POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - POL023	
RESPONSABILIDADE: TECNOLOGIA DA INFORMAÇÃO	REV. 002 DATA: 01/08/2026

SUMÁRIO

1. OBJETIVO

Estabelecer as diretrizes para a governança da Segurança da Informação na Steelmast, assegurando que as informações e os ativos que as suportam sejam protegidos de forma compatível com sua criticidade, com os riscos aos quais estão expostos e com os objetivos estratégicos da organização.

Esta Política visa promover a proteção da confidencialidade, integridade, disponibilidade e autenticidade das informações corporativas, fortalecer a gestão de riscos, apoiar a continuidade das operações, assegurar a conformidade com os requisitos legais, regulatórios e contratuais aplicáveis e fomentar uma cultura organizacional voltada à segurança da informação.

2. DOCUMENTOS DE REFERÊNCIA

Código de Conduta da Steelmast;
Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018);
Política de Proteção de Dados Pessoais;
Demais políticas, normas e procedimentos internos relacionados à governança, tecnologia da informação e segurança da informação.

3. DEFINIÇÕES

Informação - qualquer informação, sistema, equipamento, software, banco de dados, documento, infraestrutura, serviço ou recurso que possua valor para a Steelmast e que necessite de proteção.

Backup – cópia de segurança de informações, sistemas ou dados, mantida com a finalidade de possibilitar sua recuperação em caso de perda, indisponibilidade, corrupção ou comprometimento dos dados.

Confidencialidade - garantia de que as informações sejam acessadas apenas por pessoas autorizadas.

Incidente de Segurança da Informação - evento confirmado ou suspeito que comprometa ou possa comprometer a confidencialidade, integridade, disponibilidade ou autenticidade das informações ou dos ativos de informação.

Dados Pessoais – informação relacionada a pessoa natural identificada ou identificável, nos termos da Lei Geral de Proteção de Dados Pessoais – LGPD.

Disponibilidade – garantia de que as informações e os recursos necessários ao seu acesso estejam disponíveis e acessíveis às pessoas autorizadas quando necessários.

Segurança da Informação – conjunto de princípios, processos, controles e medidas destinados à proteção das informações e dos ativos que as suportam, visando preservar sua confidencialidade, integridade, disponibilidade e autenticidade.

Ameaça – circunstância, evento ou agente com potencial para explorar uma vulnerabilidade e causar impacto negativo sobre as informações ou ativos de informação.

Integridade - garantia de que as informações permaneçam completas, íntegras, precisas e protegidas contra alterações não autorizadas.

Usuário - qualquer pessoa autorizada a acessar informações, sistemas, recursos tecnológicos ou ativos de informação da Steelmast.

4. DIRETRIZES GERAIS

4.1 Governança da Segurança da Informação

A Segurança da Informação integra o sistema de governança corporativa da Steelmast e constitui elemento estratégico para a proteção dos ativos de informação, a gestão de riscos, a continuidade das operações e o atendimento aos requisitos legais, regulatórios e contratuais aplicáveis.

Sua gestão deverá ocorrer de forma integrada às práticas de governança, gestão de riscos, compliance e controles internos, assegurando que decisões relacionadas à proteção das informações considerem sua criticidade, os riscos envolvidos, os impactos ao negócio e os objetivos estratégicos da organização.

A implementação dos controles de Segurança da Informação deverá observar critérios de proporcionalidade, efetividade e melhoria contínua, buscando fortalecer a resiliência organizacional e reduzir a exposição a ameaças internas e externas.

4.2 Gestão dos Ativos de Informação

Os ativos de informação deverão ser identificados, classificados, protegidos e gerenciados durante todo o seu ciclo de vida, considerando sua relevância para os processos da organização, seu valor estratégico e os riscos associados à sua utilização.

Cada ativo deverá possuir responsável definido, cabendo a este assegurar sua adequada utilização, proteção e conservação durante todo o seu ciclo de vida.

Os controles aplicáveis deverão considerar, entre outros fatores, a criticidade da informação, seu valor estratégico, os riscos associados e os requisitos legais, regulatórios e contratuais incidentes.

4.3 Classificação da Informação

As informações produzidas, recebidas, armazenadas ou compartilhadas pela Steelmast deverão ser classificadas de acordo com seu nível de criticidade, sensibilidade e necessidade de proteção, considerando os impactos decorrentes de seu acesso, divulgação, alteração, perda ou indisponibilidade.

A classificação das informações deverá orientar a definição dos controles de segurança aplicáveis ao seu armazenamento, processamento, compartilhamento, retenção e descarte, observando os requisitos legais, regulatórios, contratuais e as necessidades do negócio.

Sempre que houver alteração na natureza da informação, em sua finalidade de utilização ou nos riscos associados, sua classificação deverá ser reavaliada, assegurando que os controles permaneçam compatíveis com sua criticidade.

4.4 Gestão de Identidades e controle de acessos

A Steelmast adotará mecanismos destinados a assegurar que o acesso às informações e aos ativos de informação seja concedido, alterado, monitorado e revogado de forma controlada, rastreável e compatível com as responsabilidades atribuídas a cada usuário.

A concessão de acessos deverá observar critérios de necessidade de negócio, segregação de funções, menor privilégio e responsabilidade individual, de forma a reduzir riscos decorrentes de acessos indevidos ou incompatíveis com as atividades desempenhadas.

