GRUPO BS2			
Norma: **POLÍTICA DE SEGURANÇA NAS COMUNICAÇÕES COM TERCEIROS E PARCEIROS DE NEGÓCIOS**		Código:	Folha: **1/7**
		Primeira Edição: **24/06/2024**	
Processo: **GESTÃO DO SGSPI**	Classificação: **PÚBLICA**	Edição: **4º**	Data: **19/10/2026**

HISTÓRICO DA ÚLTIMA MODIFICAÇÃO

EDIÇÃO	DATA	ALTERAÇÕES EM RELAÇÃO À REVISÃO ANTERIOR
1	**24/06/2024**	Elaborado por Égide Pro – Proteção de Dados e Compliance (Mayara Magda da Silva Pastor) em 29/11/2023, aprovado em 24/06/2024.
2	**01/07/2025**	Adicionado mais informações sobre o Encarregado de Proteção de Dados e canais de contato. Sem alterações na política de forma geral.
3	**06/08/2025**	Adicionado mais informações sobre o Encarregado de Proteção de Dados e no prazo do dever de comunicação que passou de 24 para 48 horas para estar em conformidade com os contratos.
4	**19/10/2026**	Ajuste no link do formulário da Centra de Privacidade.

Uso interno - Proibido qualquer tipo de divulgação sem prévia autorização
Todos os direitos reservados - Avenida Tamandaré, 100, Maringá - PR, Brasil - Cep 87013-210

Esta política de segurança nas comunicações é uma declaração formal do compromisso da ***Grupo BS2***, para com as informações e dados pessoais controlados, compartilhados ou armazenados pela organização.

Este documento se aplica a todos os fornecedores, prestadores de serviços, parceiros de negócios e terceiros que venham a ter acesso às informações e dados pessoais controlados, compartilhados e armazenados pelas empresas do grupo.

Desde já, a organização informa que mantém um Encarregado de Proteção de Dados (DPO), Mayara Pastor, e, em seus impedimentos, como substituta, Aline Barandas, sendo seus contatos descrito abaixo, o qual é responsável pela revisão e atualização contínua desta política, com base em processo de avaliação sistemática de impactos e riscos à privacidade, devidamente documentados.

Égide Pro – Proteção de Dados e Compliance (Central de Privacidade)
E-mail: dpocrmall@egidepro.com.br
Formulário: https://app.acreditese.com.br/dashboard/activityForm/1/749

É obrigação, de todas as pessoas e empresas submetidas à esta política, reportar ao Encarregado de Proteção de Dados, qualquer violação que tenham conhecimento.

Esta Política de Segurança nas Comunicações com Terceiros e Parceiros de Negócios é aderente aos princípios instituídos pela Lei Geral de Proteção de Dados Pessoais – Lei n. 13.709/2018, ISO/IEC 27001 e ISO/IEC 27701.

O objetivo desta política é orientar as ações e estabelecer as diretrizes corporativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Os objetivos principais são:

Uso interno - Proibido qualquer tipo de divulgação sem prévia autorização
Todos os direitos reservados - Avenida Tamandaré, 100, Maringá - PR, Brasil - Cep 87013-210

I – Manter e aperfeiçoar as práticas de Segurança da Informação em todos os níveis da organização e de seus parceiros de negócios;

II – Conscientizar os colaboradores, fornecedores e prestadores em relação às práticas de Segurança da Informação e privacidade e proteção dos dados pessoais;

III – Reforçar o compromisso estratégico acerca da Privacidade das comunicações e dos dados pessoais controlados, armazenados e compartilhados; e

IV – Garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais , incluindo, mas não se limitando ao due diligence necessário.

Os principais conceitos apresentados são:

- **Análise de Riscos:** processo que envolve a consideração das vulnerabilidades, causas e consequências, a fim de se determinar as probabilidades dos riscos se tornarem reais e os impactos decorrentes;

- **Risco:** é qualquer coisa, desconhecida ou incerta, que possa impedir os objetivos da instituição, é qualificado pela probabilidade da ocorrência e pelo impacto que pode causar no projeto, caso ocorra;

- **Dado Pessoal:** informação relacionada a pessoa natural identificada ou identificável;

- **Dado Pessoal Sensível:** é uma categoria especial de dados pessoais, sendo eles os relacionados à 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;

- **Tratamento de dados:** toda e qualquer operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento,

Uso interno - Proibido qualquer tipo de divulgação sem prévia autorização
Todos os direitos reservados - Avenida Tamandaré, 100, Maringá - PR, Brasil - Cep 87013-210

armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

- **Dispositivos Móveis:** qualquer equipamento ou acessório portátil, capaz de se conectar à internet e/ou armazenar dados, tais como os celulares, smartphones, tablets, notebooks, mp4, pen drives, CD/DVD e outros semelhantes;

- **Incidente de Segurança:** ocorrência de uma possível violação de segurança com potencial de causar dano à confidencialidade, integridade e disponibilidade dos dados pessoais e informações;

- ***Due Diligence*:** processo por meio do qual é medido o nível de maturidade do terceiro ou parceiro de negócio em relação à privacidade e segurança dos dados pessoais tratados nas organizações.

Todos os parceiros de negócios e terceiros deverão estar cientes e devidamente comprometidos com a presente política, garantindo a integridade, disponibilidade e confidencialidade dos dados pessoais tratados em nome da organização ou em razão do contrato celebrado entre as partes, ainda que de forma verbal.

