1. PÚBLICO-ALVO E OBJETIVOS

1.1. Esta Política tem por objetivo orientar por meio de suas diretrizes todas as ações de Segurança Cibernética para identificar, suprimir e/ou reduzir os riscos e violações de Ameaças e Vulnerabilidades a níveis aceitáveis, garantindo a confiabilidade, integridade e disponibilidade cibernética do Grupo Listo nos ambientes físicos e lógicos.

1.2. A Política de Segurança Cibernética é destinada ao controle dos ativos de tecnologia, sendo composta por um conjunto de práticas que protegem as Informações sistêmicas armazenadas, incluindo computadores, aparelhos e Dados transmitidos via rede de comunicação.

1.3. As diretrizes apresentadas nesta Política aplicam-se a todos os Colaboradores e Parceiros que utilizam os sistemas do Grupo Listo, os quais são também, responsáveis pela segurança dos ativos tecnológicos.

1.4. Estas diretrizes se aplicam tanto para o ambiente informatizado, quanto para os Ativos de qualquer natureza que armazene, transmita ou processe informações do Grupo Listo, tanto em ambiente físico quanto na nuvem, procurando sempre estar aderente aos Padrões de Segurança solicitados.

2. DIRETRIZES PARA SEGURANÇA DA INFORMAÇÃO

2.1. Segurança da Informação. Entende-se por Segurança da Informação 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.

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; e
c) **Disponibilidade**: processo responsável por garantir que todos os Colaboradores autorizados tenham acesso à Informação e aos ativos correspondentes sempre que necessário.

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.

2.2. Coleta de Informações. Entende-se por Coleta de Informações o processo de captura e validação de todos os Dados inseridos em quaisquer sistemas do Grupo Listo por quaisquer Colaboradores, Clientes e Parceiros.

2.2.1. A captura de Informações deve ser realizada sistemicamente, em tempo real, de forma segura, devendo também ser classificada sob os critérios de disponibilidade e confidencialidade, analisando possíveis Ameaças e riscos nos ambientes e imagem do Grupo Listo.

2.2.2. A captura de Informações poderá ser realizada por qualquer Usuário que possua acesso autorizado mediante senha pessoal e intransferível de acordo com a Política de Gestão de Identidade e Acessos.

2.2.3. Os sistemas devem possuir funcionalidades para validação dos Dados capturados antes que sigam ao processo de armazenamento, de tal forma a manter a persistência de Informações sistemicamente, registrando os *Logs* para viabilizar a rastreabilidade.

2.2.4. Na hipótese de qualquer Dado ser considerado inconsistente e/ou indevido, por força de legislação, regulamentação ou boas práticas de segurança, o mesmo será tratado conforme as regras da Norma de Backup, Retenção e Expurgo de Dados.

2.3. Guarda de Informações. Entende-se por Guarda de Informações o processo de armazenamento, Backup e atualização dos Dados coletados conforme as diretrizes acima.

2.3.1. Todos os Dados coletados, sensíveis ou não, devem ser armazenados em Banco de Dados hospedados em ambiente seguro e monitorado, tanto em ambiente físico (mídias) quanto virtual (nuvem).

2.3.2. As Informações relevantes devem ser armazenadas, por no mínimo de 05 (cinco) anos, período após o qual devem ser executadas as rotinas de expurgo conforme previsto.

2.3.3. Os sistemas e os ambientes devem estabelecer rotinas de Backup automatizadas como forma de garantir a disponibilidade e a restauração das Informações coletadas, mesmo em casos de possíveis incidentes.

2.3.4. A atualização de Informações poderá ser realizada por qualquer Usuário que possua acesso autorizado mediante senha pessoal e intransferível de acordo com a Política de Gestão de Identidade e Acessos.

2.3.5. Os sistemas devem possuir funcionalidades de registro de *Log* das ações de qualquer Usuário relacionado à guarda das Informações, de tal forma a viabilizar a rastreabilidade.

