

POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Política de Privacidade e Proteção de Dados Pessoais	Versão: 1.0
Autor: Compliance	Data: 05/06/2025
Revisor: Jurídico	

1. INTRODUÇÃO

Este normativo é elaborado em conformidade com as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD), demais regulamentações aplicáveis e normas técnicas relacionadas.

O presente normativo se aplica a quaisquer operações de tratamento de dados pessoais realizadas pela **INTER RISK**, englobando seus colaboradores, parceiros e prestadores de serviço.

Havendo conflito entre as disposições deste normativo e a legislação de proteção de dados aplicável, esta última prevalecerá.

2. OBJETIVOS

A Política de Privacidade e Proteção de Dados Pessoais tem como objetivo apresentar regras aplicáveis para o tratamento de dados pessoais, em atenção às disposições da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/2018), com definições para o desenvolvimento de um Programa de Governança em Privacidade que garanta a conformidade com a referida legislação e regulamentações aplicáveis.

O presente normativo, tem, ainda, como objetivo a formalização do comprometimento da **INTER RISK** na adoção de processos e normas que assegurem a proteção dos dados pessoais, estabelecendo relação de confiança com os titulares, por meio de atuação transparente. A **INTER RISK**, compreende que garantir o tratamento de dados pessoais, de forma legítima, correta e adequada à LGPD, é fundamental para o sucesso de suas atividades e para resguardar sua imagem e credibilidade perante colaboradores, prestadores de serviço, clientes, parceiros, terceiros e a Autoridade Nacional de Proteção de Dados (ANPD).

Dessa forma, é imprescindível que os colaboradores, prestadores de serviço, parceiros e terceiros que realizem o tratamento de dados pessoais tenham ciência sobre as regras relacionadas para que executem suas atividades em *compliance* com a legislação.

3. DEFINIÇÕES

- **Alta Administração**: corpo dos dirigentes máximos da organização;
- **Anonimização**: Processo por meio do qual o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, considerados os meios técnicos razoáveis e disponíveis no momento do tratamento;
- **Agentes de Tratamento**: Controlador e Operador. Responsáveis pelo tratamento dos dados pessoais.
- **ANPD**: Autoridade Nacional de Proteção de Dados.
- **Banco de dados**: conjunto de dados pessoais que pode ser em formato eletrônico ou físico;
- **Consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para a finalidade informada;
- **Controlador**: pessoa natural ou jurídica a quem competem as decisões sobre tratamento de dados pessoais;
- **Controladoria Conjunta**: a controladoria conjunta ocorre quando há uma participação conjunta na determinação de finalidades e meios de tratamento, a finalidade do tratamento pode ocorrer a partir de decisões comuns (intenção comum, com decisões em conjunto) ou convergentes (decisões distintas que se complementam);
- **Dados pessoais**: são aqueles que permitem identificar uma pessoa, ou torná-la identificável;
- **Dados pessoas sensíveis**: são aqueles 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;
- **Encarregado**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- **Operador**: pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador;
- **Relatório de impacto à proteção de dados pessoais**: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
- **Titular dos dados**: pessoa natural a quem se referem os dados pessoais objeto de tratamento;

- **Tratamento**: 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;
- **Suboperador**: Contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador.

4. PRINCÍPIOS

A aplicação do presente normativo deverá observar fundamentalmente a boa-fé e os Princípios Gerais de Proteção definidos na LGPD.

a) **Finalidade**: O tratamento dos dados pessoais deverá contar com finalidade legítima e específica, com amparo em uma das hipóteses legais previstas na LGPD. Os propósitos deverão ser explícitos e informados ao titular.

b) **Adequação**: O tratamento deverá ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

c) **Necessidade**: Apenas poderão ser tratados dados necessários para a realização das finalidades, buscando alternativas com menor potencial invasivo ao titular e restrições de acesso.

d) **Livre acesso**: Deverá ser garantido, aos titulares, consulta facilitada e gratuita sobre o tratamento dos seus dados pessoais, sendo de responsabilidade do parceiro providenciar os auxílios necessários para que as informações sejam prestadas de forma clara e completa ao titular, caso a **INTER RISK** figure como controladora dos dados pessoais relacionados.

e) **Qualidade dos dados**: Os dados deverão ser exatos, relevantes e atualizados, com disponibilização de método facilitado para eventual atualização cadastral dos titulares.

f) **Transparência**: O tratamento dos dados pessoais deve ser realizado de forma transparente, garantido informações claras, precisas e facilmente acessíveis aos titulares, por meio de Política de Privacidade, Avisos de Privacidade, Cláusulas Contratuais, Termos e demais documentações que assegurem a devida transparência;

g) **Segurança**: Deverão ser adotadas medidas técnicas e administrativas aptas a protegerem os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

h) **Prevenção**: Deverão ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

i) **Não discriminação**: A realização do tratamento para fins discriminatórios ilícitos ou abusivos é absolutamente vedada.

j) **Responsabilização e prestação de contas**: Deverão ser adotas medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas.

5. PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

A **INTER RISK**, para garantir a segurança dos dados pessoais que trata, de forma preventiva, atua em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e regulamentações aplicáveis, estabelecendo Programa de Governança em Privacidade como guia da instituição nas ações que envolvam o tratamento de dados pessoais, com observância dos seguintes critérios.

a) demonstração do comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
b) aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) implementação de políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
f) integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) implementação de planos de resposta a incidentes e remediação; e
h) atualização constante com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

A adoção de medidas eficazes e capazes de demonstrar a observância e o efetivo cumprimento das normas de proteção de dados pessoais deverão, no mínimo:

a) Abranger todo e qualquer dado pessoal tratado;
b) Dispor sobre ações, medidas técnicas e administrativas que:
  (I) previnam a ocorrência de danos decorrentes de situações acidentais ou ilícitas no tratamento dos dados pessoais; e
  (II) protejam os dados pessoais desde a concepção do produto ou serviço até a sua execução;
c) Estabelecer plano de resposta a incidentes de segurança e remediação;
d) Adotar, manter e divulgar políticas que assegurem o cumprimento de normas e boas práticas relativas à Proteção de Dados Pessoais, inclusive Política de Segurança da Informação, de Privacidade e/ou de Proteção de Dados Pessoais;
e) Prever e implementar fluxo de atendimento aos direitos dos titulares de dados pessoais previstos na LGPD;
f) Contemplar a realização de ações educativas.

A **INTER RISK** adota Normativos Internos específicos definindo os procedimentos para o tratamento adequado e a proteção de dados dos colaboradores e seus dependentes, prestadores de serviço,

clientes, terceiros e parceiros pessoas físicas, estando em conformidade com a legislação aplicável ao tema em território nacional, especificamente com a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018 (“LGPD”). As Políticas e Manuais são mantidas na Intranet.

6. AGENTES DE TRATAMENTO E ENCARREGADO (DPO)

A **INTER RISK**, no âmbito da sua atuação, atuará como controladora e/ou operadora de dados pessoais, conforme atribuições específicas em cada caso de tratamento dos dados pessoais.

A **INTER RISK**, ainda, poderá atuar em controladoria conjunta ou como suboperador dos dados pessoais.

A identificação da instituição quanto ao posicionamento relacionado aos agentes de tratamento poderá decorrer de obrigações estabelecidas em contrato ou instrumentos legais. No entanto, a efetiva atividade prestada poderá se distanciar das condições formalmente previstas. Dessa forma, a definição deverá observar as ações concretas da organização em determinada situação.

Não são considerados agentes de tratamento os indivíduos subordinados à instituição, como funcionários, servidores ou equipes de trabalho, já que atuam sob o poder diretivo do efetivo agente de tratamento.

A **INTER RISK**, para adequação à LGPD e visando garantir a nomeação de um profissional para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), mantém a contratação de um Encarregado pelo Tratamento dos Dados Pessoais (*Data Protection Officer* – DPO). Para contato com o Encarregado **INTER RISK** garante um canal de comunicação específico.

A identidade e informações de contato do Encarregado estão divulgadas publicamente, de forma clara e objetiva, no sítio eletrônico da **INTER RISK**.

- Identificação Encarregado: Russell Bedford Brasil
- Canal de Comunicação: encarregado_dpo.intercorretora@russellbedford.com.br

7. REQUISITOS PARA O TRATAMENTO DOS DADOS PESSOAIS

i. Dados Pessoais

O tratamento de dados pessoais somente ocorrerá caso a finalidade do tratamento seja correspondente a alguma das hipóteses legais previstas na LGPD, conforme itens detalhados a seguir.

a. Mediante consentimento;
b. Para cumprimento de obrigação legal ou regulatória;
c. Pela Administração pública quando necessário à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

d. Para realização de estudos por órgão de pesquisa;
e. Para execução de contrato ou procedimentos relacionados ao contrato;
f. Para exercício regular de direitos em processo judicial, administrativo ou arbitral;
g. Para proteção da vida ou da incolumidade física do titular ou de terceiros;
h. Para tutela da saúde exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
i. Para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
j. Para proteção do crédito.

