| 0 | 03 | 90 | 002 |
|---|---|---|---|

**POLÍTICAS, NORMAS E PROCEDIMENTOS**

# Política de Segurança da Informação

## 1. OBJETIVO

1.1. Esta política tem como objetivo estabelecer diretrizes e princípios gerais de segurança da informação e cibernética para a Rumo, em um esforço para garantir que os usuários atuem em observância às regras referentes ao tratamento e proteção das informações e ativos de informação, bem como assegurar a capacidade da Rumo em garantir a confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade e responsabilidade, além de prevenir, detectar e reduzir riscos de segurança da informação e cibernética.

## 2. APLICAÇÃO E ABRANGÊNCIA

2.1. Aplica-se a todos os Colaboradores da Rumo no Brasil e no exterior, desde sua data de aprovação em **08/11/2023**. Abrange a Rumo e todas as empresas controladas do Grupo Cosan.

Os Fornecedores da Rumo também estão sujeitos às diretrizes, procedimentos e controles estabelecidos nessa política sempre que realizarem o tratamento de informações ou utilizarem os ativos de informação da Rumo.

## 3. DEFINIÇÕES

| | |
|---|---|
| **Colaborador** | Empregados, contratados, subcontratados, estagiários, menores aprendizes e administradores. |
| **Usuário** | Qualquer indivíduo, processo, dispositivo ou mecanismo que acesse, use ou manipule uma informação ou ativo de informação. |
| **Fornecedor** | Todas as empresas fornecedoras, parceiras e prestadoras de serviços a Terceiros que celebraram um contrato de fornecimento, parceria e/ou prestação de serviços com as empresas da Rumo, bem como seus representantes, empregados e subcontratados. |
| **Centro de Defesa Cibernética (CDC)** | Equipe composta por profissionais que tem como objetivo monitorar e proteger a Rumo contra ameaças digitais. |
| **TI** | Tecnologia da Informação. |
| **Log** | Termo técnico utilizado para descrever o registro das transações que ocorrem quando um software é utilizado. |
| **Banco de Dados** | Coleção organizada de informações - ou dados - estruturadas, normalmente armazenadas eletronicamente em um sistema de computador. |
| **Desenvolvimento de Software** | É a atividade de criar programas computacionais, executada por um desenvolvedor ou grupo de desenvolvedores. |
| **Lei Geral de Proteção de Dados – (LGPD)** | Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais. |

A circulação ou divulgação deste documento é restrita às empresas e Colaboradores da Rumo. A divulgação externa é proibida, salvo com autorização expressa de Controles Internos.

| | |
|---|---|
| **Dados Pessoais** | Quaisquer dados que se relacionem com um indivíduo identificado ou identificável ou uma pessoa que possa ser identificada por meios razoavelmente prováveis de serem usados. Exemplificativamente, são considerados Dados Pessoais: nome, idade, sexo, filiação, endereço físico e eletrônico, números de documentos, identificadores corporativos ("CS" e "TR") identificadores eletrônicos (IP, IMEI), geolocalização, perfil de navegação na internet, perfil de consumo. |
| **Dados Pessoais Sensíveis** | Dado Pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. |
| **Software** | É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares. |
| **Malwares** | Termo utilizado para se referir a uma variedade de formas de software hostil ou intruso. |
| **Spywares** | Software espião que costuma ser instalado no celular ou no computador sem o consentimento do usuário. |
| **Botnets** | Rede de computadores que foram infectados por softwares maliciosos e podem ser controlados remotamente para executar ataques maliciosos. |
| **VPN** | Do inglês, virtual private network. Tecnologia que permite o acesso remoto à rede corporativa. |

## 4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação abrange 5 (cinco) pilares fundamentais, destacados a seguir:

- **Confidencialidade:** Garante que a informação e ativos de informação sejam acessíveis somente pelos usuários autorizados, pelo período necessário;
- **Disponibilidade:** Garante que a informação e ativos de informação estejam disponíveis para os usuários autorizados sempre que necessários aos processos de negócio ou a clientes;
- **Integridade:** Garante que a informação e ativos de informação estejam completos e íntegros e que não tenham sido modificados ou destruídos de maneira não autorizada ou acidental durante o seu ciclo de vida;
- **Autenticidade:** Garante a propriedade da informação e que esta seja proveniente da fonte anunciada e não foi alvo de alterações indevidas ao longo de um processo estabelecido.
- **Irretratabilidade (não repúdio):** Garante que uma pessoa ou entidade não possa negar a autoria da informação fornecida, como no caso do uso de certificados digitais para transações online e assinatura de documentos eletrônicos. Na gestão da segurança da informação, isso

A circulação ou divulgação deste documento é restrita às empresas e Colaboradores da Rumo. A divulgação externa é proibida, salvo com autorização expressa de Controles Internos.

significa ser capaz de provar o que foi feito, quem fez e quando fez em um sistema, impossibilitando a negação das ações dos usuários.

