
	Tipo de Documento: POLÍTICA CORPORATIVA	Data de Vigência: Julho/2024
Classificação de Publicidade: PÚBLICO EXTERNO	Nome do Documento: POLÍTICA DE CIBERSEGURANÇA PARA TERCEIROS	Versão: v1.0/2024

Política de Segurança Cibernética para Terceiros

Elaboração e Responsabilidade: ÁREA DE SEGURANÇA CIBERNÉTICA	Aprovação: DIRETORIA EXECUTIVA
Data: Junho/2024	Data: Julho/2024

NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTE DOCUMENTO O TORNA UMA CÓPIA NÃO CONTROLADA


	<p>Tipo de Documento: POLÍTICA CORPORATIVA</p>	<p>Data de Vigência: Junho/2024</p>
<p>Classificação de Publicidade: PÚBLICO EXTERNO</p>	<p>Nome do Documento: POLÍTICA DE CIBERSEGURANÇA PARA TERCEIROS</p>	<p>Versão: v2.0/2024</p>

Índice

1. INTRODUÇÃO.....	3
2. OBJETIVO.....	3
3. ABRANGÊNCIA.....	3
4. DEFINIÇÕES.....	4
5. DIRETRIZES GERAIS.....	4
6. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO.....	5
7. PROTEÇÃO DE DADOS E PRIVACIDADE.....	5
8. INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS.....	6
9. GESTÃO DE INCIDENTES.....	6
10 . LEGISLAÇÃO APLICÁVEL.....	7
11 . DOCUMENTOS RELACIONADOS.....	7
12. VIGÊNCIA.....	8
13. REGISTRO DE ALTERAÇÕES.....	8

<p>Elaboração e Responsabilidade: ÁREA DE SEGURANÇA CIBERNÉTICA</p>	<p>Aprovação: DIRETORIA EXECUTIVA</p>
<p>Data: Junho/2024</p>	<p>Data: Junho/2024</p>

NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTE DOCUMENTO O TORNA UMA CÓPIA NÃO CONTROLADA

	Tipo de Documento: POLÍTICA CORPORATIVA	Data de Vigência: Junho/2024
Classificação de Publicidade: PÚBLICO EXTERNO	Nome do Documento: POLÍTICA DE CIBERSEGURANÇA PARA TERCEIROS	Versão: v2.0/2024

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:


- (i) Proteger as informações e ativos de tecnologia da informação contra acesso, modificação, destruição ou divulgação não autorizados;
- (ii) Assegurar a continuidade do processamento das informações críticas ao negócio;
- (iii) Cumprir as leis, normas e regulamentos aplicáveis;
- (iv) 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

Elaboração e Responsabilidade: ÁREA DE SEGURANÇA CIBERNÉTICA	Aprovação: DIRETORIA EXECUTIVA
Data: Junho/2024	Data: Junho/2024

NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTE DOCUMENTO O TORNA UMA CÓPIA NÃO CONTROLADA

	Tipo de Documento: POLÍTICA CORPORATIVA	Data de Vigência: Junho/2024
Classificação de Publicidade: PÚBLICO EXTERNO	Nome do Documento: POLÍTICA DE CIBERSEGURANÇA PARA TERCEIROS	Versão: v2.0/2024

4. DEFINIÇÕES

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

“Colaborador(es)” - significa(m) os acionistas pessoas físicas, os administradores, bem como todos os funcionários da Companhia com vínculo empregatício, estagiários, menores aprendizes, empregados efetivos, temporários e terceirizados que prestem serviço em nome da Companhia;

“Parceiro(s) de Negócio(s)” - significa a 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 etc;

“Terceiros” - significa quaisquer pessoas ou empresas (públicas ou privadas) que não se enquadrem como Colaboradores ou Parceiros de Negócios, conforme conceituado acima.

5. DIRETRIZES GERAIS


O objetivo do Grupo Shopee é garantir que todos os nossos Parceiros de Negócios, Fornecedores e Terceiros tenham uma melhor experiência dos nossos produtos e serviços contando com uma segurança em suas operações de ponta a ponta. A nossa função é garantir que a nossa Política de Segurança Cibernética seja implementada, garantindo assim a: (i) integridade, (ii) confidencialidade e, (iii) disponibilidade, princípios de segurança inegociáveis para a Companhia.

6. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

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

Elaboração e Responsabilidade: ÁREA DE SEGURANÇA CIBERNÉTICA	Aprovação: DIRETORIA EXECUTIVA
Data: Junho/2024	Data: Junho/2024

NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTES DOCUMENTOS TORNA UMA CÓPIA NÃO CONTROLADA

	<p>Tipo de Documento: POLÍTICA CORPORATIVA</p>	<p>Data de Vigência: Junho/2024</p>
<p>Classificação de Publicidade: PÚBLICO EXTERNO</p>	<p>Nome do Documento: POLÍTICA DE CIBERSEGURANÇA PARA TERCEIROS</p>	<p>Versão: v2.0/2024</p>

- **Integridade:** garantir informações corretas e precisas, completas e protegidas.
- **Confidencialidade:** garantir que as informações sejam acessadas apenas por pessoas autorizadas.
- **Disponibilidade:** garantir que as informações sejam disponíveis apenas a pessoas autorizadas.

