POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

PAGSEGURO INTERNET INSTITUIÇÃO DE PAGAMENTO S.A.
E DEMAIS EMPRESAS DO CONGLOMERADO PRUDENCIAL

As diretrizes de **Segurança da Informação e Cibernética** do **PagSeguro Internet Instituição de Pagamento S.A.** ("PagBank"), líder do Conglomerado Prudencial, do **BancoSeguro S.A.** ("BancoSeguro") e **PagInvest Corretora de Titulos e Valores Mobiliarios Ltda** ("PagInvest"), instituições pertencentes ao Conglomerado Prudencial do PagSeguro, em conjunto denominadas "Companhias", aderem-se integralmente ao comprometimento da Alta Administração das Companhias, alinhadas com os objetivos estratégicos dos seus negócios, a fim de garantir a aplicação dos princípios de proteção da informação de seus clientes, parceiros, terceiros, profissionais ou qualquer instituição ou pessoa que tenha relacionamento com as Companhias.

Tais diretrizes são a base para que os processos de Governança da Segurança da Informação e Cibernética sejam atendidos e controlados, de forma a:

- Preservar a **confidencialidade, integridade, disponibilidade**, autenticidade e demais atributos de segurança das informações de sua propriedade e/ou sob sua guarda, não expondo-as, bem como oferecendo proteção adequada;
- Estabelecer diretrizes para a **classificação de dados e informações**, por meio de critérios e restrições para acesso, processamento ou transmissão da informação confidencial, sensível ou restrita das Companhias ou de seus clientes que não tenha sido autorizada pelo responsável;
- Implementar procedimentos e controles para mitigação das vulnerabilidades, incidentes e riscos de segurança, sinalizar a saúde do ambiente e produzir planos de remediação e/ou contenção, geração de riscos de segurança, além de informações sobre a situação e estado dos ativos frente as preocupações, ameaças de acordo ao apetite à risco e às estratégias das Companhias, reduzindo assim as superfícies de ataques e os respectivos riscos associados;
- Realizar a **gestão, identificação, resposta, tratamento e redução de incidentes de segurança da informação**, assim como o monitoramento proativo, a detecção e a investigação de tais ocorrências, por meio dos serviços de inteligência (*threat intelligence*) e ainda, comunicar e/ou compartilhar (quando aplicável e especialmente no caso de incidente relevante) as áreas envolvidas, os órgãos reguladores, parceiros de inteligência e entidades externas;
- Prover mecanismos de prevenção ao vazamento de dados e informações (*Data Loss Prevention* – DLP), para detecção de possíveis violações ou padrões de condutas que possam infringir regulamentos das Companhias;
- Disponibilizar mecanismos de proteção, por meio do monitoramento de atividades de *endpoints, sensores* e controles de proteção de *hardware ou software*, contra códigos maliciosos que uma vez executados possam se infiltrar ou causar danos nas redes ou ativos das Companhias;
- Prover diretrizes de utilização dos recursos de rede, ou em contexto mais abrangente, dos recursos computacionais, sejam estes ativos fixos e/ou dispositivos móveis, removíveis, visando as melhores práticas de manipulação, proteção, processamento, monitoração e compartilhamento de informações;

- Prover planos e subplanos (Impacto no Negócio, Continuidade Operacional, Recuperação de Negócios, Gerenciamento de Incidentes, Administração de Crises e Planos de Testes/Validações) de recuperação de serviços críticos para garantir a disponibilidade operacional e da **continuidade de negócio**, bem como, procedimentos operacionais que possam reduzir os impactos decorrentes da interrupção de serviços causada por desastres, crises, indisponibilidades, falhas, comprometimentos ou eventos relevantes de segurança;
- Gerenciar e monitorar via Controle de Acessos, sejam estes físicos e/ou lógicos, às informações e ativos bem como o seu armazenamento, compartilhamento e descarte, para que somente pessoas autorizadas possam utilizá-los e em conformidade com regras, permissões, perfis e/ou políticas corporativas;
- Estabelecer critérios seguros de uso e manutenção de credenciais, segredos, *tokens* e senhas no contexto de utilização dos sistemas corporativos;
- Dar ciência aos profissionais, usuários, prestadores de serviços, clientes e parceiros de que:
  - não é permitido remover controles de segurança ou aplicações utilizadas para o acesso das informações ou proteção, bem como prover alterações em ambiente produtivo sem prévia aprovação;
  - os meios de comunicação, equipamentos de acesso a sistemas de informações e infraestruturas complementares são de propriedade da Companhia e passíveis de monitoração, sendo que os acessos ao conteúdo da internet e uso de e-mail é de responsabilidade do profissional titular da conta, do prestador de serviço, cliente ou parceiro, estando sujeito à aplicação de leis, decretos e regulamentos governamentais vigentes; e
  - não é permitido o uso de qualquer recurso tecnológico ou informações proprietárias em ações ilegais e nem a instalação de recurso computacional não autorizado.
- Definir controles fundamentais para o ciclo de vida e desenvolvimento seguro de *software*, utilização de novas tecnologias que possam guiar projetos dentro do contexto *software* seguro;
- Ajudar no dimensionamento dos requisitos de segurança a partir de arquitetura de referência, uso de controles criptográficos e proteções necessárias de acordo com a complexidade e nível de segurança necessário para cada componente;
- Garantir que sistemas desenvolvidos internamente ou adquiridos de fornecedores atendam aos padrões de segurança e melhores-práticas definidos pelo mercado ou pelas necessidades de negócio;
- Estabelecer diretrizes para manutenção de cópias de segurança (*backup* e *restore*) de dados e informações para os repositórios e locais de armazenamento oficiais das Companhias, assim como regramentos para a retenção da informação e *logging*, em conformidade com os órgãos reguladores e questões legais vigentes;
- Divulgar continuamente em todos os níveis, esferas e para o maior público possível, interna e/ou externamente (aos clientes) quando aplicável, programas e **ações de conscientização, treinamentos, aculturamento e prevenção** em relação à temática de Segurança da Informação e Cibernética;
- Analisar, aprovar e classificar contratos, nos termos da legislação vigente e sob o

ponto de vista de Segurança da Informação, sejam estes para contratação de serviços relevantes (ou não) de processamento, de armazenamento e em nuvem; e

- Suportar questões de risco oferecendo um modelo e processo de risco comum, integrado e contínuo de identificação, análise, avaliação, tratamento, revisão e comunicação dos riscos mapeados, a fim de proteger os ativos das companhias em avaliações e definições de controles que possam validar o escopo desta política no intuito de aferir o nível de segurança dos controles de segurança da informação, em atendimento às áreas demandantes (Auditoria Interna, Controles Internos e *Compliance*).

A violação de controle de segurança ou o não cumprimento das diretrizes é considerada infração e poderá implicar em medidas disciplinares (sanções) a serem validadas pelos departamentos de Recursos Humanos, Jurídico, *Compliance* e Segurança da Informação PagBank, conforme sua natureza e enquadramentos previstos nas leis vigentes.

PAGSEGURO INTERNET INSTITUIÇÃO DE PAGAMENTO S.A.