Política de Segurança de Fornecedores

Segurança da informação e proteção de dados no relacionamento com fornecedores, parceiros e prestadores de serviços da PX.Center

Código:	*POL-SEG-011*
Área responsável:	*Segurança da Informação*
Data de emissão:	*24/06/2026*
Responsável pela aprovação:	*CISO / CTO*

1. FINALIDADE/OBJETIVO

Esta política estabelece as diretrizes para a gestão da segurança da informação no relacionamento com fornecedores, parceiros e prestadores de serviços da PX.Center, assegurando que os serviços prestados por terceiros preservem a confidencialidade, a integridade e a disponibilidade da informação da Organização.

Em conformidade com os controles 5.19, 5.20, 5.21 e 5.22 da ISO/IEC 27001:2022 e com a ISO/IEC 27701:2019, a política define os requisitos de seleção, contratação, monitoramento, subcontratação e encerramento aplicáveis à cadeia de fornecimento, incluindo as obrigações específicas de proteção de dados pessoais quando o fornecedor atua como operador de dados em nome da PX.Center, conforme a Lei 13.709/2018 (LGPD). Esta política deriva da Política de Segurança da Informação (POL-SEG-001) e detalha seus requisitos no domínio do relacionamento com fornecedores e da cadeia de fornecimento.

2. ESCOPO/APLICABILIDADE

Esta política aplica-se a todos os fornecedores, parceiros, prestadores de serviços terceirizados e provedores de nuvem (cloud/SaaS) cujos serviços possam impactar a segurança da informação ou envolver o tratamento de dados pessoais da PX.Center, bem como aos colaboradores internos responsáveis pela contratação, gestão e supervisão desses serviços. Abrange todo o ciclo de vida do relacionamento com o terceiro: identificação de riscos, classificação, seleção, formalização contratual, execução, monitoramento e encerramento.

Aplica-se em conjunto com a POL-SEG-029 (norma-base de tratamento de dados pessoais) sempre que a contratação envolver dados pessoais. Subordina-se à Política de Segurança da Informação (POL-SEG-001), da qual deriva, e a complementa no domínio de fornecedores.

3. USUÁRIOS/PÚBLICO-ALVO

Direção, Líder de Segurança da Informação, Encarregado de Dados (DPO), Jurídico, gestores de área requisitantes de contratação, equipe de TI e todos os colaboradores e terceiros envolvidos na contratação, gestão ou supervisão de fornecedores que tenham acesso a informações, sistemas ou dados pessoais da PX.Center.

4. DOCUMENTOS DE REFERÊNCIA

- Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD)
- ISO/IEC 27001:2022 (controles 5.19, 5.20, 5.21 e 5.22)
- ISO/IEC 27701:2019 (controle 6.12)
- POL-SEG-001: Política de Segurança da Informação
- POL-SEG-029: Política de Privacidade e Proteção de Dados Pessoais

- POL-SGI-001: Política de Ciclo de Vida da Informação
- POL-SEG-016: Política de Controle de Acessos
- POL-SEG-004: Metodologia de Avaliação e Tratamento de Riscos
- POL-SEG-002: Política de Gestão de Incidentes
- POL-SGI-002: Política de Controle de Registros
- FOR-17-001: Questionário de Due Diligence de Fornecedores

5. DIRETRIZES / REGRAS / CONTROLES

5.1 IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

A área de Segurança da Informação, em conjunto com a área requisitante e o Jurídico, identifica, avalia e trata os riscos de segurança da informação em todo processo que envolva terceiros. A avaliação ocorre antes da contratação e é revisada periodicamente ou sempre que houver alteração no escopo dos serviços. São considerados, entre outros critérios: acesso a dados sensíveis ou críticos, conexão à rede corporativa, processamento de dados de clientes ou de outros titulares e a existência de subcontratação.

Quando a contratação envolver tratamento de dados pessoais, o Encarregado de Dados (DPO) é envolvido na avaliação, conforme a seção 5.4.

5.2 CLASSIFICAÇÃO DE RISCO DE FORNECEDORES

Todo fornecedor é classificado em uma das três categorias de risco — Alto, Médio ou Baixo — previamente à contratação, com base no tipo de acesso a ativos da Organização, no volume e na sensibilidade dos dados pessoais tratados e na criticidade do serviço prestado para as operações da PX.Center. Classifica-se como de Alto Risco o fornecedor que detenha acesso privilegiado a sistemas ou à rede corporativa, que trate volume relevante de dados pessoais ou dados pessoais sensíveis, ou cujo serviço seja crítico para a continuidade do negócio.