7. PROTEÇÃO DE DADOS E PRIVACIDADE

As informações internas do Grupo Shopee são devidamente classificadas e passam por processos de (i) autenticação, (ii) criptografia, (iii) proteção contra softwares maliciosos, manutenções, (iv) proteções contra cópias indevidas, (v) segmentações de rede e (vi) detecção e prevenção de invasão. Temos um rigoroso processo de monitoramento e tratativa de incidentes, garantindo a continuidade dos negócios e realizando testes e varreduras constantes, mantendo logs e revisando periodicamente os acessos e privilégios.


O compartilhamento de informações com Parceiros de Negócios e Terceiros do Grupo Shopee é controlado com rigor em termos de conformidade e segurança da informação. Nossa equipe é comprometida e treinada para garantir o mais alto nível de segurança da informação para todos os nossos clientes.

Todo o uso de dados pessoais de Clientes, Parceiros de Negócios e Fornecedores devem estar aderentes às Políticas Institucionais da Companhia e os procedimentos de privacidade, Código de Conduta, Segurança Cibernética e Compliance, devendo atender os requisitos regulatórios e melhores práticas do mercado.

8. INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

<p>Elaboração e Responsabilidade: ÁREA DE SEGURANÇA CIBERNÉTICA</p>	<p>Aprovação: DIRETORIA EXECUTIVA</p>
<p>Data: Junho/2024</p>	<p>Data: Junho/2024</p>

NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTES DOCUMENTOS TORNA UMA CÓPIA NÃO CONTROLADA

	Tipo de Documento: POLÍTICA CORPORATIVA	Data de Vigência: Junho/2024
Classificação de Publicidade: PÚBLICO EXTERNO	Nome do Documento: POLÍTICA DE CIBERSEGURANÇA PARA TERCEIROS	Versão: v2.0/2024

A Companhia caracteriza que o incidente de segurança com dados pessoais é considerado qualquer evento adverso confirmado que viole a segurança de dados pessoais ou desempenha conduta descrita na Política Corporativa, tal como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdade do titular de dos dados pessoais.


9. GESTÃO DE INCIDENTES

A Companhia compromete-se a implementação de estratégias e estruturas de gerenciamento de incidentes, especialmente, na adoção das seguintes medidas que são:

- Identificação das ameaças potenciais e os respectivos impactos;
- Definição da estratégia de recuperação a ser utilizada caso ocorra um incidente;
- Gerenciamento de Crise para incidentes adversos que interrompam um processo crítico;
- Planejamento da continuidade e da recuperação das operações e sistemas após uma interrupção;
- Estabelecimento de procedimentos de retorno da normalidade, quando aplicável;
- Incorporar a gestão da continuidade de negócio ao desenvolvimento de novos produtos e serviços críticos e ao processo de gerência de mudanças para produtos e serviços existentes;
- Prover a continuidade das operações do negócio em um nível aceitável pré-definido;
- Aumentar o poder de recuperação da Companhia contra o rompimento ou interrupção de sua habilidade de fornecer seus produtos e serviços;

Elaboração e Responsabilidade: ÁREA DE SEGURANÇA CIBERNÉTICA	Aprovação: DIRETORIA EXECUTIVA
Data: Junho/2024	Data: Junho/2024

NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTES DOCUMENTOS TORNA UMA CÓPIA NÃO CONTROLADA

	Tipo de Documento: POLÍTICA CORPORATIVA	Data de Vigência: Junho/2024
Classificação de Publicidade: PÚBLICO EXTERNO	Nome do Documento: POLÍTICA DE CIBERSEGURANÇA PARA TERCEIROS	Versão: v2.0/2024

- Orientar ações de prevenção e mitigação dos riscos operacionais;
- Fixar normas e padrões de continuidade, compondo assim, um programa completo e consistente para a organização, devendo ser aceito e seguido inclusive pelas empresas prestadoras de serviço.

Neste sentido, os critérios mencionados acima, devem estar em consonância com o Plano de Recuperação de Desastres (PRD), para obtenção de maiores detalhes sobre o processo de recuperação de um incidente.

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;
- 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

Elaboração e Responsabilidade: ÁREA DE SEGURANÇA CIBERNÉTICA	Aprovação: DIRETORIA EXECUTIVA
Data: Junho/2024	Data: Junho/2024

NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTES DOCUMENTOS TORNA UMA CÓPIA NÃO CONTROLADA

	Tipo de Documento: POLÍTICA CORPORATIVA	Data de Vigência: Junho/2024
Classificação de Publicidade: PÚBLICO EXTERNO	Nome do Documento: POLÍTICA DE CIBERSEGURANÇA PARA TERCEIROS	Versão: v2.0/2024

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	Segunda Versão

Elaboração e Responsabilidade: ÁREA DE SEGURANÇA CIBERNÉTICA	Aprovação: DIRETORIA EXECUTIVA
Data: Junho/2024	Data: Junho/2024

NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTES DOCUMENTOS TORNA UMA CÓPIA NÃO CONTROLADA