viavoz projetos

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

## I. Objetivo

A presente Política de Segurança da Informação e Cibernética ("Política") tem por objetivo estabelecer diretrizes para proteger e salvaguardar os ativos de informação; nortear a definição de normas e procedimentos específicos de Segurança da Informação e Cibernética; e, implementar controles e procedimentos para reduzir a vulnerabilidade a incidentes da Empresa.

## II. Abrangência

Todos os colaboradores (incluindo terceirizados), estagiários, jovens aprendizes, investidores, bancos, fornecedores, concorrentes, governo, órgãos reguladores, imprensa, comunidade, sociedade, dentre outros.

## III. Princípios, Regras e Procedimentos

### 1. Sobre a segurança da informação:

1.1. A Empresa possui como objetivo desenvolver processos e produtos considerando os pilares e as boas práticas de segurança da informação, apoiada na gestão dos riscos cibernéticos como assunto estratégico ao negócio e ao fomento da cultura de segurança entre todos os colaboradores para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

### 1.2. A Empresa estabelece os seguintes pilares:

1.2.1. **Confidencialidade**: garantir que a informação somente estará acessível para pessoas autorizadas;

1.2.2. **Integridade**: garantir que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não;

1.2.3. **Disponibilidade**: garantir que a informação estará disponível sempre que for necessário;

1.2.4. **Autenticidade**: garantir que a informação é proveniente da fonte original e que não foi alvo de alterações.

1.2.5. **Irretratabilidade ou não repúdio**: garantir que o legítimo autor da informação não possa negar sua autoria.

1.2.6. **Conformidade**: garantir que os processos da Empresa estejam de acordo com os regulamentos, normativos e leis vigentes, de forma a seguir rigorosamente todos os protocolos exigidos no setor de atuação da Empresa em decorrência das suas atividades realizadas.

1.3. A Empresa considera que os ativos de informação são todos aqueles gerados ou desenvolvidos para o negócio, como consentimentos de clientes e pessoas ligadas à Empresa *(opt-in e opt-out),* dados cadastrais de clientes e colaboradores, informações de pagamentos e dos portadores desses meios de pagamento, além de conversas e gravações com os clientes. Os ativos de informação podem estar presentes em diversas formas, tais como: arquivos digitais, mídias externas, documentos impressos, documentos digitalmente assinados, dispositivos móveis, bancos de dados e gravações de áudio.

1.4. A Empresa determina que, independentemente da forma apresentada, compartilhada ou armazenada, os ativos de informação devem ser utilizados apenas para a sua finalidade devidamente autorizada, sendo sujeitos a monitoramento e auditoria.

1.5. A Empresa estabelece que todo o ativo de informação de sua propriedade possui um responsável, seja devidamente classificado quanto ao seu nível de confidencialidade de acordo com os critérios estabelecidos em norma específica e adequadamente protegido de quaisquer riscos, bem como de ameaças que possam comprometer o seu negócio.

**2. Diretrizes Gerais de Segurança da Informação e Cibernética:**

**2.1. A Empresa possui como diretrizes gerais:**

2.1.1. Resguardar a proteção dos dados contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas;

2.1.2. Realizar a adequada classificação das informações e garantir a continuidade do processamento delas, conforme os critérios e princípios indicados nos normativos internos vigentes sobre o tema;

2.1.3. Garantir que os sistemas e dados sob sua responsabilidade estejam devidamente protegidos e sejam utilizados apenas para o cumprimento de suas atribuições;

2.1.4. Zelar pela integridade da infraestrutura tecnológica na qual são armazenados, processados ou de qualquer outra forma tratados os dados, adotando as medidas necessárias para prevenir ameaças lógicas, como vírus, programas nocivos ou outras falhas que possam ocasionar acessos, manipulações ou usos não autorizados a dados internos e confidenciais.

2.1.5. Atender às leis e normas que regulamentam as atividades da Empresa.

**2.2. Em vistas ao cumprimento das diretrizes acima elencadas, a Empresa**:

2.2.1. Adota procedimentos e controles de segurança para atender aos objetivos de segurança cibernética, dentre eles: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações, conforme normativos internos vigentes.

