Quando a autoridade competente deixar de poder supervisionar eficazmente o BAIE em resultado das condições ou das circunstâncias relacionadas com o acordo contratual respectivo.

- Identificação de períodos mínimos de pré-aviso relacionado com a rescisão dos acordos contratuais, que correspondam às expectativas das autoridades competentes e das autoridades de resolução; e
- Obrigação de, após o término da relação contratual, seja por que motivo for, o terceiro prestador de serviços de TIC proceder, de forma célere e segura, à eliminação integral dos materiais, sistemas, ferramentas e dados associados à prestação do serviço previamente contratado, remetendo ao BAIE, sem demora injustificada, um comprovativo formal dessa eliminação.

Em adição aos elementos supramencionados, caso se trate de um acordo contratual relativo à utilização de serviços de TIC prestados por terceiros que suportem funções críticas ou importantes (CIF), deverão ser igualmente incluídos os seguintes elementos:

- Indicação quanto à possibilidade de subcontratação em cadeia de serviços TIC que apoiem uma função crítica ou importante, ou de partes materiais da mesma e, se for caso disso, as condições aplicáveis a essa subcontratação;
- Descrição completa dos níveis de serviço, com metas de desempenho quantitativas e qualitativas rigorosas para os níveis de serviço acordados, por forma a permitir uma monitorização eficaz, por parte do BAIE dos serviços TIC prestados, e a adopção, sem demora injustificada, de medidas correctivas, quando os níveis de serviço acordados não forem cumpridos;
- Períodos de notificação e obrigações de notificação do terceiro prestador de serviços de TIC ao BAIE, nomeadamente quanto a quaisquer desenvolvimentos que possam ter impacto material na capacidade de o terceiro prestador de serviços de TIC prestar eficazmente serviços de TIC que apoiem funções críticas ou importantes em consonância com os níveis de serviço acordados;
- Requisitos que obriguem o terceiro prestador de serviços de TIC a executar e testar planos de contingência operacional e a dispor de medidas, ferramentas e políticas de segurança no domínio das TIC que garantam um nível adequado de segurança na prestação de serviços pelo BAIE em consonância com o seu quadro regulamentar;
- Obrigação de o terceiro prestador de serviços de TIC participar e cooperar plenamente nos TLPT (Testes de Penetração baseados em Ameaças) realizados pelo BAIE, conforme referido nos Artigos 26.º e 27.º do Regulamento (UE) 2022/2554 (DORA), caso aplicável;

- Direito de monitorizar numa base contínua o desempenho do terceiro prestador de serviços de TIC, o que implica o seguinte:
    - obrigação do terceiro prestador de serviços fornecer qualquer informação relevante ou relatórios adequados sobre os serviços prestados, cujo conteúdo deve ser previamente validado e aprovado pelo BAIE (e.g., relatórios de desempenho, de incidentes, de segurança de TIC, de continuidade de negócio e teste);
    - direitos ilimitados de acesso, inspecção, auditoria e testes às TIC pelo BAIE, ou por um terceiro designado, e pela respectiva autoridade competente, nos termos dos quais o BAIE fornecerá atempadamente os pormenores sobre o âmbito, procedimentos a seguir e respectiva frequência;
    - direito de acesso do BAIE a informação relativa ao serviço prestado pelo terceiro, bem como o direito a fazer cópias da documentação importante no local, caso essa documentação seja crítica para as operações do terceiro prestador de serviços de TIC, cujo exercício efectivo não seja impedido nem limitado por outros acordos contratuais ou políticas de execução;
    - direito a acordar níveis de garantia alternativos caso sejam afectados os direitos de outros clientes,
    - obrigação de plena cooperação por parte do terceiro prestador de serviços de TIC durante as inspecções e auditorias no local realizadas pelas autoridades competentes, pela autoridade fiscalizadora principal, pelo BAIE ou por um terceiro designado, e

- Determinação de um período de transição obrigatório adequado:
    - durante o qual o terceiro prestador de serviços de TIC continuará a desempenhar as respectivas funções ou a prestar serviços de TIC com vista a reduzir o risco de perturbações no BAIE ou assegurar a sua resolução e reestruturação efectivas, e
    - que permita ao BAIE migrar para outro terceiro prestador de serviços de TIC ou passar desempenhar esses serviços internamente;

De forma a assegurar a aplicação consistente das cláusulas contratuais exigidas, devem ser elaboradas minutas contratuais em conformidade com os elementos supramencionados. Não obstante, aquando da negociação dos acordos contratuais, e sempre que aplicável, o BAIE e os terceiros prestadores de serviços de TIC devem considerar a utilização de cláusulas contratuais normalizadas, desenvolvidas pelas autoridades públicas, para serviços específicos.

