SPC GRAFENO

POLÍTICA DE GESTÃO DE TERCEIROS

SPC GRAFENO INFRAESTRUTURA E TECNOLOGIA PARA O SISTEMA FINANCEIRO S.A

Sumário

1. OBJETIVO

Esta Política tem como objetivo estabelecer as diretrizes e requisitos relacionados à Gestão de Terceiros na SPC Grafeno Infraestrutura e Tecnologia para o Sistema Financeiro S.A. (“Companhia”) a fim de mitigar riscos inerentes aos contratos pactuados, essencialmente quando se tratar de serviços críticos e terceiros relevantes.

2. ABRANGÊNCIA

Esta Política se aplica à Companhia e a todos os seus colaboradores, administradores, fornecedores e prestadores de serviços.

3. ALÇADA DE APROVAÇÃO

- Área de Compliance, CI, Riscos e SI – responsável pela elaboração e revisão do documento.
- Comitê de Riscos, Compliance e SI - responsável pela revisão e aprovação do documento.
- Conselho de Administração - responsável pela aprovação final do documento.

4. DOCUMENTOS DE REFERÊNICA

- Código de Ética e Conduta da Companhia;
- Política de Conflito de Interesses;
- Política de Governança e Compliance;
- Política de Gerenciamento de Riscos e Controles;
- Política de PLD-FT;
- Política de Segurança da Informação e Cibernética;
- Política de Continuidade de Negócios;
- Plano de Recuperação de Desastres;
- Manual de Procedimento de KYP, KYS, KYE;
- Manual de Gestão de Acessos a Sistemas e Informações;
- Resolução 304/2023 – Regulamenta a atividade de registro de ativos financeiros
- Resolução 339/2023 – Regulamento a atividade de registro de duplicatas escriturais

- PFMI - Principles for financial market Infrastructures (BIS/IOSCO)

5. PAPÉIS E RESPONSABILIDADES

5.1. ÁREAS DEMANDANTES DA CONTRATAÇÃO

Para assegurar a contratação eficiente de serviços e fornecedores, é essencial colaborar na definição do orçamento disponível e garantir que os custos estejam alinhados com as expectativas da Companhia. A avaliação das opções deve ser criteriosa, considerando experiência, reputação, preço e capacidade, além de cumprir os requisitos sobre conflito de interesses conforme o Código de Ética e Conduta da Companhia.

Adicionalmente, é necessário abrir demandas junto ao Jurídico para formalizar contratos de prestação de serviços e junto às áreas de Riscos e Controles e Compliance/PLD para avaliar os riscos inerentes à contratação. Durante a relação com fornecedores, é importante lidar prontamente com disputas e problemas que possam surgir, garantindo uma gestão eficaz e alinhada aos padrões éticos e operacionais da Companhia.

5.2. ÁREA DE CONTROLE FINANCEIRO

Para assegurar uma contratação eficaz de serviços, é essencial validar o orçamento e determinar se a terceirização é a melhor solução para as necessidades da Companhia. Selecionar fornecedores que cumpram os requisitos de qualidade, preço e prazo de entrega, além de negociar termos contratuais, como preços, prazos, garantias e cláusulas de rescisão, são etapas críticas do processo.

Adicionalmente, é importante avaliar a reputação, credibilidade, capacidade e histórico de desempenho dos fornecedores, além de solicitar que preencham o Formulário KYS (Conheça seu Fornecedor e Prestador de Serviço) para avaliação de riscos pelas áreas de Riscos, Segurança e Cyber e PLD/FT. Garantir que os custos estejam alinhados com as expectativas da Companhia e comparar as opções disponíveis com base em critérios como experiência, reputação, preço e capacidade são práticas essenciais para uma contratação bem-sucedida.

5.3. ÁREA DE TECNOLOGIA, DADOS E INOVAÇÃO

A área de Tecnologia deve definir claramente os objetivos e requisitos do projeto ou serviço a ser terceirizado, criando critérios de seleção que avaliem os candidatos com base na criticidade do serviço e na sensibilidade dos dados a serem processados. É necessário realizar uma avaliação completa da capacidade técnica, financeira e legal dos potenciais fornecedores, garantindo que estejam em conformidade com regulamentações e padrões relevantes. A colaboração com o departamento jurídico é crucial para elaborar contratos claros e abrangentes que estabeleçam expectativas, responsabilidades, prazos e métricas de desempenho.