ii. Dados Pessoais Sensíveis

O tratamento de dados pessoais sensíveis somente ocorrerá caso aplicável nas hipóteses legais previstas na LGPD e apresentadas a seguir.

a. Mediante consentimento;
b. Para cumprimento de obrigação legal;
c. Pela administração pública, para tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis;
d. Para realização estudos por órgão de pesquisa;
e. Para exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
f. Para proteção da vida ou da incolumidade física do titular ou de terceiros;
g. Para tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
h. Para garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos previstos na Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

iii. Dados de Crianças e Adolescentes

O tratamento de dados pessoais de crianças e adolescentes deverá ser realizado em seu melhor interesse e poderá ser realizado com base nas hipóteses legais previstas na Lei Geral de Proteção de Dados Pessoais (LGPD) e descritas nos tópicos anteriores, desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto.

Caso aplicável, o tratamento dos dados pessoais de crianças deverá ser realizado com consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, ressalvado os casos em que seja necessário para contatar os pais ou o responsável legal, utilizando uma única vez e sem armazenamento ou para sua proteção. Em nenhum dos casos poderão ser repassados a terceiro sem o consentimento.

iv. Condições para aplicação das hipóteses legais

a. Consentimento

O consentimento é uma das hipóteses legais que permite o tratamento de dados pessoais e dados pessoais sensíveis.

Caso o tratamento de dados pessoais tiver fundamento em outra hipótese, como cumprimento de obrigação legal, não caberá a utilização do consentimento. Dessa forma, para aplicação desta hipótese legal, o Encarregado pelo Tratamento dos Dados Pessoais (DPO) poderá ser consultado para confirmar a aplicabilidade do consentimento e revisar a sua forma de coleta – se aplicável, que deverá observar os requisitos a seguir indicados.

- **Manifestação livre**: o titular deve fornecer o consentimento de maneira livre.
- **Manifestação granular**: o titular deve fornecer a autorização (consentimento) para que o tratamento em situações específicas e determinadas.
- **Manifestação informada**: o titular deve ter acesso ao aviso de privacidade correspondente à atividade na qual foi submetido, antes do fornecimento de sua autorização, garantindo a plena ciência da finalidade e dos limites da atividade de tratamento realizada.
- **Manifestação inequívoca**: o titular deve fornecer os seus dados pessoais sem qualquer dúvida ou questionamento quanto aos limites da atividade.

O consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Dessa forma, para garantir a coleta do consentimento de forma adequada, a **INTER RISK**, providenciará documentação que demonstre o consentimento do titular, observando os requisitos mínimos, além de garantir o armazenamento das evidências e a efetiva gestão da autorização concedida.

O consentimento deverá referir-se a finalidades determinadas. Autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas.

O consentimento poderá ser revogado a qualquer momento pelo titular, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

b. Legítimo Interesse

O Legítimo Interesse é uma das hipóteses legais de dispensa de consentimento que permite o tratamento de dados pessoais. Ressalta-se que, para o tratamento de dados pessoais sensíveis, a hipótese do legítimo interesse não será aplicável.

Para o tratamento de dados pessoais com base na hipótese legal do legítimo interesse, recomenda-se que o Controlador providencie a elaboração do Relatório de Impacto à Proteção dos Dados Pessoais (RIPD).

Além disso, considerando as boas práticas, recomenda-se, ainda, que seja realizado um teste de ponderação (*Legitimate Interests Assessment* – LIA) para demonstração da proporcionalidade entre

os interesses do Controlador ou terceiros e os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

A **INTER RISK** deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

Identificada a existência de tratamento de dados pessoais com base na hipótese do Legítimo Interesse, o Encarregado pelo Tratamento dos Dados Pessoais (DPO) deverá ser consultado para confirmar a adequação do procedimento e auxiliar na estruturação dos documentos necessários, que serão produzidos pela área técnica competente, revisados pelo Encarregado e formalmente validados pela alta administração.

Outras operações de tratamento, ainda que não sejam realizadas com base na hipótese do legítimo interesse, poderão ensejar na necessidade de estruturação do Relatório de Impacto à Proteção dos Dados Pessoais (RIPD), considerando a criticidade das informações e riscos existentes no tratamento dos dados pessoais. Para esse procedimento, a **INTER RISK** realizará as análises necessárias, considerando as condições supramencionadas relacionadas ao documento.

