Identificação

Título **POL-015 Política de Segurança da Informação e Privacidade**

Classificação **PÚBLICO**

Histórico de Revisões do Documento

A tabela abaixo é um registro das revisões deste documento em ordem cronológica, sendo a última entrada à versão atual.

Versão	Data	Responsável	Comentários
01	20/08/2026	Comitê de SIP	Elaboração do documento. Esta política substitui a política de segurança da informação, bem como, a política de proteção de dados.

Strada

Sumário

1. Objetivo 3
2. Escopo e Aplicabilidade deste documento 3
3. Revisão e Atualização 4
4. Aprovação e Vigência 4
5. Referência 4
6. Termos e Definições 4
7. Governança e Responsabilidade 4
8. Princípios de Segurança da Informação e Privacidade 5
9. Estrutura para Objetivos de Segurança da Informação e Privacidade 5
10. Compromissos da Organização 6
Compromisso com Requisitos Aplicáveis 6
Compromisso com a Segurança da Informação 6
Compromisso com a Privacidade e Proteção de Dados Pessoais 6
Compromisso com os Objetivos de Segurança da Informação e Privacidade 7
Compromisso com a Gestão de Riscos 7
Compromisso com a Resposta a Incidentes 7
Compromisso com a Continuidade de Negócios 7
Compromisso com Recursos e Competência 8
Compromisso com Comunicação e Transparência 8
Compromisso com a Melhoria Contínua 8
Compromissos com Partes Interessadas em Geral 8
Compromissos da Organização 8
Responsabilidades das Partes Interessadas 9
Compromissos com Titulares de Dados Pessoais 9
Direitos dos Titulares de Dados 9
Responsabilidades dos Titulares de Dados 10
Canal para Exercício de Direitos 10
Compromissos dos Colaboradores 10
Compromissos de Terceiros e Fornecedores 11

1. Objetivo

Este documento estabelece a Política de Segurança da Informação e Privacidade da organização.

A Política de Segurança da Informação e Privacidade estabelece os princípios, diretrizes e compromissos da organização para proteger a confidencialidade, a integridade e a disponibilidade da informação, bem como os direitos e liberdades fundamentais dos titulares de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados (LGPD) e com as normas internacionais adotadas pela organização.

Esta política é apropriada ao propósito e ao contexto da organização e apoia sua direção estratégica. Esta política estabelece uma estrutura para:

- definir e alcançar objetivos de segurança da informação e de privacidade;
- responder adequadamente aos riscos relacionados à segurança da informação e à proteção de dados pessoais;
- proteger a organização, seus colaboradores, clientes, parceiros, titulares de dados e demais partes interessadas;
- assegurar o cumprimento dos requisitos legais, regulatórios e contratuais aplicáveis, incluindo a LGPD;
- promover a melhoria contínua do Sistema de Gestão Integrado de Segurança da Informação e Privacidade (SGI).

2. Escopo e Aplicabilidade deste documento

Este documento está sujeito às diretrizes do SGI da organização conforme expresso em “DIR-004 Diretrizes do SGI”, parte integrante do Framework Operacional de Governança (GOF) da organização.

Este documento integra a estrutura hierárquica de documentos definida no documento-base correspondente acima citado, bem como do GOF. Isto significa que os requisitos e definições estabelecidos nos documentos de ordem superior são vinculantes.

Esta política se aplica a toda a organização e deve ser seguida por todos os colaboradores, independentemente do tipo de vínculo contratual, e por quaisquer partes interessadas que atuem em atividade sob controle da organização e que envolva o tratamento de informação ou de dados pessoais, incluindo, mas não se limitando a terceiros e fornecedores.

A organização deve assegurar que esta política seja mantida e esteja disponível como informação documentada, acessível aos colaboradores e às partes interessadas relevantes, conforme apropriado, bem como protegida contra perda, alteração indevida ou acesso não autorizado.

Dúvidas quanto à sua aplicação devem ser direcionadas à Área de Segurança da Informação e Privacidade.

O descumprimento desta política estará sujeito às medidas previstas em RGM-010 Norma de Medidas Disciplinares da organização.

3. Revisão e Atualização

Esta política deve ser:

- revisada no mínimo a cada 12 (doze) meses;
- revisada sempre que ocorrerem mudanças significativas na organização, em seus processos ou em seu contexto;
- revisada após incidentes relevantes de segurança da informação ou de proteção de dados pessoais;
- revisada quando houver alterações em requisitos legais, regulatórios ou contratuais aplicáveis, incluindo alterações na LGPD ou em regulamentações da Autoridade Nacional de Proteção de Dados (ANPD);
- atualizada conforme necessário para manter sua adequação, suficiência e eficácia.

