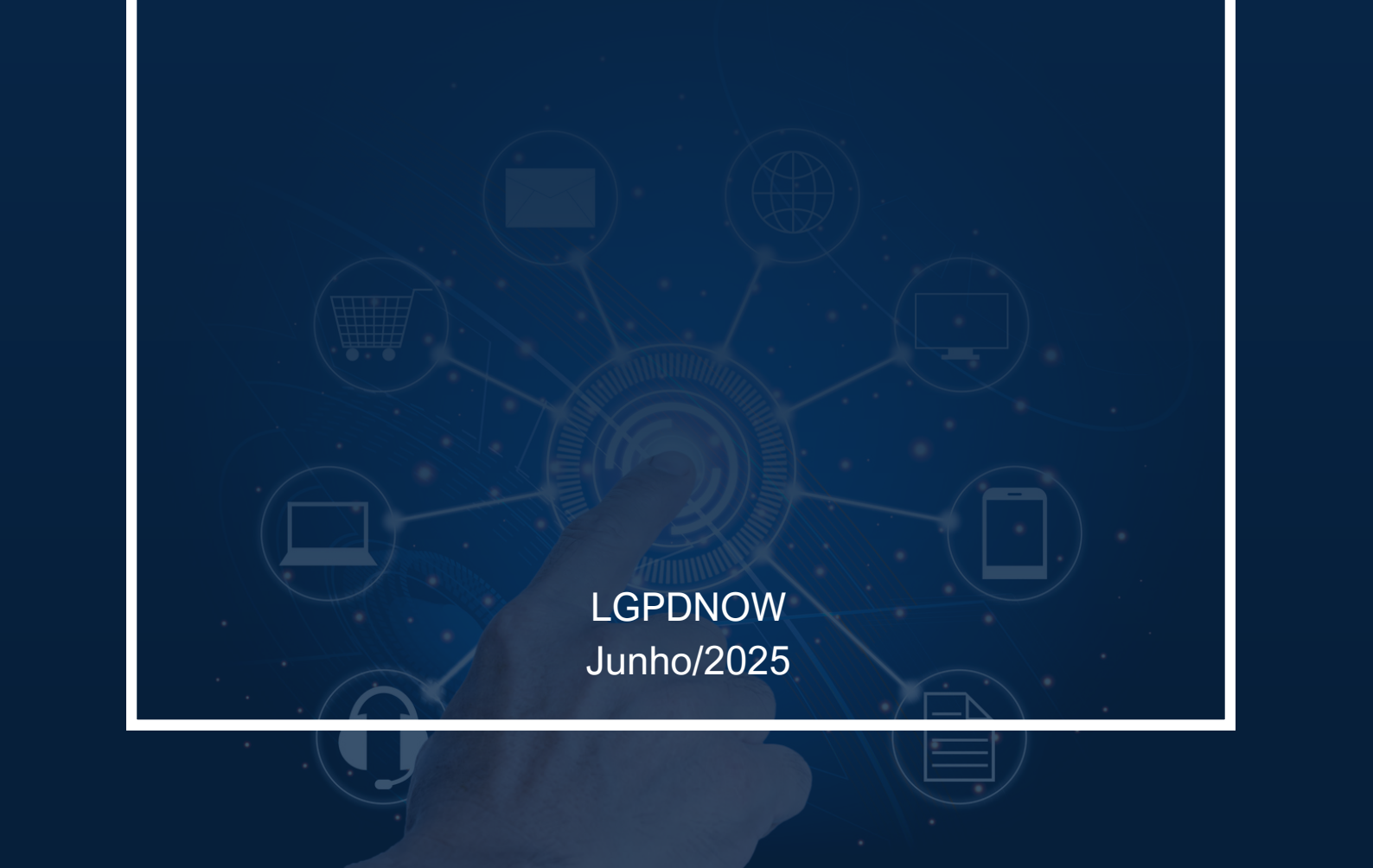
# Política de Gestão de Fornecedores/Terceiros em Conformidade com a LGPD da ETIPI - Empresa de Tecnologia da Informação do Piauí



LGPDNOW

Junho/2025

# POLÍTICA DE GESTÃO DE FORNECEDORES/TERCEIROS EM CONFORMIDADE COM A LGPD

## 1. OBJETIVO

Esta Política tem por finalidade estabelecer diretrizes, responsabilidades e procedimentos internos para a avaliação, contratação, formalização contratual e monitoramento contínuo de fornecedores e prestadores de serviço que realizem, direta ou indiretamente, o tratamento de dados pessoais sob responsabilidade da **Empresa de Tecnologia da Informação do Piauí - ETIPI**. Visa, ainda, garantir a conformidade com a LGPD (Lei nº 13.709/2018), as regulamentações da Autoridade Nacional de Proteção de Dados - ANPD e demais normas aplicáveis.