2.4. Controle de Informações. Entende-se por controle de Informações o processo de monitoramento e proteção, em tempo real, das Informações guardadas nos ambientes, viabilizando a identificação de anomalias sistêmicas, falhas de performance e Ameaças de segurança.

2.4.1. O monitoramento das Informações deve ser realizado em tempo real através de *softwares* e algoritmos para verificar quaisquer tentativas de acesso irregular e/ou indevido aos sistemas e ambientes de modo a preservar a confidencialidade, a integridade e confidencialidade, conforme as diretrizes apresentadas na Política de Gestão de Vulnerabilidades.

2.4.2. A proteção da Informação deverá ser realizada através de algoritmos e rotinas predefinidos, incluindo Sistemas IDS/IPS, de Antivírus e Firewalls.

2.5. Expurgo de Informações. Entende-se por expurgo de Informações o processo de recolhimento e descarte de Dados inconsistentes, indevidos ou que não são mais necessários perante a legislação, regulamentação ou boas práticas de segurança.

2.5.1. Os Dados passíveis de expurgo que estejam armazenados em mídias ou ambientes físicos deverão ser recolhidos tempestivamente.

2.5.2. Na hipótese de expurgo de Informações armazenadas em ambiente físico, as mídias deverão ser fragmentadas em conformidade com padrão de segurança internacional.

2.5.3. Na hipótese de expurgo de Informações armazenadas em ambiente virtual, deverão ser aplicadas rotinas de exclusão dos registros armazenados nos bancos de Dados.

3. DIRETRIZES PARA SEGURANÇA DOS EQUIPAMENTOS

3.1. Segurança de Equipamentos. Entende-se por Segurança de Equipamentos o conjunto de práticas que protegem os Equipamentos, incluindo *software* e *hardware*, desde a aquisição até o descarte, garantindo a integridade, disponibilidade e confidencialidade.

3.2. Aquisição de Equipamentos. Entende-se por aquisição de Equipamentos o processo de compra de Equipamentos para posterior utilização por Colaboradores, Clientes ou Parceiros.

3.2.1. Todos os Equipamentos devem ser adquiridos em conformidade com a Política de Gestão de Fornecedores, respeitando registros, licenças e certificados.

3.2.2. Todos os Equipamentos devem ser registrados no momento de sua aquisição nos controles contábeis de modo a permitir a rastreabilidade junto aos Parceiros.

3.2.3. No caso de Equipamentos do tipo terminais de captura de transação, somente poderão ser adquiridos mediante comprovação das certificações vigentes, atendendo as práticas do PCI-PTS.

3.2.4. No caso de Equipamentos do tipo smartphone, somente deverão ser adquiridos com configuração mínima de forma a permitir a instalação de aplicações de monitoramento e segurança.

3.2.5. No caso de Equipamentos do tipo *notebook*, somente deverão ser adquiridos com configuração mínima de forma a permitir a instalação de aplicações de segurança, incluindo Antivírus/*antimalware*, proteção a vazamento de Dados, proteção em navegação internet, IPS/IDS, Firewall, monitoração de eventos de segurança, Criptografia, Varredura para busca de Vulnerabilidades e controle de acesso.

3.2.6. No caso de Equipamentos do tipo Servidor, somente deverão ser adquiridos com configuração mínima de forma a permitir a instalação de aplicações de monitoramento de eventos de segurança, incluindo *antimalware*/Antivírus, Firewall, IDS/IPS, Varredura para busca de Vulnerabilidades e controle de acesso.

3.3. Controle de Equipamentos. Entende-se por controle de Equipamentos, o processo de monitoramento e proteção, em tempo real, dos recursos e redes utilizados pelo Grupo Listo viabilizando a identificação de anomalias sistêmicas, falhas de performance e Ameaças de segurança.

3.3.1. Os Equipamentos somente poderão ser disponibilizados aos Colaboradores após a configuração de todos os requisitos de segurança predefinidos, e assinatura do Termo de Declaração e Compromisso.

