GRUPO LISTO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

VERSÃO 1.4

28/07/2022

1. OBJETIVO E ESCOPO

1.1. Esta Política de Segurança da Informação tem como objetivo estabelecer as diretrizes das empresas do Grupo 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:

1.1.1. **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.

1.1.2. **Confidencialidade:** garantia de que os acessos às informações sejam disponibilizados somente por usuários autorizados.

1.1.3. **Disponibilidade:** garantia de que os usuários autorizados tenham acesso à informação e aos ativos, de acordo com o necessário.

1.2. 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.

1.3. 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 da Listo, procurando sempre estar aderente as Normas e melhores práticas de mercado utilizando metodologia inerentes a segurança de dados.

2. DEFINIÇÕES

2.1. As definições necessárias contidas nesta Política estão devidamente descritas no Dicionário Listo.

3. DIRETRIZES

3.1. Comportamento Seguro

3.1.1. 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.

3.1.2. 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.

3.1.3. 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.

3.1.4. 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.

3.1.5. As **senhas de usuários** ou **PIN 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.

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

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

I. 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 da própria Listo;
II. Os Colaboradores não devem permitir que visitantes tirem fotos e/ou realizem gravações nas dependências da Listo sem serem devidamente autorizados;
III. Caso algum comportamento suspeito seja identificado, o Colaborador deve entrar em contato com o Departamento de Segurança da Informação, não permitindo que o visitante circule livremente por áreas estratégicas.

3.1.8. É terminantemente proibido **copiar, armazenar** ou **compartilhar** Código Fonte, dados de cartão de crédito e documentos estratégicos classificados como confidenciais, restritos e/ou internos se utilizando de dispositivos não homologados ou não aprovados pelo Grupo Listo.

3.1.9. **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.

3.1.10. Todos os documentos devem ter sua **informação classificada** conforme o grau de confidencialidade orientado na Norma de Classificação das Informações.

3.1.11. Todos os Colaboradores deverão utilizar equipamentos da Listo homologados pelo Departamento de Infraestrutura e que possuam as regras e controles de segurança estabelecidos pelo Departamento de Segurança da Informação.

I. 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 com quaisquer dispositivos pessoais;
II. 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.
III. Todos os equipamentos que tenham capacidade de armazenamento de dados, devem possuir algum tipo tecnologia de proteção:
    - contra malwares e outras pragas digitais sempre atualizado;
    - navegação internet e/ou proxy;
    - identificação e varredura de vulnerabilidades;
    - contra o vazamento de dados e informações;
    - contra perda e integridade como criptografia de disco e senha de BIOS (Basic Input/Output System); e
IV. Todos os equipamentos devem possuir tecnologia de monitoração para:
    - Detectar acessos não autorizados;
    - Estar ingressados em domínio corporativo e/ou tecnologia equivalente que permita gestão a partir de serviço de diretórios; e
    - Identificar vulnerabilidades.

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

3.2. Itens Não Autorizados

3.2.1. 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.

3.2.2. Encaminhar quaisquer informações corporativas para e-mails pessoais.

3.2.3. 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.

3.2.4. Não é permitido 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.

3.2.5. É vedada 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 departamento de Infraestrutura de acordo com Políticas e Normas internas;

3.2.6. É proibido 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.

3.3. Mesa Limpa/Tela Limpa

3.3.1. 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.

3.3.2. 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.

3.3.3. Informações impressas devem ser armazenadas corretamente ao se ausentar da sua estação de trabalho.

3.4. Propriedade Intelectual

3.4.1. 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.

3.4.2. 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.

3.5. PRIVACIDADE

3.5.1. 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.

3.6. Confidencialidade Da Informação

3.6.1. 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.

