## 1. PÚBLICO-ALVO E OBJETIVOS

**1.1.** Esta Política estabelece as diretrizes de Segurança Cibernética para proteger as Informações, os sistemas, os Ativos Tecnológicos e os serviços do Grupo Listo, de seus Clientes e de seus Parceiros, por meio de práticas de prevenção, detecção, resposta e melhoria contínua contra riscos e incidentes cibernéticos.

**1.2.** A Segurança Cibernética é conduzida de forma compatível com o porte, o perfil de risco, o modelo de negócio, a natureza das atividades e a sensibilidade das Informações sob responsabilidade do Grupo Listo.

**1.3.** As diretrizes da Política aplicam-se a todos os Colaboradores e, conforme a natureza da relação e dos serviços prestados, a Clientes, Parceiros, fornecedores e demais terceiros que utilizem, administrem, processem, armazenem, transmitam ou tenham acesso a Informações, sistemas ou Ativos Tecnológicos do Grupo Listo.

**1.4.** A proteção abrange ambientes físicos e digitais, instalações próprias, ambientes de terceiros e serviços de computação em nuvem, durante todo o ciclo de vida das Informações e dos recursos tecnológicos.

## 2. DIRETRIZES PARA SEGURANÇA DA INFORMAÇÃO

**2.1.** **Segurança da Informação**. Entende-se por Segurança da Informação o conjunto de princípios, processos e controles destinados a proteger as Informações durante todo o seu ciclo de vida, assegurando prioritariamente sua confidencialidade, integridade e disponibilidade, bem como autenticidade, rastreabilidade, legalidade, responsabilização e melhoria contínua, quando aplicáveis.

a) **Integridade**: processo responsável por garantir que qualquer Informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
b) **Confidencialidade**: processo responsável por garantir que o acesso à Informação seja obtido somente por Colaboradores autorizados;
c) **Disponibilidade**: processo responsável por garantir que todos os Colaboradores autorizados tenham acesso à Informação e aos ativos correspondentes sempre que necessário;
d) **Legalidade**: processo responsável por garantir que as Políticas e procedimentos internos estejam alinhados as das Leis, Políticas e Normas aplicáveis;
e) **Responsabilidade**: processo responsável por garantir que todos os Colaboradores compreendam e cumpram suas obrigações quanto à proteção das Informações; e
f) **Melhoria contínua**: processo responsável por garantir a revisão contínua dos controles e processos internos visando seu aprimoramento.

2.1.1. A Informação é um Ativo essencial para as atividades do Grupo Listo e deve ser protegida de acordo com sua classificação, criticidade, finalidade e requisitos aplicáveis. Todos os Colaboradores e terceiros abrangidos por esta Política devem adotar comportamento seguro e observar os controles estabelecidos para sua proteção.

## 3. DIRETRIZES PARA GOVERNANÇA

**3.1.** A governança de Segurança Cibernética conta com o compromisso da Administração e com responsabilidades definidas para aprovação, implementação, acompanhamento e revisão da Política. Os riscos, indicadores, incidentes relevantes e planos de ação são reportados às instâncias competentes de acordo com sua criticidade.

**3.2.** A Política e o Plano de Ação e de Resposta a Incidentes são documentados, aprovados e revisados, no mínimo, anualmente e sempre que mudanças relevantes de risco, regulamentação, tecnologia, modelo de negócio ou incidentes relevantes justificarem sua atualização.

## 4. DIRETRIZES PARA PROTEÇÃO DO AMBIENTE

**4.1. Controles de Segurança Cibernética.** O Grupo Listo adota controles técnicos e administrativos compatíveis com os riscos e a criticidade de suas Informações, sistemas, serviços e Ambientes, incluindo:

a) **Gestão de Acessos:** concessão, revisão e bloqueio de acessos de forma individual, pessoal e intransferível, observando os princípios do menor privilégio e da necessidade de acesso, bem como mecanismos reforçados de autenticação, quando aplicáveis;
b) **Proteção da Informação:** proteção das Informações durante sua coleta, utilização, armazenamento, transmissão, retenção e descarte**;**
c) **Configuração Segura e Proteção de Rede**: aplicação de configurações seguras, atualizações e correções periódicas, proteção dos ambientes críticos, controle das conexões e adoção de medidas destinadas a prevenir acessos e comunicações não autorizados;
d) **Criptografia:** utilização de mecanismos criptográficos e controles de gestão de chaves compatíveis com a classificação das Informações, os riscos envolvidos e os requisitos legais, regulatórios e técnicos aplicáveis, para proteger Informações, credenciais e certificados;
e) **Monitoramento e Controle:** monitoramento de eventos, manutenção de registros e adoção de mecanismos de rastreabilidade para prevenir e detectar acessos indevidos, códigos maliciosos, intrusões e vazamentos de Informações;
f) **Gestão de Vulnerabilidades:** identificação, avaliação, priorização e correção de vulnerabilidades, incluindo a realização periódica de testes e avaliações;
g) **Desenvolvimento e Integração Seguros:** adoção de requisitos de segurança no desenvolvimento, na aquisição, na implantação e na integração de sistemas e novas tecnologias;
h) **Cópias de Segurança:** realização de cópias de segurança e testes periódicos de recuperação, de acordo com a criticidade das Informações e dos serviços; e

i) **Avaliação e Melhoria Contínua**: avaliação periódica da efetividade dos controles e tratamento das deficiências identificadas.