O fornecedor de Médio Risco mantém acesso limitado a informações internas ou trata dados pessoais em escopo restrito, e o de Baixo Risco não acessa dados pessoais nem ativos críticos. Os fornecedores classificados como de Alto Risco são submetidos a due diligence prévia à contratação e à reavaliação anual; os de Médio e Baixo Risco seguem a periodicidade de revisão proporcional definida na seção 5.8. A classificação é registrada e revista a cada renovação contratual ou alteração relevante de escopo.

5.3 SELEÇÃO E DUE DILIGENCE

A PX.Center tem como premissa contratar apenas terceiros de reputação ilibada, conduta íntegra e capacidade técnica comprovada. A área responsável pela contratação realiza a triagem do fornecedor com apoio da Segurança da Informação, verificando a conformidade com requisitos legais e regulatórios, as certificações relevantes (por exemplo, ISO 27001, SOC 2 e adequação à LGPD), o histórico de incidentes de segurança e a reputação no mercado.

Quando a contratação envolver o tratamento de dados pessoais, é realizada avaliação prévia da capacidade técnica e das medidas de segurança adotadas pelo terceiro por meio do FOR-17-001 (Questionário de Due Diligence de Fornecedores), cujas respostas são analisadas com o envolvimento do DPO. O fornecedor só é aprovado após a validação formal da análise de risco. Para terceiros já contratados antes da publicação desta política, a análise de conformidade é realizada para avaliar a pertinência de manter ou encerrar a relação contratual.

5.4 PAPEL DO DPO NA CONTRATAÇÃO DE OPERADORES DE DADOS

Sempre que a contratação envolver o tratamento de dados pessoais pelo terceiro em nome da PX.Center — caracterizando-o como operador na forma da LGPD — o Encarregado de Dados (DPO) é obrigatoriamente consultado, previamente à formalização. Cabe ao DPO definir, em conjunto com o Jurídico, os requisitos de proteção de dados pessoais aplicáveis ao contrato; avaliar as respostas do FOR-17-001 para confirmar o atendimento aos requisitos; e promover diligências recorrentes para verificar a manutenção da conformidade.

Caso o terceiro não atenda aos requisitos, medidas corretivas são definidas em conjunto com o DPO e implementadas antes do prosseguimento da contratação. O DPO é também consultado em caso de dúvidas sobre a contratação de operadores, incidentes de segurança ou qualquer questão de proteção de dados pessoais que possa afetar a conformidade com a LGPD.

5.5 REQUISITOS CONTRATUAIS DE SEGURANÇA DA INFORMAÇÃO

A inserção de cláusulas contratuais de segurança da informação é de responsabilidade do Jurídico, com apoio técnico da Segurança da Informação. Os contratos preveem, no mínimo: acordo de confidencialidade (NDA); responsabilidades sobre a proteção da informação e dos dados; requisitos mínimos de segurança; penalidades em caso de descumprimento; e regras de término, devolução ou destruição de ativos e informações. O proprietário do contrato é a área requisitante da contratação.

Para contratações que não envolvam instrumento contratual formal, é firmado Termo de Compromisso estabelecendo a observância dos requisitos de segurança e das disposições da LGPD.

5.6 PROTEÇÃO DE DADOS PESSOAIS E ACORDO DE TRATAMENTO (DPA)

Quando o fornecedor atua como operador de dados pessoais em nome da PX.Center, é obrigatória a celebração de Acordo de Tratamento de Dados Pessoais (DPA — Data Processing Agreement), elaborado pelo Jurídico em conjunto com o DPO, em atendimento à ISO/IEC 27701:2019 (6.12) e à LGPD. O DPA define, de forma expressa:

os papéis de controlador e operador; a finalidade e as categorias de dados tratados; as medidas técnicas e organizacionais de segurança; as condições para uso de suboperadores; as regras para transferências internacionais; a obrigação de notificação de incidente; o apoio ao atendimento dos direitos dos titulares; os prazos de retenção; a devolução ou eliminação dos dados ao término da relação; e o direito de auditoria da PX.Center. Os contratos definem

claramente os deveres e as responsabilidades de cada parte em caso de violação de dados pessoais.

A cláusula contratual de proteção de dados pessoais a ser incorporada aos contratos com fornecedores observa o conteúdo mínimo previsto no Anexo I desta política.

5.7 SUBCONTRATAÇÃO

O fornecedor não pode subcontratar, no todo ou em parte, os serviços contratados que envolvam acesso a informações, sistemas ou dados da PX.Center sem autorização formal, prévia e por escrito da PX.Center. A necessidade dessa autorização é estabelecida em contrato. Autorizada a subcontratação, o fornecedor permanece integralmente responsável perante a PX.Center e deve repassar contratualmente ao subcontratado todos os requisitos de segurança e de proteção de dados pessoais assumidos nesta política, garantindo que as práticas do subcontratado estejam em conformidade com este documento.