Além disso, é essencial monitorar o desempenho dos fornecedores em relação aos indicadores-chave de desempenho (KPIs) e apoiar no desenvolvimento de planos de continuidade de negócios que abordem a dependência dos serviços de terceiros, além de estabelecer procedimentos de contingência para lidar com interrupções nos serviços prestados por terceiros e resolver problemas e conflitos de forma eficaz são práticas fundamentais. Realizar revisões regulares do desempenho dos fornecedores e dos resultados alcançados ajuda a manter a qualidade e a eficiência dos serviços contratados.

Cabe à Diretoria de Tecnologia, Dados e Inovação apoiar as demais áreas na avaliação de viabilidade técnica, requisitos de integração e riscos associados aos serviços contratados, bem como zelar pela qualidade técnica dos serviços prestados por terceiros no âmbito de tecnologia.

Além disso, é de sua responsabilidade garantir a aderência aos requisitos regulatórios aplicáveis às contratações e alterações contratuais com Provedores de Serviços Críticos (PSC), em especial aqueles relacionados a serviços de tecnologia, infraestrutura e computação em nuvem. Para tanto, deverá:

- Avaliar, em conjunto com as áreas de Riscos, Jurídico e Compliance, a criticidade e a localização geográfica dos serviços contratados (Brasil ou exterior), conforme os critérios da Resolução BCB nº 304/2023;
- Assegurar que os ambientes de tecnologia utilizados, inclusive de desenvolvimento, homologação e produção, estejam devidamente identificados e que sua localização física (data centers) esteja em conformidade com os requisitos regulatórios;
- Colaborar com as áreas responsáveis no envio das minutas contratuais ou aditivos ao Banco Central do Brasil, nos casos de contratação ou alteração de serviços relevantes de processamento e armazenamento de dados localizados fora do país, respeitando o prazo mínimo de 60 (sessenta) dias antes da assinatura contratual, conforme previsto no art. 73, §4º da Resolução BCB nº 304/2023;
- Manter registro atualizado dos ambientes utilizados em nuvem (nacionais e internacionais), com indicação dos serviços contratados, suas finalidades e localização;
- Apoiar a definição e o monitoramento de acordos de nível de serviço (SLAs), indicadores de disponibilidade e demais parâmetros de desempenho técnico exigidos para os serviços contratados;
- Garantir que a documentação técnica, os controles de segurança da informação e os mecanismos de resposta a incidentes estejam disponíveis e atualizados para fins de supervisão e fiscalização.

Finalmente, a área de Tecnologia deve desenvolver planos de resposta a incidentes para lidar com emergências ou crises relacionadas aos terceiros, garantindo uma resposta eficaz e minimização de danos. Isso inclui a criação de estratégias para resolver problemas rapidamente e assegurar a continuidade dos serviços críticos, protegendo os interesses da Companhia e mantendo a integridade dos dados e processos envolvidos.

5.4. ÁREA DE SEGURANÇA DA INFORMAÇÃO

Para terceirização de serviços, é crucial definir claramente os objetivos e requisitos do projeto, assegurando que os fornecedores cumpram os padrões de segurança da informação da Companhia. Medidas de segurança, como acordos de confidencialidade e requisitos de conformidade, devem ser implementadas conforme necessário, além de desenvolver planos de continuidade de negócios para abordar a dependência dos serviços de terceiros.

Adicionalmente, fornecer treinamento e conscientização aos funcionários sobre políticas e práticas de terceirização é vital para promover uma cultura de segurança e conformidade. É igualmente importante desenvolver planos de resposta a incidentes para lidar com emergências ou crises relacionadas a terceiros, garantindo uma resposta eficaz e a minimização de danos.

