GRUPO LISTO

POLÍTICA DE SEGURANÇA CIBERNÉTICA
VERSÃO 1.3.

Data de aprovação dessa versão pelos responsáveis: 13/11/2023.

1. OBJETIVO E PÚBLICO-ALVO

1.1. Esta Política tem por objetivo estabelecer as diretrizes das empresas do Grupo Listo (ou, simplesmente, a "Listo")quanto 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 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.

1.3.1. 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 e/ou pelo mercado de meios de pagamento com cartão, tal como aplicável às atividades de cada empresa do Grupo Listo.

2. DEFINIÇÕES

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

3. DIRETRIZES

3.1. Procedimentos de 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.

3.1.1. Integridade. Entende-se por integridade o 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.

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-se por disponibilidade o processo responsável por garantir que todos os Colaboradores autorizados tenham acesso à 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 na imagem do Grupo Listo.

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 as regras corporativas 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 as regras corporativas para 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, salvo exigência ou fundamento legal ou regulamentar para armazenamento por período maior, 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 acordo com as regras corporativas 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, em prevenção a incidentes 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, de acordo com as definições corporativas de monitoramento operacional 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 as definições corporativas de monitoramento operacional 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 as regras corporativas aplicáveis, 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, especialmente junto aos clientes e/ou 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 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.

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 de eventos de segurança, incluindo antimalware/antivírus, firewall, IDS/IPS, varredura para busca de vulnerabilidades 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 pelo Grupo Listo viabilizando a identificação de anomalias sistêmicas, falhas de performance e ameaças de segurança, em prevenção a incidentes de segurança.

4.3.1. Os Equipamentos somente poderão ser disponibilizados aos Colaboradores após a configuração de todos os requisitos de segurança predefinidos e atendidas as demais regras corporativas aplicáveis, incluindo as determinadas pelo Departamento de Recursos Humanos.

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 integridade e confidencialidade dos Equipamentos e informações, de acordo com as definições corporativas de monitoramento operacional e controle de infraestrutura.

4.3.3. A proteção dos Equipamentos deverá ser realizada através de algoritmos e rotinas predefinidos, de acordo com as definições corporativas de monitoramento operacional 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 as definições corporativas de monitoramento operacional 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.

4.4.4. Na hipótese de inutilização do Equipamento por obsolescência tecnológica, o descarte ou a venda somente poderão ser realizados 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 as regras corporativas 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.

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 as regras corporativas de gestão de acessos.

5.2.4. Os acessos devem ser revisados no mínimo anualmente ou conforme alteração das atribuições de cada usuário, de acordo com as regras corporativas de gestão de acessos.

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 as regras corporativas de gestão de acessos.

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. 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.

5.3.1. Periodicamente devem ser realizados testes de vulnerabilidades técnicas, sejam teste de invasão e/ou varreduras automatizadas, mas não limitados a estes nos ativos críticos do Grupo Listo.

5.3.2. 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.

5.3.3. Nos casos em que não houver possibilidade da eliminação total da vulnerabilidade, deve ser apresentado plano de contenção ou a determinação de falso positivo conforme regras corporativas para gestão de vulnerabilidades.

5.3.4. 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.

5.4. 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.

5.4.1. O monitoramento do ambiente deve ser baseado no acompanhamento em tempo real dos indicadores de capacidade de cada Equipamento, conforme definido pelas regras corporativas de monitoramento operacional e controle de infraestrutura.

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

5.4.3. 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.

5.4.4. 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.

5.5. 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.

5.5.1. 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.

5.5.2. 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.

5.5.3. 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.

5.5.4. 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.

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. PROCEDIMENTO PARA GESTÃO DE RISCOS DE SEGURANÇA CIBERNÉTICA

7.1. 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.

7.2. O processo de gestão de riscos deve contemplar novos ativos, sistemas ou processos, quer sejam eles internos, em nuvem ou conduzidos por parceiros.

7.3. Deverão ser apresentados todos os riscos potencialmente danosos a partir da sua identificação, classificação, detecção de responsáveis e elaboração de estratégia de mitigação, ao Comitê de Gestão de Riscos periodicamente ou sempre que necessário.

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 E AUTENTICAÇÃO

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

9.2. Controles criptográficos e de autenticação 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).

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: (i) cenários de risco; (ii) estratégia de contingência; e (iii) 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 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.

11. PAPÉIS E RESPONSABILIDADES

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

11.2. Todos os Colaboradores são responsáveis por zelar pela reputação e imagem do Grupo Listo, sendo proibido o compartilhamento de informação confidencial não autorizado.

11.3. Comitê Executivo

11.3.1. Aprovar e revisar, com frequência mínima de dois anos, as políticas e estratégias de gerenciamento de riscos e assegurar sua aplicação;

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

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

11.3.4. Ser exemplo aos demais responsáveis, cumprindo todas as diretrizes descritas neste documento; e

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

11.4. Diretoria

11.4.1. 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;

11.4.2. 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;

11.4.3. Tomar decisões administrativas referentes aos casos de descumprimento das diretrizes previstas neste documento encaminhados pelo departamento responsável por realizar os procedimentos ora descritos;

11.4.4. Ser exemplo aos demais responsáveis, cumprindo todas as diretrizes descritas neste documento; e

11.4.5. Garantir que todos os Colaboradores recebam o treinamento adequado para o exercício de suas atividades.

11.5. Área de Segurança da Informação

11.5.1. 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;

11.5.2. Elaborar e manter atualizado os treinamentos de capacitação das diretrizes previstas neste documento para todos os Colaboradores;

11.5.3. Fomentar campanhas de conscientização relativas as diretrizes previstas neste documento;

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

11.5.5. Elaborar relatórios de monitoramento relativos a incidentes e interrupções dos serviços relevantes da respectiva empresa do Grupo Listo;

11.5.6. Informar tempestivamente ao Departamento de Compliance a ocorrência de incidentes e interrupções dos serviços relevantes da respectiva empresa do Grupo Listo.

11.5.7. Revisar esta Política e demais documentos relacionados, com periodicidade mínima anual.

11.6. Departamento de Compliance

11.6.1. Ser curador do presente documento;

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

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

11.6.4. Exigir que o Departamento de Segurança da Informação envie relatórios de monitoramento sobre o cumprimento das diretrizes deste documento de forma periódica ou sempre que entender necessário;

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

11.6.6. 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 comitê de Gestão de Risco identificar como uma situação de crise para a respectiva empresa do Grupo Listo; e

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

11.7. Departamento de Recursos Humanos

11.7.1. Garantir que todos os Colaboradores do Grupo Listo tenham ciência das diretrizes presentes neste documento;

11.7.2. Apoiar a elaboração dos treinamentos de capacitação sobre as diretrizes deste documento em conjunto o Gestor deste documento;

11.7.3. Manter os termos assinados por todos os Colaboradores, referente à ciência das informações contidas neste documento.

12. PENALIDADES

12.1. O Grupo Listo estabelece severas penalidades para aqueles empregados e executivos que deixem de cumprir as normativas internas e/ou regras aplicáveis as suas atividades e as empresas do Grupo Listo, sem prejuízo aos infratores responderem civil, criminal e administrativamente pelos atos ou omissões praticados, seja perante o Grupo Listo ou terceiros.

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

12.2.1. Advertência verbal;

12.2.2. Advertência por escrito;

12.2.3. Suspensão; e

12.2.4. Desligamento.