SUMÁRIO

POLÍTICA DE PRIVACIDADE

Proteção de Dados Pessoais – LGPD.

1. Apresentação

A Política de Privacidade e Proteção de Dados Pessoais estabelece os princípios, diretrizes e responsabilidades que orientam o tratamento de dados pessoais realizado pela empresa, em conformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018).

1.1 Objetivo da Política

Este documento reforça o compromisso da organização com a privacidade, a segurança da informação e a transparência no relacionamento com colaboradores, clientes, fornecedores, parceiros e demais titulares de dados. Seu propósito é garantir que toda coleta, uso, armazenamento, compartilhamento e eliminação de dados pessoais sejam realizados de forma ética, responsável e alinhada aos requisitos legais e às melhores práticas de governança.

1.2 Abrangência

Esta política aplica-se a todos os departamentos da Empresa, colaboradores, terceiros, fornecedores, prestadores de serviço, parceiros de negócio e quaisquer agentes de tratamento que realizem operações envolvendo dados pessoais em nome da organização.

1.3 Vigência

A política entra em vigor na data de sua publicação, com vigência por prazo indeterminado e revisão a cada 12 meses ou conforme necessidade.

1.4 Área técnica responsável

A área responsável por este documento é o escritório de Governança – Gestão: Governança Corporativa, Gestão, Riscos e Conformidade (GRC), juntamente com o Encarregado de Dados (DPO).

2. Conceitos e Definições

Para fins desta Política, serão considerados para a Política de Privacidade e Proteção de Dados Pessoais.

- **ANPD:** Autoridade Nacional de Proteção de Dados.
- **Controlador:** Quem toma decisões sobre o tratamento de dados.
- **Dados Pessoais:** Informação relacionada à pessoa natural identificada ou identificável.
- **Dados Sensíveis:** Origem racial/étnica, saúde, biometria, religião, vida sexual, entre outros.
- **DPO (Encarregado):** Profissional responsável pela comunicação entre a empresa, titulares e ANPD.
- **Operador:** Quem realiza o tratamento em nome do controlador.
- **Titular:** Pessoa natural a quem se referem os dados pessoais.
- **Tratamento:** Operação realizada com dados pessoais (coleta, uso, armazenamento, descarte etc.).

3. Referencial

- **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (Marco Civil da Internet). DOU, Brasília, DF, 24 abr. 2014. BRASIL.
- **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. (Lei Geral de Proteção de Dados Pessoais- LGPD). DOU, Brasília, DF, 15 ago. 2018. BRASIL.
- **Lei nº 13.853, de 14 de agosto de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a criação e as competências da Autoridade Nacional de Proteção de Dados (ANPD). Diário Oficial da União, Brasília, DF, 15 ago. 2019. BRASIL.
- **ANPD (Autoridade Nacional de Proteção de Dados)**. Consultar as principais resoluções e regulamentos emitidos pela ANPD, como o Regulamento de Dosimetria e Aplicação de Sanções Administrativas e as normas para agentes de tratamento de pequeno porte. Disponível em: [Endereço do Site da ANPD]. Acesso em: [Data do Acesso].
- **Marco Civil da Internet- Lei nº 12.965/2014**. Propósito: estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil (neutralidade, privacidade, liberdade de expressão).
- **Política de Segurança e Acesso da Informação**

4. DIRETRIZES

4.1. Gerais

4.1.1 Garantir que todo tratamento de dados pessoais esteja alinhado aos princípios da LGPD:
Inclui finalidade, adequação, necessidade, transparência e segurança. Base Legal e Privacy by Design: Garantir que todo tratamento de dados pessoais esteja fundamentado em uma base legal válida (Art. 7º e 11 da LGPD) e alinhado aos princípios. Adotar o conceito de Privacy by Design e Privacy by Default para incorporar a proteção de dados desde a concepção de novos produtos, serviços e processos.

4.1.2 Adotar controles de segurança física, lógica e organizacional compatíveis com os riscos:
Controles de Segurança e Gestão de Riscos: Implementar e manter um conjunto robusto de controles de segurança física, lógica e organizacional, compatível com o nível de risco e com as diretrizes da Política de Segurança da Informação (referencial citado).

4.1.3 Registrar e manter inventário dos tratamentos realizados (Data Mapping):
Mapeamento e Registro das Operações de Tratamento (ROPA)/Matriz de Riscos: Manter o inventário completo e atualizado de todas as operações de tratamento de dados pessoais (*Data Mapping*), gerando o Registro das Operações de Tratamento de Dados Pessoais (ROPA), conforme exigido pela LGPD (Art. 37).

4.1.4 Assegurar o atendimento eficiente aos direitos dos titulares:

Canal de Atendimento ao Titular e Data Subject Access Request (DSAR): Estabelecer um Canal de Comunicação (e-mail, portal) dedicado e procedimentos internos ágeis para atender de forma eficiente e transparente a todas as Solicitações de Acesso do Titular (DSAR), garantindo o exercício pleno dos direitos previstos na LGPD.