6.3.3. Monitorização Contínua

A monitorização contínua da contratação externa é uma componente essencial na gestão do risco de terceiros, tendo em vista a verificação regular da observância dos requisitos aplicáveis. Para este efeito, a análise da adequabilidade do prestador e a avaliação do risco realizadas na fase pré-contratual devem ser revistas periodicamente e sempre que ocorram eventuais alterações ao nível do acordo contratual ou do terceiro prestador de serviços que justifiquem essa reavaliação (e.g., novas funções que dependem do serviço prestado, aumento do nível de dependência, alteração da arquitectura técnica, introdução de subcontratação em cadeia), obedecendo aos critérios e requisitos previstos no ponto **6.3.1 Análise Prévia**.

Os riscos identificados decorrentes dos acordos contratuais para a utilização dos serviços de TIC prestados por terceiros devem ser incorporados na gestão de risco global, viabilizando uma gestão do risco integrada e abrangente.

Complementarmente, no decurso da relação contratual, a Comissão Executiva deverá ser informada atempadamente sobre quaisquer alterações significativas previstas relativas aos terceiros prestadores de serviços de TIC e do potencial impacto de tais alterações em funções críticas ou importantes (CIF) objecto dos referidos acordos, devendo ser fornecido um resumo da análise de risco para avaliar o impacto dessas alterações.

Por fim, o BAIE exerce os seus direitos de acesso, inspecção e auditoria sobre os prestadores de serviços de TIC que suportem funções críticas ou importantes (CIF) em função de uma abordagem baseada no risco, predeterminando a frequência das auditorias e das inspecções e as áreas a auditar, aderindo para este efeito a normas de auditoria comummente aceites em consonância com qualquer instrução de supervisão sobre a utilização e incorporação dessas normas de auditoria. Quando os respectivos serviços impliquem um nível elevado de complexidade técnica, o BAIE deve garantir que os auditores, sejam eles internos ou externos, possuem as aptidões e os conhecimentos adequados para realizar eficazmente as auditorias e as avaliações pertinentes.

6.3.4. Registo de Informação

Em alinhamento com o estabelecido no n. º3 do Artigo 28.º do Regulamento DORA, o BAIE deve observar o dever de manter e actualizar um registo de informação relativa a todos os acordos contratuais para utilização dos serviços de TIC prestados por terceiros (doravante designado por “registo de informação”), distinguindo claramente entre os que abrangem serviços de TIC que apoiem funções críticas ou importantes (CIF) e os que não abrangem esse tipo de funções.

O registo de informação deve conter toda a informação regulamentarmente exigida relativamente aos acordos contratuais para utilização de serviços de TIC prestados por terceiros, estruturada e preenchida de acordo com as

orientações estabelecidas no Regulamento de Delegado (UE) 2024/2956 da Comissão de 29 de Novembro de 2024 que estabelece normas técnicas de execução para a aplicação do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no respeitante aos modelos normalizados para o registo de informações. Sem prejuízo do anteriormente descrito, sempre que seja considerado pertinente para efeitos de gestão do risco ou de gestão dos acordos contratuais, pode ser incluída informação adicional, no formato mais adequado à mesma.

Por fim, e de forma a garantir que a informação constante no registo de informação se mantém actual, a mesma deve ser revista com periodicidade no mínimo anual, ou sempre que aplicável. Eventuais alterações ao nível do acordo contratual que representem ou possam representar alterações na informação associada ao mesmo no registo de informação devem ser prontamente comunicadas ao responsável pela sua manutenção, para que sejam devidamente actualizadas.

6.3.5. Deveres de Reporte

No âmbito dos acordos contratuais para a utilização de serviços de TIC prestados por terceiros, é obrigatório o reporte ao Banco de Portugal dos seguintes elementos:

- Pelo menos uma vez por ano, o número de novos acordos contratuais relativos à utilização dos serviços de TIC, das categorias dos terceiros prestadores de serviços de TIC, dos tipos de acordos contratuais e dos serviços e funções de TIC que são prestados;
- Atempadamente, perante à celebração de acordos contratuais relativos à utilização de serviços de TIC que apoiem funções críticas ou importantes (CIF), bem como quando uma determinada função passar a ser crítica ou importante; e
- A pedido deste, o registo de informação completo ou, se solicitado, secções desse registo, juntamente com as informações consideradas necessárias para permitir uma supervisão eficaz, conforme detalhado no ponto **6.3.4 Registo de Informação.**

Os deveres de reporte supramencionados devem ser desempenhados de acordo com as indicações do Banco de Portugal relativamente aos formatos e canais de reporte a utilizar.