Para fornecedores críticos e provedores cloud/SaaS, avaliam-se os subcontratados, as dependências e os componentes da cadeia de fornecimento, que é reavaliada antes de mudanças relevantes, com notificação obrigatória de alterações.

5.8 MONITORAMENTO E REVISÃO

A área requisitante, com apoio da Segurança da Informação, monitora o desempenho do fornecedor em relação aos requisitos contratuais de segurança. A revisão de conformidade tem periodicidade mínima anual para fornecedores de Alto Risco, ajustável conforme a criticidade do fornecedor e a sua classificação. Relatórios, evidências e auditorias internas podem ser exigidos conforme o contrato.

Quando há tratamento de dados pessoais, o DPO realiza diligências periódicas para confirmar a manutenção da conformidade; identificada inadequação em terceiro já contratado, é negociado prazo razoável, com base no risco, para adequação, e, não atendido o prazo, o DPO interage com o gestor do contrato para propor a substituição do fornecedor.

5.9 TREINAMENTO E CONSCIENTIZAÇÃO

A Segurança da Informação provê materiais de conscientização sobre segurança da informação a serem apresentados aos fornecedores críticos previamente à execução dos serviços. Para os colaboradores internos, treinamentos periódicos abordam os riscos da terceirização e as boas práticas no relacionamento com parceiros.

5.10 USO DE REDES SOCIAIS NO RELACIONAMENTO COM TERCEIROS

O uso de redes sociais em nome da PX.Center é permitido às funções de negócio que dele dependam, em especial Marketing e Comercial, observada a vedação à divulgação de informações confidenciais ou de dados pessoais da Organização, de seus clientes ou de seus fornecedores. Aos demais colaboradores é vedado o uso pessoal de redes sociais durante a execução de atividades que envolvam informações ou ativos da Organização.

Os fornecedores e prestadores de serviços com acesso a informações da PX.Center observam idêntica restrição, sendo-lhes vedado expor, em redes sociais ou canais externos,

qualquer informação confidencial ou dado pessoal a que tenham acesso em razão do contrato.

5.11 COMUNICAÇÃO DE VIOLAÇÕES

Toda suspeita ou ocorrência de violação desta política, dos requisitos de segurança ou das obrigações de proteção de dados pessoais é comunicada de imediato pelos canais oficiais da PX.Center. As questões relativas a privacidade e proteção de dados pessoais são reportadas ao Encarregado de Dados (DPO), pelo canal dpo@px.center; as questões relativas a segurança da informação são reportadas à área de Segurança da Informação, pelo canal security@px.center.

As comunicações são tratadas de forma diligente e confidencial, e, confirmada a violação, são adotadas as medidas corretivas e disciplinares cabíveis.

5.12 ENCERRAMENTO DE CONTRATO, REVOGAÇÃO DE ACESSO E DEVOLUÇÃO DE ATIVOS

A área requisitante informa à Segurança da Informação toda mudança de escopo ou término de contrato. A SI avalia e atualiza os riscos, documenta os resultados e os encaminha às áreas de Compliance e Jurídico. A equipe de TI, sob orientação da Segurança da Informação, garante a revogação dos acessos e a devolução dos ativos tecnológicos (notebooks, tokens, credenciais e demais recursos) ao término do contrato.

A devolução ou destruição das informações e dos dados pessoais compartilhados é confirmada e registrada no encerramento da relação, assegurando que o fornecedor não mantenha qualquer forma de acesso aos dados ou sistemas da Organização.

6. RESPONSABILIDADES

6.1 Gestor da área requisitante (proprietário do contrato): exige que os terceiros sigam as regras de segurança e privacidade da PX.Center e as disposições contratuais; encaminha o FOR-17-001 ao fornecedor previamente à contratação; remete as respostas ao DPO para análise quando houver tratamento de dados pessoais; monitora continuamente a execução do serviço; e comunica de imediato à Segurança da Informação e ao DPO os incidentes e situações que afetem a conformidade.

6.2 Segurança da Informação: identifica, classifica e trata os riscos de fornecedores; define as métricas e os requisitos de segurança nos contratos previamente à execução dos serviços; orienta os terceiros quanto à PSI; acompanha a aplicação dos controles ao longo do contrato; e atua como responsável interno pela apuração das violações relativas à segurança da informação, recebidas pelo canal security@px.center.

6.3 Jurídico: elabora, em conjunto com o DPO, os modelos de contrato, de DPA e de Termo de Compromisso; e garante a inclusão dos requisitos de segurança e de proteção de dados pessoais nos novos contratos, nas revisões e nas renovações.

