GRUPO LISTO

POLÍTICA DE SEGURANÇA CIBERNÉTICA

VERSÃO 1.01

Gestor	**Gerente Segurança da Informação**	**Assinatura**	DocuSigned by: Thiago Velloso B76AB77402B74E4...
Nome	Thiago Velloso		
E-mail	thiago.velloso@soulisto.com.br	**Data** 10/12/2020	
Tel.	+55 (11) 4861-9510		

Av. Brigadeiro Faria Lima, 1663 – 8° Andar / São Paulo, SP
CEP – 01452-001

1. OBJETIVO E ESCOPO

1.1. Esta Política tem por objetivo orientar por meio de suas Normas 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 pelos Órgãos Reguladores.

2. DEFINIÇÕES

2.1. **AGENTE DLP:** Conjunto de aplicativos e algoritmos que previnem a perda de informações;
2.2. **ATAQUES DDOS E BOTNETS**: Ataques em massa ou não, objetivando gerar atrasos e negações de acesso a serviços e/ou sistemas;
2.3. **COLABORADORES**: funcionários do Grupo Listo, parceiros e/ou empresas prestadoras de serviços contratadas com finalidade especificada e prazo determinado;
2.4. **COMITÊ DE GESTÃO DE RISCO**: significa o Comitê composto por 01 membro do Departamento Jurídico, 01 membro do Departamento de Infraestrutura, 01 membro do Departamento de Recursos Humanos e 02 membros indicados pela Diretoria do Grupo Listo;
2.5. **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;
2.6. **ESTATUTO**: significa o Estatuto Social de qualquer companhia, pela qual se disciplina o relacionamento interno e externo da sociedade;
2.7. **GESTOR DA POLÍTICA**: significa o Colaborador responsável pelas atividades de gestão da respectiva política, incluindo mas não se limitando a: (i) elaboração de novas políticas, (ii) acompanhamento do processo de aprovação da política, (iii) controle de armazenamento e divulgação da política, (iv) fiscalização da política e (v) revisão das políticas vigentes;
2.8. **GRUPO LISTO:** Nome dado ao conjunto de empresas que integram o Grupo incluindo coligadas, subsidiárias e controladas diretas e indiretas;
2.9. **IDS/IPS**: Sistema de Detecção e Prevenção de Intrusão;
2.10. **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 em decorrência do Contrato;
2.11. **PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN):** conjunto de processos e ações definidas

para manutenção das operações críticas do negócio durante e após a ocorrência de situações adversas;

2.12. 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;

2.13. PLATAFORMA LISTO FÁCIL: tecnologia operacional de controle de operações de captura, roteamento, transmissão, processamento e liquidação financeira das transações. Essas atividades realizadas pelo Sistema Listo Fácil constituem um conjunto de serviços interligados e interconectados;

2.14. SEGURANÇA CIBERNÉTICA: 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 pelos Órgãos Reguladores;

2.15. TERMO DE DECLARAÇÃO E COMPROMISSO: termo que dispõe sobre o uso de Equipamentos de propriedade do Grupo Listo que o Colaborador utilizará para o exercício de suas funções;

2.16. VULNERABILIDADE: fragilidade ou fraqueza que pode ser explorada por ameaças e tornar-se um incidente.

3. PROCEDIMENTOS DE SEGURANÇA DE INFORMAÇÃO

3.1. Entende-se por segurança de 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.

3.1.1. Integridade. Entende-se por integridade o processo responsável por garantir que qualquer informação seja mantida e seu estado original, visando protege-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

3.1.2. Confidencialidade. Entende-se por confidencialidade o processo responsável por garantir que o acesso à informação seja obtido somente por Colaboradores autorizados.

3.1.3. Disponibilidade. Entende por disponibilidade o processo responsável por garantir que todos os Colaboradores autorizados tenham acesso a informação e aos ativos correspondentes sempre que necessário.

3.2. 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.

3.2.1. 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 da Empresa.

3.2.2. 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 Acesso.

3.2.3. 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.

