1. PÚBLICO-ALVO E OBJETIVOS

1.1. Esta Política de Segurança da Informação tem como objetivo estabelecer as diretrizes das empresas do Grupo Listo (ou, simplesmente, a "Listo") para a proteção dos Ativos de Informação e a mitigação dos riscos, garantindo a confiabilidade, integridade e disponibilidade de Informações. Essas diretrizes abrangem os principais requisitos de segurança:

a) **Integridade**: garantia de autenticidade da Informação, que a Informação seja mantida no seu estado inicial e que tem origem em fonte anunciada, de modo que seja possível confirmar a sua autoria e originalidade;
b) **Confidencialidade**: garantia de que os acessos às Informações sejam disponibilizados somente por Usuários autorizados; e
c) **Disponibilidade**: garantia de que os Usuários autorizados tenham acesso à Informação e aos ativos, de acordo com o necessário.

1.2. A Política de Segurança da Informação é destinada ao controle dos Ativos de Informação, sendo composta por um conjunto de práticas que protegem as Informações desde a Classificação da Informação até quem pode acessá-la.

1.3. As diretrizes apresentadas nesta Política aplicam-se a todos os Colaboradores, prestadores e parceiros que utilizam direta ou indiretamente os sistemas de informação da Listo, os quais são também, responsáveis pela segurança dos Ativos do Grupo Listo, estando estes cientes de seu compromisso com a proteção e uso adequado da Informação.

1.4. As diretrizes estabelecidas nesta Política se aplicam tanto para o ambiente informatizado, quanto para os Ativos de qualquer natureza que capture, armazene, transmita ou processe Informações do Grupo Listo, procurando sempre estar aderente as Normas e melhores práticas de mercado utilizando metodologia inerentes a segurança de Dados.

2. DIRETRIZES

2.1. Comportamento seguro. Entende-se por comportamento seguro o conjunto de práticas que protegem todo o ciclo de vida da Informação desde a coleta até o expurgo, garantindo a integridade, disponibilidade e confidencialidade.

2.1.1. A Informação é um Ativo muito importante para a Listo, e, por esse motivo, este bem deve ser preservado em qualquer forma que exista. Por isso, é importante que todos os Colaboradores adotem comportamento seguro com o objetivo de proteger as Informações pertencentes à Listo.

2.1.2. Todos os Colaboradores devem assumir atitude proativa no que diz respeito à proteção das Informações da Listo, para isto, devem compreender sobre as Ameaças internas ou externas que podem afetar a Segurança das Informações da Listo, tais como pragas digitais, acesso não autorizado, indisponibilidade, uso indevido de imagem, interceptação de mensagens eletrônicas, engenharia social, uso de dispositivos não autorizados e homologados ao ambiente, acesso a conteúdo suspeito e malicioso, bem como fraudes.

2.1.3. São proibidos todos os acessos à Informação da Listo, bem como seu transporte em qualquer tipo de mídia sem as devidas proteções quando não forem explicitamente autorizados.

2.1.4. Todos os Colaboradores devem utilizar o padrão de assinatura definido pelo Grupo Listo, não sendo autorizado modificações em seus elementos e/ou substituições de Informações previamente compartilhadas.

2.1.5. As senhas de Usuários ou de acesso devem ser pessoais e intransferíveis, não podendo ser reveladas, compartilhadas, registradas em locais vulneráveis, como papel, etiquetas e dispositivos eletrônicos, bem como sua criação não deve ser de fácil dedução e descobrimento por parte de pessoas mal-intencionadas.

2.1.6. Todos os Colaboradores devem utilizar crachás de identificação nas dependências da Listo em local visível e com a sua identificação voltada para frente.

2.1.7. Todos os Visitantes devem usar uma rede segmentada unicamente com acesso à internet e sem qualquer comunicação com a rede da Listo.

a) devem estar adequadamente identificados, física e sistemicamente, e devem ter seu acesso aprovado e formalizado conforme as regras dos edifícios onde se encontram as dependências da Listo e as regras do Grupo Listo;
b) os Colaboradores não devem permitir que Visitantes tirem fotos e/ou realizem gravações nas dependências da Listo sem serem devidamente autorizados; e
c) caso algum comportamento suspeito seja identificado, o Colaborador deve entrar em contato com o Núcleo de Segurança da Informação, não permitindo que o Visitante circule livremente por áreas estratégicas.