## 4.1. ASPECTOS GERAIS

a. A proteção das informações e ativos de informação da Rumo deve ser uma prioridade constante em todas as áreas de negócio e de suporte, de forma a reduzir riscos, bem como danos e/ou prejuízos que possam comprometer a imagem e os objetivos organizacionais;

b. A proteção das informações e ativos de informação deve ser aplicada de forma compatível com seu impacto a Rumo, abrangendo todos os processos, informatizados ou não. As informações sob responsabilidade da Rumo devem ser manuseadas de acordo com as leis vigentes e normas internas e utilizadas apenas para a finalidade para a qual foram coletadas, evitando o comprometimento de sua confidencialidade, integridade, disponibilidade e autenticidade, inclusive, mas não se limitando, quando no uso de soluções, plataformas e recursos externos, como por exemplo: aplicativos de mensagens, redes sociais, aplicativos de inteligência artificial etc. O colaborador se responsabiliza por ações ocorridas no trato dos dados de titularidade da Rumo e/ou Terceiros que lhe tenham sido confiados em virtude de sua atividade profissional, em todo o seu ciclo de vida. Assim, garante que o responsável responda por tais questões, inclusive diante da lei;

c. Uma pessoa ou entidade não pode negar a autoria da informação fornecida, portanto, a irretratabilidade garante a autenticidade de ações tomadas sob um determinado usuário ou processo;

d. Caso aplicável, e sempre que possível, os processos da Rumo devem garantir a segregação das funções por meio da participação de mais de um Colaborador ou equipe de Colaboradores nas atividades, a fim de evitar o conflito de interesse e reduzir o risco de uso indevido acidental ou proposital dos ativos de informação e sistemas.

e. Todos os Colaboradores e Fornecedores da Rumo, conforme aplicável, devem ter ciência de que o uso dos ativos de informação, dos sistemas e ambientes, e respectivas políticas de senhas, podem ser monitorados e que os registros podem ser utilizados para detecção de violações desta Política e procedimentos de segurança da informação, servindo de evidência para a aplicação de medidas disciplinares, processos administrativos e/ou legais.

A circulação ou divulgação deste documento é restrita às empresas e Colaboradores da Rumo. A divulgação externa é proibida, salvo com autorização expressa de Controles Internos.

f. Os riscos de segurança da informação, bem como dúvidas sobre a Política e procedimentos relacionadas devem ser reportados à área Corporativa de Segurança da Informação e/ou ao representante local de segurança da informação (Business Information Security Officer – BISO);

g. Exceto com a expressa autorização do seu proprietário responsável, as tecnologias, marcas, metodologias e quaisquer informações da Rumo não devem ser repassadas ou compartilhadas com terceiros, assim como para fins pessoais, ainda que tenham sido obtidas ou desenvolvidas pelo próprio colaborador durante o exercício de suas funções.

## 5. DIRETRIZES, CONTROLES E PROCESSOS

### 5.1. UTILIZAÇÃO SEGURA DE RECURSOS DE TI

5.1.1. Os recursos corporativos, conforme procedimento interno "Uso seguro de recursos de TI", devem ser somente utilizados para fins profissionais, sendo resguardado as empresas da Rumo, o direito de controlar e monitorar a utilização dos recursos fornecidos aos colaboradores e terceiros.

### 5.2. CLASSIFICAÇÃO DAS INFORMAÇÕES

5.2.1. Quando aplicável, toda informação criada deve ser classificada e protegida ao longo de todo seu ciclo de vida, nos termos do Procedimento de Classificação da Informação. O ciclo de vida das informações compreende sua criação ou coleta, manuseio, armazenamento, transporte e descarte.

Para assegurar a proteção adequada das informações, elas devem ser classificadas de acordo com o seu valor, requisitos legais, relevância, sensibilidade e criticidade para a Rumo. Os critérios de classificação devem considerar as necessidades de negócio, demandas regulatórias, compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

Abaixo os níveis de sigilo recomendados (Público, Interno, Confidencial e Restrito). Entretanto, as empresas da Rumo podem estabelecer seus próprios rótulos desde que sejam equiparáveis aos listados nessa Política, conforme Procedimento interno "Classificação da Informação"

A classificação da informação (nível de sigilo) é de responsabilidade da área que a gerou.