3.3.2. O monitoramento dos Equipamentos deve ser realizado em tempo real através de *softwares* e algoritmos para verificar quaisquer tentativas de acesso irregular e/ou indevido aos Equipamentos de modo a preservar, a integridade e confidencialidade dos Equipamentos e informações.

3.3.3. A proteção dos Equipamentos deverá ser realizada através de algoritmos e rotinas predefinidos, conforme as diretrizes da Política de Gestão de Vulnerabilidade.

3.4. Manutenção de Equipamentos. Entende-se como manutenção de Equipamentos o processo de inspeção, atualização, reparação e descarte dos Equipamentos visando assegurar o bom funcionamento dos mesmos.

3.4.1. Todos os Equipamentos deverão ser inspecionados no mínimo anualmente para identificar a necessidade de atualização, reparo ou descarte do mesmo.

3.4.2. A atualização dos Equipamentos poderá ser realizada por equipe especializada através de acesso remoto e controlado, seguindo sempre as diretrizes das Políticas e Normas associadas.

3.4.3. A reparação dos Equipamentos deverá ser realizada preferencialmente por Parceiro credenciado pelo fabricante original, respeitando os registros, licenças e certificações e em conformidade com a Política de Gestão de Fornecedores.

3.4.4. Na hipótese de inutilização do Equipamento por obsolescência tecnológica, o descarte deve somente poderá ser realizado após o Backup do Equipamento bem como a restauração das configurações iniciais.

3.4.5. Na hipótese de inutilização do Equipamento por furto ou roubo, considerando a incapacidade de descarte físico do Equipamento, deverá ser realizado o descarte lógico das Informações mediante o bloqueio do acesso realizado de acordo com a Política de Gestão de Identidade e Acessos.

4. DIRETRIZES PARA SEGURANÇA DO AMBIENTE

4.1. Segurança do ambiente. Entende-se por segurança de ambiente o conjunto de práticas que protegem os Ambientes, incluindo a gestão de acesso, o monitoramento do ambiente e a transmissão de Dados.

4.2. Gestão de Acesso. Entende-se por Gestão de Acesso o processo de concessão, revisão e bloqueio de acessos às aplicações, ambientes e rede, conforme Política de Gestão de Identidade e Acessos.

4.2.1. A concessão de acesso a quaisquer sistemas e ambientes tecnológicos deve ser nominal, pessoal e intransferível.

4.2.2. Qualquer tentativa de acesso não autorizado deve ser contida por meio de algoritmos e aplicações de segurança, incluindo Antivírus e Firewall.

4.2.3. Os acessos podem ser concedidos a: (i) Colaboradores, mediante a necessidade e a responsabilidade atribuídas ao seu cargo; (ii) Clientes, conforme as funcionalidades contratadas; e (iii) Parceiros, de acordo com as atribuições informadas pelo Colaborador responsável pela Parceria e de acordo com a Política de Gestão de Fornecedores.

4.2.4. Os acessos devem ser revisados no mínimo anualmente ou conforme alteração das atribuições de cada Usuário, de acordo com a Política de Gestão Identidade e Acessos.

4.2.5. Na hipótese de encerramento, temporário ou definitivo, da relação de qualquer Usuário com o Grupo Listo, o acesso deverá ser bloqueado tempestivamente, de acordo com a Política de Gestão de Identidade e Acessos.

4.2.6. Na hipótese de identificação de um acesso ou tentativas de acesso maliciosas, incluindo ataques DDoS e *Botnets*, deverão ser executadas rotinas de bloqueio imediatos, de acordo com o Plano de Resposta a Incidentes.

4.3. Identificação e análise de Vulnerabilidades Técnicas. Entende-se por identificação e análise de Vulnerabilidade como o processo de busca por fragilidades sistêmicas e/ou em tecnologias, seja ele realizado por método manual ou automatizado.

4.3.1. Periodicamente devem ser realizados testes de Vulnerabilidades técnicas, sejam teste de invasão e/ou Varreduras automatizadas, mas não limitados a estes nos Ativos críticos da Listo.