Encarregado pelo Tratamento de Dados Pessoais (DPO):

O Encarregado de Dados é o responsável por atuar como canal de comunicação entre a INACE IATES LTDA, os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD), conforme disposto no art. 41 da Lei nº 13.709/2018 (LGPD).

O contato com o DPO pode ser realizado por meio do e-mail: lgpd_dpo@inace.com.br

4.2. Governança e Gestão da Privacidade.

4.2.1 Programa de Privacidade:

A empresa implementa um programa contínuo estruturado em um Programa de Governança em Privacidade (PGP): A empresa deve implementar um Programa de Governança em Privacidade (PGP) contínuo e cíclico (*PDCA - Plan-Do-Check-Act*), estruturado nos seguintes pilares:

- **Avaliação e Gerenciamento de Riscos de Privacidade**: Realizar Relatórios de Impacto à Proteção de Dados Pessoais (RIPD/DPIA) em processos de alto risco e executar análises de Gap Assessment periódicas para identificação e mitigação de vulnerabilidades;
- **Documentação e Compliance Normativo**: Revisar e atualizar anualmente (ou conforme eventos críticos) as Políticas de Privacidade, Termos de Uso e demais Normas e Procedimentos Internos, assegurando o compliance com a LGPD e as regulamentações da ANPD;
- **Auditoria e Monitoramento Contínuo:** Estabelecer um ciclo de auditorias internas e externas para verificar a efetividade dos controles de privacidade, garantindo a melhoria contínua do PGP;
- **Estrutura de Governança:** Formalizar o Comitê de Privacidade e Segurança da Informação, que deve incluir o Encarregado de Dados (DPO), para supervisionar a execução do PGP e tomar decisões estratégicas.

4.3. Segurança da Informação Aplicada à LGPD

4.3.1 Controles Técnicos e Cibersegurança: Implementar medidas técnicas e tecnológicas robustas:

- **Controle de acesso baseado no menor privilégio:** Princípio do Mínimo Privilégio (Least Privilege): Garantir que o acesso aos dados pessoais seja estritamente limitado ao necessário para o desempenho da atividade (need-to-know), com revisões de acesso periódicas;
- **Criptografia de dados sensíveis:** Anonimização e Pseudonimização: Adotar a criptografia, pseudonimização e/ou anonimização dos dados pessoais, especialmente os dados sensíveis, tanto em trânsito quanto em repouso (data at rest);

- **Backup seguro:** Gestão de Continuidade e Backup, manter uma política de backup segura e testada, alinhada a um Plano de Recuperação de Desastres (DRP), visando a disponibilidade e resiliência dos dados;
- **Uso obrigatório de senhas fortes e MFA:** Autenticação Reforçada: Implementar o uso obrigatório de Autenticação de Múltiplos Fatores (MFA) e políticas de senhas complexas para acesso a sistemas críticos;
- **Sistemas críticos devem adotar logs e monitoramento contínuo:** Registro de Auditoria (Logging) e Monitoramento: Manter registros de auditoria (logs) detalhados e realizar monitoramento contínuo (SIEM) em sistemas críticos e ambientes de tratamento de dados pessoais.
- **A área de TI deve assegurar atualização de patches e antivírus corporativo:** Gestão de Vulnerabilidades e Patch Management. A área de TI deve implementar um processo formal de Gestão de Patches e Vulnerabilidades e assegurar a utilização e atualização contínua de soluções de proteção (antimalware, endpoint protection).

4.3.2 Controles Administrativos:

- **Mapeamento de riscos de privacidade:** Treinamento e Conscientização: Realizar treinamentos obrigatórios e periódicos para todos os colaboradores sobre a LGPD, políticas internas, classificação de dados e procedimentos de segurança;
- **Termos de confidencialidade obrigatórios**: Cláusulas Contratuais de Compliance: Assegurar a inclusão de cláusulas específicas sobre LGPD e confidencialidade em contratos com colaboradores, fornecedores e operadores de dados (incluindo o termo de confidencialidade/NDA);
- **Plano de Resposta a Incidentes (PRI):** Procedimentos de resposta a incidentes de segurança, para manter e testar um Plano de Resposta a Incidentes de Segurança (PRI) com fluxos claros de comunicação, remediação e o procedimento de Comunicação de Incidente de Segurança à ANPD e aos Titulares (conforme Resoluções da ANPD).

5. DIVULGAÇÃO E DISSEMINAÇÃO

Com o compromisso de fortalecer nossa cultura de privacidade e garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD), comunicamos que a Política de Privacidade e Proteção de Dados Pessoais da empresa está oficialmente publicada e disponível para todos os colaboradores, como também reforçada nos treinamentos institucionais.

Este documento estabelece princípios, responsabilidades e diretrizes essenciais para o tratamento adequado de dados pessoais em todas as atividades corporativas. Sua leitura é obrigatória e fundamental para assegurar a proteção das informações que manejamos diariamente.