2.2.2. Controla, monitora, restringe o acesso aos ativos de informação a menor permissão e privilégios possíveis, conforme descrito em normas internas específicas.

2.2.3. Aplica os procedimentos e controles citados anteriormente, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da Empresa.

2.2.4. Possui controles específicos, incluindo os voltados para a rastreabilidade da informação, que buscam garantir a segurança das informações sensíveis.

2.2.5. Realiza ações para prevenir, identificar, registrar e responder incidentes e crises de segurança que envolvam o ambiente tecnológico da Empresa e que possam ocasionar o

comprometimento dos pilares de segurança da informação ou gerar impacto de imagem, financeiros ou operacionais.

2.2.6. Classifica os incidentes de segurança da informação e cibernética conforme sua relevância e de acordo com (i) a classificação das informações envolvidas; e (ii) o impacto na continuidade dos negócios da Empresa, conforme descritos em normas internas específicas. A definição de relevância dos incidentes no ambiente tecnológico segue o padrão corporativo de riscos estabelecido em documento específico.

2.2.7. Realiza o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Empresa, que abrangem, inclusive, informações recebidas de empresas prestadoras de serviços a terceiros.

2.2.8. Estabelece e documenta em normativo interno os critérios que configurem situações de crises, bem como elabora inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança considerados nos testes de continuidade de serviços de pagamento prestados e realiza testes anuais para garantir a eficácia dos processos, além de produzir anualmente um relatório de resposta a incidentes no ambiente tecnológico da Empresa.

2.2.9. Possui critérios para classificação da relevância dos serviços de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, conforme procedimento interno.

2.2.10. Previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem serão adotados os procedimentos previstos na regulamentação do Banco Central do Brasil (“BCB”) em vigor específico sobre o tema.

2.2.11. Avalia, previamente à contratação de empresas prestadoras de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução de atividades operacionais da Empresa, se adotam procedimentos e controles voltados à prevenção e ao tratamento de incidentes em níveis de complexidade, abrangência e precisão compatíveis com os adotados pela Empresa para o tipo de serviço prestado.

2.2.12. Realiza a avaliação periódica de empresas prestadoras de serviço que realizam o tratamento de informações relevantes à Empresa com objetivo de acompanhar o nível

de maturidade de seus controles de segurança, dentre eles, os utilizados para a prevenção e o devido tratamento dos incidentes.

2.2.13. Adota iniciativas para compartilhamento de informações sobre os incidentes relevantes por meio da filiação em fóruns de discussão.

2.2.14. Estabelece regras e padrões para assegurar que a informação receba o nível adequado de proteção quanto à sua relevância conforme normativo interno. Toda informação possui um proprietário, é obrigatoriamente classificada e recebe os devidos controles que garantam a confidencialidade dela, condizendo com as boas práticas de mercado e regulamentações vigentes.

2.2.15. Adota mecanismos para disseminação da cultura de segurança da informação e cibernética na Empresa, incluindo:

2.2.15.1. A implementação de programa de treinamento anual para colaboradores;

2.2.15.2. A implementação de programa de avaliação periódica de colaboradores quanto ao nível de conhecimento do tema segurança da informação e cibernética;

2.2.15.3. A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos; e

2.2.15.4. O comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

**IV. Gestão de Consequências**

Colaboradores, fornecedores ou outros stakeholders (públicos de interesse) que observarem quaisquer desvios às diretrizes desta Política, poderão relatar o fato ao Canal de Ética, podendo ou não se identificar.

Internamente, o não cumprimento das diretrizes desta Política enseja a aplicação de medidas de responsabilização dos agentes que a descumprirem, conforme a respectiva gravidade do descumprimento e de acordo com normativos internos, sendo aplicáveis a todas as pessoas descritas no item “Abrangência” desta Política, incluindo a liderança.

