Política de Fornecedores

Data Criação:	30 de Dezembro de 2022
Data Aprovação:	20 de Janeiro de 2023
Versão:	3
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

Índice

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 para montantes iguais ou superiores a 5.000 EUR, 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;

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 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.

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.

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;
- 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;
- 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.

Departamento de *Compliance* (DdC) - Departamento responsável, no âmbito dos procedimentos de contratação:

- Pela revisão da Política de Fornecedores e sucessivas actualizações;
- 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 Norma 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.

Unidade de Eficiência Operacional (UEO) – Estrutura integrada no Departamento de Eficiência e Operações (DEO-UEO), no âmbito das suas funções, responsável pela:

- Gestão, centralização da informação e documentação dos acordos de contratação, assegurando a sua disponibilização a entidades internas ou externas, sempre que solicitado; e
- Manutenção actualizada do registo e custódia dos acordos de contratação.

Função da Segurança da Informação (FSI) - Estrutura responsável, no âmbito das suas funções, pela definição, actualização e monitorização dos procedimentos respeitantes à segurança da informação. No âmbito da contratação, sempre que haja tratamento e transferência de dados, a FSI tem a responsabilidade de:

- Identificar e avaliar riscos de segurança da informação, confidencialidade e protecção de dados e definir nível de acessos;
- Garantir que as actividades de terceiros são realizadas em conformidade com as Políticas de Segurança de Informação do Banco, executando os controlos necessários para o efeito e promovendo, 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.

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, em colaboração com o Departamento de Compliance, eventuais situações de conflitos de interesses;
- Apresentar propostas de contratação para aprovação junto do Administrador de Pelouro;
- Assegurar e revisão do acordo/ contrato pela Unidade de Apoio Jurídico (UAJ);
- Monitorizar a execução do acordo de contratação e proceder às respectivas avaliações.

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.

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;
- 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; 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 aplicabilidade de presente Política dirige-se a todos as compras ou fornecimento de serviços de montante igual ou superior a 5.000 EUR.

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:**
  - (i) Promovam práticas comerciais justas, razoáveis e éticas;
  - (ii) Previnam tentativas de fraude, suborno, conflitos de interesse, ofertas, pagamentos ou benefícios indevidos para influenciar a decisão;
  - (iii) Respeitam a confidencialidade e asseguram a protecção da informação.

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

(viii) Proíbam o trabalho forçado e permitam que os colaboradores sejam livres de rescindir o seu contrato após aviso prévio;

(ix) Tenham a liberdade de aderir ou não a um órgão de representação de trabalhadores.

- **No âmbito Ambiental**:

  (i) Cumpram a legislação ambiental em vigor;

  (ii) Tenham práticas de identificação e mitigação dos riscos ambientais na sua actividade;

  (iii) Favoreçam a implementação de tecnologias e instrumentos favoráveis ao ambiente;

  (iv) Promovam a utilização sustentada de recursos naturais;

  (v) Promovam a reutilização e, se não for possível, a reciclagem dos seus produtos ou serviços;

  (vi) Introduzam sistemas de gestão de resíduos perigosos e não perigosos;

  (vii) Introduzam medidas de gestão carbónica e de outros gases relacionados com as alterações climáticas e implementem objectivos de redução de emissões;

  (viii) 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)**:

  (i) Cumpram a legislação em vigor nesta matéria;

  (ii) Garantam as condições de segurança de trabalho em conformidade com a legislação em vigor;

  (iii) Tenham práticas de identificação, minimização e controlo dos riscos de saúde e de segurança;

  (iv) Promovam acções de formação no âmbito da SST;

  (v) Identificam e implementam oportunidades de melhoria no desempenho da SST.

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 serviços não 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, sempre que possível, 3 (três) propostas de entidades diferentes, sujeitando o candidato elegível a uma análise do risco de conformidade.
  - **Aprovação –** A decisão pela aprovação do serviço será delegada no Administrador de Pelouro da estrutura proponente;
  - **Adjudicação –** A adjudicação destes serviços poderá ser realizada via digital ou formalizada por contrato escrito. No *onboarding* do fornecedor/ prestador de serviço é necessário assegurar que o mesmo tome conhecimento da presente Política e do Código de Conduta do Banco.