4. PAPÉIS E RESPONSABILIDADES

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

4.2. Comitê Executivo

4.2.1. Aprovar e revisar, com frequência mínima de dois anos, as Políticas e estratégias de gerenciamento de riscos e assegurar sua aplicação;
4.2.2. Analisar, debater e aprovar os temas relativos ao objeto deste documento, assim como todas as revisões necessárias, com periodicidade mínima anual;
4.2.3. Autorizar, quando necessário, exceções às Políticas e aos procedimentos estabelecidos;
4.2.4. Ser exemplo aos demais responsáveis, cumprindo todas as diretrizes descritas neste documento; e
4.2.5. Requerer que todos os responsáveis do Grupo Listo cumpram com as suas responsabilidades quanto aos termos relacionados a este documento.

4.3. Diretoria

4.3.1. Apoiar e incentivar todos os responsáveis na Listo a cumprirem com suas responsabilidades quanto à Segurança das Informações e a mitigação de riscos;
4.3.2. Analisar, debater e aprovar a Política de Segurança da Informação, assim como todas as revisões sugeridas pelo Departamento de Segurança da Informação;
4.3.3. Tomar decisões administrativas referentes aos casos de descumprimento da Política de Segurança da Informação e/ou de suas Normas encaminhados pelo Departamento de Segurança da Informação;
4.3.4. Ser exemplo aos demais responsáveis pela Segurança da Informação no Grupo Listo, cumprindo todas as diretrizes descritas nesta Política; e
4.3.5. Debater e tomar decisão sobre solicitações vindas do Departamentos de Infraestrutura e de Segurança da Informação.

4.4. Gerência

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

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

4.4.3. *G*arantir que todos os Colaboradores tenham os treinamentos adequados sobre Segurança da Informação para o exercício de suas atividades; e

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

4.5. Departamento de Segurança da Informação

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

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

4.5.3. Ser agente facilitador para a implantação de controles identificados no processo de gestão de vulnerabilidades;

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

4.5.5. Atuar na criação de documentação, divulgação e procedimentos referente a Segurança da Informação e respostas a incidentes;

4.5.6. Administrar ativos de tecnologia de segurança, colocando em prática as diretrizes e processos descritas nesta e em documentações associadas;

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

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

4.5.9. 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;

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

4.5.11. 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;

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

4.5.13. Revisar esta Política anualmente ou sempre que se fizer necessário;

4.5.14. Submeter a Diretoria quaisquer solicitações que requeiram investimentos financeiros;

4.5.15. Analisar os casos de descumprimento desta Política e Normas de Segurança da Informação, encaminhando-os para Diretores, quando necessário.

4.6. Departamento de Desenvolvimento

4.6.1. Criar, desenvolver e manter código fonte de aplicações utilizadas pelas empresas do Grupo Listo em local seguro em repositório homologado para o Grupo Listo;

4.6.2. Não copiar, reproduzir ou compartilhar integral ou parcialmente qualquer parte do código fonte das aplicações em ambientes externos;

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

4.6.4. Analisar e tratar as vulnerabilidades sistêmicas que venham a comprometer a continuidade do negócio; e
4.6.5. Participar dos treinamentos de desenvolvimento seguro.

4.7. Departamento de Infraestrutura

4.7.1. 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;
4.7.2. Garantir que todos os equipamentos destinados a Colaboradores possuam pacotes de *softwares* standard e aplicativos homologados para o Grupo Listo;
4.7.3. Garantir e manter atualizado o inventário de equipamentos tecnológicos durante todo o ciclo de vida do ativo;
4.7.4. Tratar as vulnerabilidades tecnologias que venham a comprometer a continuidade do negócio;
4.7.5. Garantir que todos os ativos do tipo servidor, dispositivos de rede e demais componentes de infraestrutura tecnológica possuam os recursos tecnológicos homologados;
4.7.6. Gerenciar o ambiente de dados de cartão com total segurança, responsabilidade e estabilidade devido a serem os únicos a possuir acesso a tal; e
4.7.7. Manter, efetuar e garantir a preservação dos dados hospedados nas infraestruturas tecnológicas em backup a partir da sua sensibilidade para continuidade dos processos.