8. DIREITOS DOS TITULARES

Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, intimidade, privacidade e proteção dos dados pessoais.

A **INTER RISK** garante o devido atendimento, de forma facilitada e gratuita, dos direitos dos titulares, possibilitando solicitações baseadas nos seguintes direitos:

- **a.** Confirmação da existência de tratamento.
- **b.** Acesso aos dados.
  Simples: Extrato simplificado dos dados pessoais;
  Completa: Dados pessoais envolvidos, informação sobre a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial.
- **c.** Correção de dados incompletos, inexatos ou desatualizados.
- **d.** Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade.
- **e.** Portabilidade de seus dados a outro fornecedor de serviço ou produto.
- **f.** Revogação do Consentimento, caso o tratamento dos seus dados pessoais seja realizado com base na coleta de seu consentimento.
- **g.** Eliminação dos dados tratados com consentimento do Titular.
- **h.** Obtenção de informações sobre as entidades públicas ou privadas com as quais a **INTER RISK** compartilhou seus dados.
- **i.** Informação sobre a possibilidade de não fornecer o seu consentimento, bem como de ser informado sobre as consequências, em caso de negativa.

j. Revisão de decisão automatizada.

Os direitos dos titulares deverão ser exercidos por meio do Canal de Comunicação com o Encarregado (DPO).

Para o respectivo atendimento, o titular de dados deverá observar os procedimentos que garantam a autenticação da sua identidade.

Caso os colaboradores ou prestadores de serviço identifiquem o recebimento de solicitações relacionadas aos direitos dos titulares, previstos na LGPD, deverão redirecionar o requerimento, imediatamente, ao canal do Encarregado para providências cabíveis.

9. RELACIONAMENTO COM TERCEIROS

A **INTER RISK** dispõe de política de Gestão de Terceiros, na qual se encontram os procedimentos de proteção à dados pessoais e sensíveis a serem adotados na contratação de parceiros, fornecedores e demais terceiros.

10. ACULTURAMENTO

A **INTER RISK** atuará na disseminação da cultura de proteção de dados pessoais e segurança cibernética, incluindo a conscientização de Gerentes, Diretores, Supervisores, Colaboradores, Prestadores de Serviço e, nos casos aplicáveis, de clientes e terceiros.

A participação dos agentes internos, que realizem tratamento dos dados pessoais, nos treinamentos e atividades de conscientização será considerada obrigatória, visando garantir que o Programa de Governança em Privacidade seja desenvolvido adequadamente. Eventuais impossibilidades de comparecimento ou desenvolvimento das ações de aculturamento deverão ser devidamente justificadas. Setores e funções estratégicos para proteção dos dados pessoais poderão exigir capacitações específicas e especializadas.

Ainda, considerando condições relacionadas a responsabilização das instituições bancárias por fraudes, recomenda-se que haja constante disponibilização de informações auxiliando os clientes a protegerem suas informações e detalhando os procedimentos relacionados a fraudes, tentativas de golpes e outras condições que permeiam a realidade da instituição.

11. CICLO DE VIDA DO DADO PESSOAL

11.1. Condições Gerais

Os colaboradores e prestadores de serviço devem ter conhecimento sobre o ciclo de vida dos dados que são tratados, assim como as medidas de segurança aplicáveis.

A proteção dos dados pessoais, incluindo a definição de hipótese legal para o tratamento, deverá ser observada durante todo o ciclo de vida dos dados.

A **INTER RISK** manterá registro das operações de tratamento de dados pessoais, nos termos da legislação vigente.

11.2. Coleta

Apenas são coletadas informações pessoais necessárias para as específicas finalidades definidas, em observância aos princípios da necessidade e da finalidade.

11.3. Armazenamento

Os dados pessoais armazenados pela **INTER RISK** são mantidos em ambiente seguro, com adoção de medidas para garantir a segurança e proteção das informações, evitando perdas e roubos, bem como acesso, divulgação, cópia, uso ou modificação não autorizados. As informações são acessadas internamente apenas por profissionais devidamente autorizados, respeitando o princípio da proporcionalidade, necessidade e adequação aos objetivos para os quais foram coletados, assegurando o compromisso de confidencialidade e preservação de privacidade.

11.4. Compartilhamento

A **INTER RISK** somente compartilhará as suas informações pessoais em casos específicos, para o cumprimento de finalidades legítimas e informadas ao titular.