4. Aprovação e Vigência

Esta Política de Segurança da Informação e Privacidade entra em vigor a partir de sua aprovação pela Alta Direção e ratificação pelo Conselho de Administração, e permanece válida até que seja substituída por versão atualizada.

A Alta Direção e o Conselho de Administração reafirmam formalmente seu compromisso com a segurança da informação, com a proteção de dados pessoais e com os direitos dos titulares, garantindo que esta política seja aplicada de forma consistente em toda a organização.

5. Referência

Este documento herda as referências estabelecidas em DIR-004 Diretrizes do SGI e em DIR-001 Diretrizes do GOF, e nas respectivas referências desses documentos.

6. Termos e Definições

Aplicam-se os termos e definições estabelecidos em DIR-001 Diretrizes do GOF, DIR-004 Diretrizes do SGI e ESQ-015 Termos e Definições.

7. Governança e Responsabilidade

O **Conselho de Administração** é responsável por ratificar esta política e avaliar a governança da organização em relação à segurança da informação e à privacidade.

A **Alta Direção** é responsável por aprovar esta política, garantir sua implementação, assegurar sua adequação contínua e promover sua integração à estratégia organizacional.

O **Comitê de Segurança da Informação e Privacidade (Comitê de SIP)** é responsável pela definição e revisão desta política, pela definição dos objetivos de segurança da

informação e privacidade, e pela análise crítica do SGI, conforme detalhado em DIR-004 Diretrizes do SGI.

A **Área de Segurança da Informação e Privacidade** é responsável pela operacionalização do SGI e pela gestão dos riscos, controles e incidentes de segurança da informação e privacidade.

O **Encarregado de Dados (DPO)** é responsável por atuar como canal de comunicação entre a organização, os titulares de dados e a ANPD, e por apoiar a aplicação desta política.

Os **gestores das áreas** são responsáveis por assegurar que esta política seja seguida por seus liderados e por reportar riscos relevantes.

Os **colaboradores** da organização devem assimilar, aceitar e aplicar esta política.

8. Princípios de Segurança da Informação e Privacidade

A organização estabelece que a Segurança da Informação e a Privacidade devem ser:

- integradas à governança organizacional;
- baseadas em risco;
- orientadas à proteção da confidencialidade, integridade e disponibilidade da informação;
- orientadas à proteção dos direitos e liberdades fundamentais dos titulares de dados pessoais;
- fundamentadas nos princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas, conforme o art. 6º da LGPD;
- compatíveis com o contexto e o propósito da organização;
- suportadas por recursos adequados;
- avaliadas periodicamente;
- continuamente aprimoradas;
- alinhadas às demais políticas da organização.

9. Estrutura para Objetivos de Segurança da Informação e Privacidade

Esta política estabelece que os objetivos de segurança da informação e de privacidade devem:

- ser definidos em níveis estratégico, tático e operacional;
- considerar os resultados da avaliação de riscos de segurança da informação e de riscos aos direitos e liberdades dos titulares de dados pessoais;
- incluir critérios mensuráveis de desempenho, quando aplicável;
- possuir responsáveis designados;

- possuir prazos definidos;
- ser monitorados regularmente;
- ser revisados periodicamente.

10. Compromissos da Organização

A Alta Direção declara e assume os seguintes compromissos formais:

Compromisso com Requisitos Aplicáveis

A organização compromete-se a:

- cumprir a LGPD e demais requisitos legais, regulatórios, contratuais e societários aplicáveis à segurança da informação e à proteção de dados pessoais;
- cumprir requisitos normativos e internos do SGI, incluindo instruções de trabalho, procedimentos, políticas, normas e demais documentos de governança da organização;
- manter processos para identificar, avaliar e atualizar continuamente os requisitos aplicáveis;
- cooperar com a ANPD e demais autoridades competentes.

Compromisso com a Segurança da Informação

A organização compromete-se a:

- preservar a confidencialidade, a integridade e a disponibilidade das informações e dos ativos de informação sob sua responsabilidade;
- identificar, analisar, avaliar e tratar os riscos e oportunidades relacionados à segurança da informação;
- implementar controles de segurança da informação proporcionais aos riscos identificados;
- prevenir, detectar e responder a incidentes de segurança da informação de forma estruturada e tempestiva.

Compromisso com a Privacidade e Proteção de Dados Pessoais

A organização compromete-se a:

- tratar dados pessoais apenas para finalidades legítimas, específicas, explícitas e previamente informadas ao titular;
- adotar medidas técnicas, administrativas e organizacionais adequadas para proteger os dados pessoais sob sua responsabilidade;
- observar, em todo tratamento de dados pessoais, os princípios estabelecidos no art. 6º da LGPD;
- assegurar base legal adequada para cada operação de tratamento de dados pessoais;

- adotar a privacidade desde a concepção e por padrão (privacy by design and by default) no desenvolvimento de produtos, serviços e processos;
- realizar avaliação de impacto à proteção de dados pessoais quando aplicável;
- manter registro das operações de tratamento de dados pessoais.