3.2.4. Na hipótese de qualquer dado ser considerado inconsistente e/ou indevido, por força de legislação, regulamentação ou boas práticas de segurança, o mesmo seguirá para o Roteiro Operacional de Expurgo.

3.3. Guarda de Informações. Entende-se por guarda de informações o processo de armazenamento, backup e atualização dos dados coletados conforme as diretrizes acima.

3.3.1. 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).

3.3.2. As informações relevantes devem ser armazenadas, por no mínimo de 05 anos, período após o qual devem ser executadas as rotinas de expurgo conforme previsto.

3.3.3. 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.

3.3.4. 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 Acesso.

3.3.5. 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.

3.4. 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.

3.4.1. 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 Roteiro Operacional de Monitoramento e Controle de Infraestrutura.

3.4.2. A proteção da informação deverá ser realizada através de algoritmos e rotinas predefinidos, incluindo Sistemas IDS/IPS, de antivírus e firewalls, de acordo com o Roteiro Operacional de Monitoramento e Controle de Infraestrutura.

3.5. 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.

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

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

3.5.3. Na hipótese de expurgo de informações armazenadas em ambiente virtual, deverão ser aplicadas rotinas de exclusão dos registros armazenados nos bancos de dados.

4. PROCEDIMENTOS DE SEGURANÇA DE EQUIPAMENTOS

4.1. 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.

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

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

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

4.2.3. 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.

4.2.4. 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.

4.2.5. No caso de Equipamentos do tipo notebook, somente deverão ser adquiridos com configuração mínima de forma a permitir a instalação de aplicações de monitoramento e segurança, incluindo antivírus, Agente DLP, firewall e controle de acesso.

4.2.6. No caso de Equipamentos do tipo servidor, somente deverão ser adquiridos com configuração mínima de forma a permitir a instalação de aplicações de monitoramento e segurança, incluindo antivírus, firewall, IDS/IPS e controle de acesso.

4.3. Controle de Equipamentos. Entende-se por controle de equipamentos, o processo de monitoramento e proteção, em tempo real, dos recursos e redes utilizados pela Empresa viabilizando a identificação de anomalias sistêmicas, falhas de performance e ameaças de segurança.

4.3.1. Os Equipamentos somente poderão ser disponibilizados aos Colaboradores após a configuração de todos os requisitos de segurança predefinidos, conforme Roteiro Operacional de Monitoramento e Controle de Infraestrutura, e assinatura do Termo de Declaração e Compromisso.

4.3.2. 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 confidencialidade, a integridade e confidencialidade dos Equipamentos e informações, conforme Roteiro Operacional de Monitoramento e Controle de Infraestrutura.

4.3.3. A proteção dos Equipamentos deverá ser realizada através de algoritmos e rotinas predefinidos, de acordo com o Roteiro Operacional de Monitoramento e Controle de Infraestrutura.

4.4. 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.

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

4.4.2. A atualização dos Equipamentos poderá ser realizada por equipe especializada

através de acesso remoto e controlado, de acordo com o Roteiro Operacional de Monitoramento e Controle de Infraestrutura.

4.4.3. 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.

4.4.4. 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.

4.4.5. 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 Acessos.

5. PROCEDIMENTO DE SEGURANÇA DE AMBIENTE

5.1. 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.

5.2. 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 Acesso.

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

5.2.2. Qualquer tentativa de acesso não autorizado deve ser contida por meio de algoritmos e aplicações de segurança, incluindo antivírus e firewall.

5.2.3. 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.

5.2.4. Os acessos devem ser revisados no mínimo anualmente ou conforme alteração das atribuições de cada usuário, de acordo com a Política de Gestão de Acesso.

5.2.5. 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 Acesso.

5.2.6. 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.

5.3. 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.

5.3.1. 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.

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

5.3.3. 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.

5.3.4. 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.

5.4. 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.

5.4.1. 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.

5.4.2. 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.

5.4.3. Em se tratando de dados sensíveis ou confidenciais e de acordo com as regras de monitoramento, o compartilhamento poderá requerer a aprovação adicional, conforme a Política de Segurança da Informação.

5.4.4. 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.

