



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

PAGSEGURO S.A.
LÍDER DO CONGLOMERADO PRUDENCIAL

	POLÍTICA DE SEGURANÇA CIBERNÉTICA	Áreas responsáveis:	Segurança da Informação & Compliance
		Data:	Fevereiro/2021

As diretrizes de **Segurança da Informação e Cibernética** do **PagSeguro Internet S.A.** ("PagSeguro"), líder do Conglomerado Prudencial, e do **BancoSeguro S.A.** ("BancoSeguro"), instituição pertencente 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, 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, sinalizar a saúde do ambiente e produzir planos de remediação e/ou contenção, geração de riscos, além de informações sobre a situação e estado dos ativos frente as preocupações, ameaças e apetite à risco 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 das Companhias;
- Prover planos e subplanos (Impacto no Negócio, Continuidade Operacional, Recuperação de Negócios, Gerenciamento de Incidentes, Administração de Crises e Planos de Qualquer alteração neste documento deverá ser previamente analisada pelas áreas de Segurança da Informação e Compliance.

	POLÍTICA DE SEGURANÇA CIBERNÉTICA	Áreas responsáveis:	Segurança da Informação & Compliance
		Data:	Fevereiro/2021

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 cia 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*) de dados e informações para os repositórios e locais de armazenamento oficiais das Companhias, assim como regramentos para a retenção da informação, em conformidade com os órgãos reguladores participantes;

Qualquer alteração neste documento deverá ser previamente analisada pelas áreas de Segurança da Informação e Compliance.

	POLÍTICA DE SEGURANÇA CIBERNÉTICA	Áreas responsáveis:	Segurança da Informação & Compliance
		Data:	Fevereiro/2021

- 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, acultramento 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, armazenamento e em nuvem ou não; e
- Suportar tanto a área de Risco Operacional, oferecendo um modelo e procedimento de risco comum e integrado, a partir de um processo contínuo de identificação, análise, avaliação, tratamento, revisão e comunicação dos riscos mapeados, a fim de proteger os ativos da companhia, quanto as áreas auxiliares (Auditoria Interna, Controles Internos e *Compliance*) 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.

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 PagSeguro, conforme sua natureza e enquadramentos previstos nas Leis vigentes.

PAGSEGURO INTERNET S.A.