Compromisso com os Objetivos de Segurança da Informação e Privacidade

A organização compromete-se a:

- estabelecer objetivos de segurança da informação e de privacidade mensuráveis, quando aplicável;
- alinhar os objetivos à estratégia organizacional;
- garantir a coerência dos objetivos com os riscos identificados;
- monitorar o desempenho dos objetivos definidos;
- revisar periodicamente os objetivos;
- promover ações corretivas e preventivas quando necessário.

Compromisso com a Gestão de Riscos

A organização compromete-se a:

- identificar riscos que possam afetar a segurança da informação e os direitos e liberdades dos titulares de dados pessoais;
- avaliar impactos potenciais sobre a organização, seus colaboradores e os titulares de dados;
- definir controles e estratégias para o tratamento dos riscos identificados;
- monitorar continuamente os riscos relacionados à segurança da informação e à privacidade;
- revisar os riscos após mudanças significativas no contexto organizacional.

Compromisso com a Resposta a Incidentes

A organização compromete-se a:

- manter processo estruturado de gestão de incidentes de segurança da informação e de incidentes relacionados a dados pessoais;
- comunicar à ANPD e aos titulares afetados os incidentes de segurança que possam acarretar risco ou dano relevante, nos termos exigidos pela LGPD e pela regulamentação da ANPD;
- registrar e tratar não conformidades e ações corretivas decorrentes de incidentes.

Compromisso com a Continuidade de Negócios

A organização compromete-se a assegurar que os princípios e controles de segurança da informação e privacidade sejam mantidos durante situações de disrupção, resposta a incidentes e recuperação das operações, em alinhamento com o documento específico de Continuidade de Negócios.

Compromisso com Recursos e Competência

A organização compromete-se a:

- disponibilizar os recursos humanos, tecnológicos e financeiros necessários ao funcionamento do SGI;
- assegurar a competência das pessoas envolvidas na segurança da informação e na proteção de dados pessoais;
- promover treinamento e conscientização contínuos;
- manter estrutura organizacional adequada para a gestão da segurança da informação e da privacidade.

Compromisso com Comunicação e Transparência

A organização compromete-se a:

- estabelecer processos formais de comunicação interna e externa relacionados à segurança da informação e à privacidade;
- assegurar que esta política seja comunicada internamente, compreendida pelas pessoas e disponibilizada às partes interessadas relevantes;
- disponibilizar esta política no website institucional, por e-mail quando solicitado por parte interessada, e via intranet;
- comunicar esta política aos colaboradores na admissão, via intranet, no âmbito do programa de conscientização e sempre que houver alterações em seu conteúdo;
- ser transparente quanto às finalidades do tratamento de dados pessoais e aos direitos dos titulares, sem prejuízo da proteção de informações classificadas como restritas.

Compromisso com a Melhoria Contínua

A organização compromete-se a:

- melhorar continuamente a eficácia do SGI, da segurança da informação e da privacidade;
- monitorar o desempenho por meio de indicadores, auditorias e análises críticas;
- tratar não conformidades e oportunidades de melhoria;
- analisar criticamente, em intervalos planejados, a adequação desta política;
- incorporar melhorias identificadas por auditorias, incidentes e pelo retorno de colaboradores e partes interessadas.

Compromissos com Partes Interessadas em Geral

Para os fins desta seção, consideram-se partes interessadas aquelas destacadas em ESQ-002 Partes Interessadas.

Compromissos da Organização

A organização compromete-se a:

- identificar e compreender as necessidades e expectativas legítimas das partes interessadas relevantes;
- manter comunicação transparente e tempestiva com as partes interessadas sobre temas de segurança da informação e privacidade;
- cooperar com autoridades e órgãos reguladores competentes no exercício de suas atribuições legais;
- considerar os requisitos das partes interessadas na definição do escopo e dos objetivos do SGI.

Responsabilidades das Partes Interessadas

As partes interessadas que atuem em atividade sob controle da organização devem:

- observar esta política e as demais normas aplicáveis quando em interação com a organização;
- utilizar os canais oficiais da organização para comunicação, dúvidas e solicitações;
- reportar à organização qualquer violação, risco ou incidente de que tenham conhecimento e que possa afetar a segurança da informação ou a proteção de dados pessoais.

