



POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES E LGPD

ÍNDICE

1	Objetivo	4
2	Âmbito	4
3	Conceitos e definições	4
4	Princípios Básicos.....	5
5	Papéis e Responsabilidade.....	6
6	Controle de acesso e autenticação	6
7	Segurança física e do ambiente.....	7
8	Operações, comunicações e redes.....	7
9	Tratamento de incidentes de segurança.....	8
10	Conscientização e treinamento.....	8
11	Conformidade, auditoria e revisão.....	8
12	Vigência e aprovação.....	9

1. OBJETIVO

Definir as diretrizes, responsabilidades e controles para proteger os ativos de informação da 3 GEO, contra acessos não autorizados, uso indevido, divulgação, destruição ou interrupção dos serviços. Além de estabelecer diretrizes para o tratamento de dados pessoais pela 3 GEO, assegurando o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e a proteção dos direitos dos titulares.

2. ÂMBITO

Aplica-se a todos os colaboradores, prestadores de serviços, terceirizados, bem como qualquer sistema, rede, dispositivo, infraestrutura (física ou lógica) e dados pessoais sob responsabilidade da empresa, em toda a GEO e regiões de atuação.

3. CONCEITOS E DEFINIÇÕES

- **Ativo de informação:** qualquer bem tangível ou intangível que tenha valor para a organização e que suporte, contenha ou transmita informação.
- **Informação confidencial/sensível:** dados cujo acesso, divulgação ou modificação não autorizada pode gerar risco para a empresa, clientes ou partes interessadas.
- Usuário, gestor, operador etc.

4. PRINCÍPIOS BÁSICOS

- **Confidencialidade:** garantir que a informação seja acessada apenas por quem tem autorização.
- **Integridade:** garantir que a informação seja completa, exata e não tenha sido modificada de forma não autorizada.
- **Disponibilidade:** garantir que a informação e os recursos estejam acessíveis quando necessário.
- **Responsabilidade:** todos têm papel na segurança da informação.
- **Conformidade:** estar em conformidade com legislação aplicável, contratos, normas internas e melhores práticas. O tratamento dos dados ocorrerá com fundamento em uma das bases legais previstas no art. 7º da LGPD, como:
 - *Consentimento do titular;*
 - *Cumprimento de obrigação legal ou regulatória;*
 - *Execução de contrato;*
 - *Exercício regular de direitos;*
 - *Legítimo interesse.*

. Direitos do Titular

- O titular pode, a qualquer momento:
- Solicitar confirmação ou acesso aos dados;
- Pedir correção, exclusão ou anonimização;
- Revogar consentimento;
- Solicitar portabilidade;
- Reclamar à Autoridade Nacional de Proteção de Dados (ANPD).
- Os pedidos devem ser enviados ao e-mail: [e-mail do encarregado (DPO)].

5. PAPÉIS E RESPONSABILIDADES

- Direção / Alta gestão: aprovar a política, disponibilizar recursos, demonstrar suporte.
- Gestor de Segurança da Informação: definir controles, monitorar cumprimento, promover formação e conscientização.
- Gestores de área/linha: aplicar e assegurar cumprimento na respectiva equipe.
- Todos os colaboradores: cumprir esta política, participar de treinamentos, reportar incidentes.

6. CONTROLE DE ACESSO E AUTENTICAÇÃO

- Acesso concedido com base no princípio do menor privilégio.
- Autenticação forte (por exemplo, senhas complexas + autenticação multifatorial).
- Reavaliação periódica de perfis de acesso, remoção de contas inativas ou desnecessárias.

Compartilhamento de Dados LGPD

Os dados pessoais poderão ser compartilhados apenas com:

- Parceiros e prestadores de serviços essenciais à execução das atividades;
- Autoridades públicas, quando houver obrigação legal;

- Sempre observando a segurança e a confidencialidade das informações

7. SEGURANÇA FÍSICA E DO AMBIENTE

- Acesso físico restrito a áreas de TI, servidores, salas de controle.
- Proteção de equipamentos, uso seguro de dispositivos móveis
- Backup, redundância de sistemas para garantir disponibilidade.

A organização adota medidas técnicas e administrativas para proteger os dados pessoais, incluindo:

- *Controle de acesso;*
- *Criptografia e autenticação;*
- *Backup seguro;*
- *Política de senhas e antivírus;*
- *Treinamento de colaboradores.*

8. OPERAÇÕES, COMUNICAÇÕES E REDES

- Uso seguro de redes (internas, externas, remotas) com protocolos seguros
- Monitoramento, logging, análise de incidentes.
- Atualização regular de software e hardware para mitigar vulnerabilidades.

9. TRATAMENTO DE INCIDENTES DE SEGURANÇA

- Definição de processo claro para reporte, investigação, resposta e recuperação de incidentes.
- Comunicação interna e externa conforme legislação ou contrato.
- Lições aprendidas e melhorias após cada incidente.

10. CONSCIENTIZAÇÃO E TREINAMENTO

- Realização periódica de treinamentos sobre segurança da informação, uso de dispositivos e boas condutas.
- Campanhas de conscientização para reforçar cultura de segurança.

Gestão de Incidentes

Em caso de incidente de segurança que possa causar risco ou dano relevante aos titulares, a empresa notificará a ANPD e os titulares afetados, conforme o art. 48 da LGPD

11. CONFORMIDADE, AUDITORIA E REVISÃO

- Verificação periódica da conformidade com a política, normas, contratos e legislação (ex: Lei Geral de Proteção de Dados Pessoais – LGPD).
- A política será revista no mínimo a cada 1 ano ou sempre que ocorrer mudança relevante no ambiente ou regulamentação.

- Sanções para descumprimento: poderão incluir advertência, suspensão de acesso, ou outras medidas disciplinares conforme normativa interna e legislação.

12. VIGÊNCIA E APROVAÇÃO

- Esta política entra em vigor na data de sua aprovação pela direção da empresa e permanecerá em vigência até que seja revisada ou revogada.
- Versões anteriores são substituídas pela nova revisão desta política.

Responsável	Cargo	Assinatura	Data
Warley Moura	Diretor Adm Financeiro		
Viviane Souza	Gerente de R. Humanos		