- **Informação Pública**: pode ser disponibilizada sem restrições. O conhecimento dessa informação por qualquer indivíduo não causa impactos aos objetivos da Companhia.

A circulação ou divulgação deste documento é restrita às empresas e Colaboradores da Rumo. A divulgação externa é proibida, salvo com autorização expressa de Controles Internos.

- **Informação Interna**: somente pode ser disponibilizada para os usuários da Companhia. Informações deste nível de sigilo são operacionais e o seu conhecimento por terceiros não impacta os objetivos de negócio.
- **Informação Confidencial**: indica forte restrição ao uso e o acesso indevido. Pode acarretar impacto financeiro, operacional ou perda de vantagem competitiva. Quando extraviada ou indevidamente utilizada, pode prejudicar gravemente os objetivos de negócio. O gestor responsável deve indicar explicitamente quais funções podem ter acesso.
- **Informação Restrita**: informação cujo uso e acesso são restritos a um grupo específico de colaboradores designados nominalmente, não podendo ser divulgado a pessoas não autorizadas, total ou parcialmente, em qualquer que seja o formato. Compreende assuntos, documentos, imagens, ou quaisquer materiais estratégicos, altamente sensíveis e críticos. A sua indisponibilidade, divulgação ou alteração não autorizadas causam graves prejuízos aos objetivos de negócios.

## 5.3. PROTEÇÃO DE DADOS PESSOAIS E DADOS SENSÍVEIS

5.3.1. A Rumo leva a sério a proteção de dados pessoais e de dados sensíveis e as medidas de segurança estabelecidas nesta Política são essenciais para garantir o cumprimento da legislação acerca da proteção de dados pessoais (LGPD). Para atender aos termos da presente Política e da Política de Privacidade e Proteção de Dados, a Rumo estabelece o Programa de Privacidade e Proteção de Dados.

## 5.4. SEGURANÇA CIBERNÉTICA

5.4.1. De forma a auxiliar na implantação das diretrizes estabelecidas nesta Política e dos controles, processos e procedimentos do Sistema de Gestão de Segurança de Informação e da Segurança Cibernética da Rumo, são adotados, por padrão, as boas práticas disponíveis no mercado:

a. Medidas de autenticação capazes de individualizar usuários que acessam ativos de informação, sistemas e ambientes da Rumo;

b. Emprego de criptografia, mascaramento e ofuscação, quando aplicável, para o armazenamento de informações relevantes e sensíveis, inclusive dados pessoais, em ativos de informação, sistemas e ambientes da Rumo e de fornecedores;

c. Soluções de prevenção e detecção de intrusão e acessos não-autorizados aos ativos de informação, sistemas e ambientes da Rumo;

A circulação ou divulgação deste documento é restrita às empresas e Colaboradores da Rumo. A divulgação externa é proibida, salvo com autorização expressa de Controles Internos.

d. Uso de procedimentos e controles para prevenir o vazamento de informações; e. Testes e varreduras periódicas para a detecção de falhas e vulnerabilidades nos procedimentos, controles, sistemas e ambientes da Rumo;

e. Soluções de proteção contra softwares maliciosos (malwares, spywares, trojans, vírus, botnets, etc) que podem afetar ativos de informação, sistemas e ambientes da Rumo;

f. Sistemas de rastreamento de atividade e registros (logs) para as atividades realizadas pelo Centro de Defesa Cibernética (CDC);

g. Controle de acesso dos usuários que fazem uso dos sistemas e ambientes da Rumo;

h. Segregação e segmentação dos diferentes ambientes de rede disponibilizados pela Rumo ou fornecedores por ele contratado aos seus colaboradores, fornecedores e clientes, quando aplicável e validado pela área de Segurança da Informação;

i. Manutenção de cópias de segurança (backup) das informações;

j. Os controles mínimos listados também devem ser aplicados no desenvolvimento de novos produtos, soluções, aplicativos, sistemas e ambientes, bem como na aquisição de novas tecnologias e serviços que integrarão as atividades operacionais. Da mesma forma, os controles mínimos listados também deverão ser adotados, conforme aplicável, por fornecedores que processam ou armazenam informações sensíveis ou relevantes para a condução das atividades operacionais da Rumo.

## 5.5. GESTÃO DE IDENTIDADES E ACESSOS

5.5.1. Os processos de concessão, alteração e exclusão de acesso aos ativos de informação, sistemas de informação e/ou ambientes da Rumo são realizados pela área competente mediante aprovação formal do gestor do solicitante e do respectivo proprietário do sistema e/ou perfil, sempre quando necessário para o desempenho das atividades, conforme procedimento interno "Gestão de Identidades e Acessos".