- **Fornecedores críticos:**

  .

  - **Análise e selecção** – Definidos os critérios e necessidades de subcontratação e ponderado o perfil do prestador de serviço a consultar, inicia-se o processo de selecção respectivo. Neste processo devem ser analisadas, sempre que possível, 3 (três) propostas de entidades diferentes, sujeitando o candidato elegível a uma análise do risco de conformidade. Para mais informações, consultar o ponto "Orientações Específicas – Análise prévia e avaliação de riscos inicial" e o ponto "Orientações Específicas - Exame prévio" da Política de Subcontratação;
  - **Aprovação –** O órgão de decisão pela aprovação dos serviços subcontratados reside na Comissão Executiva. Tratando-se de uma subcontratação de funções essenciais ou importantes é, ainda, necessário a emissão de um parecer prévio pelo órgão de fiscalização do Banco. Para mais informações, consultar o ponto "Subcontratação de funções essenciais ou importantes" da Política de Subcontratação;
  - **Adjudicação –** 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. Para mais informações, consultar o ponto "Orientações Específicas – Fase contratual" da Política de Subcontratação.

6.3. Orientações Específicas – Segurança da Infomação

Sempre que o fornecedor ou prestador de serviços for considerado crítico, inclua a transferência de dados pessoais do Banco e/ou seu tratamento pelo prestador de serviços são definidas as seguintes directrizes.

6.3.1. Requisitos – Tratamento de Dados

Nos acordos estabelecidos com fornecedores ou prestadores de serviços, designadamente quando existe tratamento ou transferência de dados, devem ser incluídos requisitos específicos para mitigar riscos de segurança de informação no âmbito da prestação do serviço, complementares aos já estabelecidos com aqueles.

Para assegurar o bom desempenho da sua actividade, o Banco deve identificar quais os fornecedores críticos e que requerem maior atenção, bem como conhecer a sua cadeia de fornecimento (por exemplo, o fornecedor é responsável pelo serviço ou subcontrata serviços a terceiros).

Os requisitos específicos de segurança de informação para os serviços críticos devem ser aplicados aos fornecedores críticos ou subcontratados, inclusive definidas regras específicas para propagação da informação ao longo da cadeia de fornecimento (Política de Segurança da Informação).

Deve ainda ser implementado um processo de monitorização e métodos aceitáveis que permitam ao Banco validar efectivamente se as tecnologias de informação e comunicação aderem aos requisitos de segurança definidos por este.

O BAIE deverá dispor de processos específicos para serviços críticos que contemplem a gestão do seu ciclo de vida, disponibilidade e riscos de segurança associados. Deve ser considerado neste contexto, o risco de interrupção do fornecimento do serviço (por exemplo, em caso de saída do fornecedor do mercado ou avanços tecnológicos).

Adicionalmente, devem ser definidos procedimentos de controlo de qualidade para assegurar o alinhamento do serviço de TI e comunicações com os seus requisitos.

6.3.2. Requisitos - Na vertente dos sistemas de informação

Os requisitos de segurança necessários à mitigação dos riscos associados ao acesso a activos do BAIE por parte de fornecedores ou prestadores de serviços devem fazer parte dos acordos estabelecidos entre as partes. Para tal, a gestão da relação com aqueles deve ser assegurada num processo padronizado e documentado, garantindo que todos os requisitos de segurança foram considerados, mitigando os riscos para o Banco. Devem igualmente ser abordados os processos e procedimentos a serem implementados 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 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;
- Controlos de validação da exactidão e completude da informação ou processamento da informação 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 processo 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, 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;

- 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).

6.3.2.1. Formalidades observar nos Acordos

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 ou fornecedores de infra-estruturas de TI.

