POLÍTICA RESUMIDA | 4893 Seção II - Art. 5º

Pólítica de Segurança da Informação Resumida	Data: 12/04/2023

Em aderência a ***Resolução CMN n° 4.893 de 26/2/2021***, a Instituição possui em sua estrutura organizacional uma Política de Segurança da Informação que abrange também a Segurança Cibernética, e que tem como principal objetivo garantir a confidencialidade, integridade, disponibilidade e rastreabilidade dos dados, sistemas e ativos da informação, através das seguintes diretrizes:

- Garantir o comprometimento da Alta Administração da instituição com a melhoria contínua dos procedimentos relacionados à Segurança da Informação;
- Assegurar a confidencialidade, integridade, disponibilidade e rastreabilidade das informações através do uso de mecanismos de Segurança da Informação e Cibernética, com base em fatores de risco, tecnologia e modelos de negócio;
- Assegurar que todo acesso à informação seja restrito e concedido com os privilégios mínimos para que colaboradores e prestadores de serviço acessem apenas as informações necessárias ao desempenho de suas funções, estando sujeitos ainda a monitoração, rastreabilidade e auditoria;
- Assegurar a existência de controles para proteção das informações, sistemas e ativos contra acesso indevido, cópia, modificação ou vazamento e/ou divulgação não autorizada, assim como uso de ferramentas de proteção contra malwares e atividades maliciosas;
- Assegurar que seus colaboradores e prestadores de serviço participem de Campanhas de Conscientização e Treinamentos internos em Segurança da Informação e Cibernética;
- Assegurar a existência de um processo de Continuidade dos Negócios, para garantir a resiliência operacional e a recuperação de atividades críticas em caso de incidentes e interrupções;
- Assegurar que clientes e usuários recebam informações sobre as precauções necessárias relacionadas à Segurança da Informação e Cibernética, para a utilização segura de produtos e serviços financeiros;
- Garantir que ativos de informação relevantes sejam monitorados e testados periodicamente para detecção e correção de vulnerabilidades;
- Assegurar a existência de um plano de ação e de resposta adequado aos incidentes de Segurança da Informação que possam impactar serviços e ativos de informação;
- Garantir que a confidencialidade e a integridade dos dados relevantes sejam protegidas através do uso de Criptografia em conformidade com as regras definidas pela Instituição e aderentes a órgão reguladores.

CANAL DE COMUNICAÇÃO

No caso de alertas e/ou incidentes de segurança, recomenda-se encaminhar as notificações pelo canal de comunicação: ***seguranca.ti@supplier.com.br.***

PENALIDADES / VIOLAÇÕES DE SEGURANÇA

O não cumprimento desta Política e das demais diretrizes e procedimentos de Segurança da Informação da Instituição poderá resultar em medidas legais e/ou disciplinares.