## 2. ÂMBITO DE APLICAÇÃO

Aplica-se a todas as contratações ou renovações contratuais com fornecedores que, no exercício de suas atividades, tratem direta ou indiretamente dados pessoais, independentemente do seu porte, localização ou natureza jurídica.

## 3. DEFINIÇÕES

Para melhor compreensão desta Política, apresenta-se os seguintes conceitos:

- **Terceiro:** fornecedor ou prestador de serviços, pessoa natural ou jurídica, que no âmbito da relação contratual com a organização realize operações de tratamento de dados pessoais, atuando como operador ou controlador, conforme o caso;
- **Controlador:** a quem competem as decisões sobre o tratamento de dados pessoais;
- **Operador:** quem realiza o tratamento em nome do controlador;
- **Tratamento dos dados pessoais:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
- **Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- **Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

- **Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- **Transferência internacional de dados**: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
- **Uso compartilhado de dados**: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
- **Incidente de segurança:** qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais;
- **Medidas de segurança:** medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **Encarregado de Dados (DPO):** profissional designado como canal entre o controlador, os titulares dos dados e a ANPD;
- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;
- **Dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **Dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

## 4. PRINCÍPIOS GERAIS

Todos os fornecedores contratados devem:

a. Tratar dados pessoais exclusivamente para as finalidades definidas contratualmente, abstendo-se de utilizá-los para qualquer outro fim não autorizado;
b. Observar e aplicar integralmente os princípios da LGPD, notadamente os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas;
c. Implementar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

d. Assegurar que seus colaboradores, prepostos, subcontratados e demais pessoas autorizadas a tratar dados pessoais estejam devidamente capacitados e comprometidos com as obrigações previstas na legislação e no contrato;
e. Comunicar imediatamente à organização qualquer incidente de segurança que possa acarretar risco ou dano relevante aos titulares dos dados pessoais, colaborando com a apuração dos fatos e mitigação dos impactos;
f. Atender, de forma tempestiva, às solicitações dos titulares de dados encaminhadas pela organização, bem como prestar suporte para o exercício dos direitos previstos no artigo 18 da LGPD;
g. Submeter-se a auditorias, inspeções e outras formas de verificação de conformidade conduzidas pela organização ou por terceiros por ela indicados;
h. Garantir que eventual compartilhamento de dados com sub operadores seja precedido de autorização expressa da organização e que estes assumam obrigações equivalentes às aqui previstas.

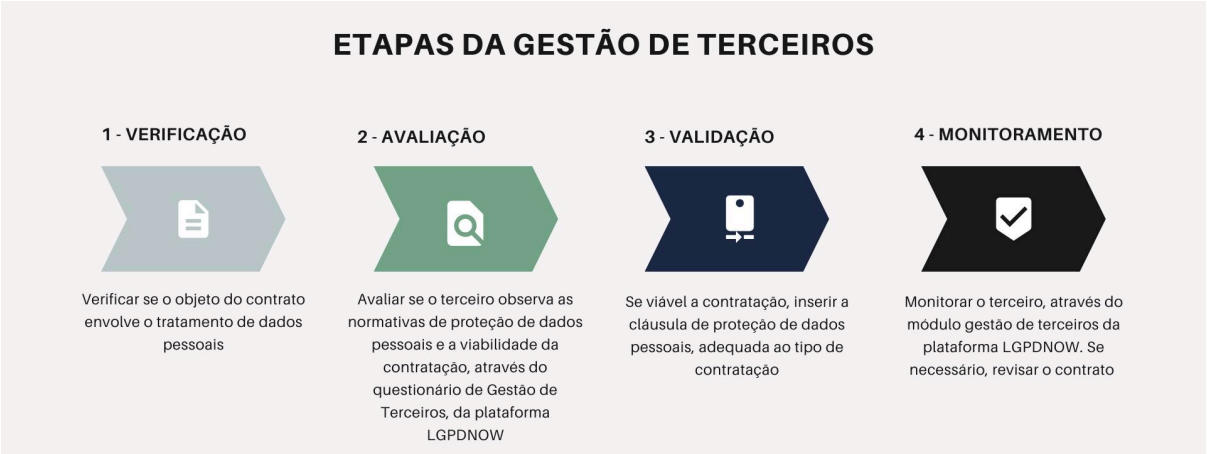
Todas as obrigações e responsabilidades do fornecedor no tocante à Privacidade e Proteção de dados devem estar devidamente previstas contratualmente.