Compromissos com Titulares de Dados Pessoais

Compromissos da Organização com os Titulares de Dados

A organização compromete-se a:

- proteger os dados pessoais dos titulares por meio de medidas físicas, administrativas e tecnológicas adequadas;
- atender às solicitações dos titulares no exercício de seus direitos, nos prazos e condições previstos na LGPD;
- informar aos titulares, de forma clara e acessível, sobre o tratamento de seus dados pessoais, observados os limites de sigilo aplicáveis;
- disponibilizar canal formal para o exercício dos direitos previstos na LGPD.

Direitos dos Titulares de Dados

A LGPD assegura aos titulares, entre outros, os seguintes direitos em relação aos seus dados pessoais:

- confirmação da existência de tratamento;
- acesso aos dados;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados tratados em desconformidade com a lei;
- portabilidade dos dados a outro fornecedor de serviço ou produto;
- eliminação dos dados pessoais tratados com base no consentimento, quando aplicável;

- informação sobre as entidades públicas e privadas com as quais a organização compartilhou dados;
- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- revogação do consentimento, quando esta for a base legal do tratamento;
- revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, quando aplicável.

Estes direitos não são absolutos e podem ser limitados nas hipóteses previstas em lei, notadamente quando a organização deva cumprir obrigação legal ou regulatória. As solicitações serão respondidas cumprindo o prazo legal.

Responsabilidades dos Titulares de Dados

Cabe ao titular de dados pessoais, no relacionamento com a organização:

- fornecer dados pessoais corretos e atualizados;
- exercer seus direitos por meio do canal oficial disponibilizado pela organização;
- comunicar à organização qualquer suspeita de uso indevido de seus dados pessoais de que tenha conhecimento.

Canal para Exercício de Direitos

Solicitações relacionadas ao tratamento de dados pessoais pela organização em atendimento aos direitos dos titulares previstos na LGPD e resoluções da ANPD, devem ser dirigidas ao Encarregado de Dados (DPO), por meio do canal: **dpo@strada.log.br** e serão respondidas dentro do prazo previsto em Lei.

Compromissos dos Colaboradores

Compromissos da Organização com os Colaboradores

A organização compromete-se a:

- fornecer treinamento e conscientização adequados em segurança da informação e privacidade;
- disponibilizar os recursos e ferramentas necessários para que os colaboradores protejam a informação e os dados pessoais sob sua responsabilidade;
- manter canais claros e acessíveis para reporte de violações, riscos, incidentes e não conformidades;
- não retaliar colaboradores que reportem, de boa-fé, violações, riscos ou incidentes.

Deveres dos Colaboradores

É dever de todos os colaboradores, de acordo com seus papéis, autoridades e responsabilidades atribuídas:

- cumprir esta política e as demais normas aplicáveis do SGI, bem como instruções de trabalho, procedimentos, políticas, normas e demais documentos de governança da organização;
- atuar de forma transparente e responsável para evitar a perda da confidencialidade, integridade e disponibilidade das informações tratadas pela organização, bem como dos ativos de informação utilizados para este fim;
- tratar dados pessoais no âmbito de suas atividades apenas com finalidade específica e identificada;
- classificar documentos, incluindo os que contenham dado pessoal ou dado pessoal sensível, conforme RGM-002 Norma de Classificação de Ativos de Informação;
- reportar qualquer violação desta política, evento, incidente, risco, oportunidade ou não conformidade relacionada à segurança da informação ou à privacidade;
- comprometer-se com a melhoria contínua da segurança da informação, da privacidade e do SGI;
- ser diligente e cuidadoso com o tratamento de informações, não divulgando informação que não seja expressamente autorizada pela organização.

Compromissos de Terceiros e Fornecedores

Compromissos da Organização com Terceiros e Fornecedores

A organização compromete-se a:

- selecionar terceiros e fornecedores considerando padrões adequados de segurança da informação e de proteção de dados pessoais, proporcionais ao serviço contratado;
- estabelecer, quando aplicável, cláusulas contratuais de confidencialidade e de proteção de dados pessoais;
- comunicar aos terceiros e fornecedores os requisitos de segurança da informação e privacidade aplicáveis à relação contratual.

Deveres de Terceiros e Fornecedores

Todos os terceiros e fornecedores que prestem serviços à organização ou tratem dados pessoais em seu nome devem:

- cumprir os requisitos contratuais relacionados à segurança da informação e à proteção de dados pessoais;
- manter níveis adequados de segurança da informação e, quando atuarem como operadores de dados pessoais, tratá-los estritamente nos limites e finalidades autorizados pela organização;
- comunicar prontamente à organização qualquer incidente que possa impactar a organização, seus colaboradores ou os titulares de dados pessoais;
- cooperar com auditorias e avaliações de conformidade quando solicitado;
- cumprir os requisitos legais, regulatórios e contratuais aplicáveis.