Política de Segurança da Informação da Nexum

Versão 1.0

Sumário

1. Objetivo 3

2. Escopo 3

3. Princípios e Compromissos 3

4. Responsabilidades 4

5. Comunicação e Conscientização 5

6. Tratamento de Descumprimentos 5

7. Conformidade 6

8. Revisão e Atualização 6

Política de Segurança da Informação da Nexum

1. Objetivo

Estabelecer os princípios e compromissos da Nexum para a proteção das informações e orientar o estabelecimento, implementação, manutenção e melhoria contínua do Sistema de Gestão da Segurança da Informação — SGSI.

Esta Política é apropriada ao propósito institucional da Nexum de impulsionar a reinvenção digital de organizações com sentido humano, conectando pessoas, processos e tecnologias para transformar negócios e vidas, ao estabelecer princípios para a proteção das informações, processos e tecnologias que suportam suas atividades e soluções.

Esta Política fornece a estrutura para o estabelecimento dos objetivos de segurança da informação e para a definição dos controles necessários, considerando o contexto da Nexum, os riscos e os requisitos aplicáveis.

2. Escopo

Esta Política aplica-se às pessoas, processos, informações, ativos, sistemas e recursos abrangidos pelo SGSI da Nexum.

Aplica-se aos colaboradores, prestadores, terceiros autorizados e demais partes que possuam responsabilidades relacionadas às informações ou aos recursos abrangidos, conforme a natureza de suas atividades, acessos e responsabilidades.

Para serviços, ambientes ou recursos operados por clientes ou fornecedores, aplicam-se as responsabilidades contratuais de cada parte e os controles sob responsabilidade da Nexum.

3. Princípios e Compromissos

A Nexum reconhece a informação como recurso relevante para suas atividades e compromete-se a protegê-la de forma proporcional ao seu valor, classificação, criticidade e riscos associados.

A segurança da informação deverá considerar, principalmente:

a) **confidencialidade:** acesso e divulgação das informações somente por pessoas ou partes autorizadas;

b) **integridade:** proteção da exatidão, completude e consistência das informações contra alterações indevidas;

c) **disponibilidade:** acesso às informações, sistemas e serviços pelas partes autorizadas quando necessário.

Para apoiar esses princípios, a Nexum compromete-se a:

a) identificar, avaliar e tratar os riscos de segurança da informação de forma proporcional ao contexto, às necessidades do negócio e aos requisitos aplicáveis;

b) estabelecer e acompanhar objetivos de segurança da informação coerentes com esta Política e com os resultados da avaliação e tratamento de riscos;

c) definir e manter controles organizacionais, de pessoas, físicos e tecnológicos necessários ao tratamento dos riscos e demais necessidades do SGSI;

d) atender aos requisitos legais, regulatórios, contratuais e demais requisitos aplicáveis relacionados à segurança da informação;

e) proteger as informações durante seu ciclo de vida, considerando sua classificação, utilização, armazenamento, acesso, transferência, retenção e descarte, conforme aplicável;

f) controlar os acessos às informações e recursos de acordo com as necessidades das funções e responsabilidades atribuídas;

g) considerar os riscos de segurança da informação relacionados a fornecedores, serviços externos e demais dependências relevantes;

h) promover competência, conscientização e responsabilidade das pessoas cujas atividades possam afetar o SGSI;

i) tratar eventos, incidentes, vulnerabilidades, não conformidades e outras situações relevantes de acordo com os processos definidos no SGSI;

j) considerar requisitos de continuidade e recuperação proporcionais às necessidades dos processos e serviços abrangidos; e

k) melhorar continuamente a pertinência, adequação e eficácia do SGSI.

Os requisitos específicos para cada tema deverão ser estabelecidos nas políticas, procedimentos, planos, programas e demais informações documentadas vigentes do SGSI.

4. Responsabilidades

Para fins desta Política, aplicam-se as seguintes responsabilidades:

- **Alta Direção:** aprovar esta Política, estabelecer direção e objetivos compatíveis com o SGSI, disponibilizar recursos adequados e apoiar sua implementação e melhoria.

- **Comitê do SGSI:** apoiar a governança desta Política, acompanhar assuntos relevantes de segurança da informação e avaliar necessidades de atualização ou

melhoria conforme suas atribuições.