5.5. ÁREA JURÍDICA

A área Jurídica deve garantir que os contratos estejam alinhados com os objetivos estratégicos da Companhia e cumpram regulamentações e políticas internas, assegurando que contenham as cláusulas obrigatórias conforme a regulação aplicável.

5.5. ÁREA DE RISCOS E CONTROLES

A área de Riscos e Controles deve identificar e avaliar os riscos associados à contratação de terceiros, incluindo riscos operacionais, de segurança da informação, de proteção de dados, de compliance e judiciais, dentre outros, fornecendo um parecer sobre a contratação. Além disso, deve participar da elaboração de contratos que incluam cláusulas de gestão de riscos, responsabilidades e medidas de mitigação, fornecendo informações e análises para apoiar decisões informadas sobre a contratação, continuação ou rescisão de terceiros.

5.6. ÁREA DE COMPLIANCE/PLD

Realizar verificações de antecedentes de terceiros, incluindo pesquisa de registros públicos, histórico financeiro, reputação comercial e conformidade legal e regulatória, comunicando os resultados à Área de Riscos e Controles Internos para classificação dos riscos associados. Relatar irregularidades ou suspeitas de atividades ilícitas às autoridades competentes quando necessário, fornecendo informações e análises para apoiar decisões informadas sobre a contratação, continuação ou rescisão de terceiros.

5.7. AUDITORIA INTERNA

A Auditoria Interna deve avaliar periodicamente o processo de gestão de terceiros críticos, cobrindo governança, controles, segurança da informação e continuidade.

6. DIRETRIZES

6.1. OBRIGAÇÕES RELACIONADAS AO PRESTADOR DE SERVIÇO E FORNECEDOR

Os prestadores de serviços terceirizados e fornecedores da SPC Grafeno são obrigados a cumprir todos os requisitos da legislação brasileira aplicável, comprometendo-se a proteger informações contra acesso, alteração, destruição ou divulgação não autorizada, garantindo a confidencialidade. Devem assegurar que os recursos disponibilizados sejam utilizados exclusivamente para fins aprovados pela SPC Grafeno e que os sistemas e informações sob sua responsabilidade estejam devidamente protegidos, garantindo a continuidade do processamento de informações críticas de negócios.

Além disso, esses prestadores devem cumprir leis e regulamentos relacionados à propriedade intelectual e às atividades da SPC Grafeno e seu mercado de atuação. É necessário escolher mecanismos de segurança da informação que equilibrem fatores de risco, tecnologia e custo. Qualquer violação da Política de Segurança da Informação deve ser imediatamente informada à SPC Grafeno.

Quando envolvidos no armazenamento e/ou processamento de dados pessoais de clientes, funcionários, dados financeiros ou prestação de serviços de nuvem, os prestadores de serviço/fornecedores devem estar em conformidade com as leis aplicáveis. Aqueles classificados como críticos devem passar por um processo de avaliação de Segurança da Informação, incluindo uma verificação in loco, tanto na pré-contratação quanto durante a contratação, para garantir a segurança adequada dos dados e serviços.

6.2. CONTRATAÇÃO DE FORNECEDORES E PRESTADORES DE SERVIÇOS

O fluxo operacional para a contratação de fornecedores e prestadores de serviços, descreve as etapas essenciais que as áreas envolvidas da Companhia devem seguir ao buscar, selecionar e contratar fornecedores e prestadores de serviços. Desde a identificação das necessidades até a assinatura de contratos e o estabelecimento de relacionamentos de longo prazo, este processo requer uma abordagem estratégica e cuidadosa para garantir que a parceria seja benéfica para todas as partes envolvidas e contribua para o alcance dos objetivos da Companhia.

6.2.1. Identificação da Necessidade

Todas as necessidades de contratação de fornecedores e prestadores de serviços, devem estar previstas no planejamento orçamentário, o qual deve estar aprovado pela Diretoria Executiva da Companhia.

As áreas de demandantes podem sugerir ao departamento Controle Financeiro (Compras) os fornecedores e prestadores de serviços com os quais pretende manter relacionamento.