2.1.8. É terminantemente proibido copiar, armazenar ou compartilhar Código Fonte, Dados de Cartão e documentos estratégicos classificados como confidenciais, restritos e/ou internos se utilizando de dispositivos não homologados ou não aprovados pelo Grupo Listo.

2.1.9. Assuntos confidenciais só podem ser falados/comentados em áreas restritas da Listo, não podendo ser reveladas em ambientes públicos, como elevadores, taxis, restaurantes, redes sociais, comunidade de desenvolvedores, dentre outros.

2.1.10. Todos os documentos devem ter sua Informação classificada conforme o grau de confidencialidade orientado nas regras corporativas de Classificação da Informação.

2.1.11. Todos os Colaboradores deverão utilizar Equipamentos da Listo homologados pelo Núcleo de Infraestrutura e que possuam as regras e controles de segurança estabelecidos pelo Núcleo de Segurança da Informação.

a) os Equipamentos da Listo não devem ser utilizados para fins pessoais, estando o seu propósito limitado ao uso dos serviços corporativos, sendo proibido também, o vínculo de quaisquer sistemas internos da Listo com quaisquer dispositivos pessoais, exceto se previamente autorizados pelo Núcleo de Segurança da Informação;

b) todos os Dispositivos Móveis pertencentes à Listo devem possuir um meio de segurança individual, tais como: senha de acesso, Criptografia e/ou demais tecnologias de múltiplo fator de autenticação segura; e
c) todos os Equipamentos que tenham capacidade de armazenamento de Dados, devem possuir algum tipo tecnologia de proteção: (i) contra *Malwares* e outras pragas digitais sempre atualizado; (ii) navegação internet e/ou *proxy*; (iii) identificação e Varredura de Vulnerabilidades; (iv) contra o vazamento de Dados e Informações; e (v) contra perda e integridade como Criptografia de disco e senha de BIOS (*Basic Input/Output System*); e
d) todos os Equipamentos devem possuir tecnologia de monitoração para: (i) detectar acessos não autorizados; (ii) estar ingressados em domínio corporativo e/ou tecnologia equivalente que permita gestão a partir de serviço de diretórios; e (iii) identificar Vulnerabilidades.

2.1.12. Ao utilizar **espaços comuns**, as Informações ou anotações da lousa devem ser apagadas e desfragmentadas quando aplicável.

2.1.13. **Não é permitido:**

a) fotografar documentos, Informações ou anotações (mesmo nas lousas das salas de reunião), copiar, transferir e/ou armazenar documentos da Listo, mediante a sua classificação, através de discos rígidos locais, mídias eletrônicas removíveis, transferências sistêmicas e comunicadores instantâneos;
b) encaminhar quaisquer Informações corporativas para **e-mails pessoais**;
c) uso de VPN Corporativa em Equipamentos pessoais ou uso destes para quaisquer conexões físicas ou remotas as redes da Listo, da mesma forma para uso por terceiros sem aprovação formalizada;
d) personalizar o Equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio ou promover qualquer modificação que altere as características originais do equipamento;
e) a abertura e/ou automanutenção de Equipamentos para qualquer tipo de atividade, bem como a instalação de *softwares* ou sistemas nas estações de trabalho pelos Colaboradores. Estes procedimentos só poderão ser realizados pelo Núcleo de Infraestrutura de acordo com Políticas e Normas internas; e
f) a navegação na internet a partir dos Equipamentos e redes da Listo a portais de conteúdo malicioso, impróprio ou que exponha a Listo a riscos.