Na redacção dos acordos com os prestadores de serviços devem ser considerados os seguintes aspectos:

- Tipo de informação acessível pelo prestador e meios de acesso, no âmbito das suas funções;
- Classificação da informação do Banco, e se necessário, o respectivo mapeamento entre o esquema de classificação do Banco e do fornecedor (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 informações, consultar a Norma de Compliance da Segurança da Informação e Norma de Protecção de Dados Pessoais;
- Definição de controlos a implementar pelas partes no âmbito do controlo de acessos, avaliação de desempenho, monitorização, reporte e auditoria. Para mais informações, consultar a Norma de Controlo de Acessos e Gestão de Utilizadores;
- Tomada de conhecimento, por parte do prestador de serviço, das regras de uso aceitável da informação em vigor no BAIE. Para mais informações, consultar a Norma de Utilização Aceitável de Activos;
- Tomada de conhecimento e aceitação, por parte do prestador de serviço, das Política de Segurança da Informação do Banco, revelantes 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 informações, consultar a Política de Segurança de Recursos Humanos;
- Meios e condições a assegurar pelo prestador de serviços, em resposta a necessidades específicas de resiliência e recuperação;
- Pontos de contacto do prestador de serviços para temas de segurança da informação;
- Requisitos legais e regulatórios relevantes a observar em caso de subcontratação, incluindo os controlos a serem implementados (por exemplo, protecção de dados pessoais);
- 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 informações, consultar a Norma de Segurança de Recursos Humanos;
- O direito de auditar os processos e controlos do prestador de serviços relacionados com o contrato;
- 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.

Na eventualidade do prestador se tornar incapaz de prestar os serviços contratualizados ou facultar os seus produtos, o acordo estabelecido deve ainda considerar procedimentos de contingência de forma a evitar que esta situação tenha impacto na capacidade do BAIE em continuar a operar (por exemplo, o fornecedor presta serviços que são imprescindíveis à continuidade das operações do Banco).

6.4. 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; e
- Processo de gestão da mudança, para gerir eventuais alterações aos produtos ou serviços.

6.4.1. 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).

No caso de serviços críticos, caso seja necessário, podem ser realizadas auditorias aos controlos do prestador de serviço, 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.

6.4.2. 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, documentação e comunicação)

8.1. Registo

Todos os acordos com fornecedores e prestadores de serviços 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, 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 e subcategoria da actividade contratada e que permita identificar os diferentes tipos de acordos;
e) Grau de dependência do prestador de serviço; e
f) Data de início, data do termo e, se for caso disso, a data da próxima renovação do contrato e existência de períodos de pré-aviso.

Sempre que se tratar de um fornecedor ou prestador de serviços crítico para o Banco, são observados os registos indicados na Política de Subcontratação.

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 centralizada na Unidade de Eficiência Operacional integrada no Departamento de Eficiência e Operações (DEO-UEO).

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 de dois em dois anos ou sempre que as circunstâncias da actividade do Banco ou alterações legais ou regulamentares o justifiquem.

Compete, assim, ao DEO-UEO proceder à sua actualização, ao Departamento de Compliance (DdC) e à Função de Segurança da Informação (FSI) 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 na plataforma de arquivo digital.

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;
- 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*);
- Compromisso do Banco de Portugal com a Sustentabilidade e o financiamento Sustentável (2020);
- 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; e
- Norma ISO/IEC 27002:2013.

11. Relação com outros documentos

- Código de Conduta;
- Política de Gestão de Riscos;
- Política de Subcontratação;
- Plano de Continuidade de Negócio;
- Política de Segurança de Informação;
- Norma de Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
- Política de Prevenção ao Branqueamento de Capitais e Financiamento do Terrorismo.

Aprovado em Conselho de Administração em 20-01-2023.

Luís Lélis Presidente do Conselho de Administração	Inokcelina de Carvalho Administradora Não Executiva	César Gonçalves Administrador Não Executivo - Independente
Omar Guerra Presidente da Comissão Executiva	Nuno Leal Administrador Executivo	Henrique Gonçalves Administrador Executivo