6.3.6. Estratégias de Saída

No âmbito da contratação externa de serviços de TIC que suportem funções críticas ou importantes (CIF), deve ser assegurada a elaboração de estratégias de saída devidamente documentadas, realistas, viáveis, baseadas em cenários plausíveis e pressupostos razoáveis e que permitam implementar medidas adequadas para manter a continuidade do negócio e evitar efeitos negativos para a resiliência operacional digital, tendo em conta os riscos que possam surgir a nível dos terceiros prestadores de serviços de TIC, podendo ser activadas caso se verifique qualquer uma das seguintes situações:

- Perturbação das actividades devido a falha ou desadequação da prestação dos serviços de TIC ou qualquer risco material relacionado com o desempenho adequado e contínuo do respectivo serviço de TIC;
- Deterioração da qualidade dos serviços de TIC prestados (e.g., interrupções de serviço imprevistas e/ou persistentes); ou
- Rescisão dos acordos contratuais em qualquer das circunstâncias enumeradas no n.º 7 do Artigo 28.º do Regulamento DORA e transpostas no ponto **6.3.2 Disposições Contratuais** da presente Política.

Neste sentido, **o conteúdo das referidas estratégias deverá integrar, pelo menos**, os elementos elencados infra:

- Identificação dos recursos humanos e materiais necessários à implementação da estratégia de saída;
- Descrição dos serviços prestados, incluindo a identificação das funções críticas ou importantes (CIF) suportadas;
- Definição dos objectivos da estratégia de saída;
- Estabelecimento dos critérios determinantes para o sucesso da transição;
- Atribuição de funções e responsabilidades para a gestão da estratégia e respectivo processo de transição;
- Identificação de soluções alternativas capazes de prestar o serviço contratado com níveis de serviço e qualidade equivalentes;
- Avaliação da possibilidade de reintegração do serviço contratado;
- Elaboração de um plano de acção para a estratégia de saída, identificando as abordagens possíveis e descrevendo, de forma estruturada, as respectivas actividades a executar para garantir uma saída eficaz (podendo contemplar soluções de curto e de médio-longo prazo); e
- Definição de um calendário de execução planeado, alinhado com as condições de saída e de rescisão estabelecidas nos acordos contratuais.

Por fim, estas estratégias devem, sempre que possível, ser regular e suficientemente testadas a fim de assegurar a sua viabilidade e adequabilidade (e.g., exercício de *table-top*, análise dos potenciais custos, impactos, recursos e implicações operacionais).

6.4. Orientações Específicas de Segurança da Informação

Sempre que a prestação de um serviço inclua a possibilidade de acesso, processamento, armazenamento ou transmissão de informação (incluindo dados pessoais) do Banco por parte de um terceiro, devem ser seguidas as directrizes estabelecidas no presente subcapítulo.

Para assegurar uma gestão do risco adequada e eficaz, devem ser identificados os prestadores que têm acesso a informação do Banco e aqueles que requerem maior atenção (de acordo com a sua criticidade), bem como conhecer a sua cadeia de fornecimento, caso aplicável. Os requisitos específicos de segurança da informação devem ser aplicados aos terceiros e aos seus subcontratados, inclusive através da definição de regras específicas para propagação da informação ao longo da cadeia de fornecimento (Política de Segurança da Informação).

6.4.1. Requisitos gerais

De forma a mitigar os riscos específicos de segurança da informação, sempre que a prestação de um serviço contemple a possibilidade de acesso, processamento, armazenamento ou transmissão de informação (incluindo dados pessoais) do Banco por parte de um terceiro, devem ser abordados os processos e procedimentos a implementar pelo Banco, bem como os processos e procedimentos que o Banco deve exigir que o fornecedor ou prestador de serviços implemente, incluindo:

- Identificação, documentação e manutenção de um inventário dos prestadores de serviços com acesso aos seus activos, e respectiva tipificação do acordo com o tipo de serviço prestado (por exemplo, serviços de TI ou logística), pelos departamentos utilizadores de informação;
- Definição e implementação de um processo padronizado para gestão do ciclo de vida da segurança da informação na relação com prestadores de serviços;
- Tipificação da informação a que cada prestador de serviços poderá aceder (Norma de Classificação da Informação) e os requisitos de monitorização e controlo de acesso (Norma de Controlo de Acessos e Gestão de Utilizadores);
- Identificação dos requisitos mínimos de segurança, no que respeita a cada tipo de informação e de acesso, servindo como base à definição dos acordos com os prestadores de serviços, em função das necessidades e requisitos do BAIE, assim como do perfil de risco associado;
- Definição e implementação de processos e procedimentos de monitorização do nível de aderência aos requisitos de segurança da informação, para cada prestador de serviços e tipologia de acesso, incluindo, revisão por terceiros e validação de produtos;
- Assegurar a exactidão e completude da informação ou do processamento da informação (i.e., integridade) facultada por qualquer uma das partes;

- Obrigações aplicáveis aos prestadores de serviços na protecção da informação;
- Capacidade de resiliência e recuperação de falhas/desastres, bem como a definição de um ou mais planos de contingência, de forma a assegurar a disponibilidade ou processamento da informação por qualquer uma das partes;
- Realização de acções de formação e sensibilização sobre as políticas, normas, planos, processos e procedimentos aplicáveis, aos colaboradores envolvidos em processos de aquisição, promovidas pela FSI;
- Realização de acções de formação e sensibilização aos colaboradores responsáveis por interagir com os prestadores de serviços, quanto às regras de participação e comportamento esperados, por estes e respectivo acesso aos sistemas e informação do BAIE, promovidas pela DSI;
- Formalização de um acordo de prestação de serviços, com valor jurídico, que considere a definição clara das responsabilidades no âmbito da segurança da informação. Esta formalização deve ser assegurada pelos departamentos utilizadores de informação responsáveis, em colaboração com a Unidade de Apoio Jurídica; e
- Existência de canais disponíveis para o prestador de serviços comunicar incidentes de segurança (Norma de Gestão de Incidentes de Segurança da Informação e Tecnológicos).

6.4.2. Disposições Contratuais

Nos acordos estabelecidos com fornecedores ou prestadores de serviços, designadamente quando existe possibilidade de acesso, processamento, armazenamento ou transmissão de informação, devem ser incluídos requisitos específicos e complementares para mitigar riscos de segurança de informação no âmbito da prestação do serviço. Devem ser acordados e documentados os requisitos de segurança de informação a observar na relação contratual com cada prestador de serviço com possibilidade de acesso, processamento, armazenamento, transmissão de informação.

Desta forma, todos os acordos contratuais que contemplem o acesso de terceiros a informação do Banco, devem conter obrigatoriamente os seguintes elementos mínimos:

- Identificação do tipo de informação acessível ao terceiro e meios de acesso, no âmbito das suas funções;
- Classificação da informação acessível ao terceiro, e se necessário, o respectivo mapeamento entre o esquema de classificação do Banco e do fornecedor. Para mais informação, consultar a Norma de Classificação de Informação;
- Obrigações legais e regulamentares aplicáveis (por exemplo, protecção e privacidade da informação confidencial, incluindo dados pessoais e protecção da propriedade intelectual). Para mais informação, consultar a Norma de Compliance da Segurança da Informação e Norma de Protecção de Dados ;

- Definição de controlos a implementar pelas partes no âmbito do controlo de acessos, avaliação de desempenho, monitorização, reporte e auditoria. Para mais informação, consultar a Norma de Controlo de Acessos e Gestão de Utilizadores;
- Confirmação da tomada de conhecimento, por parte do prestador, das regras de uso aceitável da informação em vigor no BAIE. Para mais informação, consultar a Norma de Utilização Aceitável de Activos;
- Confirmação da tomada de conhecimento e aceitação, por parte do prestador, da Política de Segurança da Informação do Banco e demais documentação normativa considerada relevante por parte do Banco no contexto da prestação do serviço;
- Lista exaustiva de colaboradores do fornecedor autorizados a prestar serviços ou, em alternativa, procedimento a adoptar pelo prestador de serviços para solicitar autorização ou remoção da autorização de acesso aos seus colaboradores;
- Requisitos e procedimentos a adoptar, pelo prestador de serviços e seus colaboradores, na gestão de incidentes de segurança de informação, em alinhamento com a Norma de Gestão de Incidentes de Segurança da Informação (por exemplo, reporte de incidentes e apoio na resolução de incidentes);
- Requisitos de formação e sensibilização nos procedimentos e requisitos de segurança da informação específicos (por exemplo, resposta a incidentes e procedimentos de autorização). Para mais informação, consultar a Política de Segurança de Recursos Humanos;
- Pontos de contacto do prestador de serviços para temas de segurança da informação;
- Requisitos de validação das referências e credenciais profissionais de todos os colaboradores que fazem parte da equipa do prestador de serviços e definição dos procedimentos necessários no caso do processo de verificação não ter sido efectuado ou suscite dúvidas ao Banco. Para mais informação, consultar a Norma de Segurança de Recursos Humanos;
- Os processos de resolução de conflitos entre as partes;
- A obrigação do prestador de serviços apresentar periodicamente um relatório independente sobre a efectividade dos controlos, plano de mitigação para os problemas identificados no relatório; e
- Todo e qualquer requisito adicional no âmbito da segurança da informação do BAIE a assegurar pelo prestador de serviços.