Reforçamos a importância de que todos conheçam, compreendam e apliquem as orientações da Política, contribuindo para um ambiente mais seguro, ético e alinhado às melhores práticas de governança e conformidade.

6. CONSEQUÊNCIAS

A aderência rigorosa a esta Política de Proteção de Dados Pessoais e seus instrumentos normativos complementares é obrigatória para todos os colaboradores, prestadores de serviço e terceiros que, porventura, acessem ou tratem dados pessoais sob a responsabilidade desta instituição. As violações apuradas por meio de processo administrativo disciplinar ou sindicância, em conformidade com a legislação aplicável, poderão resultar na aplicação de sanções disciplinares severas, que variam conforme a natureza, gravidade e reincidência da infração.

7. RESPONSABILIDADES

7.1. Departamento de Governança, Riscos e Conformidade / DPO - Encarregado de Dados (DPO/DGO) e Escritório de Privacidade:

- **Governança e Compliance:** Manter esta Política e seus documentos acessórios atualizados (versão, ata e aprovação) e garantir a conformidade normativa e legal com a LGPD e regulada pela ANPD;
- **Gerenciamento de Riscos de Privacidade:** Coordenar e supervisionar a realização dos Relatórios de Impacto à Proteção de Dados (RIPD/DPIA) para tratamentos de alto risco e realizar auditorias periódicas de privacidade.
- **Orientação e Treinamento:** Atuar como canal de comunicação e orientação para as áreas da organização sobre as obrigações legais, princípios da LGPD e as melhores práticas de tratamento de dados.
- **Comunicação Institucional:** Atuar como o ponto de contato oficial para comunicações, requisições e incidentes junto à Autoridade Nacional de Proteção de Dados (ANPD).
- **Gestão de Direitos dos Titulares (DSAR):** Gerenciar o fluxo e garantir o atendimento eficiente às solicitações de exercício dos direitos dos titulares de dados (Data Subject Access Request – DSAR). O Departamento de Governança, Riscos e Conformidade, por meio do Encarregado de Dados (DPO), atua como ponto de contato oficial junto aos titulares de dados e à Autoridade Nacional de Proteção de Dados (ANPD), podendo ser acionado pelo e-mail: lgpd_dpo@inace.com.br

7.2. Comitê de Governança de Privacidade e Segurança da Informação:

- **Decisão e Risk Acceptance:** Analisar, deliberar e aprovar a estratégia de resposta e notificação a incidentes de segurança, decidindo sobre a aceitação de riscos (quando aplicável) e a necessidade de comunicação à ANPD.
- **Direcionamento Estratégico**: Apoiar a alta gestão na tomada de decisões estratégicas relativas à proteção de dados e segurança, garantindo que o Programa de Privacidade esteja alinhado aos objetivos organizacionais.

- **Melhoria Contínua:** Aprovar os Planos de Ação Corretiva e Preventiva resultantes de auditorias, RIPDs ou incidentes, monitorando sua implementação para a melhoria contínua da conformidade.

7.3 Tecnologia da Informação (TI) e Segurança da Informação:

- **Controles Técnicos**: Implementar, manter e documentar os controles técnicos e de segurança (como criptografia, firewalls e MFA) para proteger os dados pessoais, conforme a Política de Segurança e Acesso da Informação.
- **Infraestrutura Segura:** Gerenciar a infraestrutura de TI, garantindo o ciclo de gestão de patches e a manutenção atualizada das soluções de proteção (antivirus, EDR).
- Resposta a Incidentes Técnicos: Atuar na contenção, erradicação e recuperação em caso de incidentes de segurança e garantir a preservação de evidências digitais (forensics) para fins de investigação e compliance.

7.4 Todos os Colaboradores e Prestadores de Serviços:

- **Adesão Integral:** Conhecer, aderir e cumprir integralmente todas as diretrizes desta Política, das normas complementares e da legislação vigente;
- **Dever de Confidencialidade:** Garantir o tratamento de dados pessoais em estrita observância ao princípio da finalidade e manter a confidencialidade de todas as informações acessadas;
- **Capacitação:** Participar ativamente e concluir com sucesso os treinamentos e campanhas de conscientização obrigatórios promovidos pela Organização;
- **Comunicação de Risco:** Reportar imediatamente ao DPO ou ao canal oficial qualquer suspeita de incidente, violação de segurança ou não conformidade.

8. EXCEÇÕES

Situações excepcionais serão tratadas pelo setor do escritório de Governança e Gestão Corporativa avaliará a tomada de decisão emergencial sobre a medida a ser adotada e caso exista a necessidade de a adequação e inclusão futura nesta política.

Cientifique-se e cumpra-se.

Fortaleza, 11 de setembro de 2025.

Aprovação

Nome	Assinatura	Data
Flávio Gil Bezerra Barros	Flávio Gil Bezerra de Barros	02/09/2025
Flávia Maria Gradvohl Bezerra de Barros	INACE IATES LTDA	02/09/2025
Robert Gil Gradvohl Bezerra	Robert Gil Bezerra INACE IATES LTDA	02/09/2025