4.3.2. Após os levantamentos, as comparações e identificações das classificações das brechas e seus possíveis riscos devem ser executados, possibilitando o tratamento de acordo com seus níveis.

4.3.3. Nos casos em que não haver possibilidade da eliminação total da Vulnerabilidade, deve ser apresentada plano de contenção ou a determinação de falso positivo conforme previsto na Instrução de Trabalho para Tratativa de Incidente de Segurança Cibernética.

4.3.4. Acompanhamento periódico ou auditorias regulares devem verificar a conformidade com as exigências técnicas dos sistemas e das redes, e serem apresentadas formalmente em fóruns entre os envolvidos.

4.4. Controle do Ambiente. Entende-se por controle de ambiente o processo de monitoramento e proteção, em tempo real, da capacidade e disponibilidade de processamento do ambiente, viabilizando a identificação de anomalias sistêmicas, falhas de performance e Ameaças de segurança.

4.4.1. O monitoramento do ambiente deve ser baseado no acompanhamento em tempo real dos indicadores de capacidade de cada Equipamento, conforme definido no Roteiro Operacional de Monitoramento e Controle de Infraestrutura.

4.4.2. Os ambientes produtivos devem possuir algoritmos de identificação de IPs originando acessos maliciosos, incluindo, mas não se limitando a Ataques DDoS e *Botnets*.

4.4.3. Após a identificação dos IPs maliciosos, deverão ser executadas rotinas de bloqueio imediato do acesso dos mesmos registrando-os em lista restritiva, de acordo com o Plano de Resposta a Incidentes.

4.4.4. Na hipótese de aumento significativo no tráfego do ambiente, o mesmo deve estabelecer mecanismos automáticos de balanceamento de carga e escalonamento dos Equipamentos, conforme o Plano de Resposta a Incidentes.

4.5. Transmissão de Dados. Entende-se por transmissão de Dados o processo de transporte de Dados, sensíveis ou não, incluindo o compartilhamento e o recebimento das Informações, visando garantir confidencialidade e integridade no compartilhamento.

4.5.1. O compartilhamento de Dados somente poderá ser realizado através de vias monitoradas, não sendo permitida a gravação de Dados em mídias sem a prévia autorização.

4.5.2. Quando aplicável, os Dados poderão ser compartilhados, preferencialmente, com Criptografia e através de conexões seguras, desde que respeitadas as restrições da Política de Segurança da Informação.

4.5.3. Em se tratando de Dados Sensíveis ou Informações Confidenciais e de acordo com as regras de monitoramento, o compartilhamento poderá requerer a aprovação adicional, conforme a Política de Segurança da Informação.

4.5.4. O recebimento de Informações a partir de qualquer mídia será autorizado após verificação da integridade da mesma de acordo com a Política de Segurança da Informação.

5. DIRETRIZES PARA MONITORAMENTO E CONTROLE

5.1. Deve ser mantido um sistema de monitoramento em tempo real dos sistemas que visa identificar quaisquer incidentes incluindo anomalias, falhas de performance, interrupção de comunicações e Ameaças de segurança.

5.2. Deve ser mantido um sistema centralizado de registro com todos os incidentes relacionados a quaisquer sistemas, ambientes ou ativos tecnológicos de modo a permitir a rastreabilidade das ações desde sua ocorrência até sua resolução contendo os envolvidos em sua resolução.

5.3. Os incidentes relacionados no sistema centralizado de registro devem ser consolidados e apresentadas juntamente com sugestões de melhoria para o Comitê de Gestão de Risco, contendo: (i) Ativos afetados; (ii) tipo de incidente; (iii) impacto; (iv) severidade; (v) análise da causa raiz; (vi) tempo de resolução; e (vii) mecanismo de controle dos efeitos.