As credenciais de acesso são de uso pessoal e intransferível, cabendo a cada usuário adotar as medidas necessárias para sua adequada utilização e proteção.

Os acessos deverão ser periodicamente revisados e atualizados sempre que houver alterações funcionais, desligamentos, mudanças de atribuições ou outras situações que justifiquem sua adequação.

Sempre que compatível com o nível de risco envolvido, a Steelmast poderá adotar mecanismos adicionais de autenticação e proteção dos acessos aos seus ativos de informação.

4.5 Segurança da Infraestrutura tecnológica

A infraestrutura tecnológica da Steelmast deverá ser administrada de forma a assegurar a disponibilidade, integridade, confiabilidade e resiliência dos recursos que suportam os processos de negócio.

Os controles técnicos e administrativos adotados deverão considerar a criticidade dos ativos, a evolução das ameaças, as vulnerabilidades identificadas e os riscos associados ao ambiente tecnológico, buscando preservar a continuidade das operações e reduzir a exposição a incidentes de Segurança da Informação.

Os sistemas, equipamentos, redes, aplicações e demais recursos tecnológicos deverão ser mantidos em condições adequadas de funcionamento e proteção, observando as diretrizes estabelecidas pela organização e as boas práticas aplicáveis à Segurança da Informação.

4.6 Gestão de incidentes de segurança da informação

A Steelmast manterá processos destinados à identificação, registro, comunicação, tratamento e acompanhamento dos incidentes de Segurança da Informação, visando minimizar impactos aos seus ativos de informação, preservar a continuidade das operações e fortalecer seus controles internos.

Todo evento ou suspeita de evento que possa comprometer a confidencialidade, integridade, disponibilidade ou autenticidade das informações deverá ser comunicado tempestivamente aos responsáveis competentes, possibilitando a adoção das medidas de contenção, investigação, mitigação e recuperação cabíveis.

Os incidentes deverão ser avaliados quanto às suas causas, impactos e riscos associados, podendo resultar na implementação de ações corretivas, preventivas ou de melhoria dos processos, controles e mecanismos de governança da Segurança da Informação.

4.7 Segurança na relação com fornecedores e terceiros

A Steelmast estabelecerá requisitos de Segurança da Informação aplicáveis aos terceiros que, em razão da execução de suas atividades, tenham acesso às informações, sistemas, ambientes tecnológicos ou demais ativos de informação da organização.

Os riscos decorrentes da contratação de terceiros deverão ser avaliados de forma proporcional à natureza dos serviços prestados, ao nível de acesso concedido e à criticidade das informações envolvidas, podendo ser adotados mecanismos de *due diligence,* avaliação de controles, monitoramento periódico e demais medidas de mitigação de riscos.

Sempre que aplicável, os requisitos de Segurança da Informação deverão ser formalizados por meio de instrumentos contratuais, cláusulas específicas de confidencialidade ou outros mecanismos destinados à proteção dos ativos de informação da Steelmast.

4.8 Monitoramento, auditoria e melhoria contínua

A Steelmast manterá mecanismos destinados ao monitoramento da efetividade dos controles de Segurança da Informação, utilizando, sempre que aplicável, indicadores de desempenho, avaliações de riscos, auditorias, verificações de conformidade e demais instrumentos de governança.

Os resultados obtidos deverão subsidiar a revisão dos controles existentes, a definição de ações corretivas e preventivas, a atualização desta Política e a melhoria contínua do sistema de governança da Segurança da Informação.

A Segurança da Informação será objeto de avaliação contínua, considerando alterações no ambiente organizacional, evolução das ameaças, mudanças tecnológicas, requisitos legais e regulatórios, bem como os objetivos estratégicos da Steelmast.

5. VIOLAÇÕES DA POLÍTICA

O descumprimento das disposições desta Política poderá sujeitar o responsável à adoção das medidas administrativas, disciplinares, contratuais, civis ou penais cabíveis, conforme a legislação vigente, o Código de Conduta e Ética da Steelmast, os contratos firmados e demais normas internas aplicáveis.

Sem prejuízo das medidas aplicáveis, a organização poderá adotar ações destinadas à contenção dos riscos, preservação dos ativos de informação, apuração dos fatos, implementação de controles adicionais e prevenção de recorrências.

6. DISPOSIÇÕES FINAIS

Esta Política entra em vigor na data de sua aprovação pela Alta Direção e permanecerá vigente por prazo indeterminado, devendo ser revisada periodicamente ou sempre que houver alterações relevantes na estrutura organizacional, nos processos de negócio, no ambiente tecnológico, nos requisitos legais ou regulatórios, ou nos riscos relacionados à Segurança da Informação.

As diretrizes estabelecidas nesta Política deverão ser observadas em conjunto com as demais políticas, normas e procedimentos internos da Steelmast relacionados à governança corporativa, gestão de riscos, proteção de dados pessoais, tecnologia da informação e controles internos.

Os casos omissos serão analisados pelas áreas competentes, observadas suas atribuições, em conjunto com a área de Tecnologia da Informação e, quando aplicável, pelas áreas responsáveis por GRC ou Jurídico.

HISTÓRICO DE VERSÕES		
Revisão	**Motivo**	**Data**
001	Versão Inicial	06/10/2022
002	Atualização da Política	01/08/2026