2.1.14. **Mesa e Tela limpa**

a) as estações de trabalho devem permanecer bloqueados (*logoff*) nos períodos de ausência do Colaborador e devem ser desligados ao término do expediente, diminuindo o período de exposição à ataques e invasões;
b) ao utilizar um recurso de uso comum, como sala de reuniões ou estações de teste, é de responsabilidade do Colaborador remover as Informações, sessões ou credenciais que foram utilizadas anteriormente; e
c) Informações impressas devem ser armazenadas corretamente ao se ausentar da sua estação de trabalho.

3. PAPÉIS E RESPONSABILIDADES

Todos os Colaboradores são responsáveis pela Segurança da Informação, tendo estes um papel fundamental para garantir a confiabilidade, integridade e disponibilidade das informações.

3.1. Comitê Executivo

3.1.1. Aprovar e revisar, com frequência mínima de dois anos, as políticas e estratégias para Segurança da Informação e assegurar sua aplicação.

3.1.2. Analisar, debater e aprovar os temas relativos ao objeto deste documento, assim como todas as revisões necessárias, com periodicidade mínima anual.

3.1.3. Autorizar, quando necessário, exceções às políticas e aos procedimentos estabelecidos.

3.1.4. Ser exemplo aos demais responsáveis, cumprindo todas as diretrizes descritas neste documento.

3.1.5. Requerer que todos os responsáveis do Grupo Listo cumpram com as suas responsabilidades quanto aos termos relacionados a este documento.

3.2. Administradores

3.2.1. Apoiar e incentivar o engajamento de todos os Colaboradores do Grupo Listo a cumprirem suas responsabilidades quanto à Segurança da Informação.

3.2.2. Analisar, debater e aprovar esta Política.

3.2.3. Tomar decisões administrativas referentes aos casos de descumprimento desta Política e/ou de suas normas aplicáveis.

3.2.4. Revisar este documento e os seus respectivos investimentos, processos e pessoas.

3.2.5. Ser exemplo aos demais responsáveis do Grupo Listo, cumprindo todas as diretrizes descritas nesta Política.

3.2.6. Debater e tomar decisão sobre solicitações vindas dos Núcleos de Infraestrutura e de Segurança da Informação.

3.3. Gestores

3.3.1. Disseminar a ideia de Segurança da Informação e o conhecimento das Normas técnicas com as suas respectivas equipes.

3.3.2. Determinar responsáveis em cada uma das gerências, para que estes desenvolvam documentação de processos operacionais que sigam esta Política.

3.3.3. Garantir que todos os Colaboradores tenham os treinamentos adequados sobre Segurança da Informação para o exercício de suas atividades.

3.3.4. Receber primariamente toda e qualquer Informação de suspeita de violação de segurança por parte de Colaboradores bem como filtrar e direcionar solicitação ao Núcleo de Segurança da Informação, para que este avalie possíveis eventos.

3.4. Núcleo de Segurança da Informação

3.4.1. Desenvolver, propor, melhorar as Políticas e Normas de Segurança da Informação.

3.4.2. Ser agente facilitador para a implantação dos controles descritos nesta Política, nas Normas ou qualquer outra documentação técnica desenvolvida no Grupo Listo.

3.4.3. Ser agente facilitador para a implantação de controles identificados no processo de gestão de Vulnerabilidades.

3.4.4. Atuar no processo de monitoramento e resposta a incidentes de Segurança da Informação.

3.4.5. Realizar auditorias e testes periódicos visando o cumprimento das diretrizes previstos neste documento.

3.4.6. Monitorar e analisar os alertas e Informações de segurança, distribuindo-as para as equipes apropriadas.

3.4.7. Gerir, mapear, documentar e compartilhar toda Vulnerabilidade identificada, bem como sua forma de mitigação, prevenção ou remediação com as equipes responsáveis pelo tratamento.

3.4.8. Mapear as Ameaças e os possíveis riscos de segurança e seus respectivos impactos para correta mitigação ou tratamento destes para viabilidade da continuidade de negócio.

3.4.9. Trabalhar em conjunto com o Núcleo de Recursos Humanos com objetivo de criar e disseminar treinamentos de conscientização da Segurança da Informação para todos os Colaboradores da Listo.