## 5.6. USO DE SENHAS

5.6.1. A senha é de responsabilidade de cada Colaborador, que deve considerar minimamente as seguintes regras:

a. A senha é pessoal e intransferível;

A circulação ou divulgação deste documento é restrita às empresas e Colaboradores da Rumo. A divulgação externa é proibida, salvo com autorização expressa de Controles Internos.

b. O uso de senhas corporativas em computadores e dispositivos móveis não homologados pela Rumo é expressamente proibido;

c. O armazenamento de senha em navegadores da web deve ser evitado;

d. As senhas não devem ser anotadas ou armazenadas em meios físicos e digitais (ex.: e-mail, planilhas, bloco de notas, arquivos na rede etc.);

e. Devem ser usadas senhas diferentes para diferentes serviços. Senhas de uso particular devem ser diferentes das senhas corporativas;

f. Se o Colaborador desconfiar que a senha foi descoberta, deve solicitar alteração e/ou bloqueio imediato;

g. É proibido o uso do nome de qualquer empresa, produtos ou serviços da Rumo, e números sequenciais na formação da senha.

## 5.7. GERENCIAMENTO DE ATIVOS

5.7.1. O inventário de ativos de TI precisa ser constantemente mantido e atualizado contemplando os principais ativos de informação, tais como: sistemas, aplicações, bancos de dados e servidores. O hardware deve ser adquirido apenas de Fornecedores aprovados, e mantido considerando as seguintes diretrizes:

a. Somente configurações de Software aprovadas devem ser aplicadas ao novo hardware;

b. Os usuários finais devem tomar os devidos cuidados com qualquer hardware que lhes tenha sido entregue;

c. O hardware perdido e/ou roubado deve ser relatado imediatamente para o Service Desk ou área de TI competente;

d. O hardware em fim de vida útil deve ser descartado com segurança de acordo com as orientações do Service Desk ou área de TI competente.

## 5.8. GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO

5.8.1. A Rumo possui um processo estruturado de monitoramento, análise e identificação dos riscos, vulnerabilidades, ameaças e impactos sobre os ativos de informação, para que sejam identificados os controles adequados e a eficácia periodicamente testada, como referenciado no procedimento “Gestão de Riscos em Segurança da Informação”.

A circulação ou divulgação deste documento é restrita às empresas e Colaboradores da Rumo. A divulgação externa é proibida, salvo com autorização expressa de Controles Internos.

## 5.9. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

5.9.1. A Rumo adota procedimentos, requisitos e controles específicos para a prevenção e resposta a incidentes ocorridos, de acordo com o "Procedimento de Resposta a Incidentes IT & OT".

Os procedimentos, controles e requisitos para Fornecedores devem estar alinhados com os próprios níveis de complexidade, abrangência e precisão da Rumo.

## 5.10. TREINAMENTO E CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

5.10.1. Como parte do seu compromisso, a Rumo adota ações e iniciativas para promover a capacitação, aculturamento e avaliação dos Colaboradores sobre o tema segurança da informação, reforçando as diretrizes declaradas nesta política.

## 5.11. AVALIAÇÃO DE SEGURANÇA DA INFORMAÇÃO NA CONTRATAÇÃO DE SERVIÇOS

5.11.1. Os processos e os controles necessários para reduzir os riscos associados às iniciativas de terceirização, incluindo acordos de computação em nuvem, devem fazer parte dos acordos comerciais entre os Fornecedores e as empresas da Rumo.

As empresas da Rumo se reservam ao direito de avaliar se o Fornecedor atende aos requisitos de segurança da informação, baseados em normas e boas práticas de mercado e no procedimento "Avaliação de riscos de Segurança da Informação em Fornecedores".

Os contratos com Terceiros devem garantir que a equipe ou subcontratados da organização externa cumpram os documentos normativos de segurança da informação da Rumo.

## 5.12. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SOFTWARE

5.12.1. O processo de aquisição de software deve respeitar todos os direitos autorais de software de computador e os termos de todas as licenças de software das quais as empresas da Rumo são parte.

As empresas da Rumo devem gerenciar seus ativos de software e assegurar somente o uso de software legal em suas estações de trabalho e servidores.

Cópias de software de terceiros, com direitos autorais do desenvolvedor do software, a menos que expressamente autorizado, são proibidas, conforme procedimento de Uso seguro de recursos de TI.