5.4. O CGN deve apurar e informar, no menor prazo possível,ao Núcleo de Compliance a ocorrência dos incidentes e das interrupções dos serviços relevantes identificados como uma situação de crise para a respectiva empresa do Grupo Listo, devendo o Núcleo de Compliance reportar as referidas situações ao Órgão Regulador competente, conforme legislação vigente.

5.5. Mediante as Informações apresentadas, deve ser promovida a revisão da Política de Segurança Cibernética bem como o PCN e do Plano de Resposta a Incidentes, com periodicidade mínima anual.

6. DIRETRIZES PARA GESTÃO DE RISCOS DE SEGURANÇA CIBERNÉTICA

6.1. A gestão de riscos de segurança cibernética deve ser realizada através de um processo que contemple a identificação, análise, avaliação, priorização, comunicação, tratamento e monitoração dos riscos que podem afetar negativamente os negócios do Grupo Listo.

6.2. Deve contemplar novos Ativos, sistemas ou processos, quer sejam eles internos, em nuvem ou conduzidos por parceiros.

6.3. Todos os riscos potencialmente danosos a partir da sua identificação, classificação, responsáveis e estratégia de mitigação ao devem ser apresentados ao CGN periodicamente ou sempre que necessário.

7. DIRETRIZES PARA SEGURANÇA NA CADEIA DE SUPRIMENTOS

7.1. Cuidados adicionais devem ser tomados quando se tratar de seleção e contratação de terceiros, temporários e prestadores de serviços oriundos de fornecedores ou de empresas especializadas, que processem e armazenem Dados da Listo.

7.2. Avaliações de segurança para a prestação de serviço de terceiros que tenham contato direto e/ou indireto com os ambientes computacionais das empresas do Grupo Listo deverão ser executados considerando uma avaliação de risco e classificação dos fornecedores (estratégico, tático, operacional).

8. CÓPIAS DE SEGURANÇA

8.1. O processo de execução de Backups deve ser realizado, periodicamente, nos Ativos de Informação do Grupo Listo, de forma a evitar ou minimizar a perda de Dados diante da ocorrência de incidentes.

9. CRIPTOGRAFIA

9.1. Toda solução de Criptografia utilizada no Grupo deve seguir as regras de Segurança da Informação e os padrões de segurança dos Órgãos reguladores.

9.2. Controles criptográficos devem ser solicitados, estabelecidos e/ou desenvolvidos, para garantir os níveis de confidencialidade das informações trafegadas, segundo a sua classificação (definido pelo proprietário da Informação).

9.3. Somente algoritmos de Criptografia aprovados pelo Núcleo de Segurança da Informação podem ser utilizados nas soluções e sistemas adotados pelo

10. PLANO DE CONTINUIDADE DE NEGÓCIO (PCN) E PLANO DE AÇÃO E DE RESPOSTAS A INCIDENTES (PARI)

10.1. Entende-se por PCN/PARI as diretrizes e as estratégias para garantir o funcionamento ininterrupto das operações, no qual são definidos os procedimentos gerais para identificação e gestão dos riscos associados a manutenção dos processos de negócio em nível adequado até a normalização da situação, durante e após a ocorrência de eventos ou incidentes que possam desestabilizar ou interromper a disponibilidade dos serviços de maior impacto para o negócio.

10.2. O PCN/PARI deve definir: cenários de risco; estratégia de contingência; e mecanismos de comunicação:

10.2.1. **Cenários de Risco**. Entende-se por cenários de risco as situações hipotéticas que podem impactar a continuidade de negócio, as quais são classificadas em termos de probabilidade de ocorrência e grau de severidade, podendo variar de altíssimo risco até baixíssimo risco.

10.2.2. **Estratégia de Contingência**. Entende-se por estratégia de contingência o conjunto de ações que deverão ser executadas para manter os processos críticos de negócio em funcionamento durante o incidente.

10.2.3. **Mecanismos de Comunicação**. Entende-se por mecanismos de comunicação o conjunto de ações que deverão ser executadas para informar todos os Usuários impactados pelo incidente para conter eventuais crises.