## 5. ETAPAS DA GESTÃO DE FORNECEDORES

Considerando que a ETIPI está sujeita a procedimentos licitatórios regidos por normativas internas e princípios da Administração Pública, o fluxo de implementação da gestão de terceiros com foco em proteção de dados deve ser integrado aos trâmites licitatórios e contratuais, respeitando os princípios da legalidade, impessoalidade e eficiência.

Quando identificado que a contratação envolverá o tratamento de dados pessoais e que esta demanda processo licitatório, é indicado que seja exigido no certame a comprovação de adequação à Lei Geral de Privacidade e Proteção de Dados, podendo, se for o caso, condicionar esta contratação a esta comprovação, que deverá ser fruto de avaliação da área responsável.

O fluxo de análise do fornecedor engloba as seguintes etapas, detalhadas a seguir:




### 5.1. Etapa 1: VERIFICAÇÃO

**1º** A área demandante deverá identificar se haverá tratamento de dados pessoais no escopo da contratação e, em caso positivo, preencher o formulário (ANEXO I) e encaminhá-lo à área de Compliance (ou o Encarregado, juntamente com outra área responsável pela Privacidade da organização) (ou Encarregado, juntamente com outra área responsável pela Privacidade da organização).

**2º** A área de Compliance (ou o Encarregado, juntamente com outra área responsável pela Privacidade da organização) (ou Encarregado, juntamente com outra área responsável pela Privacidade da organização) analisará as informações e providenciará o envio do questionário de avaliação ao fornecedor vencedor do certame (ou ao contratado em caso de dispensa/inexigibilidade), após a definição do resultado da contratação.

**3º** O fornecedor terá o prazo de até 15 (quinze) dias úteis para responder ao questionário, anexando a documentação comprobatória ou apresentando justificativas formais, quando não for possível anexá-la.

### 5.2. Etapa 2: AVALIAÇÃO

**4º** O questionário será analisado pela equipe de Compliance (ou o Encarregado, juntamente com outra área responsável pela Privacidade da organização) (ou Encarregado, juntamente com outra área responsável pela Privacidade da organização), que avaliará as respostas e classificará o fornecedor em um dos níveis de conformidade:

- **Nível A – Conformidade Plena: requisitos atendidos, sem restrições;**
- **Nível B – Conformidade com ajustes menores: pequenas adequações podem ser exigidas;**
- **Nível C – Conformidade Condicionada: sujeito à adoção de medidas mitigatórias obrigatórias;**
- **Nível D – Risco Elevado: risco considerável, contratação não recomendada sem mitigação robusta;**
- **Nível E – Não Conformidade: fornecedor incompatível com os requisitos legais e da organização, contratação vedada.**

**5º** O resultado da avaliação será enviado à área demandante, à Comissão de Licitação ou setor responsável pela contratação para ciência e eventuais deliberações.

**6º** Fornecedores classificados nos níveis D ou E somente poderão ser contratados em situações excepcionais, mediante aprovação fundamentada da Diretoria Executiva, com plano de mitigação de riscos.

### 5.3. Etapa 3: ANÁLISE

**7º** A área jurídica deverá incluir cláusulas de proteção de dados pessoais no instrumento contratual, considerando o tipo de tratamento envolvido e a classificação do fornecedor.

**8º** Para fornecedores classificados como Nível C ou D (com mitigação possível), devem ser previstas cláusulas adicionais, como planos de adequação, obrigações específicas de segurança e comunicação de incidentes.

**9º** Fornecedores com risco não mitigado ou classificados como Nível E não poderão ser contratados.

### 5.4. Etapa 4: MONITORAMENTO

- Todos os fornecedores contratados, independentemente da data da contratação ou do nível de conformidade anteriormente atribuído, estarão sujeitos a monitoramento periódico, conforme diretrizes da área de Compliance (ou o Encarregado, juntamente com outra área responsável pela Privacidade da organização);
- Fornecedores classificados como Nível B, C ou D terão acompanhamento reforçado, com periodicidade definida com base em critérios de risco, podendo incluir monitoramentos semestrais ou anuais
- As ações de monitoramento significam a reaplicação do questionário de avaliação de fornecedores, exigência de evidências de cumprimento contratual, revalidação de cláusulas de proteção de dados e revisão de planos de mitigação;
- Incidentes envolvendo dados pessoais deverão ser comunicados imediatamente à organização e serão objeto de análise técnica e jurídica para eventuais sanções, revisão contratual ou rescisão.