Também é dever dos parceiros de negócio e terceiros manter em suas redes, sistemas e softwares as melhores práticas de segurança da informação e privacidade.

Para tanto, dentre as políticas já adotadas, o terceiro e parceiro de negócio declara que:

➤ Processará os dados pessoais e informações apresentadas na qualidade de operadora de dados única e exclusivamente para fins de cumprimento do objeto contratado;

➤ Em caso de utilização de sistemas, o sistema deverá estar adequado às boas práticas exigidas pela LGPD, com login e senha fortes, níveis de acesso, e demais fatores de segurança da informação e garantia da privacidade;

Uso interno - Proibido qualquer tipo de divulgação sem prévia autorização
Todos os direitos reservados - Avenida Tamandaré, 100, Maringá - PR, Brasil - Cep 87013-210

➤ As eventuais solicitações, por parte dos titulares de dados, recebidas pelos terceiros/parceiros, relativamente a dados pertinentes à relação entre as partes, deverão serem informadas à Central de Privacidade, por meio do e-mail de contato do encarregado *dpocrmall@egidepro.com.br*, ou pelo formulário de contato em https://egidepro.inpakta.tech/crmall de forma imediata, ou no prazo de 48 horas sempre justificando o motivo da demora;

➤ Implementará e manterá medidas de segurança administrativas, organizacionais, técnicas e físicas apropriadas para proteger os dados pessoais tratados contra destruição acidental ou ilegal, alteração, divulgação ou qualquer tipo de vazamento e/ou acesso não autorizado e contra formas de processamento;

➤ Implementará e manterá atualizada uma Política de Segurança da Informação e Privacidade de Dados que garantirá no mínimo: **a)** realização de backup periódico, salvos em lugares reportados seguros, e de acordo com as normas estabelecidas pelo fabricante; **b)** não realização de transferência internacional de dados sem a prévia ciência e concordância da Controladora; **c)** adoção de medidas de proteção de segurança da informação, como *firewall*, criptografia de ponta a ponta, ou por meio de chaves, etc.; **d)** não compartilhamento de dados com terceiros estranhos à presente relação, salvo em caso de prévia ciência e concordância da Controladora; **e)** atendimento dos direitos do titulares e; **f)** respeito aos princípios e fundamentos da Lei Geral de Proteção de Dados;

➤ Inexistindo outra finalidade declarada para o tratamento de dados pessoais compartilhados os dados pessoais, ora compartilhados, deverão ser eliminados de forma segura, com registro de tal operação, mantendo somente em sua égide os necessários para cumprimento de suas obrigações legais, tais como: leis, relatórios financeiros, preservação de provas, etc;

➤ Elaborar um plano escrito e estruturado para o caso de ocorrência de incidentes de segurança envolvendo dados pessoais. O plano de resposta deverá conter, minimamente: **a)** data e hora do incidente; **b)** data e hora da ciência; **c)** relação dos tipos de dados afetados pelo incidente; **d)** número de usuários afetados e a relação dos titulares; **e)** dados do

Uso interno - Proibido qualquer tipo de divulgação sem prévia autorização
Todos os direitos reservados - Avenida Tamandaré, 100, Maringá - PR, Brasil - Cep 87013-210

responsável pela proteção dos dados, ou ainda, outra pessoa junto a qual seja possível obter maiores informações sobre o ocorrido; e por fim, **f)** descrição das possíveis consequências do evento.

➤ Na ocorrência de incidentes de segurança envolvendo dados pessoais, notificar imediatamente a Controladora, no e-mail do Encarregado já designado, contendo no mínimo: **a)** data e hora do incidente; **b)** data e hora da ciência e quem detectou; **c)** relação dos tipos de dados afetados pelo incidente; **d)** número de usuários afetados e a relação dos titulares; **e)** dados do responsável pela proteção dos dados, ou ainda, outra pessoa junto a qual seja possível obter maiores informações sobre o ocorrido; e por fim, **f)** descrição das consequências do evento, medidas de contenção e erradicação, danos conhecidos;

➤ Responderá o formulário de *due diligence* anexo a esta política com respostas verossímeis, enviando sempre que possível as evidências requeridas;

➤ Adotará, sempre que possível e imprescindível, as sugestões do Grupo BS2 para aprimoramento das medidas de privacidade e proteção de dados e segurança da informação;

A não observância do disposto nesta política implicará responsabilidade ao terceiro/parceiro descumpridor perante a ANPD, à Controladora e os titulares de dados por todo e qualquer dano ocorrido, eximindo a controladora de qualquer responsabilidade, garantido inclusive a mesma o direito de regresso, caso venha a ser demandada. O procedimento de apuração será conduzido pelo Comitê de Privacidade e Proteção de Dados, e o parecer final poderá resultar em:

➤ Advertência por escrito;

➤ Rescisão Contratual.

No mais, a organização se reserva ao direito de regresso, buscando a reparação moral e material, nos termos da legislação vigente.

Uso interno - Proibido qualquer tipo de divulgação sem prévia autorização
Todos os direitos reservados - Avenida Tamandaré, 100, Maringá - PR, Brasil - Cep 87013-210

O *Grupo BS2* se reserva ao direito de modificar, a qualquer momento, as presentes normas, especialmente para adaptá-las aos requisitos de segurança, aos padrões de boas práticas e de governança.

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado, com revisão anual.

Uso interno - Proibido qualquer tipo de divulgação sem prévia autorização
Todos os direitos reservados - Avenida Tamandaré, 100, Maringá - PR, Brasil - Cep 87013-210