monee	Tipo de Documento: POLÍTICA CORPORATIVA	Data de Vigência: Julho/2025
Classificação de Publicidade: PÚBLICO EXTERNO	Nome do Documento: POLÍTICA DE CIBERSEGURANÇA PARA TERCEIROS	Versão: v3.0/2025

Política de Segurança Cibernética para Terceiros

Elaboração e Responsabilidade: ÁREA DE SEGURANÇA CIBERNÉTICA	Aprovação: DIRETORIA EXECUTIVA
Data: Julho/2025	Data: Julho/2025

Índice

1. INTRODUÇÃO

No Grupo Shopee desenvolvemos soluções simples e seguras, totalmente digitais para que nossos clientes tenham total liberdade do uso da tecnologia e o uso do seu dinheiro. Valorizamos nossos clientes e entendemos que a segurança cibernética é de extrema importância para que todos utilizem-se dos nossos produtos e serviços com tranquilidade.

Temos estratégias aplicadas e implementadas visando camadas de segurança, com o objetivo de mitigar todo e qualquer comprometimento das nossas camadas de defesas.

2. OBJETIVO

Esta Política tem como objetivo:

- Proteger as informações e ativos de tecnologia da informação contra acesso, modificação, destruição ou divulgação não autorizados;
- Assegurar a continuidade do processamento das informações críticas ao negócio;
- Cumprir as leis, normas e regulamentos aplicáveis;
- Estabelecer os mecanismos de gestão de riscos cibernéticos.

3. ABRANGÊNCIA

Esta Política aplica-se ao Grupo Shopee e a todas as suas demais coligadas (conjuntamente consideradas simplesmente como “Companhia”), devendo ser seguida por todos os seus colaboradores, parceiros de negócios, terceiros, consultores, fornecedores que transmitam, armazenem ou processem informações pertencentes ou sob a guarda da Shopee

4. DEFINIÇÕES

Para os fins desta Política, os termos abaixo deverão ser assim considerados:

"Colaborador(es)" - refere-se aos acionistas pessoas físicas, administradores, bem como a todos os funcionários da Companhia com vínculo empregatício, incluindo estagiários, menores aprendizes, empregados efetivos, temporários e terceirizados que prestem serviços em nome da Companhia;

"Parceiro(s) de Negócio(s)" - refere-se à pessoa física ou jurídica com quem a Companhia mantém relacionamento, comercial ou não, remunerado ou não, em caráter eventual ou permanente, incluindo, mas não se limitando a prestadores de serviços, fornecedores de produtos, parceiros comerciais, agentes, consultores, advogados, despachantes, corretoras, entre outros;

"Terceiros" - refere-se a quaisquer pessoas físicas ou jurídicas (públicas ou privadas) que não se enquadrem como Colaboradores ou Parceiros de Negócios, conforme definido acima.

5. DIRETRIZES GERAIS

O objetivo do Grupo Shopee é assegurar que todos os nossos Parceiros de Negócios, Fornecedores e Terceiros tenham a melhor experiência possível com nossos produtos e serviços, contando com segurança em suas operações de ponta a ponta. Nossa função é garantir a implementação da Política de Segurança Cibernética, assegurando os seguintes princípios de segurança, considerados inegociáveis para a Companhia:

- Integridade;
- Confidencialidade;
- Disponibilidade.

6. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

O Sistema de Segurança da Informação da Companhia, em consonância com as melhores práticas de mercado, adota os seguintes princípios:

- **Integridade**: assegurar que as informações sejam corretas, precisas, completas e protegidas contra alterações não autorizadas;
- **Confidencialidade:** garantir que as informações sejam acessadas exclusivamente por pessoas devidamente autorizadas;
- **Disponibilidade**: assegurar que as informações estejam acessíveis, no momento necessário, às pessoas autorizadas.

7. PROTEÇÃO DE DADOS E PRIVACIDADE

As informações internas do Grupo Shopee são devidamente classificadas e protegidas por meio de processos rigorosos, que incluem:

- Autenticação;
- Criptografia;
- Proteção contra softwares maliciosos e manutenções não autorizadas;
- Mecanismos de proteção contra cópias indevidas;
- Segmentação de redes; e
- Detecção e prevenção de invasões.

Contamos com um processo robusto de monitoramento e tratamento de incidentes, assegurando a continuidade dos negócios. Realizamos testes e varreduras constantes, mantemos logs de atividades e revisamos periodicamente os acessos e privilégios concedidos.