3.4.10. Acompanhar os controles referentes à Segurança da Informação e que atendam ao programa PCI e demais regulações nacionais ou internacionais de segurança da informação ou cibernética.

3.4.11. Implementar programas de gestão de conformidade de segurança para medição, acompanhamento e das regras de segurança aqui previstas e em documentos de apoio.

3.4.12. Revisar esta Política anualmente ou sempre que se fizer necessário.

3.4.13. Analisar os casos de descumprimento desta Política e Normas de Segurança da Informação, encaminhando-os para a Diretoria, quando necessário.

3.5. Núcleo de Desenvolvimento

3.5.1. Criar, desenvolver e manter Código Fonte de aplicações utilizadas pelas empresas do Grupo Listo em local repositório seguro e homologado para o Grupo Listo.

3.5.2. Não copiar, reproduzir ou compartilhar integral ou parcialmente qualquer parte do Código Fonte das aplicações em ambientes externos.

3.5.3. Utilizar de boas práticas e métodos de desenvolvimento seguro no desenvolvimento das aplicações das empresas do Grupo Listo.

3.5.4. Analisar e tratar as Vulnerabilidades sistêmicas que venham a comprometer a continuidade do negócio.

3.5.5. Participar dos treinamentos de desenvolvimento seguro.

3.6. Núcleo de Infraestrutura

3.6.1. Criar, desativar e/ou remover acessos de Colaboradores desligados da Listo, após o desvinculo do mesmo, assim como gerenciar e monitorar os Visitantes habilitando as contas de acesso somente no momento da prestação do serviço/suporte e desabilitando-as imediatamente após a realização do trabalho.

3.6.2. Garantir que todos os Equipamentos destinados a Colaboradores possuam pacotes de *softwares standard* e aplicativos homologados para o Grupo Listo.

3.6.3. Garantir e manter atualizado o inventário de Equipamentos tecnológicos durante todo o ciclo de vida do Ativo.

3.6.4. Tratar as Vulnerabilidades tecnológicas que venham a comprometer a continuidade do negócio.

3.6.5. Garantir que todos os Ativos do tipo Servidor, Componentes de Sistema e demais componentes de infraestrutura tecnológica possuam os recursos tecnológicos homologados.

3.6.6. Gerenciar o ambiente de Dados de Cartão com total segurança, responsabilidade e estabilidade devido a serem os únicos a possuir acesso a tal.

3.6.7. Manter, efetuar e garantir a preservação dos Dados hospedados nas infraestruturas tecnológicas em backup a partir da sua sensibilidade para continuidade dos processos.

3.7. Núcleo de Compliance

3.7.1. Ser curador do presente documento.

3.7.2. Garantir que o documento esteja atualizado de acordo com a sua periodicidade mínima.

3.7.3. Ser agente facilitador para implantação dos controles descritos neste documento ou qualquer outro documento relacionado.

3.7.4. Exigir que o Núcleo de Segurança da Informação envie os relatórios de monitoramento sobre o cumprimento das diretrizes deste documento com a periodicidade mínima trimestral.

3.7.5. Reportar ao Comitê Executivo e à Diretoria quaisquer desvios no cumprimento das diretrizes deste documento.

3.7.6. Analisar casos de descumprimento deste documento, encaminhando-os para o Núcleo Jurídico, quando necessário.

3.8. Núcleo de Recursos Humanos

3.8.1. Trabalhar em conjunto com o Núcleo de Segurança da Informação, com o objetivo de criar e disseminar treinamentos de conscientização da Segurança da Informação para todos os Colaboradores da Listo.

3.8.2. Garantir que todos os Colaboradores da Listo tenham ciência das diretrizes de Segurança da Informação presentes na Política.

3.8.3. Manter os termos assinados por todos os Colaboradores, referente à ciência das informações contidas na Política de Segurança da Informação.

3.8.4. Comunicar o desligamento de Colaboradores aos Núcleos de Infraestrutura e Segurança da Informação, para que sejam desabilitados/removidos todos os acessos da pessoa desligada.