## V. Responsabilidades

- **Administradores**, **Colaboradores** e **Prestadores de Serviço**: Observar e zelar pelo cumprimento da presente Política e, quando assim se fizer necessário, acionar o sócio administrador e o setor de Riscos, Compliance, Prevenção e Segurança para consulta sobre situações que envolvam conflito com esta Política ou mediante a ocorrência de situações nela descritas. Atuar de forma ética e responsável quando tomar conhecimento de incidentes, compartilhando informações com os responsáveis pelo seu tratamento em tempo hábil e tomando todas as ações cabíveis para minimizar os potenciais danos. Por fim, compreender o papel da segurança da informação em suas atividades diárias e participar dos programas de conscientização.
- **Setor de Riscos**, **Compliance**, **Prevenção e Segurança**: Cumprir as diretrizes estabelecidas nesta Política, mantê-la atualizada anualmente de forma a garantir que quaisquer alterações no direcionamento da Empresa sejam incorporadas a mesma e esclarecer dúvidas relativas ao seu conteúdo e a sua aplicação.
- **Fornecedores**: Observar e zelar pelo cumprimento das melhores práticas de Segurança da Informação, bem como dos requisitos de segurança da informação e cibernética exigidos contratualmente durante o vínculo com a Empresa. Atuar de forma ética e responsável quando tomar conhecimento de incidentes, compartilhando informações com os responsáveis pelo seu tratamento em tempo hábil e tomando todas as ações cabíveis para minimizar os potenciais danos, de acordo com o procedimento Plano de Resposta a Incidentes – CSIRT Via Voz.

## VI. Documentação Complementar

- ABNT NBR ISO 27001 – Segurança da Informação.
- Código de Conduta Ética da Via Voz
- Lei Nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet.

- Lei Nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais ("LGPD").

**VII. Conceitos e Siglas**

- **Clientes**: Pessoa física ou jurídica que utiliza os produtos e/ou serviços oferecidos pela Via Voz.
- **Dado(s) e/ou Informação(ões)**: são todos os dados referentes às atividades desenvolvidas pela Empresa na execução de seu objeto social, incluindo dados de Clientes, pessoais ou não, e classificados de acordo com a norma interna específica sobre o tema.
- **Diretoria-Executiva**: é o órgão responsável pela gestão dos negócios da sociedade, executando a estratégia e as diretrizes gerais aprovadas. Por meio de processos e políticas formalizados, a Diretoria-Executiva viabiliza e dissemina os propósitos, princípios e valores da organização.
- **Incidentes**: qualquer ocorrência que realmente ou potencialmente comprometa a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação que o sistema processa, armazena ou transmite ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitáveis.
- **Prestador de Serviço**: pessoa física ou jurídica, devidamente contratada pela Empresa, prestadora de serviços: (i) de tecnologia; (ii) de armazenamento ou qualquer forma de tratamento de Dados e Informações; ou (iii) que venha a ter acesso, por conta do escopo de sua contratação, a Dados confidenciais, como classificados nesta Política.
- **Riscos Cibernéticos**: são os riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, entre outros, que possam expor Dados, redes e sistemas da Empresa, causando danos financeiros e/ou de reputação consideráveis, podendo, em algumas circunstâncias, prejudicar a continuidade das atividades da Empresa.

- **Segurança da Informação**: conjunto de conceitos, técnicas e estratégias, as quais visam proteger os ativos de informação da Empresa.
- **Segurança Cibernética**: conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado.
- **Stakeholders (públicos de interesse)**: todos os públicos relevantes com interesses pertinentes à Empresa, bem como indivíduos ou entidades que assumam algum tipo de risco, direto ou indireto, em face da sociedade. Entre outros, destacam-se: acionistas, investidores, colaboradores, sociedade, clientes, fornecedores, credores, governos, órgãos reguladores, concorrentes, imprensa, associações e entidades de classe, usuários dos meios eletrônicos de pagamento e organizações não governamentais.
- **Opt-In**: Opção para receber informações, contatos ou aderir a serviços.
- **Opt-Out**: Opção para não receber informações, contatos ou desligar-se de serviços.

**VIII. Disposições Gerais**

É competência do Comissão de Gestão do Programa de Integridade – CGPI alterar esta Política sempre que se fizer necessário. Esta Política entra em vigor na data de sua aprovação pelo Conselho de Administração e revoga quaisquer documentos em contrário.

**Sinval Ladeira**

Sócio Administrador