10.3. O PCN/PARI deve ser revisado com periodicidade mínima anual ou conforme incidentes relatados que possam alterar a avaliação dos cenários de risco, conforme apresentação de Relatório Anual ao CGN, contendo: (i) efetividade da implementação das ações executadas ao longo do exercício; (ii) o resumo dos resultados obtidos na implantação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizadas na prevenção e respostas dos incidentes; (iii) os incidentes relevantes relacionadoscom ambiente cibernético; e (iv) os resultados dos testes de continuidade de negócio.

11. PAPÉIS E RESPONSABILIDADES

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

11.1. Comitê Executivo

11.1.1. Aprovar e revisar, com frequência mínima de dois anos, as políticas e estratégias para Segurança Cibernética e assegurar sua aplicação.

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

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

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

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

11.2. Administradores

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

11.2.2. Analisar, debater e aprovar esta Política.

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

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

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

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

11.3. Gestores

11.3.1. Disseminar a ideia de Segurança Cibernética e o conhecimento das Normas técnicas com as suas respectivas equipes.

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

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

11.3.4. 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.

11.4. Núcleo de Segurança da Informação

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

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

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

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

11.4.5. Realizar auditorias e testes periódicos visando o cumprimento das diretrizes previstas neste documento.

11.4.6. Monitorar e analisar os alertas e informações de segurança, distribuindo-as para as equipes apropriadas.

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

11.4.8. 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.

11.4.9. Trabalhar em conjunto com o Núcleo de Recursos Humanos com objetivo de criar e disseminar treinamentos de conscientização, capacitação e, quando pertinente, avaliação periódica, nos temas de Segurança cibernética para todos os Colaboradores da Listo.

11.4.10. 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.

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

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

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

11.5. Núcleo de Compliance

11.5.1. Ser curador do presente documento.

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

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

11.5.4. Apoiar e monitorar as áreas responsáveis para o desenvolvimento e divulgação de materiais que promovam a conscientização no tema de segurança cibernética, inclusive, mas não se limitando a, quando pertinente, prestar informações sobre condutas e ações preventivas recomendáveis no uso de determinadas funcionalidades, produtos ou serviços;

11.5.5. 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.

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

11.5.7. Comunicar aos Órgãos Reguladores competentes, quando aplicável, em cumprimento às determinações legais vigentes, a ocorrência dos incidentes e das interrupções dos serviços relevantes que o CGN identificar como uma situação de crise para a respectiva empresa do Grupo Listo.

11.5.8. Analisar casos de descumprimento deste documento, encaminhando-os para o Núcleo Jurídico e Núcleo de Recursos Humanos, quando necessário.

11.6. Núcleo de Recursos Humanos

11.6.1. Trabalhar em conjunto com o Núcleo de Segurança da Informação, com o objetivo de criar e disseminar treinamentos de conscientização, capacitação e, quando pertinente, avaliação periódica, nos temas de Segurança Cibernética para todos os Colaboradores da Listo.

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

11.6.3. Manter os termos assinados por todos os Colaboradores, referente à ciência das informações contidas na Política de Segurança Cibernética e Normas associadas.

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

11.7. Colaboradores

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

11.7.2. 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.

11.7.3. 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.

11.7.4. 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.

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

11.7.6. Cumprir todas as diretrizes descritas na Política e Normas de Segurança Cibernética.

11.7.7. 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.

12. PROPRIEDADE INTELECTUAL

12.1. 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.

12.2. 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.

13. PRIVACIDADE

13.1. 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.

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

14. CONFIDENCIALIDADE DA INFORMAÇÃO

14.1. 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.

15. PENALIDADES

15.1. 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.

15.2. 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.

15.3. 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.

15.4. 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.

