POLÍTICA RESUMIDA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

OBJETIVO

O documento estabelece as regras e os princípios da Política de Segurança da Informação e Cibernética, que deve nortear as ações dos fornecedores/parceiros da Alelo.

Esta é uma versão resumida para divulgação pública da Política Interna, aprovada pelo Conselho de Administração da Alelo, em atendimento à Resolução BCB Nº 85, de 8 de abril 2021.

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação abrange três pilares básicos, destacados nos princípios a seguir:

- **Confidencialidade**:

  Garante que a informação seja acessível somente pelas pessoas autorizadas e durante o período necessário.

- **Disponibilidade**:

  Garante que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessário aos processos de negócio ou a clientes da Alelo.

- **Integridade**:

  Garante que a informação esteja completa e íntegra, bem como não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

ESCOPO DA POLÍTICA

Este documento está embasado na política específica de segurança da informação e cibernética da empresa Alelo, cujo escopo abarca os seguintes requisitos:

1. Classificação e utilização das informações;
2. Acesso lógico;
3. Segurança de rede;
4. Cópias de segurança (Backup);
5. Logs e trilhas de auditoria;
6. Dispositivos e controles de mídias;
7. Uso de equipamentos;
8. Mesa e tela limpa;
9. Proteção e combate à vírus;
10. Uso de Internet e Correio Eletrônico;

11. Criptografia;
12. Redes sociais;
13. Gestão de vulnerabilidades;
14. Incidentes de segurança da informação e cibernética;
15. Gestão de riscos;
16. Terceiros e prestadores de serviços;
17. Segurança para infraestrutura;
18. Compartilhamento de informações de incidentes;
19. Plano de Continuidade de Negócios;
20. NIST (*National Institute of Standards and Technology - USA*);
21. Contratação de serviços de processamento e armazenamento de dados e de computação em nuvem;
22. Disposições especificamente relacionadas à implementação dos pontos da resolução 85 que tratam da segurança cibernética, quais sejam:

22.1 Plano de Ação e de Resposta a Incidentes e Relatório Anual;

DIRETRIZES GERAIS

Na Alelo a Segurança da Informação e Cibernética é uma responsabilidade coletiva, em especial: i) Colaboradores e Terceiros; ii) Gente e Gestão; iii) Segurança da Informação; iv) Áreas de Tecnologia; v) Gestores da Informação; vi) Alta Administração; e vii) Privacidade de Dados.

As informações da Alelo dos clientes e do público em geral, são tratadas em conformidade com as determinações da regulamentação vigente e de forma alguma são manuseadas por pessoas não autorizadas pela Companhia.

São diretrizes que regem a interpretação e a implementação da Política: a confidencialidade, a integridade, a conformidade e a disponibilidade.

As diretrizes expressas nesta Política aplicam-se a todas as informações pertinentes a Alelo, que estiverem sob sua direta gestão ou custódia de terceiros.

As informações geridas são utilizadas apenas para os propósitos definidos pela Alelo não sendo permitido a qualquer momento ou sob qualquer pretexto a apropriação ou utilização dessas informações em benefício próprio.

Todos os colaboradores, terceiros e parceiros da Alelo devem estar cientes sobre a presente Política e recebem treinamento anual e adequado para utilizar as informações do negócio.

As informações geradas e manuseadas no âmbito da Alelo possuem classificações que consistem no nível de proteção e cuidado que cada dado deve receber. O Gestor da Informação, indicado como responsável por determinado ativo informacional, deverá classificá-lo com base nas seguintes espécies de Classificação: Informação Pública, Informação de Uso Interno, Informação de Uso Restrito e Informação Confidencial.

Informações classificadas como internas, restritas ou confidenciais não devem ser divulgadas em ambiente público de internet, redes sociais, fóruns, grupos de discussão ou semelhantes.

As informações geradas pela Alelo são de propriedade intelectual exclusiva e não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador e terceiros em seu ambiente de trabalho.

A utilização dos sistemas de informação, rede corporativa, servidores e bancos de dados ocorre por meio da identificação de credencial de acesso individual, que é confidencial e não deve ser revelada em hipótese alguma, mesmo para outros colaboradores ou terceiros.

Informações confidenciais não devem ficar expostas nas mesas e nos armários e os gaveteiros devem ser trancados quando não utilizados, se os colaboradores e terceiros se ausentarem de suas mesas devem bloquear suas estações de trabalho.

Os incidentes de Segurança da Informação e cibernética da Alelo são registrados, sua causa e impacto são analisados e os fatores de criticidade são definidos pela área impactada, para que posteriormente sejam reportados à Diretoria de TI e devidamente acompanhados pelos seus colaboradores.

A Alelo garantirá a continuidade do negócio em caso de incidentes que possam comprometer o funcionamento normal de suas atividades. Para tanto, utilizarão o seu PCN – Plano de Continuidade de Negócios, o qual é periodicamente revisado com o objetivo contínuo de melhoria.

A Alelo possui um rigoroso processo de segurança em relação ao acesso físico, aos ativos físicos e lógicos, conforme preconizam as melhores práticas do mercado.

Exige-se dos fornecedores e parceiros o mesmo rigor em relação a proteção dos ativos físicos e lógicos, mediante formalização desta em nossos contratos que disciplinam a prestação dos serviços.

Demandamos que as atividades do fornecedor observem as exigências contratuais de segurança em todos os seus processos.

Regulamentação Aplicável:	NBR ISO/IEC 27001:2013 - Sistemas de Gestão da Segurança da Informação; NBR ISO/IEC 27002:2013 - Código de Prática para Controles da Segurança da Informação; NBR ISO/IEC 27005:2019 – Gestão de Riscos de Segurança da Informação; NBR ISO/IEC 27017:2016 - Código de prática para Controles de Segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em Nuvem; PCI DSS – (Payment Card Industry Data Security Standard) – Trata-se do Padrão de Segurança de Dados da Indústria de Cartões de Pagamento, o qual foi desenvolvido para incentivar e aprimorar a segurança dos dados do titular do cartão e promover a ampla adoção de medidas de segurança cibernética; NIST – (National Institute of Standards and Technology) / CSF (Cybersecurity Framework); Marco Civil da Internet – Lei N° 12.965, de 23 de abril de 2014 – Leis n° 12.735 e 12.737; Resolução BCB Nº 85, de 8 de abril 2018; Lei Geral de Proteção de Dados (LGPD) – Lei Nº 13.709, de 14 de agosto de 2018.