Política de Segurança da Informação e Cibernética

I. Objetivo

Estabelecer diretrizes que permitam à Acelera Tecnologia salvaguardar seus ativos de informação, nortear a definição de normas e procedimentos específicos de Segurança da Informação e Cibernética, bem como a implementação de controles e procedimentos para reduzir a vulnerabilidade da empresa a incidentes.

II. Abrangência

Todas as pessoas que compõem a estrutura organizacional da Acelera Tecnologia, assim como terceiros, prestadores de serviço e/ou fornecedores que tiverem acesso a informações dos clientes destas empresas.

III. Princípios, Regras e Procedimentos

1. Sobre a segurança da informação:

1.1. A Acelera Tecnologia, para garantir a segurança da informação, exerce suas atividades baseadas nos seguintes pilares:

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

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

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

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

1.1.5. Irretratabilidade ou não repúdio: garantir que o legítimo autor da informação não possa repudiar sua autoria, como, por exemplo, ao dar aceite em um contrato digital utilizando credenciais de acesso, entende-se que o aceitante não pode negar a sua assinatura posteriormente.

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

1.2. A Acelera Tecnologia considera ativos de informações todas as informações geradas ou desenvolvidas para o negócio e podem estar presentes em diversas formas, tais como: arquivos digitais, consentimentos de clientes e pessoas ligadas à Acelera Tecnologia (opt-in e opt-out), equipamentos, mídias externas, documentos impressos, documentos digitalmente assinados, sistemas, dispositivos móveis, bancos de dados, conversas e gravações.

1.3. A Acelera Tecnologia 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.

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

2. Diretrizes Gerais de Segurança Cibernética

2.1. Com relação à segurança cibernética, a Acelera Tecnologia 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, 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, por meio, dentre outros aspectos: (i) da manutenção de softwares antivírus instalados e atualizados; (ii) da manutenção dos programas de computador instalados no ambiente; e

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

2.2. Em vistas ao cumprimento das diretrizes acima elencadas, a Acelera Tecnologia:

2.2.1. Possui como objetivo de segurança cibernética: prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

2.2.2. Com relação às medidas de segurança, adota procedimentos e controles para reduzir a vulnerabilidade da Acelera Tecnologia a incidentes e 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.

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

2.2.4. 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.

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

2.2.6. 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.

2.2.7. 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 Acelera Tecnologia.

2.2.8. Classifica os incidentes de segurança conforme sua relevância e de acordo com (i) a classificação das informações envolvidas; e (ii) o impacto na continuidade dos negócios da Acelera Tecnologia, descritos em normas internas específicas.

2.2.9. Realiza a avaliação periódica de empresas prestadoras de serviço que realizam o tratamento de informações relevantes à Acelera Tecnologia com objetivo de acompanhar o nível de maturidade de seus controles de segurança para a prevenção e o devido tratamento dos incidentes.

2.2.10. Possui critérios para classificação da relevância dos serviços de processamento e armazenamento de dados e de computação em nuvem no país, conforme procedimento interno. A Acelera Tecnologia não envia, processo ou armazena dados no exterior.

2.2.11. Previamente à contratação de serviços relevantes de processamentos e armazenamento de dados e de computação em nuvem serão adotados os procedimentos previstos na regulamentação em vigor específica sobre o tema.

2.2.12. 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 Acelera Tecnologia, 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 Acelera Tecnologia.

2.2.13. 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 da mesma, condizendo com as boas práticas de mercado e regulamentações vigentes.

2.2.14. Realiza ações para prevenir, identificar, registrar e responder incidentes e crises de segurança que envolvam o ambiente tecnológico da Acelera Tecnologia e que possam ocasionar o comprometimento dos pilares de segurança da informação ou gerar impacto de imagem, financeiros ou operacionais. A definição de relevância dos incidentes no ambiente tecnológico segue padrão corporativo de riscos estabelecido em norma específica.

2.2.15. Adota mecanismos para disseminação da cultura de segurança da informação e cibernética na Acelera Tecnologia, 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.

2.2.16. Adota iniciativas para compartilhamento de informações sobre os incidentes relevantes através de fóruns de discussão.

IV. Gestão de Consequências

Colaboradores, fornecedores ou outros stakeholders que observarem quaisquer desvios às diretrizes desta Política, poderão relatar o fato ao Canal de Denúncias (https://app.portaldedenuncia.com.br/acelera-tecnologia), podendo ou não se identificar.

Internamente, o descumprimento das diretrizes desta Política enseja a aplicação de medidas de responsabilização dos agentes que a descumprirem, conforme a respectiva gravidade do descumprimento.

V. Responsabilidades

Administradores e Colaboradores: Observar e zelar pelo cumprimento da presente Política e, quando assim se fizer necessário, acionar a área de Compliance e Tecnologia para consulta sobre situações que envolvam conflito com esta Política ou mediante a ocorrência de situações nela descritas. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias e participe dos programas de conscientização.

Técnicos, Compliance, Prevenção e Segurança: Cumprir as diretrizes estabelecidas nesta Política, mantê-la atualizada anualmente de forma a garantir que quaisquer alterações no direcionamento da Acelera Tecnologia sejam incorporadas a mesma e esclarecer dúvidas relativas ao seu conteúdo e a sua aplicação.

Administradores, Colaboradores, Fornecedores e Terceiros: 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 da Acelera Tecnologia.

Sócio Administrador: Após avaliação prévia pelos técnicos, deliberar sobre a aprovação anual do (i) relatório sobre a implementação do plano de ações e de resposta a incidentes para cumprimento da Política de Segurança da Informação e Cibernética da Acelera Tecnologia, e (ii) Plano de Resposta a Incidentes da Acelera Tecnologia.

Fórum Gestor de Segurança da Informação e Prevenção a Fraudes: Atuar de forma proativa, apoiando a gestão de Segurança da Informação no cumprimento das tarefas relacionadas à proteção dos negócios da Acelera Tecnologia e dos seus clientes.

VI. Documentação Complementar

Código de Conduta Ética da Acelera Tecnologia.

Plano de Resposta a Incidentes da Acelera Tecnologia.

PCI-Data Security Standard.

ABNT NBR ISO 27001 - Segurança da Informação.

Normas e procedimentos internos aperfeiçoados constantemente, aprovados pelas alçadas competentes e disponibilizados a todos os colaboradores.

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

Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet.

VII. Conceitos e Siglas

Segurança da Informação: Conjunto de conceitos, técnicas e estratégias, as quais visam proteger os ativos de informação da Acelera Tecnologia.

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 relevantes com interesses pertinentes à Acelera Tecnologia, 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.

Clientes: empresas que contrataram os serviços da Acelera Tecnologia.

Dado(s) e/ou Informação(ões): são todos os dados referentes às atividades desenvolvidas pela Acelera Tecnologia 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.

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 Acelera Tecnologia, 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 Acelera Tecnologia, causando danos financeiros e/ou de reputação consideráveis, podendo, em algumas circunstâncias, prejudicar a continuidade das atividades da Acelera Tecnologia.

VIII. Disposições Gerais

É competência do Sócio Administradora da Acelera Tecnologia alterar esta Política sempre que se fizer necessário.

Esta Política entra em vigor na data de sua aprovação e revoga quaisquer documentos em contrário.

São Paulo – SP, 5 de maio de 2022

Acelera Tecnologia