6.4 Encarregado de Dados (DPO): define com o Jurídico os requisitos de proteção de dados pessoais nos contratos com operadores; avalia o FOR-17-001; promove diligências recorrentes; presta esclarecimentos sobre a aplicação desta política nas questões de proteção de dados pessoais; e atua como responsável interno pela apuração das violações relativas à privacidade e à proteção de dados pessoais, recebidas pelo canal dpo@px.center.

6.5 Equipe de TI: executa a revogação de acessos e a devolução de ativos ao término do contrato, sob orientação da Segurança da Informação.

Aprovação: CISO / CTO.

7. GESTÃO DE REGISTROS

Os registros relacionados a fornecedores — classificações de risco, avaliações, questionários FOR-17-001, contratos e DPA, relatórios de monitoramento, evidências de diligências e de devolução de ativos — são armazenados em repositório seguro e controlado pela área responsável, com acesso restrito por necessidade de conhecimento. A PX.Center mantém planilha-padrão de controle de registros conforme a Política de Gestão de Registros. Os registros são preservados com integridade e mantidos disponíveis para auditorias internas e externas do SGI.

8. VALIDADE / GESTÃO DOCUMENTAL

Esta política entra em vigor em 23/06/2026, com validade por prazo indeterminado. É revisada anualmente ou diante de mudança relevante na estratégia de segurança da Organização, na legislação ou em orientações da ANPD, ou de necessidade de adequação tecnológica. O proprietário do documento é a área de Segurança da Informação, sob aprovação do CISO / CTO. O descumprimento desta política pelos colaboradores, contratados ou prestadores de serviços sujeita o infrator às medidas disciplinares previstas nas normas internas da PX.Center, sem prejuízo das sanções legais e contratuais cabíveis.

9. ANEXOS

FOR-17-001 — Questionário de Due Diligence de Fornecedores: instrumento de avaliação prévia da capacidade técnica e das medidas de segurança e de proteção de dados pessoais do terceiro, aplicado na seleção e nas diligências periódicas. Os demais registros operacionais residem nos repositórios indicados na seção Gestão de Registros.

ANEXO I — CLÁUSULA CONTRATUAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Cláusula a ser incorporada aos contratos celebrados com fornecedores que tratem dados pessoais em nome da PX.Center, com a numeração ajustada ao instrumento contratual respectivo.

Da Proteção de Dados. As Partes declaram ter conhecimento das disposições previstas na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados — LGPD), responsabilizando-se por seu integral cumprimento, bem como por obter as autorizações de seus respectivos clientes e titulares quando necessária a eventual disponibilização de dados a terceiros, isentando a Parte contrária de responsabilidade nesse sentido ou por eventual descumprimento da referida legislação.

O tratamento de dados pessoais é realizado única e exclusivamente para as finalidades necessárias à execução dos serviços contratados, vedado o uso para finalidades diversas sem o consentimento expresso do Contratante ou do titular dos dados, quando necessário, observada a responsabilidade solidária das Partes nos termos da LGPD.

As Partes comprometem-se a adotar todas as medidas técnicas e organizacionais cabíveis para proteger os dados pessoais contra acesso não autorizado, perda, destruição, vazamento ou qualquer forma de incidente ou tratamento ilícito, utilizando-os somente para o cumprimento do contrato.

As Partes obrigam-se a comunicar, uma à outra, em até 48 (quarenta e oito) horas da ciência, a ocorrência de qualquer evento que represente incidente de segurança da informação com potencial violação de privacidade de titulares de dados pessoais. O comunicado, ainda que provisório, contempla, no mínimo: data e horário de ciência do incidente; descrição do incidente; tipos de dados potencialmente expostos; volume de titulares potencialmente expostos; e medidas adotadas para atenuar ou remediar os impactos, sob pena das penalidades previstas na LGPD.

Encerrado o contrato, independentemente do motivo, a Contratada elimina todos os dados pessoais obtidos em seu contexto, exceto quando a retenção for legalmente permitida ou exigida.

O descumprimento desta cláusula sujeita a Parte infratora à responsabilização por danos diretos ou indiretos, de ordem moral, material ou regulatória, bem como à aplicação das penalidades previstas na LGPD e nas demais legislações aplicáveis.

Todas as regras referentes ao tratamento de dados pessoais realizado pelo Contratante, inclusive os direitos dos titulares, constam do Aviso de Privacidade do Contratante, ao qual a Contratada declara ter tido acesso, lido e concordado.

HISTÓRICO DE ALTERAÇÕES

Versão	Data	Criador	Descrição de Alterações
00	09/06/2025	Setor de TI e Cybersegurança - SI	Criação e Revisão
01	24/06/2026	SGI	Recodificação para sigla