O compartilhamento de informações com Parceiros de Negócios e Terceiros é conduzido sob critérios rigorosos de conformidade e segurança da informação. Nossa equipe é treinada e comprometida com os mais altos padrões de proteção de dados, garantindo segurança a todos os nossos clientes.

O uso de dados pessoais de Clientes, Parceiros de Negócios e Fornecedores deve estar estritamente alinhado às Políticas Institucionais da Companhia, aos procedimentos de privacidade,

ao Código de Conduta, às diretrizes de Segurança Cibernética e às normas de Compliance, observando os requisitos regulatórios e as melhores práticas do mercado.

8. INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

A Companhia caracteriza como incidente de segurança com dados pessoais qualquer evento adverso confirmado que comprometa a segurança dessas informações ou configure conduta descrita na Política Corporativa. Isso inclui acessos não autorizados, acidentais ou ilícitos que resultem em destruição, perda, alteração, vazamento ou qualquer forma de tratamento inadequado ou ilegal de dados pessoais, os quais possam representar risco aos direitos e liberdades do titular.

9. GESTÃO DE INCIDENTES

A Companhia compromete-se com a implementação de estratégias e estruturas eficazes para o gerenciamento de incidentes, especialmente por meio da adoção das seguintes medidas:

- Identificação de ameaças potenciais e avaliação de seus respectivos impactos;
- Definição de estratégias de recuperação a serem aplicadas em caso de incidentes;
- Estabelecimento de mecanismos de gerenciamento de crise para eventos adversos que interrompam processos críticos;
- Planejamento da continuidade e recuperação das operações e sistemas após uma interrupção;
- Definição de procedimentos para retorno à normalidade, quando aplicável;
- Integração da gestão de continuidade de negócios ao desenvolvimento de novos produtos e serviços críticos, bem como ao processo de gerenciamento de mudanças nos produtos e serviços existentes;
- Garantia da continuidade das operações da Companhia em um nível aceitável e previamente definido;

- Fortalecimento da capacidade de recuperação da Companhia frente a interrupções ou falhas em sua capacidade de fornecer produtos e serviços;
- Direcionamento de ações voltadas à prevenção e mitigação de riscos operacionais;
- Estabelecimento de normas e padrões de continuidade, formando um programa robusto e consistente, a ser seguido por toda a organização, incluindo empresas prestadoras de serviço.

Essas diretrizes devem estar alinhadas ao Plano de Recuperação de Desastres (PRD), o qual contém os detalhes específicos sobre os processos de resposta e recuperação em caso de incidentes.

10 . LEGISLAÇÃO APLICÁVEL

- **Resolução BCB nº 85, de 12 de abril de 2021:** Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil;
- **Resolução CMN nº 4.893, de 26 de fevereiro de 2021**: Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.
- **Lei nº 13. 709, de 14 de agosto de 2018**: Lei Geral de Proteção de Dados Pessoais (LGPD).

11 . DOCUMENTOS RELACIONADOS

- Política de Cibersegurança;
- Política de Gestão de Continuidade de Negócios;
- Manual de Procedimento de Respostas a Incidentes;

- Política de Gerenciamento de Incidente;
- Plano de Recuperação de Desastres.

12. VIGÊNCIA

Esta Política entra em vigor na data indicada no quadro do cabeçalho e deverá ser revisada: (i) obrigatoriamente a cada 12 (doze) meses; (ii) em caso de alteração na legislação aplicável que impacte o disposto neste documento; (iii) quando houver determinação expressa nesse sentido por parte dos órgãos reguladores; (iv) quando houver alterações dos processos internos da Companhia que altere diretrizes aqui descritas.

13. REGISTRO DE ALTERAÇÕES

Versão nº	Data de Elaboração	Elaborador	Descrição de Mudanças
1.0	Maio/2023	Área de Segurança da Informação	Versão Inicial
2.0	Junho/2024	Área de Segurança da Informação	Inclusão do capítulo “8. Incidente de segurança com dados pessoais”; “9. Gestão de incidentes”; “10. Legislação aplicável”; “11. Documentos relacionados”; “13. Registro de alterações”, bem como inclusão do Grupo Shopee.
3.0	Julho/2025	Área de Segurança da Informação	Revisão Anual e Inserção da Resolução CMN nº 4.893/2021.