6. MONITORAMENTO E CONTROLE

6.1. 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.

6.2. 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.

6.3. 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, conforme fluxograma correspondente.

6.3.1. O Comitê de Gestão de Risco deve apurar e informar, no menor prazo possível, ao Departamento de Compliance a ocorrência dos incidentes e das interrupções dos serviços relevantes que o comitê de Gestão de Risco identificar como uma situação de crise para a respectiva empresa do Grupo Listo para que o Departamento de Compliance possa reportar referidas situações ao Órgão Regulador competente, conforme legislação vigente.

6.4. Mediante as informações apresentadas, deve ser promovida a revisão da Política de Segurança Cibernética bem como o Plano de Continuidade do Negócio e do Plano de Resposta a Incidentes, com periodicidade mínima anual.

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

(PARI)

7.1. 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.

7.2. O PCN/PARI deve definir: (i) cenários de risco; (ii) estratégia de contingência; e (iii) mecanismos de comunicação.

7.2.1. 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.

7.2.2. 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.

7.2.3. 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.

7.3. 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 Comitê de Gestão de Risco, 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 relacionados com ambiente cibernético; e (iv) os resultados dos testes de continuidade de negócio.

8. DIVULGAÇÃO E TREINAMENTO

8.1. A presente política deverá ser disponibilizada a todos os Colaboradores e Parceiros através de sítio eletrônico dedicado a divulgação assim como através de e-mail corporativo mediante qualquer alteração.

8.2. Todos os Colaboradores e Parceiros estratégicos deverão receber treinamento específico sobre esta Política bem como as boas práticas de segurança de informação e segurança cibernética para exercício das suas funções com periodicidade mínima anual.

8.3. Deverá ser envidado os melhores esforços para a conscientização dos Clientes referente a esta Política bem como as boas práticas de segurança de informação e segurança cibernética através da Plataforma Listo Fácil, páginas do Grupo Listo em mídias digitais e quaisquer outras comunicações eletrônicas disponíveis.

9. PAPÉIS E RESPONSABILIDADES

9.1. Todos os Colaboradores são responsáveis pela manutenção e aplicação da Política de Segurança Cibernpetica, tendo papel fundamental na identificação, avaliação e monitoramento de casos considerados suspeitos.

9.2. Todos os Colaboradores são responsáveis por zelar pela reputação e imagem do Grupo Listo, sendo proibido o compartilhamento de Informação Confidencial não permitido.

9.3. Comitê Executivo

9.3.1 Requerer que todos os responsáveis no Grupo Listo cumpram com as suas responsabilidades quanto aos termos relacionados a este documento;
9.3.2 Analisar, debater e aprovar os temas relativos ao objeto deste documento, assim como todas as revisões necessárias, com periodicidade mínima anual; e
9.3.3 Ser exemplo aos demais responsáveis, cumprindo todas as diretrizes descritas neste documento.

9.4. Diretoria

9.4.1. Estabelecer os princípios, padrões, orientações e procedimentos para prevenir e detectar operações e práticas de negócios que pretendam violar as regras determinadas neste documento, aprovando inclusive os termos e aplicação do mesmo;
9.4.2. Garantir que os procedimentos previstos neste documento sejam cumpridos de forma correta de acordo com todas as regras aqui estabelecidas, assim como aquelas previstas em seus documentos relacionados;
9.4.3. Tomar decisões administrativas referentes aos casos de descumprimento das diretrizes previstas neste documento encaminhados pelo departamento responsável por realizar os procedimentos ora descritos;
9.4.4. Ser exemplo aos demais responsáveis, cumprindo todas as diretrizes descritas neste documento; e
9.4.5. Garantir que todos os Colaboradores recebam o treinamento adequado para o exercício de suas atividades.