- **Responsável pelo SGSI ou Segurança da Informação:** coordenar ou apoiar a manutenção desta Política, orientar sua aplicação, acompanhar requisitos pertinentes e apoiar sua comunicação e análise crítica.

- **Gestores e responsáveis por processos:** aplicar os requisitos de segurança da informação pertinentes às atividades sob sua responsabilidade e apoiar o tratamento dos riscos e ações correspondentes.

- **TI e responsáveis técnicos:** implementar e manter os controles tecnológicos sob sua responsabilidade conforme os documentos aplicáveis do SGSI.

- **Gestores de contratos:** acompanhar os requisitos de segurança da informação relacionados aos fornecedores e serviços sob sua responsabilidade.

- **Colaboradores, prestadores e terceiros autorizados:** conhecer e observar esta Política e os demais requisitos aplicáveis às suas atividades, proteger as informações sob sua responsabilidade e comunicar eventos, suspeitas ou desvios relevantes.

As responsabilidades específicas deverão permanecer definidas nos documentos e registros organizacionais pertinentes.

5. Comunicação e Conscientização

Esta Política deverá ser comunicada às pessoas abrangidas pelo SGSI de forma compatível com suas responsabilidades e necessidade de conhecimento.

A conscientização sobre seus princípios deverá integrar as ações previstas na Política de Treinamento, Conscientização e Comunicação e no Programa de Treinamento, Conscientização e Comunicação vigentes da Nexum.

As pessoas deverão estar conscientes de:

a) suas responsabilidades de segurança da informação;

b) sua contribuição para a eficácia do SGSI; e

c) consequências do descumprimento dos requisitos aplicáveis.

A Política deverá ser disponibilizada às partes interessadas pertinentes, conforme apropriado e pelos meios institucionais definidos pela Nexum.

6. Tratamento de Descumprimentos

Descumprimentos desta Política deverão ser avaliados conforme sua natureza, impacto, risco e evidências disponíveis.

Quando aplicável, poderão ser encaminhados aos processos de:

a) orientação ou treinamento;

b) gestão de incidentes;

c) ações corretivas;

d) controle ou revisão de acessos;

e) gestão de riscos;

f) processo disciplinar; ou

g) medidas contratuais ou legais pertinentes.

As medidas adotadas deverão ser proporcionais à situação identificada e observar os documentos internos, contratos e requisitos aplicáveis.

7. Conformidade

Esta Política relaciona-se principalmente ao requisito 5.2 — Política da ABNT NBR ISO/IEC 27001:2022 e, conforme a aplicabilidade registrada na Declaração de Aplicabilidade da Nexum, ao controle:

- **A.5.1** — Políticas de segurança da informação.

Outros requisitos e controles da ABNT NBR ISO/IEC 27001:2022 são tratados pelas políticas, procedimentos, planos, programas, controles e registros específicos integrantes do SGSI.

A existência desta Política, isoladamente, não demonstra a implementação ou eficácia dos controles do SGSI, que deverão ser avaliadas com base nas evidências e resultados pertinentes.

8. Revisão e Atualização

Esta Política deverá ser analisada criticamente em intervalos planejados e quando ocorrerem mudanças significativas que possam afetar sua adequação.

A revisão deverá considerar, conforme aplicável:

a) mudanças no contexto, escopo ou objetivos da Nexum;

b) mudanças relevantes nos riscos de segurança da informação;

c) alterações legais, regulatórias ou contratuais;

d) mudanças significativas em processos, tecnologias, fornecedores ou formas de

trabalho;

e) incidentes, não conformidades ou resultados de auditorias que indiquem necessidade de revisão;

f) alterações relevantes nos requisitos das partes interessadas; e

g) resultados da análise crítica pela Direção.

As alterações deverão observar o processo de controle da informação documentada e as alçadas de aprovação vigentes no SGSI.

Bauru, 26 de agosto de 2026.

Rodrigo Certo Junqueira

Chief Executive Officer da Nexum

Fábio Duran Marques

Chief Operating Officer da Nexum

Ana Carolina Certo Junqueira Ponce

Chief Financial Officer da Nexum