POLÍTICA RESUMIDA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

OBJETIVO

O documento estabelece as regras e os princípios sucintos 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 Circular nº 3.909.

DIRETRIZES GERAIS

Na Alelo a Segurança da Informação e Cibernética é uma responsabilidade coletiva da Companhia, 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 princípios que regem a interpretação e 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 Companhia 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 Interna, Informação Confidencial e Informação Sigilosa.

Informações classificadas como internas, confidenciais ou sigilosas 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 da organização 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, os armários e gaveteiros devem ser trancados quando não utilizados e 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, utilizará o seu PCN – Plano de Continuidade de Negócios, o qual é periodicamente revisado com o objetivo contínuo de melhoria.

Possuímos um rigoroso processo de segurança em relação ao acesso físico aos nossos ativos físicos e lógicos, conforme preconizam as melhores práticas do mercado:

Exigimos dos fornecedores e parceiros o mesmo rigor em relação a proteção dos ativos físicos e lógicos mediante formalizaçãoo desta reinvindicação 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 27001:2005 - Sistemas de Gerência da Segurança da Informação; NBR ISO/IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação; PCI DSS; Marco Civil da Internet – Lei N° 12.965, de 23 de abril de 2014 – Leis n° 12.735 e 12.737; Circular Nº 3.909, DE 16 de agosto 2018 do Banco Central do Brasil. Lei Geral de Proteção de Dados (LGPD) – Lei Nº 13.709, de 14 de agosto de 2018