RESUMO PÚBLICO

Política de Segurança da Informação da Declink

Documento de referência	PO-SIN-001 — Política de Segurança da Informação
Revisão / Data da política	Rev. 00 — 22/05/2026
Tipo de publicação	Resumo público para divulgação institucional
Finalidade	Apresentar, de forma objetiva, os compromissos da Declink com segurança da informação, proteção de dados e melhoria contínua.

1. Compromisso da Declink

A Declink reconhece a segurança da informação como elemento essencial para a confiança de seus clientes, colaboradores, parceiros e demais partes interessadas. A Política de Segurança da Informação estabelece diretrizes para proteger informações, ativos tecnológicos, dados pessoais, sistemas e serviços sob responsabilidade da organização, em alinhamento às boas práticas de governança, à ISO/IEC 27001, à ISO/IEC 27002, à LGPD e aos requisitos contratuais aplicáveis.

Este resumo público apresenta os principais compromissos assumidos pela Declink, sem substituir a versão integral da política interna, que orienta os procedimentos, controles, responsabilidades e evidências mantidas no âmbito do Sistema de Gestão de Segurança da Informação — SGSI.

2. Abrangência

As diretrizes de segurança da informação aplicam-se a diretores, colaboradores, estagiários, prestadores de serviço, parceiros, fornecedores, terceiros autorizados e demais pessoas que acessem informações, ambientes, sistemas, redes, aplicações ou ativos tecnológicos da Declink.

A política abrange informações em meio digital, físico, verbal, audiovisual e lógico, bem como os ativos associados, tais como computadores, notebooks, dispositivos móveis, sistemas corporativos, serviços em nuvem, contas de e-mail, redes, documentos, bases de dados, backups e ambientes de desenvolvimento, homologação e produção.

3. Princípios de Segurança da Informação

A Declink adota como fundamentos de segurança da informação a proteção da confidencialidade, integridade, disponibilidade e auditabilidade das informações e sistemas.

- Confidencialidade: proteção contra acesso, divulgação ou uso não autorizado das informações.
- Integridade: preservação da exatidão, consistência e completude das informações.
- Disponibilidade: garantia de que informações e sistemas estejam acessíveis quando necessários.
- Auditabilidade: manutenção de rastreabilidade das ações, transações e eventos relevantes.

4. Diretrizes Gerais de Segurança

- As informações devem ser acessadas apenas por pessoas autorizadas e na medida necessária ao desempenho de suas atividades.
- Os acessos devem observar o princípio do menor privilégio, a segregação de funções e a rastreabilidade das ações executadas.

- Dados pessoais e informações confidenciais devem receber tratamento compatível com sua criticidade, sensibilidade e requisitos legais ou contratuais.
- Os recursos de tecnologia da informação devem ser utilizados prioritariamente para finalidades profissionais e institucionais.
- Incidentes, fragilidades, perdas, vazamentos, acessos indevidos e suspeitas de comprometimento devem ser reportados imediatamente pelos canais definidos pela organização.
- Os controles de segurança devem ser proporcionais aos riscos do negócio, revisados periodicamente e aprimorados de forma contínua.

5. Principais Controles Adotados

- **Controle de acesso e identidade:** Cada usuário deve possuir identificação individual, única e intransferível. A concessão, alteração, revisão e revogação de acessos deve seguir fluxo formal e rastreável.
- **Proteção de equipamentos e softwares:** Somente softwares autorizados devem ser instalados ou utilizados. Os equipamentos devem observar controles como senha, bloqueio automático, proteção contra malware, atualização e demais mecanismos definidos pela área responsável.
- **E-mail, internet e comunicações:** O e-mail corporativo e o acesso à internet devem ser utilizados de forma segura e compatível com as atividades profissionais. Mensagens suspeitas, tentativas de phishing e links não confiáveis devem ser reportados.
- **Classificação, armazenamento e descarte:** As informações devem ser classificadas e tratadas conforme sua sensibilidade, necessidade de negócio, obrigações legais, requisitos contratuais e prazos de retenção aplicáveis.
- **Terceiros e serviços em nuvem:** Fornecedores, parceiros e terceiros devem cumprir requisitos de confidencialidade, privacidade, segurança da informação e continuidade compatíveis com o risco do serviço prestado.
- **Incidentes de segurança:** Eventos suspeitos ou confirmados que possam comprometer informações ou serviços devem ser registrados, analisados, tratados e, quando aplicável, comunicados às partes interessadas.
- **Logs e rastreabilidade:** A Declink mantém registros de logs e eventos, conforme aplicável, para apoiar auditoria, diagnóstico, investigação de incidentes, continuidade dos serviços e conformidade.
- **Continuidade do negócio:** A Declink mantém diretrizes para avaliar riscos, proteger ativos e apoiar a continuidade dos serviços diante de eventos que possam afetar atividades críticas.

6. Proteção de Dados Pessoais e Privacidade

A Declink trata dados pessoais e informações confidenciais observando critérios de necessidade, finalidade, segurança, prevenção e responsabilização. Quando houver envolvimento de dados pessoais, as medidas adotadas devem considerar a LGPD, os contratos firmados, a natureza dos dados, a criticidade do processo e os riscos aos titulares.

A organização orienta que o uso, armazenamento, compartilhamento, retenção e descarte de informações sejam realizados por meios autorizados, seguros e compatíveis com a classificação da informação e com as obrigações legais e contratuais aplicáveis.

7. Responsabilidades

A segurança da informação é de responsabilidade compartilhada. A Diretoria aprova a política, provê recursos e direcionamento estratégico. O Comitê de Segurança da Informação e o responsável pela Segurança da Informação coordenam a manutenção da política, apoiam a gestão de riscos, acompanham incidentes relevantes e promovem melhorias.

Gestores devem garantir que suas equipes cumpram as diretrizes estabelecidas. A área de Tecnologia da Informação implementa controles técnicos, administra identidades e acessos, mantém registros e apoia o monitoramento. Colaboradores e terceiros autorizados devem conhecer e cumprir as diretrizes, proteger credenciais, zelar pelos ativos sob sua guarda e reportar imediatamente qualquer situação de risco.

8. Monitoramento, Conformidade e Melhoria Contínua

A Declink poderá adotar mecanismos excepcionais de monitoramento, registro, auditoria e análise de uso dos recursos corporativos, respeitando os limites legais e as finalidades legítimas de segurança, continuidade, investigação e conformidade.

O descumprimento das diretrizes de segurança poderá ensejar medidas administrativas, disciplinares, contratuais, civis ou criminais, conforme a gravidade do fato e a legislação aplicável. A política deve ser revisada periodicamente e sempre que houver mudanças relevantes no negócio, na tecnologia, nos requisitos legais, contratuais ou no cenário de riscos da organização.

9. Comunicação de Eventos de Segurança

Qualquer suspeita de phishing, malware, vazamento de dados, acesso indevido, perda de equipamento, indisponibilidade relevante, uso indevido de credenciais, exposição pública de informações ou violação de política deve ser comunicada imediatamente pelos canais oficiais definidos pela Declink.

10. Declaração Final

A Declink reafirma seu compromisso com a proteção das informações, a confiança dos clientes, a conformidade legal e contratual, a segurança dos serviços e a melhoria contínua do seu Sistema de Gestão de Segurança da Informação.

Nota: este documento é uma versão resumida e pública da Política de Segurança da Informação da Declink. A versão integral interna contém regras operacionais e controles detalhados para aplicação no âmbito do SGSI.