Caso haja dúvidas quanto a possibilidade de realizarem compartilhamentos de dados com terceiros, o Encarregado pelo Tratamento dos Dados Pessoais (DPO) deverá ser consultado, assim como departamentos pertinentes, como jurídico.

11.5. Eliminação

Os dados pessoais devem ser eliminados após o término do seu tratamento, observando as peculiaridades de cada caso, sendo autorizada a conservação das informações para fins de cumprimento de obrigação legal ou regulatória.

12. RESPONSABILIDADES

Para que o presente normativo produza os efeitos pretendidos, todos os envolvidos no tratamento dos dados pessoais deverão observar as previsões deste documento.

Para a garantia do cumprimento das normas de privacidade e proteção de dados pessoais, as definições a seguir devem ser devidamente observadas, sem prejuízo dos demais itens desta norma.

- A alta administração deverá guiar o estabelecimento na cultura de proteção de dados pessoais, analisando e priorizando as ações consideradas urgentes.
- A alta administração deverá estar envolvida nas decisões relacionadas ao tratamento dos dados pessoais, demonstrando seu apoio às políticas, procedimentos e controles, com participação ativa nas atividades direcionadas ao aculturamento da organização em privacidade, segurança e proteção dos dados pessoais.
- A alta administração deverá disponibilizar recursos suficientes para aplicação de medidas de segurança, investindo de forma adequada em recursos para segurança das informações e resiliência cibernética.
- A alta administração deverá realizar o acompanhamento contínuo da efetividade do programa de governança em privacidade.
- A alta administração deverá realizar a análise e validação dos normativos internos relacionados à proteção de dados pessoais.
- A alta administração deverá realizar a análise e validação dos documentos relacionados à proteção de dados pessoais, como Relatório de Impacto (RIPD), comunicações de incidentes de segurança com dados pessoais à ANPD e titulares, atendimento de requisições da ANPD ou demais órgãos ou entidades de fiscalização.
- Todos os integrantes da **INTER RISK** e eventuais operadores de dados pessoais tem a obrigação de comunicar a ocorrência de incidentes de segurança com dados pessoais, conforme procedimento definido na Política de Incidentes de Segurança com Dados Pessoais da instituição.
- Todos os integrantes da **INTER RISK** têm a obrigação de comunicar eventual tratamento de dados pessoais em desacordo com as regras previstas nos normativos internos da Inter Risk Services relacionados ao tratamento de dados pessoais.
- Todos os integrantes da **INTER RISK** devem garantir a integridade, disponibilidade e confidencialidade dos dados pessoais tratados no exercício de sua função;
- Todos os integrantes da **INTER RISK** devem utilizar apenas informações necessárias para o cumprimento das finalidades pretendidas e para o regular o exercício de suas funções;
- Os dados pessoais devem ser manipulados apenas por pessoas autorizadas, reduzindo, assim, os riscos de falhas humanas propiciarem um vazamento ou uso inadequado da informação;
- O acesso de cada empregado ou prestador de serviço ao banco de dados da **INTER RISK** é individual e protegido por senha própria e intransferível, garantindo o tratamento setorizado dos dados a pessoas autorizadas;
- O tratamento dos dados pessoais deverá, necessariamente, observar as finalidades inicialmente propostas, sendo vedado o uso das informações para fim incompatível,

excessivo ou para finalidades diversas, sem que haja a expressa autorização da **INTER RISK**;

- Os dados pessoais tratados deverão necessariamente ser armazenados em local seguro e oficialmente aprovados pela **INTER RISK**;
- Os dados pessoais tratados, como regra, não poderão ser enviados para endereços de e-mail pessoal ou dispositivos remotos, assegurando o pleno controle das informações pela **INTER RISK**.

Todos os integrantes da **INTER RISK** terão à disposição o atendimento do Encarregado (DPO) da empresa para realizarem eventual consulta necessária relacionada ao tratamento dos dados pessoais.

13. SANÇÕES

O descumprimento deste regulamento e/ou demais instrumentos normativos complementares ao processo de segurança da informação constitui falta grave, passível de penalidades administrativas e contratuais.

14. VIGÊNCIA

O presente normativo passa a vigorar a partir da data de sua aprovação, sendo válido por tempo indeterminado.

Após a aprovação, para que o normativo continue satisfatório, serão implantados controles de melhoria contínua, com revisão periódica, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

15. DISPOSIÇÕES FINAIS

Eventual omissão, nesta norma, de definições ou orientações relacionadas, deverá ser esclarecida pelo interessado, providenciando o envio de consulta formal ao Encarregado pelo Tratamento dos Dados Pessoais (DPO).