

Política de Segurança da Informação - Versão Pública

Classificação: PÚBLICO | Código: PUB-SEG-003 | Versão: 1.0 | Última atualização: 08/09/2026

A informação é um ativo essencial para a GNX GROUP. Esta versão pública apresenta os princípios e compromissos gerais utilizados para proteger informações corporativas, de clientes, candidatos, colaboradores, parceiros e demais titulares, sem divulgar configurações técnicas, arquiteturas ou controles operacionais que possam aumentar riscos de segurança.

1. Objetivo e escopo

A GNX GROUP adota diretrizes de segurança destinadas a prevenir acessos não autorizados, uso indevido, duplicação, perda, modificação e divulgação indevida de informações. As diretrizes alcançam sistemas, equipamentos, serviços, documentos, pessoas e terceiros que tratem informações sob responsabilidade ou custódia da organização.

2. Princípios fundamentais

Princípio	Compromisso
Confidencialidade	As informações são acessadas somente por pessoas devidamente autorizadas e de acordo com necessidade funcional.
Integridade	Alterações, inclusões e exclusões devem ocorrer de forma autorizada, controlada e rastreável.
Disponibilidade	Informações e serviços devem permanecer disponíveis às pessoas autorizadas quando necessários à operação e às obrigações aplicáveis.

3. Governança e gestão de riscos

A segurança da informação é acompanhada por estruturas internas de governança, com responsabilidades definidas para aprovação de diretrizes, avaliação de riscos, acompanhamento de controles, tratamento de desvios e melhoria contínua. A análise de risco orienta a priorização de medidas de proteção proporcionais à criticidade das informações e dos serviços.

4. Classificação da informação

As informações podem ser classificadas de acordo com seu nível de sensibilidade e impacto, incluindo categorias públicas, internas, confidenciais e restritas. A classificação orienta controles de acesso, compartilhamento, armazenamento, transmissão e descarte.

5. Controle de acesso e autenticação

O acesso aos sistemas e ambientes é controlado e concedido de acordo com função, necessidade e autorização. A GNX GROUP utiliza identificação individual de usuários, mecanismos de autenticação,

revisão de acessos e revogação quando a permissão deixa de ser necessária, inclusive em mudanças de função ou desligamentos.

6. Proteção de dados pessoais e informações confidenciais

Dados pessoais e informações confidenciais são protegidos contra acesso, uso, alteração, compartilhamento e divulgação não autorizados. Os controles aplicáveis podem incluir restrição de acesso, autenticação, criptografia quando adequada ao risco, armazenamento em ambientes corporativos, monitoramento, rastreabilidade e descarte seguro.

7. Terceiros e fornecedores

Terceiros que armazenem, processem ou acessem informações da GNX GROUP devem observar requisitos de segurança compatíveis com o risco. Conforme a atividade, podem ser adotadas avaliações de segurança, obrigações contratuais, compromissos de confidencialidade e requisitos de retenção e exclusão.

8. Monitoramento, vulnerabilidades e auditoria

A GNX GROUP mantém processos de monitoramento e verificação de conformidade compatíveis com o risco, incluindo trilhas de auditoria, análise de eventos de segurança, avaliação de vulnerabilidades e auditorias periódicas. Atividades suspeitas são analisadas e tratadas de acordo com procedimentos internos.

9. Gestão de incidentes

A organização mantém processo de resposta a incidentes para identificação, contenção, investigação, correção, preservação de evidências e adoção de medidas de comunicação quando exigidas pela legislação ou pela regulamentação aplicável.

10. Treinamento e conscientização

Colaboradores e terceiros sujeitos às regras corporativas recebem orientações e ações de conscientização relacionadas à segurança da informação, ao uso adequado dos recursos e à proteção de informações.

11. Continuidade de negócios

A GNX GROUP mantém práticas de continuidade destinadas a preservar processos críticos e reduzir impactos decorrentes de indisponibilidade ou eventos de segurança, de forma compatível com os requisitos do negócio e os riscos identificados.

12. Retenção e descarte

Informações deixam de ser mantidas quando encerrada sua finalidade e inexistente obrigação de conservação. O descarte deve observar a classificação da informação, a Política de Retenção, Armazenamento e Exclusão de Dados e os procedimentos técnicos aplicáveis.

13. Privacidade e contato

Eventos ou dúvidas relacionados à proteção de dados pessoais podem ser comunicados pelo Canal de Privacidade: privacidade@gnxgroup.com.br. Informações detalhadas sobre tratamento de dados pessoais estão disponíveis na Política de Privacidade e Proteção de Dados da GNX GROUP.

14. Atualização

Esta versão pública poderá ser atualizada para refletir mudanças relevantes na governança, nos requisitos legais ou nos controles de segurança, preservado o sigilo das informações operacionais e técnicas que não sejam apropriadas para divulgação externa.