A circulação ou divulgação deste documento é restrita às empresas e Colaboradores da Rumo. A divulgação externa é proibida, salvo com autorização expressa de Controles Internos.

Os sistemas e aplicativos desenvolvidos internamente ou por especificação das empresas da Rumo devem estar em conformidade com o "Procedimento de desenvolvimento seguro de sistemas e aplicações" e garantir:

a. Avaliação de impacto em privacidade deve ser concluída para as principais alterações de software;
b. Os requisitos de segurança do software devem ser documentados como parte do processo de desenvolvimento;
c. As alterações de software devem estar sujeitas a procedimentos de controle;
d. Somente usuários autorizados têm permissão para implantar alterações de software; e. Garantia de conceito de segregação de funções tanto para atividades de negócio quanto para administração de TI;
e. Garantia de autenticação e configuração de segurança para senhas de acesso;
f. Segregação de ambientes para desenvolvimento, qualidade e produção;
g. A contratação de serviços para manutenção e desenvolvimento de aplicações deverá conter requisitos de segurança (ex.: utilizando um modelo de RFP ou documento específico para contratações);
h. Garantia de avaliação de segurança em código antes da promoção para ambientes produtivos.

## 6. DIVULGAÇÃO DESTA POLÍTICA

6.1. Esta política é divulgada para todos os colaboradores da Rumo e está disponível nos canais de comunicação de cada empresa (ex.: Intranet, Biblioteca de Conhecimento no Workplace, POC etc.).

## 7. MEDIDAS DISCIPLINARES

7.1. A suspeita de não observância dos procedimentos desta Política por colaboradores ou terceiros será apurada pelos Comitês competentes e avaliada pelo Conselho de Administração ou equivalente, conforme previsto no procedimento de apuração interna.

Colaboradores eventualmente infratores estarão sujeitos às sanções disciplinares previstas na Política de Medidas Disciplinares e no Código de Conduta, sem prejuízo da Rumo adotar as medidas administrativas, civis e penais cabíveis conforme o caso.

Terceiros eventualmente infratores estarão sujeitos às sanções comerciais contratuais cabíveis, incluindo a imediata rescisão contratual, com aplicação das penalidades decorrentes da rescisão, sem prejuízo de ação indenizatória e outras providências legais cabíveis.

A circulação ou divulgação deste documento é restrita às empresas e Colaboradores da Rumo. A divulgação externa é proibida, salvo com autorização expressa de Controles Internos.

## 8. REPORTE E DÚVIDAS

8.1. Constitui responsabilidade de todos os colaboradores e terceiros garantir o cumprimento desta Política.

Indícios de descumprimento ou dúvidas acerca do cumprimento desta Política ou do Código de Conduta poderão ser reportados ao gestor imediato do colaborador, ao departamento de Recursos Humanos, à Auditoria Interna, ao Compliance ou por meio de um dos Canais de Comunicação disponíveis (0800-725-0039 ou www.canaldeetica.com.br/cosan).

A Rumo não tolera qualquer retaliação contra qualquer pessoa, interna ou externa, que comunique de boa-fé uma violação ou suspeita de violação a esta Política ou ao seu Código de Conduta, sendo garantida a confidencialidade acerca da identidade de qualquer pessoa que comunicar eventual violação.

A prática de retaliação é sujeita a medidas disciplinares que podem resultar, inclusive, no desligamento do colaborador da Rumo ou encerramento de um contrato, conforme o caso.

## 9. REVISÃO DESTA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

9.1. Esta Política deve ser revisada ao menos uma vez por ano, e eventuais alterações devem ser aprovadas pelo Conselho de Administração.

## 10. REVISÃO E APROVAÇÃO

| Etapa | Nome | Cargo/Função | |
|---|---|---|---|
| **Elaboração** | Thiago Kysyk Campo Nogueira | Coordenador de Segurança da Informação | **Revisão 2** |
| **Revisão** | André Novaes Frutuoso | Gerente Segurança da Informação | |
| **Aprovação** | Fernando Madureira | Diretor de Segurança da Informação Cibernética (CISO) | |
| **Elaboração** | Cristiane Belitardo Pagoti de Britto | Analista de Segurança da Informação | **Revisão 1** |
| **Revisão** | André Novaes Frutuoso | Gerente Segurança da Informação | |
| **Revisão** | Wagner de Cicco | Head de Auditoria e Controles Internos | |
| **Aprovação** | Fernando Madureira | Head de Segurança da Informação (CISO) | |

A circulação ou divulgação deste documento é restrita às empresas e Colaboradores da Rumo. A divulgação externa é proibida, salvo com autorização expressa de Controles Internos.