3.9. Colaboradores

3.9.1. Ter ciência das Políticas, Normas e Procedimentos de Segurança da Informação da Listo, bem como as penalidades legais quando do descumprimento destas.

3.9.2. Não conectar à rede da Listo qualquer Ativo tecnológico para uso nas dependências da Listo sem prévia autorização do Núcleo de Segurança da Informação e ciência do Núcleo de Infraestrutura.

3.9.3. Ter ação proativa e informar imediatamente ao Núcleo de Segurança da Informação quando ocorrer, presenciar ou souber da ocorrência ou suspeita de incidentes de Segurança da Informação ou ações que não estejam condizentes com as Políticas internas e cultura de segurança da Listo.

3.9.4. Reportar imediatamente toda e qualquer suspeita relacionada a uma possível falha de Segurança da Informação, Ameaça externa ou quando há suspeita de que documentos, Dados ou Informação Confidencial estejam em posse indevida e que seu uso poderá incorrer em prática de concorrência desleal.

3.9.5. Participar sempre que solicitado dos treinamentos regulares de conscientização, capacitação ou reforço das práticas de segurança da Informação.

3.9.6. Reconhecer e concordar que, em razão dos serviços prestados para a Listo, poderá ter acesso a Informações Confidenciais ou criá-las no desempenho de suas atividades e comprometer-se a, por si e por seus sucessores, manter o mais completo e absoluto sigilo e não divulgar, revelar, publicar, reproduzir, comunicar, emprestar, sublicenciar, comercializar, ceder, transferir, distribuir, locar, modificar, traduzir, fazer engenharia reversa, discutir e/ou utilizar, em benefício próprio ou de terceiros, no todo ou em parte e a que título for, as Informações Confidenciais de que venha a tomar conhecimento.

3.9.7. Cumprir todas as diretrizes descritas na Política e Normas de Segurança da Informação.

4. PROPRIEDADE INTELECTUAL

4.1. Todos os documentos produzidos por intermédio de recurso de processamentos da Listo são de propriedade da Listo, assim como, todo e qualquer registro de Dados, voz e/ou imagem armazenados em meio magnético, óptico, eletrônico, impresso ou qualquer outro veículo de exibição. Toda Informação de propriedade da Listo deve ser tratada de acordo com a sua classificação.

4.2. O Colaborador reconhece que todos resultados de suas atividades desempenhadas em decorrência do contrato de trabalho ou por meio de ferramentas disponibilizadas pela Listo, em conjunto com outras pessoas ou não, serão considerados como feitos sob encomenda ou por força de contrato de trabalho ou prestação de serviços, sendo todos os direitos de propriedade intelectual, sobre tais resultados, de titularidade exclusiva da Listo.

5. PRIVACIDADE

5.1. Todas as Informações armazenadas, tratadas ou enviadas pelos canais de comunicação utilizados pela Listo estão sujeitas a monitoramento sem aviso prévio, reservando o direito da Listo de realizar avaliações quando identificar necessidade. Ao utilizar qualquer recurso da Listo, os Usuários estão consentindo com este monitoramento.

5.2. É proibido a transmissão por e-mail ou qualquer outro tipo de comunicação, física ou eletrônica, de números PANs desprotegidos.

6. CONFIDENCIALIDADE DA INFORMAÇÃO

6.1. Todas as Informações relacionadas à Listo e seus clientes serão tratadas com segurança e confidencialidade e deverão ser utilizadas exclusivamente para exercício de suas funções, responsabilidades e obrigações, buscando sempre proteger a privacidade da informação, bem como garantir a total transparência no tratamento das Informações disponibilizadas.

7. PENALIDADES

7.1. O Grupo Listo estabelece severas penalidades para aqueles Colaboradores que deixem de cumprir os procedimentos estabelecidos em suas políticas e demais regras internas, sem prejuízo de os responsáveis responderem por penalidades criminais, cíveis e administrativas que lhe sejam aplicáveis por seus atos praticados, tanto perante o Grupo Listo, quanto perante terceiros.