4.8. Departamento de Compliance

4.8.1. Ser curador do presente documento;
4.8.2. Garantir que o documento esteja atualizado de acordo com a sua periodicidade mínima;
4.8.3. Ser agente facilitador para implantação dos controles descritos neste documento ou qualquer outro documento relacionado;
4.8.4. 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;
4.8.5. Reportar ao Comitê Executivo e à Diretoria quaisquer desvios no cumprimento das diretrizes deste documento; e
4.8.6. Analisar casos de descumprimento deste documento, encaminhando-os para o Departamento Jurídico, quando necessário.

4.9. Departamento de Recursos Humanos

4.9.1. Trabalhar em conjunto com o Departamento de Segurança da Informação, com o objetivo de criar e disseminar treinamentos de conscientização da Segurança da Informação para todos os Colaboradores da Listo;
4.9.2. Garantir que todos os Colaboradores da Listo tenham ciência das diretrizes de Segurança da Informação presentes na Política;
4.9.3. Manter os termos assinados por todos os Colaboradores, referente à ciência das informações contidas na Política de Segurança da Informação; e
4.9.4. Comunicar o desligamento de Colaboradores aos Departamentos de Infraestrutura e Segurança da Informação, para que sejam desabilitados/removidos todos os acessos da pessoa desligada.

4.10. Colaboradores

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

4.10.2. Não conectar à rede da Listo qualquer ativo tecnológico para uso nas dependências da Listo sem prévia autorização do Departamento de Segurança da Informação e ciência do Departamento de Infraestrutura;

4.10.3. Ter ação proativa e informar imediatamente ao Departamento 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;

4.10.4. 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, Informação Confidencial ou *Trade Secret* estejam em posse indevida e que seu uso poderá incorrer em prática de concorrência desleal;

4.10.5. Participar sempre que solicitado a treinamentos regulares de conscientização, capacitação ou reforço das práticas de segurança da informação;

4.10.6. 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; e

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

5. PENALIDADES

5.1. 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 doColaborador quanto do Grupo, bem como criminais, cíveis e administrativas.

5.2. As principais penas as quais os Colaboradores do Grupo Listo estão sujeitossão:

5.2.1. Advertência;

5.2.2. Advertência verbal;

5.2.3. Advertência por escrito;

5.2.4. Suspensão; e

5.2.5. Desligamento.

5.3. 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 um dos itens presentes nesta Política e Normas associadas implicará em sansões disciplinares e administrativas.

5.4. Ao observar uma violação a esta Política de Segurança da Informação o Colaborador deve comunicar a infração aos responsáveis pela Segurança da Informação da Listo através do canal infosec@soulisto.com.br. Caso seja detectado que o Colaborador não comunicou a infração, mesmo sabendo da sua existência, o mesmo pode ser considerado coautor do evento e assim sofrer sansões internas e /ou legais.

5.5. Em nenhuma hipótese será admitida a alegação de desconhecimento para o não cumprimento desta Política e Normas de Segurança da Informação relacionadas. Todos os Colaboradores devem estar cientes de que o não cumprimento das diretrizes desta Política poderá acarretar sansões, de natureza administrativa, legal e/ou regulatória, dependendo do grau da infração identificada.

6. DOCUMENTOS RELACIONADOS

- Política de Controle de Acesso Físico e Lógico
- Norma de Classificação da informação
- Norma de Backup Corporativo
- RO – Gestão de Vulnerabilidades
- Formulário – Responsabilidade de Uso de Equipamento
- 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

7. CONTROLE DE ALTERAÇÕES

Versão	Alterações	Data
1.0	Versão inicial da Política	24/08/2017
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 Departamento 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	- Atualização de texto do item 1.1; - Atualização de texto do item 2. Definições - Adequação dos itens 3.1, 3.2 e 3.3 - Exclusão dos itens: 5.1, 5.2, 6.1, 6.2, 7.1, 7.2, 7.3, 8, 9.1, 9.2, 9.4, 9.5, 9.6, 10.1, 10.2 e 11; - Renumeração dos demais itens.	23/05/2022

Data de aprovação dessa versão pelos responsáveis: 28/07/2022.