

# **POLÍTICA DE GESTÃO DE TERCEIROS**

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

<b>Política de Gestão de Terceiros</b>	<b>Código:</b> POL.RIS.03
<b>Áreas:</b> Riscos e Segurança da Informação	<b>Criado em:</b> 24/09/2020
<b>Diretoria:</b> Riscos, CI, Compliance e SI	<b>Revisão:</b> 04

## Sumário

<b>1. OBJETIVO .....</b>	<b>3</b>
<b>2. ABRANGÊNCIA.....</b>	<b>3</b>
<b>3. ALÇADA DE APROVAÇÃO .....</b>	<b>3</b>
<b>4. DOCUMENTOS DE REFERÊNCIA .....</b>	<b>3</b>
<b>5. PAPÉIS E RESPONSABILIDADES.....</b>	<b>3</b>
Áreas demandantes da contratação .....	4
Área de Controle Financeiro.....	4
Área de Tecnologia, Dados e Inovação.....	4
Área de Segurança da Informação.....	5
Área Jurídica .....	5
Área de Riscos e Controles .....	5
Área de Compliance/PLD.....	5
<b>6. DIRETRIZES.....</b>	<b>6</b>
<b>6.1. OBRIGAÇÕES RELACIONADAS AO PRESTADOR DE SERVIÇO E FORNECEDOR .....</b>	<b>6</b>
<b>6.2. CONTRATAÇÃO DE FORNECEDORES E PRESTADORES DE SERVIÇOS .....</b>	<b>6</b>
Identificação da Necessidade .....	6
Aprovação Orçamentária .....	7
Conflito de Interesse.....	7
Análise de Riscos.....	7
Análise de Compliance/PLD .....	7
Elaboração de Contratos .....	7
Encerramento do Contrato.....	8
<b>6.3. GERENCIAMENTO DE RISCOS DE FORNECEDORES E PRESTADORES DE SERVIÇOS .....</b>	<b>8</b>
<b>6.4. CONDUTA E REQUISITOS DE SEGURANÇA PARA TERCEIROS .....</b>	<b>9</b>
<b>6.5. GESTÃO DE TERCEIROS RELEVANTES (TI E SI) .....</b>	<b>10</b>
Verificação Adicional para Serviços de Dados .....	10
Procedimentos de Avaliação de Riscos.....	10
Requisitos Adicionais para Serviços no Exterior.....	10
Comunicação com o Banco Central do Brasil .....	10
<b>7. DISPOSIÇÕES GERAIS .....</b>	<b>11</b>
<b>7.1. VIGÊNCIA.....</b>	<b>11</b>
<b>7.2. CASOS OMISSOS .....</b>	<b>11</b>
<b>7.3. DIVISIBILIDADE .....</b>	<b>11</b>
<b>8. REVISÃO DA POLÍTICA.....</b>	<b>11</b>
<b>9. VIOLAÇÕES.....</b>	<b>11</b>
<b>10. CONTROLE DE VERSÕES .....</b>	<b>11</b>

<b>Política de Gestão de Terceiros</b>	<b>Código:</b> POL.RIS.03
<b>Áreas:</b> Riscos e Segurança da Informação	<b>Criado em:</b> 24/09/2020
<b>Diretoria:</b> Riscos, CI, Compliance e SI	<b>Revisão:</b> 04

## 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 REFERÊNCIA

- 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.

## 5. PAPÉIS E RESPONSABILIDADES

<b>Política de Gestão de Terceiros</b>	<b>Código:</b> POL.RIS.03
<b>Áreas:</b> Riscos e Segurança da Informação	<b>Criado em:</b> 24/09/2020
<b>Diretoria:</b> Riscos, CI, Compliance e SI	<b>Revisão:</b> 04

## 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.

## 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.

## 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

<b>Política de Gestão de Terceiros</b>	<b>Código:</b> POL.RIS.03
<b>Áreas:</b> Riscos e Segurança da Informação	<b>Criado em:</b> 24/09/2020
<b>Diretoria:</b> Riscos, CI, Compliance e SI	<b>Revisão:</b> 04

dos fornecedores e dos resultados alcançados ajuda a manter a qualidade e a eficiência dos serviços contratados.

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.

### **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.

### **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.

### **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.

### **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,

<b>Política de Gestão de Terceiros</b>	<b>Código: POL.RIS.03</b>
<b>Áreas: Riscos e Segurança da Informação</b>	<b>Criado em: 24/09/2020</b>
<b>Diretoria: Riscos, CI, Compliance e SI</b>	<b>Revisão: 04</b>

fornecendo informações e análises para apoiar decisões informadas sobre a contratação, continuação ou rescisão de terceiros.

## 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.

#### 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.

<b>Política de Gestão de Terceiros</b>	<b>Código: POL.RIS.03</b>
<b>Áreas: Riscos e Segurança da Informação</b>	<b>Criado em: 24/09/2020</b>
<b>Diretoria: Riscos, CI, Compliance e SI</b>	<b>Revisão: 04</b>

## **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.

## **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.

## **Análise de Riscos**

Inicialmente, uma avaliação de riscos é realizada para identificar os principais riscos associados a cada fornecedor em potencial. Isso pode incluir riscos financeiros, legais, de conformidade e operacionais.