7.2. As principais penas as quais os Colaboradores do Grupo Listo estão sujeitos são:

a) Advertência verbal;
b) Advertência por escrito;
c) Suspensão; e
d) Desligamento.

7.3. Todos os Colaboradores estarão sujeitos às ações judiciais de natureza criminal, cível e administrativa, bem como às sanções internas disciplinares, incluindo seu possível desligamento em caso de descumprimento de qualquer legislação, regulamentação ou de qualquer Política, Norma ou Roteiros Operacionais do Grupo Listo.

7.4. Sem prejuízo ao acima disposto, os Colaboradores estão sujeitos a serem responsabilizados por eventuais danos patrimoniais causados ao Grupo Listo por sua comprovada culpa ou dolo, seja por ação ou omissão, com relação aos recursos ou dispositivos aos quais tiver acesso para desempenho de suas funções.

8. DOCUMENTOS RELACIONADOS

- Política de Gestão de Identidades e Acesso (PC-SIGL-004)
- Norma Classificação da Informação (NR-SIGL-004)
- Norma Gestão do Escopo PCI (NR-SIGL-005)
- Norma Utilização de Acesso Lógico e Físico (NR-SIGL-006)
- ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão de Segurança da Informação
- ABNT NBR ISO/IEC 27002:2013 – Código de Prática para Gestão da Segurança da Informação
- ABNT NBR 16167 – Diretrizes Para Classificação, rotulação e tratamento da informação

9. REGISTRO DE VERSÃO

VERSÃO	ALTERAÇÕES	DATA
1.0	Versão inicial da Política	24/08/2016
1.1	- Alteração template institucional - Inclusão do item 2.2, 2.3, 2.6 e 2.7 no glossário - Inclusão do item 3.5.4, 3.5.5, 4.1.9, 4.1.10, 4.1.11 e 7.1 - Área de Infraestrutura e Segurança da Informação substituída por: pelo Núcleo responsável por Infraestrutura e Segurança da Informação - Inclusão do item 4.1.6	17/07/2017
1.2	- Alteração *template* institucional - Adequação do item 3.2.2, 3.2.3, 3.3.5, 3.3.15, 3.5.2, 4.1.9, 4.1.10, 5.1.1, 9.1.2 - Adequação de título 3.3 - Remoção texto duplicado em outro item 3.4.5, 5.1.4 - Item 5.1.5 movido para item 4.1.15 - Inclusão de item 11 - Revisão Anual - Inserção dos novos diretores	30/08/2018
1.3	Alteração: template institucional; -Inclusão: Definições Pin, Hardening, Malwares, Patches, GMUD, Trade Secret, PCI SSC, Antivírus, Firewall, IDS, IPS, F.I.M, SIEM; -Atualização de Papeis e responsabilidades.; -Atualização do Item 10 -Documentos Associados	24/03/2020
1.4	Inclusão: Definições Antimalwares, Cofre de Senhas, Backup, Terceiros/prestador de serviço, Visitante, Ativo, Ataque, Ameaça, Vulnerabilidade, Risco; -Atualização de Papéis e responsabilidades; -Alteração: Ambiente Escopo de avaliação PCI/DSS Revisão Anual	01/11/2021
1.5	Revisão anual e ajustes formais	13/11/2023
2.0	Nova versão da Política	16/07/2024

10. APROVAÇÃO

Data de aprovação dessa versão pelos responsáveis: 16/07/2024.