## 6. RESPONSABILIDADES

As responsabilidades serão divididas da seguinte forma:

- **Área Demandante:** identificar, no momento da solicitação, se a contratação envolve tratamento de dados pessoais; preencher o formulário do ANEXO I; acompanhar a execução contratual com foco nas obrigações de proteção de dados;
- **Área de Compliance (ou o Encarregado, juntamente com outra área responsável pela Privacidade da organização):** Analisar os dados

recebidos, encaminhar questionário, avaliar riscos, emitir parecer de conformidade;

- **Jurídico:** revisar instrumentos contratuais e incluir cláusulas obrigatórias;
- **Fornecedor:** Garantir a conformidade com a LGPD e com as cláusulas contratuais, cooperar com auditorias, responder tempestivamente ao questionário LGPDNOW e manter medidas de segurança adequadas.

## 7. DISPOSIÇÕES FINAIS

Esta política entra em vigor na data de sua aprovação e será revisada anualmente ou sempre que houver alterações legais ou normativas relevantes. O descumprimento de seus termos pode ensejar sanções administrativas, contratuais e legais.

**ANEXO I – FORMULÁRIO DE IDENTIFICAÇÃO DE TRATAMENTO DE DADOS PESSOAIS DE FORNECEDORES**

Este Formulário é de preenchimento obrigatório pela área demandante sempre que houver contratação de fornecedor que, direta ou indiretamente, envolva o tratamento de dados pessoais.

Após o preenchimento, este formulário deve ser enviado à área de Compliance (ou o Encarregado, juntamente com outra área responsável pela Privacidade da organização) da ETIPI para prosseguimento da avaliação.

**DADOS DO FORNECEDOR:**

**Razão Social:**
**CNPJ:**
**Nome do Encarregado de Dados ou Responsável:**
**E-mail de Contato:**

**INFORMAÇÕES SOBRE O CONTRATO:**

1. **Qual é o serviço a ser contratado?**_____
   _____
   _____

2. **O contrato envolve tratamento de dados pessoais?** (  ) Sim (  ) Não

3. **Quais dados pessoais serão tratados?** (Ex: nome, CPF, e-mail, telefone, dados financeiros, dados sensíveis etc.)_____
   _____

4. **Quem são os titulares dos dados?** (Ex: funcionários, candidatos, clientes, fornecedores, visitantes etc.)_____
   _____

5. **Qual a finalidade do tratamento dos dados pessoais?**_____
   _____

6. **Haverá compartilhamento com suboperadores?** (  ) Sim (  ) Não
   Se sim, identifique os suboperadores e suas respectivas funções:_____
   _____

7. **Observações adicionais relevantes:**
   _____
   _____

**Área Demandante:**

**Data:** ____ / ____ / _____

## ANEXO II – MODELO DE COMUNICADO AVALIAÇÃO DE FORNECEDORES

### COMUNICADO AVALIAÇÃO DE FORNECEDORES

Local e data.

Prezado(a),

Como forma de manter estruturado o seu Programa de Privacidade e Proteção de Dados, conforme as diretrizes estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD) e as melhores práticas de mercado, a ETIPI entende que é essencial a implantação de uma gestão de terceiros efetiva, através de processos e controles rigorosos para garantir que seus fornecedores estejam seguindo a legislação e protegendo os direitos e a privacidade dos titulares de dados pessoais envolvidos em cada contratação.

Diante disso, solicitamos que, no prazo máximo de 5 (cinco) dias corridos, a contar do recebimento deste comunicado, seja informado pela sua organização o nome e o e-mail do Encarregado de Proteção de Dados (DPO) - caso se aplique -, ou outro profissional apto a responder o questionário que será enviado por meio da Plataforma LGPDNOW, para que sejam verificados os aspectos relativos à Privacidade e Proteção de Dados Pessoais e Segurança da Informação.

Ressaltamos que é necessário que sejam anexados ao questionário as respectivas evidências / documentos relacionados. Caso não seja possível em alguma das perguntas, sugerimos que uma justificativa seja apresentada fundamentando a impossibilidade.