6.5. Monitorização e Avaliação

A capacidade de entrega do prestador de serviços, em alinhamento com o acordo definido, requer a supervisão por parte da estrutura contratante, designadamente quanto à implementação de:

- Mecanismos de monitorização e avaliação dos serviços;
- Processo de gestão da mudança, para gerir eventuais alterações aos produtos ou serviços;
- Actualização e manutenção dos acordos contratuais no *software* disponibilizado pelo Banco

6.5.1. Monitorização e Avaliação dos Serviços

Na avaliação do desempenho do prestador de serviços, o Banco deverá atender aos seguintes parâmetros:

- Riscos que lhe estão associados (por exemplo, risco de segurança da informação);
- Qualidade do serviço prestado;
- Níveis de serviço acordados; e
- Adopção de uma conduta responsável equiparável (Código de Conduta e os compromissos de âmbito Ético, Social, Ambiental, Continuidade de Negócio e Saúde e Segurança no Trabalho do BAIE, Segurança da Informação).

No caso de serviços críticos, caso seja necessário, podem ser realizadas auditorias aos controlos do prestador de serviço (ex. âmbito de segurança da informação) , assegurando a sua conformidade com o acordo estabelecido.

Por outro lado, o BAIE deve sempre manter o controlo e visibilidade sobre todos os aspectos associados a informação sensível ou crítica, assim como dos equipamentos e instalações, que estão no âmbito de actuação dos prestadores de serviço.
Neste contexto, compete à estrutura contratante:

- Conservar os relatórios de serviço, elaborados pelo prestador de serviço;
- Manter um registo de problemas operacionais, falhas e interrupções relacionadas com o serviço prestado;
- Rever as medidas de monitorização aplicadas pelo prestador sobre terceiros subcontratados por este, com o objectivo de garantir o cumprimento dos requisitos de segurança definidos;
- Gerir e solucionar quaisquer problemas identificados na prestação do serviço ou no cumprimento dos requisitos de segurança;

- Comunicar, prontamente, à FSI qualquer falha ou quebra de segurança de informação identificada, ou através dos meios e procedimentos de reporte a incidentes definidos na Política de Gestão de Incidentes de Segurança de Informação; e
- Realizar reuniões de progresso.

6.5.2. Gestão da Mudança

Caso se verifiquem alterações ao contexto em que ocorre a prestação de serviços, deve ser avaliada a necessidade de rever as políticas, processos e controlos existentes, associados à mesma, considerando a criticidade da informação de negócio, os sistemas e processos relacionados e a reavaliação dos riscos.

Assim, no âmbito do processo de gestão da mudança (substituibilidade, integração ou abandono do serviço prestado), devem ser avaliados os seguintes factores:

- Resultado da avaliação de desempenho do prestador de serviço;
- Alterações dos acordos com os prestadores;
- Alterações na actividade do Banco, seus sistemas ou aplicações, políticas, processos e/ou controlos; e
- Alterações nos serviços prestados pelos prestadores, como por exemplo, alterações tecnológicas, desenvolvimento de novos produtos ou disponibilização de novas versões, alteração da localização física ou recurso a subcontratação.

7. Incumprimento

Qualquer incumprimento ou violação da presente política deve ser imediatamente reportado ao DdC.