ANEXO I- GLOSSÁRIO

NOME	DEFINIÇÃO
Ameaça	condição ou atividade que pode fazer com que as informações ou os recursos de processamento de informações sejam intencionalmente ou acidentalmente perdidos, modificados, expostos, inutilizados ou de outra forma afetados em detrimento da organização.
Ativo	pessoas, propriedades e informações. Ativos do tipo pessoas podem incluir colaboradores, clientes ou contratados. Os ativos imobiliários consistem em itens tangíveis e intangíveis aos quais pode ser atribuído um valor. Os ativos intangíveis incluem reputação e informações proprietárias. As informações podem incluir bancos de dados, código de software, registros críticos da empresa e muitos outros itens intangíveis.
Ativo de Informação	conjunto de conhecimento organizado e gerenciado que tem valor para o Grupo Listo, pois sustenta um ou mais processos de negócio de uma unidade ou área em função de sua manipulação direta ou indireta.
Classificação da Informação	conjunto de critérios, associados a níveis de proteção, que diferenciam a Informação de acordo com o seu grau de confidencialidade, disponibilidade e integridade respeitando sua importância para a manutenção das atividades do Grupo Listo.
Código Fonte	é qualquer sequência ou declaração escrita em alguma linguagem de programação. Estas linguagens são a ponte de comunicação entre o programador e o computador. Quando o programa está finalizado, é feita uma compilação do código fonte, que o transforma em linguagem de máquina para que o computador consiga interpretar.
Colaboradores	funcionários do Grupo Listo, parceiros e/ou empresas prestadoras de serviços contratadas com finalidade especificada e prazo determinado.
Componentes do Sistema	incluem dispositivos de rede (firewall, switch, roteador, roteador sem fio), banco de dados, Servidor web, Servidor de arquivos, sistemas de backup, sistema operacional e sistemas desenvolvidos.
Criptografia	método de proteção de Dados que consiste na transformação da forma original de um Dado para outra forma ilegível, através de funções matemáticas, conhecidas por algoritmos criptográficos.
Dado	representação quantificada de valores, números e constatações que quando juntos, podem se transformar numa informação.
Dados de Cartão	conjunto de informações utilizadas em um processo de autenticação do cartão, tais como: número do cartão (PAN); número do cartão truncado (seis primeiros e os quatro últimos dígitos do cartão); nome do titular do cartão; data de

	vencimento; código de serviço; dados em tarja magnética ou equivalente em chip; código de validação (CAV2/ CVC2/ CVV2/ CID); e Senha (PIN).
Dispositivo Móvel	qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pelo Núcleo de Infraestrutura, como: notebooks, smartphones, tablets e/ou pen drives
Equipamentos	todo o ativo tecnológico utilizado para o funcionamento da Empresa, incluindo, mas não se limitando a terminais de captura de transação, servidores, computadores, notebooks e smartphones.
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.
Informação Confidencial	todos os documentos, memorandos, relatórios, arquivos, dados, software, e seus respectivos materiais, filmes, desenhos, documentos e informações, escritos ou não, disponibilizados em meio físico, eletrônico ou digital, sejam de natureza estratégica, técnica, operacional, financeira, econômica, administrativa, patrimonial, legal, contábil, comercial, de engenharia ou qualquer outra, entregues, revelados ou fornecidos pelo Grupo Listo ao Colaborador, acessados pelo Colaborador em decorrência de suas atividades ou elaborados pelo Colaborador para o Grupo Listo em decorrência de qualquer contrato celebrado entre Colaborador e o Grupo Listo.
Malware	código malicioso, programa malicioso, software nocivo, software mal-intencionado ou software malicioso, é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações.
PAN	trata-se do número da conta principal ou o número do cartão de pagamento sendo um identificador de cartão (normalmente para cartões de crédito ou débito) que identifica o emissor e a conta específica do titular do cartão.
Servidor	software ou computador, com sistema de computação centralizada que fornece serviços a uma rede de computadores, chamada de cliente.
Usuário	qualquer pessoa autorizada que utiliza, algum recurso computacional da empresa, incluindo pessoas físicas ou jurídicas, que acessam os recursos via rede eletrônica ou em salas de computadores da empresa e aquelas que utilizam qualquer rede da empresa para conectar uma máquina pessoal e qualquer outro sistema ou serviço.
Varreduras	ação realizada pelo software de antivírus para identificação de ameaças (vírus, malware, trojans etc.) nos recursos de tecnologia da informação

Visitante	terceiros que em visita às dependências das empresas do Grupo Listo devem ter seu acesso formalizado conforme as regras dos respectivos edifícios onde se encontram.
Vulnerabilidade	fragilidade ou fraqueza que pode ser explorada por ameaças e tornar-se um incidente.