6.2.2. Aprovação Orçamentária

O orçamento para a contratação do fornecedor é revisado e aprovado pela equipe financeira. Qualquer orçamento adicional necessário para cobrir riscos identificados também deve ser considerado.

6.2.3. Conflito de Interesse

Para assegurar a imparcialidade e a integridade do processo de contratação, é essencial identificar e gerenciar potenciais conflitos de interesse. Qualquer colaborador envolvido no processo de contratação deve declarar, formalmente, qualquer interesse pessoal ou financeiro com os fornecedores e prestadores de serviços em potencial, conforme Política de Conflito de Interesses.

6.2.4. Análise de Riscos

A SPC Grafeno realiza a avaliação de riscos de fornecedores e prestadores de serviços de forma estruturada, tanto no momento da contratação inicial quanto durante o monitoramento da relação comercial, conforme critérios estabelecidos pelas áreas de Riscos, Controles Internos e Compliance.

A avaliação pré-contratual considera fatores como:

- Natureza do serviço a ser prestado;
- Acesso a sistemas ou dados sensíveis;
- Relevância operacional e/ou regulatória;
- Histórico reputacional e integridade;
- Riscos associados à LGPD e Segurança da Informação.

Para fornecedores já contratados, poderão ser conduzidas **avaliações periódicas de risco**, com foco em:

- Continuidade da operação e dependência crítica;
- Cibersegurança e proteção de dados pessoais;
- Riscos legais, financeiros e regulatórios;
- Conformidade contratual e operacional.

A periodicidade da reavaliação será definida conforme o nível de risco atribuído ao fornecedor, podendo ser semestral para fornecedores classificados como de risco elevado, ou sob demanda, sempre que houver mudança relevante no escopo, incidente identificado, ou solicitação das áreas envolvidas.

As análises poderão incluir formulários estruturados, entrevistas, checklist de conformidade, consulta a bases públicas (Ex: órgãos reguladores, reputação, processos judiciais), ou coleta de evidências documentais específicas, conforme o escopo do risco.

6.2.5. Análise de Compliance/PLD

Com base nas informações fornecidas no formulário de KYS (*Know Your Supplier*) e em pesquisas adicionais, as áreas de Riscos, Compliance (PLD/FT) e Segurança da Informação realizam uma análise mais aprofundada dos riscos associados a cada fornecedor e prestador de serviço.

Para a antecipação do processo de análise de riscos, a área demandante poderá solicitar à área de Riscos e Controles Internos a análise prévia de um ou mais fornecedores ou prestadores de serviços, antes mesmo do início do processo junto à área de Controle Financeiro (Compras).

O resultado dessa análise pode ser positiva para o prosseguimento da contratação ou negativa devido aos riscos avaliados para a Companhia (contratante). Existe a possibilidade de ainda estabelecer medidas mitigatórias através de cláusulas contratuais para a continuidade da contratação ou manutenção do relacionamento.

6.2.6. Elaboração de Contratos

Com os fornecedores e prestadores de serviços selecionados, o departamento Jurídico e áreas demandantes, trabalham em conjunto para elaborar contratos detalhados que abordem todos os aspectos do relacionamento, incluindo preços, prazos, responsabilidades, cláusulas de mitigação de riscos e cláusulas obrigatórias exigidas pela regulação.

Sempre quando aplicável, os contratos devem ter uma vigência de, no mínimo, 12 (doze) meses.

Após a aprovação de todas as partes envolvidas, os contratos são assinados pelos representantes da Companhia, conforme designado em Estatuto Social, e pelos responsáveis da empresa fornecedora ou prestadora do serviço.

Todos os contratos com empresas que alocarão profissionais com acesso aos sistemas ou dados da SPC Grafeno deverão prever cláusulas específicas de segurança da informação, acesso lógico e físico, confidencialidade, tratamento de dados pessoais e responsabilidades em caso de falha ou incidente.

6.2.7. Encerramento do Contrato

No final do contrato, as áreas demandantes avaliam o desempenho geral do fornecedor e prestador de serviço e decide se deve renovar o contrato ou buscar novas opções com base no histórico de desempenho e nos riscos identificados.