**4.2. Gestão de Riscos Cibernéticos:** O Grupo Listo mantém processo contínuo de identificação, avaliação, priorização, tratamento, monitoramento e revisão dos riscos de Segurança Cibernética. O processo considera a criticidade dos Ativos, sistemas, serviços, tecnologias e terceiros envolvidos, bem como os possíveis impactos sobre as operações e as partes afetadas.

**4.3. Gestão de Incidentes de Segurança:** O Grupo Listo mantém processos para identificar, registrar, classificar, investigar, conter e tratar incidentes de Segurança Cibernética, recuperar os serviços afetados, preservar evidências e incorporar as lições aprendidas. Quando aplicável, os incidentes relevantes são comunicados às autoridades, aos reguladores, aos titulares e às demais partes afetadas, conforme a legislação, a regulamentação e as obrigações contratuais vigentes.

**4.4. Gestão do Ambiente**: Os ambientes tecnológicos utilizados pelo Grupo Listo na prestação de serviços financeiros e de pagamentos devem observar os requisitos de segurança estabelecidos pelo Banco Central do Brasil, bem como os demais requisitos regulatórios e técnicos aplicáveis.

## 5. DIRETRIZES PARA GERENCIAMENTO DE TERCEIROS E SERVIÇOS EM NUVEM

**5.1.** Fornecedores, Parceiros e prestadores de serviços que tenham acesso a Informações, sistemas ou processos do Grupo Listo são avaliados de acordo com o risco, a criticidade do serviço e a natureza das Informações envolvidas.

**5.2.** As contratações relevantes, inclusive de processamento, armazenamento de Dados e computação em nuvem, contemplam requisitos de segurança, privacidade, continuidade, monitoramento, comunicação de incidentes, gestão de subcontratados, acesso a evidências e encerramento seguro do serviço, conforme a regulamentação e os contratos aplicáveis.

## 6. DIRETRIZES PARA CONTINUIDADE DOS SERVIÇOS

**6.1.** O Grupo Listo mantém planos de continuidade de negócios e de resposta a incidentes para sustentar ou recuperar processos e serviços críticos diante de indisponibilidades e eventos adversos. Esses planos consideram responsabilidades, dependências, estratégias de recuperação, canais de comunicação e testes periódicos.

## 7. DIRETRIZES PARA PROTEÇÃO DE DADOS PESSOAIS

**7.1.** O tratamento de Dados Pessoais observa os princípios e requisitos da legislação aplicável. Incidentes que envolvam Dados Pessoais são avaliados quanto ao risco ou dano relevante e, quando aplicável, comunicados à Autoridade Nacional de Proteção de Dados e aos titulares afetados, nos prazos e nas condições previstos na regulamentação vigente.

## 8. CONSCIENTIZAÇÃO E RESPONSABILIDADES

**8.1.** O Grupo Listo promove ações de conscientização e capacitação para fortalecer a cultura de Segurança Cibernética. Colaboradores e terceiros devem observar as diretrizes e os controles aplicáveis às suas atividades, proteger credenciais e Informações e comunicar prontamente suspeitas, fragilidades ou incidentes pelos canais estabelecidos.

**8.2.** Clientes e usuários devem adotar práticas seguras na utilização dos produtos e serviços, manter seus dispositivos protegidos, não compartilhar senhas ou códigos de autenticação e verificar a legitimidade das comunicações recebidas.

## 9. COMUNICAÇÃO DE SUSPEITAS E INCIDENTES

**9.1.** Qualquer suspeita de fraude, uso indevido de informações ou evento que comprometa a segurança dos produtos e serviços do Grupo Listo deve ser relatada através dos canais oficiais de atendimento disponíveis no site institucional: infosec@soulisto.com.br.

## 10. REVISÃO E VIGÊNCIA

**10.1.** Este resumo público será revisado, no mínimo, anualmente e sempre que houver alteração relevante na Política Institucional de Segurança Cibernética ou nas obrigações legais e regulatórias aplicáveis.

## 11. APROVAÇÃO

Aprovada em 03/11/2026.

Grupo Listo
Olavo Viana Cabral Netto
Diretor Presidente

## ANEXO I- GLOSSÁRIO

| NOME | DEFINIÇÃO |
|---|---|
| **Ativo** | qualquer recurso, informação, pessoa, serviço, processo, sistema, equipamento, infraestrutura ou outro elemento que possua valor para o Grupo Listo e necessite proteção compatível com sua criticidade. |
| **Colaboradores** | funcionários do Grupo Listo, parceiros e/ou empresas prestadoras de serviços contratadas com finalidade especificada e prazo determinado. |
| **Criptografia** | conjunto de técnicas matemáticas e mecanismos destinados a proteger Dados e Informações por meio de propriedades como confidencialidade, integridade, autenticidade e não repúdio, conforme o mecanismo utilizado. |
| **Dado** | representação elementar de fatos, eventos, atributos ou valores que pode ser armazenada, processada ou transmitida e que, quando contextualizada, pode compor uma Informação. |
| **Grupo Listo** | nome Dado ao conjunto de empresas que integram o Grupo incluindo coligadas, subsidiárias e controladas diretas e indiretas. |
| **Informação** | conjunto ou consolidação dos Dados de forma a fundamentar o conhecimento. |
| **Vulnerabilidade** | fragilidade em sistema, processo, configuração, componente, controle ou comportamento que pode ser explorada por uma Ameaça e resultar em impacto de Segurança da Informação ou Segurança Cibernética |