Os fornecedores em potencial devem preencher um formulário de KYS (*Know Your Supplier*) que coleta informações detalhadas sobre a empresa contratada, incluindo sua estrutura organizacional, histórico financeiro, políticas de conformidade e outros dados relevantes.

## **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.

## **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.

<b>Política de Gestão de Terceiros</b>	<b>Código: POL.RIS.03</b>
<b>Áreas:</b> Riscos e Segurança da Informação	<b>Criado em:</b> 24/09/2020
<b>Diretoria:</b> Riscos, CI, Compliance e SI	<b>Revisão: 04</b>

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.

### **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. GERENCIAMENTO DE RISCOS DE FORNECEDORES E PRESTADORES DE SERVIÇOS**

Além da avaliação de riscos realizada previamente à contratação de fornecedores e prestadores de serviços, conforme descrito no item 6.2 deste documento, semestralmente, a área de Riscos e Controles realiza a avaliação de riscos dos fornecedores e prestadores de serviços com contratos vigentes com a Companhia. As análises poderão ser realizadas com uma periodicidade inferior a 6 meses para fornecedores e prestadores de serviços classificados como de alto risco.

Este processo, chamado de TPRM (*Third Party Risk Management*), segue as principais etapas:

- **Extração de Pagamentos:** Solicitação ao Financeiro (Contas a Pagar) de uma lista com todos os pagamentos realizados para fornecedores e prestadores de serviços no semestre anterior;
- **Exclusão de pagamentos por categoria:** Da lista fornecida pelo Contas a Pagar, excluem-se os pagamentos realizados como: Aluguel e Infra, impostos, pessoal, Depósito Judicial, Serviços de telefonia (Vivo, Claro, etc.), Correios, Capex, Eventos internos, Facilities (aquisição de café), Passagens e hospedagem das compras (não realizadas por agência de viagens), Plano de saúde e odontológico, IOF, licenças Adobe, seguros, dentre outros;
- **Consolidação de Fornecedores:** Serão selecionados os pagamentos realizados com o valor mensal superior à média dos pagamentos realizados no semestre anterior;
- **Matriz de Critérios de Relevância:** Aplicam-se critérios de pontuação, de acordo com a Matriz de Riscos de Terceiros, para os fornecedores filtrados, como:
  - Relevância Financeira;
  - Concentração de pagamento
  - Importância x Raridade
  - Dependência
  - Risco Legal
  - Relacionamento com Órgãos Públicos
  - Risco de Imagem

<b>Política de Gestão de Terceiros</b>	<b>Código:</b> POL.RIS.03
<b>Áreas:</b> Riscos e Segurança da Informação	<b>Criado em:</b> 24/09/2020
<b>Diretoria:</b> Riscos, CI, Compliance e SI	<b>Revisão:</b> 04

- Risco de Continuidade
  - LGPD
  - Cyber Security
- 
- **Média de Pontuação:** Serão selecionados os fornecedores que atingiram ou superaram a média de pontuação entre todos os critérios de relevância.
  - **Escopo de Avaliação de Fornecedores:** Dentro do escopo de avaliação, compreendem-se as respostas preenchidas no Formulário KYS, as avaliações de cláusulas obrigatórias nos contratos vigentes e a avaliação e PLD/FT através de ferramenta de apoio.
  - **Relatório de Avaliação:** Após a avaliação realizada, a área de Riscos e Controles elabora um Relatório final contendo os fornecedores selecionados no período, o resultado da avaliação e a lista de planos de ação para que a área contratante e/ou o departamento Jurídico implementem em prazo estabelecido.

#### 6.4. 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. O acesso só é concedido após o treinamento de segurança e a aceitação do Termo de Responsabilidade. Para acesso remoto, o gestor deve providenciar um acesso via VPN 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 terceirizada deve comunicar qualquer desligamento de colaboradores para que seus acessos sejam cancelados. O compartilhamento de usuários e senhas entre prestadores de serviços é estritamente proibido.

<b>Política de Gestão de Terceiros</b>	<b>Código: POL.RIS.03</b>
<b>Áreas: Riscos e Segurança da Informação</b>	<b>Criado em: 24/09/2020</b>
<b>Diretoria: Riscos, CI, Compliance e SI</b>	<b>Revisão: 04</b>

## 6.5. 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.

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.

### 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.

### Procedimentos de Avaliação de Riscos

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

### 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).

### 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.

<b>Política de Gestão de Terceiros</b>	<b>Código:</b> POL.RIS.03
<b>Áreas:</b> Riscos e Segurança da Informação	<b>Criado em:</b> 24/09/2020
<b>Diretoria:</b> Riscos, CI, Compliance e SI	<b>Revisão:</b> 04

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.

## 7. DISPOSIÇÕES GERAIS

### 7.1. VIGÊNCIA

Esta Política vigorará por prazo indeterminado.

### 7.2. CASOS OMISSOS

Os casos omissos serão regulados pelo Conselho de Administração 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

<b>Política de Gestão de Terceiros</b>	<b>Código: POL.RIS.03</b>
<b>Áreas: Riscos e Segurança da Informação</b>	<b>Criado em: 24/09/2020</b>
<b>Diretoria: Riscos, CI, Compliance e SI</b>	<b>Revisão: 04</b>

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

\*\*\*