O encerramento do contrato (distrato) deve ser direcionada ao departamento Jurídico, para a elaboração da formalização junto ao fornecedor.

6.3. CONDUTA E REQUISITOS DE SEGURANÇA PARA TERCEIROS

Os prestadores de serviços e fornecedores da SPC Grafeno devem seguir diretrizes rigorosas de segurança e conduta. O gestor responsável pela contratação deve solicitar o acesso lógico ao ambiente da rede interna por meio de uma ferramenta de chamados, que será avaliada conforme a necessidade e as diretrizes de Segurança da Informação.

Terceiros críticos devem demonstrar capacidade tecnológica, plano de evolução e processos de gestão de mudanças compatíveis com requisitos de resiliência da SPC Grafeno.

Os prestadores de serviços devem estar sujeitos às cláusulas contratuais específicas que tratem do uso de credenciais, revogação de acessos, confidencialidade, responsabilidade por incidentes, tratamento de dados pessoais e demais diretrizes de segurança da informação.

Para acesso remoto, o gestor deve providenciar um acesso via VPN, quando aplicável, com usuário único e individual, limitado aos recursos necessários para o trabalho. É responsabilidade do gestor informar a validade do contrato e solicitar a remoção do acesso quando não for mais necessário. Conexões de computadores de terceiros na rede interna requerem aprovação prévia e devem estar protegidos por softwares de segurança licenciados.

A SPC Grafeno proíbe a conexão de computadores de terceiros sem aprovação da alta direção de Segurança da Informação e exige que esses dispositivos estejam protegidos por software antivírus e anti-malware licenciados. Também é proibido o acesso, download ou distribuição de conteúdo que infrinja direitos autorais, propriedade intelectual ou conteúdo pornográfico, incluindo o que viole o Estatuto da Criança e Adolescente. As credenciais de acesso fornecidas aos terceiros são de uso exclusivo e não podem ser compartilhadas.

A empresa contratada deve informar formalmente a SPC Grafeno sobre o desligamento, substituição ou mudança de escopo dos colaboradores alocados em projetos, com antecedência mínima, permitindo a revogação oportuna dos acessos. A não comunicação poderá acarretar sanções contratuais, principalmente em casos de incidentes relacionados ao uso indevido de acessos.

Sempre que o prestador de serviços necessitar acesso privilegiado (Ex: contas administrativas, root etc.), deverá ser aprovada solicitação formal pela área de SI. A SPC Grafeno manterá um inventário centralizado de contas privilegiadas de terceiros, sendo vedado o uso compartilhado dessas credenciais.

Qualquer necessidade de acesso aos sistemas fora do horário de expediente da Companhia deverá ser autorizada previamente pelo líder técnico responsável, devendo estar devidamente registrada em sistema de chamados.

6.4. GESTÃO DE TERCEIROS RELEVANTES (TI E SI)

Terceiros relevantes são prestadores de serviços cuja atuação é vital para a organização, podendo acarretar riscos sistêmicos significativos se não forem devidamente fiscalizados.

A SPC Grafeno manterá plano de comunicação com participantes em incidentes envolvendo terceiros críticos, garantindo transparência e informações tempestivas.

Na avaliação da relevância do serviço a ser contratado pelas áreas de TI ou SI, a Companhia deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pela empresa a ser contratada, especialmente os relacionados a processamento e armazenamento de dados em nuvem.

Após identificar a relevância do serviço, a SPC Grafeno solicitará informações adicionais usando o formulário de KYS para verificar:

- Cumprimento da legislação e regulamentação vigente.
- Acesso da SPC Grafeno aos relatórios de auditoria independente sobre procedimentos e controles.
- Provisão de informações e recursos de gestão para monitorar os serviços.
- Acesso do Banco Central do Brasil para supervisão.

6.4.1. Verificação Adicional para Serviços de Dados

Para serviços relevantes de processamento e armazenamento de dados, a SPC Grafeno fará a checagem de acesso, confidencialidade, integridade, disponibilidade, recuperação e segregação dos dados, além da conformidade com certificações e qualidade dos controles de acesso, através do formulário de KYS.