16. DOCUMENTOS RELACIONADOS

- Política de Segurança da Informação (PC-SIGL-001)
- 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

17. REGISTRO DE VERSÃO

VERSÃO	ALTERAÇÕES	DATA
1.0	- Emissão inicial	25/05/2019
1.1	- Alteração template institucional; atualização do item 6.3; inclusão do item 6.3.1; atualização do item 9; e atualização do item 10	07/12/2020
1.2	- Atualização do texto do item 1.1; exclusão do item 2; atualização do texto do item 9.1; exclusão do item 9.3; exclusão do item 11; exclusão do item 12; renumeração e adequação dos demais itens.	23/05/2022
1.3	- Revisão anual e ajustes formais.	13/11/2023
2.0	- Nova versão da Política	16/07/2024

18. APROVAÇÃO

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

ANEXO I- GLOSSÁRIO

NOME	DEFINIÇÃO
Antivírus	são sistemas de segurança desenvolvidos para prevenir, detectar e eliminar vírus de computador dos componentes de tecnologia.
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.
Backup	cópia de segurança frequentemente utilizada para indicar a existência de cópia de um ou mais arquivos guardados em diferentes dispositivos de armazenamento. Se, por qualquer motivo, houver perda dos arquivos originais, a cópia de segurança armazenada pode ser restaurada.
Colaboradores	funcionários do Grupo Listo, parceiros e/ou empresas prestadoras de serviços contratadas com finalidade especificada e prazo determinado.
Comitê de Gestão de Riscos (CGN)	grupo de colaboradores responsáveis por identificar, avaliar, monitorar e responder aos riscos que a Listo enfrenta e que deve garantir que estes sejam gerenciados de forma eficaz e em conformidade com as Políticas e Normas do Grupo Listo.
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.
Dado Sensível	qualquer informação que, se divulgada ou acessada por terceiros não autorizados, possa causar prejuízos, constrangimentos ou danos à pessoa a quem se refere. Isso inclui informações como dados pessoais, financeiros, genéticos, de saúde, religião, opiniões políticas, orientação sexual, entre

	outros, que são considerados particularmente sensíveis e requerem cuidados especiais em sua coleta, armazenamento e compartilhamento.
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.
Firewall	é uma solução de segurança baseada em hardware e/ou software que, a partir de um conjunto de critérios, analisa o tráfego de informações para determinar quais ações de transmissão ou recepção de dados podem ser executadas.
Grupo Listo	nome Dado ao conjunto de empresas que integram o Grupo incluindo coligadas, subsidiárias e controladas diretas e indiretas.
IDS/IPS	programa componente que automatiza o monitoramento e coleta de informações no computador/host que possam levar a identificação de ataques.
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.
Log	registros ou trilhas de auditoria, são dados que possibilitam monitorar, alertar e analisar eventos, geralmente quando algo falha. Além disso, são úteis para acompanhar o progresso dos processos. Identificar a causa de um problema ou comprometimento se torna desafiador, se não impossível, na ausência de registros ou logs das atividades do sistema.

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.
PCI-PTS	padrão de segurança dos dispositivos usados na Indústria de Pagamentos
Plano de Ação e de Respostas a Incidentes (PARI)	conjunto de procedimentos e ações definidas para recuperação da operação normal após acionamento do PARI em resposta a um desastre ocorrido.
Plano de Continuidade de Negócio (PCN)	conjunto de processos e ações definidas para manutenção das operações críticas do negócio durante e após a ocorrência de situações adversas.
Servidor	software ou computador, com sistema de computação centralizada que fornece serviços a uma rede de computadores, chamada de cliente.
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.
PCI-PTS	padrão de segurança dos dispositivos usados na Indústria de Pagamentos
Plano de Ação e de Respostas a Incidentes (PARI)	conjunto de procedimentos e ações definidas para recuperação da operação normal após acionamento do PARI em resposta a um desastre ocorrido.
Plano de Continuidade de Negócio (PCN)	conjunto de processos e ações definidas para manutenção das operações críticas do negócio durante e após a ocorrência de situações adversas.
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.
Vulnerabilidade	fragilidade ou fraqueza que pode ser explorada por ameaças e tornar-se um incidente.