POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

INSIDE RESEARCH LTDA • CNPJ/ME nº 33.289.677/0001-40

Sumário

1. OBJETIVO E ABRANGÊNCIA

Esta Política de Segurança da Informação ("Política") tem como objetivo estabelecer as diretrizes, os princípios e os procedimentos para a proteção das informações sob responsabilidade da Inside Research Ltda. ("Inside"), inscrita no CNPJ/ME sob o nº 33.289.677/0001-40, preservando sua confidencialidade, integridade e disponibilidade, bem como o tratamento adequado dos dados pessoais, em observância à Lei nº 13.709, de 14 de agosto de 2018 ("LGPD"), e às demais normas aplicáveis.

Esta Política aplica-se a todos os Colaboradores da Inside, assim entendidos os sócios, administradores, empregados, estagiários e prestadores de serviço, e a todos os ativos de informação, físicos ou lógicos. É complementar ao Código de Conduta Ética, à Política de Compliance e à Política de Segregação de Atividades da Inside.

Qualquer dúvida a respeito de sua aplicação pode ser sanada por meio de contato com a área de Compliance, pelo e-mail **compliance@insideapp.com.br**.

2. DEFINIÇÕES

- **Ativo de Informação:** qualquer dado, informação, sistema, equipamento ou recurso que tenha valor para a Inside;

- **Dado Pessoal:** informação relacionada a pessoa natural identificada ou identificável, nos termos da LGPD;
- **Incidente de Segurança:** qualquer evento que comprometa, ou possa comprometer, a confidencialidade, a integridade ou a disponibilidade da informação; e
- **Confidencialidade, Integridade e Disponibilidade:** respectivamente, a garantia de que a informação seja acessível apenas a quem de direito, a manutenção de sua exatidão e completude, e a sua disponibilização quando necessária.

3. PRINCÍPIOS

A gestão da segurança da informação na Inside orienta-se pelos pilares da confidencialidade, da integridade e da disponibilidade, observando, ainda, os princípios da necessidade de conhecer (*need to know*), do menor privilégio e da responsabilização pelo uso dos ativos de informação.

4. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações deverão ser classificadas de acordo com o seu grau de sensibilidade, de modo a orientar os controles aplicáveis. A título exemplificativo, adotam-se os níveis:

a) Pública: informação que pode ser livremente divulgada, sem risco para a Inside;

b) Interna: informação de uso restrito aos Colaboradores, cuja divulgação indevida possa causar impacto limitado;

c) Confidencial: informação cuja divulgação não autorizada possa causar prejuízo relevante à Inside, a seus clientes ou a terceiros, incluindo informação privilegiada.

5. CONTROLE DE ACESSO

O acesso aos ativos de informação será concedido de forma individual, mediante credenciais pessoais e intransferíveis, observado o princípio do menor privilégio. As senhas são de uso pessoal e sigiloso, sendo vedado o seu compartilhamento. Os acessos serão revistos periodicamente e revogados tempestivamente nas hipóteses de desligamento ou de alteração de funções.

6. USO DE RECURSOS DE TI E DISPOSITIVOS

Os recursos de tecnologia da informação disponibilizados pela Inside destinam-se ao desempenho das atividades profissionais. Os Colaboradores deverão:

- Utilizar os recursos de forma responsável, abstendo-se de instalar programas não autorizados ou de acessar conteúdos ilícitos;
- Adotar procedimentos de mesa limpa e tela limpa e bloquear estações de trabalho quando ausentes;

- Observar cuidados equivalentes em regime de trabalho remoto e no uso de dispositivos móveis; e
- Abster-se de transmitir informações confidenciais por meios não autorizados ou inseguros.

7. PROTEÇÃO DE DADOS PESSOAIS (LGPD)

O tratamento de dados pessoais pela Inside observará as bases legais, os princípios e os direitos dos titulares previstos na LGPD, limitando-se às finalidades legítimas e informadas, pelo tempo necessário, com a adoção de medidas técnicas e administrativas aptas a proteger tais dados de acessos não autorizados e de situações acidentais ou ilícitas.

8. GESTÃO DE INCIDENTES

Todo Colaborador que tomar conhecimento de incidente de segurança da informação, real ou suspeito, deverá comunicá-lo imediatamente à área de Compliance. Os incidentes serão registrados, analisados e tratados, adotando-se as medidas de contenção, correção e comunicação cabíveis, inclusive, quando aplicável, a comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados, nos termos da LGPD.

9. CONTINUIDADE E CÓPIAS DE SEGURANÇA

A Inside adotará rotinas de cópia de segurança (*backup*) e medidas de continuidade compatíveis com o seu porte, de modo a assegurar a recuperação das informações essenciais em caso de falha, perda ou indisponibilidade dos recursos.

10. RESPONSABILIDADES

Compete ao Diretor de Compliance, ou ao responsável por ele designado, zelar pela implementação, supervisão e atualização desta Política. Compete a todos os Colaboradores conhecer e observar suas disposições, protegendo os ativos de informação a que tenham acesso e reportando prontamente quaisquer incidentes ou vulnerabilidades. O dever de sigilo persiste após o término do vínculo do Colaborador com a Inside.

11. PENALIDADES

A inobservância das diretrizes desta Política será considerada infração grave, sujeitando o infrator às medidas disciplinares cabíveis, que podem chegar ao desligamento do profissional, independentemente das sanções legais ou regulatórias aplicáveis. A Inside sempre cumprirá com o seu dever de informar as autoridades competentes no caso de qualquer infração às normas legais e infralegais.

12. VIGÊNCIA E ATUALIZAÇÃO

Esta Política tem vigência por prazo indeterminado e será atualizada sempre que necessário, a depender de exigências dos órgãos reguladores, em razão de alterações legais, ou

necessidades do mercado. A presente Política está disponível no endereço eletrônico da Inside: **https://lvntcorp.com.br/**.