9.5. Departamento de Segurança da Informação

9.5.1. Garantir que as diretrizes deste documento estejam em conformidade com a legislação vigente, envidando os melhores esforços para adequá-las às melhores práticas de mercado;
9.5.2. Elaborar e manter atualizado os treinamentos de capacitação das diretrizes previstas neste documento para todos os Colaboradores;
9.5.3. Fomentar campanhas de conscientização relativas as diretrizes previstas neste documento;
9.5.4. Realizar auditorias periódicas visando o cumprimento das diretrizes previstos neste documento;
9.5.5. Elaborar relatórios de monitoramento relativos a incidentes e interrupções dos serviços relevantes da respectiva empresa do Grupo Listo;
9.5.6. Informar tempestivamente ao Departamento de Compliance a ocorrência de incidentes e interrupções dos serviços relevantes da respectiva empresa do Grupo Listo.

9.6. Departamento de Compliance

9.6.1. Ser curador do presente documento;
9.6.2. Garantir que o documento esteja atualizado de acordo com a sua periodicidade mínima;

9.6.3. Ser agente facilitador para implantação dos controles descritos neste documento ou qualquer outro documento relacionado;
9.6.4. Exigir que o Departamento de Segurança da Informação envie os relatórios de monitoramento sobre o cumprimento das diretrizes deste documento com a periodicidade mínima trimestral;
9.6.5. Reportar ao Comitê Executivo e à Diretoria quaisquer desvios no cumprimento das diretrizes deste documento;
9.6.6. Comunicar aos Órgão Reguladores competentes, quando aplicável, em cumprimento às determinações legais vigentes, a ocorrência dos incidentes e das interrupções dos serviços relevantes que o comitê de Gestão de Risco identificar como uma situação de crise para a respectiva empresa do Grupo Listo; e
9.6.7. Analisar casos de descumprimento deste documento, encaminhando-os para o Departamento Jurídico, quando necessário.

9.7. Departamento de Recursos Humanos

9.7.1. Garantir que todos os Colaboradores do Grupo Listo tenham ciência das diretrizes de presentes neste documento;
9.7.2. Apoiar a elaboração dos treinamentos de capacitação sobre as diretrizes deste documento em conjunto o Gestor deste documento;
9.7.3. Manter os termos assinados por todos os Colaboradores, referente à ciência das informações contidas neste documento.

10. PENALIDADES

10.1. O Grupo Listo estabelece severas penalidades para aqueles que deixem de cumprir os procedimentos estabelecidos em suas políticas e demais regras internas tanto na esfera do Colaborador quanto do Grupo, bem como criminais, cíveis e administrativas.

10.1.1. As principais penas as quais os Colaboradores do Grupo Listo estão sujeitos são: Advertência;
10.1.2. Multa pecuniária e inabilitação temporária, pelo prazo de até 10 (dez) anos, para o exercício do cargo de administrador estatutário;
10.1.3. Cassação ou suspensão da autorização para o exercício de atividade, operação ou funcionamento;
10.1.4. Suspensão; e
10.1.5. Desligamento .

10.2. 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.

11. DOCUMENTOS RELACIONADOS

- Política de Gestão de Fornecedores
- Política de Gestão de Acessos
- Plano de Continuidade de Negócio
- Política de Segurança da Informação
- Roteiro Operacional de Monitoramento e Controle de Infraestrutura
- Roteiro Operacional de Expurgo

12. CONTROLE DE ALTERAÇÕES

Versão	Alterações	Data
1.00	- Emissão inicial	25.05.2019
1.01	- 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

13. APROVAÇÕES

13.1 Qualificação do Curador desta Política

Cargo	**Gerente Jurídico**	**Assinatura**	DocuSigned by: Adriana Beline Maran C36D8A2C6D0F411...
Nome	Adriana Beline		
Email	adriana.maran@soulisto.com.br	**Data** 10/12/2020	
Tel	+55 11 3995-0996		

13.2 Quadro de Aprovações

Cargo	Nome	Data	Assinatura
Diretor	Olavo Viana Cabral Netto	10/12/2020	DocuSigned by: CF64B9EB4F9A4E9...
Diretor	Ravin Harshad Mehta	10/12/2020	DocuSigned by: Ravin Mehta 4F288271AAD84E6...
Diretora	Karine Lima de Carvalho	10/12/2020	DocuSigned by: Karine Barreto E03404502DC44D1...