6.4.2. Procedimentos de Avaliação de Riscos

A avaliação de riscos dos terceiros relevantes deve seguir os procedimentos descritos no item 6.2 deste documento.

6.4.3. Requisitos Adicionais para Serviços no Exterior

Para serviços relevantes de processamento, armazenamento de dados e computação em nuvem no exterior, a Companhia deve observar as disposições da Resolução nº 304 do Banco Central do Brasil (BCB).

6.4.4. Comunicação com o Banco Central do Brasil

A área de Compliance deve informar ao Banco Central do Brasil todas as contratações e alterações relacionadas a terceirizações relevantes no prazo de até 10 (dez) dias após a contratação ou alteração contratual.

Para contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, as minutas contratuais devem ser enviadas ao Banco Central do Brasil pelo menos 60 (sessenta) dias antes da assinatura dos contratos.

As regras e controles descritos no item 6.3 aplicam-se integralmente aos terceiros relevantes em Tecnologia da Informação e Segurança da Informação, incluindo o controle de acessos privilegiados, necessidade de autorização prévia para acessos fora do horário de expediente, e obrigações contratuais claras sobre revogação e responsabilização.

7. DISPOSIÇÕES GERAIS

7.1. VIGÊNCIA

Esta Política vigorará por prazo indeterminado.

7.2. CASOS OMISSOS

Os casos omissos serão regulados pelo Comitê de Ética da Companhia, conforme necessário.

7.3. DIVISIBILIDADE

A invalidade ou ineficácia de qualquer disposição desta Política não afetará os demais dispositivos, que permanecerão em pleno vigor e efeito.

8. REVISÃO DA POLÍTICA

Esta Política poderá ser revisada anualmente. Eventuais correções ou aprimoramentos devem ser objeto de recomendação ao Conselho de Administração.

9. VIOLAÇÕES

As violações dos termos da presente Política serão examinadas pelo Comitê de Ética da SPC Grafeno e poderá aplicar as ações disciplinares descritas na Política de Consequências, reportando ao Conselho de Administração.

10. CONTROLE DE VERSÕES

Versão	Data	Responsável	Ocorrência
1.0	24/09/2020	Diretoria de Operações	Elaboração e Revisão do documento
1.0	24/09/2020	Conselho de Administração	Aprovação do documento
2.0	23/05/2022	Compliance/PLD	Revisão da 1.0 e criação da versão 2.0

2.0	09/12/2022	Diretoria de Operações	Revisão do documento
2.0	19/12/2023	Conselho de Administração	Aprovação do documento
3.0	15/09/2023	Comitê de Gerenciamento de Riscos	Revisão/Aprovação do documento
3.0	29/09/2023	Conselho de Administração	Aprovação final do documento
4.0	31/07/2024	Compliance e Riscos	Revisão do documento
4.0	05/08/2024	Segurança da Informação	Revisão do documento
4.0	27/08/2024	Comitê de Riscos, Compliance e SI	Revisão/Aprovação do documento
4.0	03/10/2024	Conselho de Administração	Aprovação final do documento
5.0	28/05/2025	Área de Riscos e Controles Internos	Revisão do documento: • Reforço nas responsabilidades da Dir. Tecnologia sobre a contratação ou alteração de serviços referentes aos provedores de serviços críticos; • Ajuste no processo de análise de riscos de fornecedores e prestadores de serviços; • Inclusão de regras de acessos aos sistemas pelos prestadores de serviços com necessidade de acesso ao nosso ambiente, com previsão em contratos.
5.0	11/06/2025	Comitê de Riscos, Compliance e SI	Revisão e aprovação do documento
5.0	24/06/2025	Conselho de Administração	Aprovação final do documento.
6.0	01/10/2025	Área de Riscos e Controles	Revisão do documento: Inclusão da Resolução 339/23 – Escrituradora Inclusão de responsabilidade da Auditoria Interna Inclusão de referência ao PFMI
6.0	07/11/2025	Comitê de Riscos, Compliance e SI	Revisão e aprovação do documento
6.0	07/11/2025	Conselho de Administração	Aprovação final do documento.

***