O preenchimento do questionário é obrigatório e deverá ser concluído em até 15 (quinze) dias úteis após o seu envio.

O engajamento de sua organização é fundamental para assegurar a conformidade com as exigências legais e garantir a continuidade de um trabalho conjunto pautado na responsabilidade e no compromisso com a proteção dos dados pessoais.

Permanecemos à disposição para esclarecimentos ou suporte necessário durante este processo.

Cordialmente,

*(assinatura da pessoa responsável pela Comunicação)*

**ANEXO III - MANUAL DE PROCEDIMENTOS OPERACIONAIS – GESTÃO DE FORNECEDORES EM PRIVACIDADE E PROTEÇÃO DE DADOS**

# MANUAL DE PROCEDIMENTOS OPERACIONAIS – GESTÃO DE FORNECEDORES EM PRIVACIDADE E PROTEÇÃO DE DADOS

## 1. OBJETIVO

Estabelecer os procedimentos operacionais para implementação da Política de Gestão de Fornecedores da ETIPI, com foco em privacidade e proteção de dados pessoais, garantindo a conformidade com a LGPD e com as diretrizes da organização.

## 2. ATORES ENVOLVIDOS

Segue abaixo o rol das pessoas/áreas envolvidas:

- Área Demandante;
- Área de Compliance (ou o Encarregado, juntamente com outra área responsável pela Privacidade da organização);
- Área Jurídica;
- Fornecedor; e
- Comissão de Licitação (quando aplicável).

## 3. PROCEDIMENTOS OPERACIONAIS

### 3.1. Etapa 1: Verificação

- A área demandante verifica se o contrato envolverá tratamento de dados pessoais. Em caso afirmativo:
  - Preenche o **Anexo I** com as informações solicitadas; e
  - Encaminha à área de Compliance (ou o Encarregado, juntamente com outra área responsável pela Privacidade da organização) antes da instrução do processo de contratação/licitação.

- A área de Compliance (ou o Encarregado, juntamente com outra área responsável pela Privacidade da organização):
  - Emite o **Comunicado de Avaliação de Terceiros** ao fornecedor;
  - Cadastra o fornecedor na plataforma LGPDNOW; e
  - Envia o questionário.

- O fornecedor:
  - Informa o responsável, sendo este o Encarregado pelo tratamento dos dados pessoais da organização ou alguém apto para realizar tal preenchimento, em até cinco dias corridos do recebimento do comunicado; e
  - Responde ao questionário em até 15 (quinze) dias úteis, anexando evidências documentais ou justificando, em caso de ausência da documentação em questão.

### 3.2. Etapa 2: Avaliação

- A área de Compliance (ou o Encarregado, juntamente com outra área responsável pela Privacidade da organização):
    - Avalia o questionário e documentos;
    - Classifica o fornecedor nos níveis A à E, conforme disposto na Política de Gestão de Fornecedores/Terceiros em conformidade com a LGPD; e
    - Emite parecer e envia à área demandante e à comissão de licitação (se houver).

### 3.3. Etapa 3: Validação

- A área jurídica:
    - Inclui as cláusulas obrigatórias de proteção de dados pessoais; e
    - Solicita a inclusão dos aditivos ou planos de mitigação conforme o risco (C ou D) disposto na Política de Gestão de Fornecedores/Terceiros em conformidade com a LGPD (lembrando que fornecedores Nível E ou com risco não mitigado não são contratados, salvo exceção justificada pela diretoria).

- A contratação só é formalizada com parecer favorável da Compliance (ou o Encarregado, juntamente com outra área responsável pela Privacidade da organização); e
- As cláusulas de proteção de dados pessoais são incorporadas ao contrato, devidamente assinado e publicizado.

### 3.4. Etapa 4: Monitoramento

- Todos os fornecedores serão monitorados pela área de Compliance (ou pelo Encarregado, juntamente com outra área responsável pela Privacidade da organização):
    - Reaplicação do questionário LGPDNOW;
    - Auditorias e revisões contratuais periódicas; e
    - Acompanhamento de planos de mitigação e obrigações contratuais.

## 4. REVISÃO E APERFEIÇOAMENTO

Este Manual será atualizado pela área de Compliance (ou o Encarregado, juntamente com outra área responsável pela Privacidade da organização) sempre que houver revisão da Política ou alterações legais relevantes.