8. Monitorização (registo e documentação)

8.1. Registo

Todos os acordos com fornecedores celebrados com o Banco são objecto de registo com indicação das seguintes informações:

a) Identificador único de cada acordo;
b) O nome do prestador de serviços, o número de registo da sociedade, o código de actividade económica (CAE), morada da sede social e informações de contacto pertinentes, bem como, o nome da empresa-mãe (se aplicável);
c) Breve descrição do serviço contratado, incluindo a existência tratamento ou transferência de dados pessoais;
d) Categoria da actividade contratada e que permita identificar os diferentes tipos de acordos; e
e) Data de início, data do termo e, se for caso disso, a data da próxima renovação do contracto e existência de períodos de pré-aviso;
f) Identificação da estrutura e colaborador responsáveis pelo acordo contratual.

Sempre que se tratar de um fornecedor ou prestador de serviços crítico para o Banco, são observados os registos indicados na Política de Subcontratação. De igual forma, sempre que se tratar de um acordo contratual para a utilização de serviços de TIC prestados por terceiros, devem ser observados cumulativamente os requisitos estabelecidos no ponto **6.3.4 Registo de Informação**.

O registo dos acordos de contratação inclui os acordos já terminados e deve ser mantido permanentemente actualizado e disponibilizado às autoridades de supervisão sempre que for solicitado.

8.2. Documentação

A formalização dos acordos com prestadores de serviços é assegurada pelas estruturas contratantes.

O acompanhamento desses acordos deve também ser documentado pelas estruturas contratantes, onde se inclui eventuais alterações contratuais, denúncias e os resultados da avaliação de desempenho.

O registo e conservação de toda esta documentação é realizada pelas estruturas contratantes no *software* disponibilizado pelo Banco. Toda esta documentação e respectivo registo são conservadas por um período de 10 anos a contar da respectiva data de cessação, excepto se o tipo de acordo de contratação for legal ou regulamentarmente sujeito a conservação por prazo distinto.

9. Revisão, Aprovação e Divulgação

A presente política é revista anualmente ou sempre que as circunstâncias da actividade do Banco ou alterações legais ou regulamentares o justifiquem. As alterações introduzidas na política devem ser aplicadas em tempo útil e logo que possível nos acordos contratuais pertinentes, devendo ser documentado o calendário previsto para a sua implementação.

Compete, assim, ao DdC proceder à sua actualização, ao CF a sua revisão e ao CA a sua aprovação.

A sua divulgação será realizada pelo DEO-UEO a todos os colaboradores do BAIE, estando disponível para consultas no Portal QPR.

10. Enquadramento legal e regulamentar

Na elaboração da presente política, foram consideradas a legislação, regulamentação e outras boas práticas nacionais e internacionais reconhecidas ao nível dos sectores de actuação do Banco, como por exemplo:

- Aviso do Banco de Portugal n.º 3/2020 (versão consolidada) que regula o Sistema de Controlo Interno;
- Regulamento (EU) 2019/2088 do Parlamento Europeu e do Conselho de 27 de Novembro de 2019 relativo à divulgação de informações relacionada com a sustentabilidade no sector dos serviços financeiros (*Sustainable Finance Disclosure Regulation*);
- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Protecção de Dados);
- Norma ISO/IEC 27001:2013;
- Norma ISO/IEC 27002:2013;
- Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de Dezembro de 2022 relativo à resiliência operacional digital do sector financeiro (Regulamento DORA);
- Regulamento Delegado (UE) 2024/1773 da Comissão de 13 de Março de 2024 que complementa o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação que especificam o conteúdo pormenorizado da Política relativa aos acordos contratuais em matéria de utilização de serviços de TIC de apoio a funções críticas ou importantes prestados por terceiros prestadores de serviços de TIC; e
- Regulamento de Delegado (UE) 2024/2956 da Comissão de 29 de Novembro de 2024 que estabelece normas técnicas de execução para a aplicação do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no respeitante aos modelos normalizados para o registo de informações;
- Orientações EBA/GL/2025/01, relativas à gestão dos riscos ambientais, sociais e de governação (ASG);

- Guia do BCE sobre riscos climáticos e ambientais – Expectativas prudenciais relacionadas com a gestão e a divulgação de riscos.

11. Relação com outros documentos

- Código de Conduta;
- Política de Gestão de Riscos;
- Política de Subcontratação;
- Plano de Continuidade de Negócio;
- Política de Segurança da Informação;
- Política de Prevenção ao Branqueamento de Capitais e Financiamento do Terrorismo.
- Norma de Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
- Norma de Gestão dos Riscos Climáticos e Ambientais;
- Manual do Processo – Pedidos de Compra;
- Manual do Processo - Gestão de Fornecedores TIC, Críticos e Subcontratantes.

Aprovado em Conselho de Administração no dia 30-09-2025 (Acta nº 140)