Política de Segurança da Informação

Revisão: Dez/2025

1. Objetivo

O propósito deste documento é instituir a Política de Segurança da Informação da NEWB ADMINISTRADORA E CORRETORA DE SEGUROS LTDA. Integrada ao sistema de gestão corporativa e em conformidade com as melhores práticas de mercado, esta política visa blindar os ativos de tecnologia, os processos operacionais e as pessoas envolvidas no ecossistema da empresa.

2. Abrangência

As diretrizes aqui descritas aplicam-se obrigatoriamente a todos os colaboradores, fornecedores de serviços e quaisquer indivíduos que possuam autoridade para representar a NEWB ou suas controladas. A política abrange qualquer pessoa que tenha, teve ou terá acesso a dados da Companhia ou que utilize sua infraestrutura computacional, respeitando-se os acordos operacionais vigentes.

3. Termos e Definições

Para a correta interpretação deste documento, consideram-se:

- **Ativo:** Qualquer elemento capaz de criar, armazenar, transmitir ou descartar informações críticas que agreguem valor ao negócio.
- **Comitê de Segurança da Informação:** Responsável por propor e apoiar a execução de estratégias de segurança.
- **Confidencialidade:** Garantia de que a informação não será acessada ou revelada a pessoas ou sistemas não autorizados.
- **Disponibilidade:** Garantia de que a informação estará acessível para uso por pessoas autorizadas sempre que necessário.
- **Incidente de Segurança:** Qualquer evento, suspeito ou confirmado, que ameace a segurança dos ativos tecnológicos e possa comprometer a confidencialidade, integridade ou disponibilidade dos dados.
- **Integridade:** Garantia de que a informação se mantenha exata, completa e inalterada indevidamente.
- **Risco de Segurança:** O impacto gerado pela incerteza em relação ao cumprimento dos objetivos de segurança.
- **Segurança da Informação:** Conjunto de ações para preservar a confidencialidade, integridade e disponibilidade dos dados da NewB ou sob sua guarda.

- **Usuário da Informação:** Colaboradores, terceiros ou entidades autorizadas a manipular ativos da NewB para fins profissionais, independentemente do tipo de vínculo contratual.
- **Violação:** Qualquer ato ou omissão que desrespeite as normas e políticas de segurança estabelecidas pela empresa.
- **Vulnerabilidade:** Fragilidade que pode originar um incidente de segurança, colocando em risco as operações ou informações da empresa.

4. Princípios

Para garantir a efetividade desta política, a NewB adota os seguintes princípios fundamentais:

- **Conformidade e Proteção:** Criação e cumprimento rigoroso de normas e procedimentos para assegurar a tríade de segurança (confidencialidade, integridade e disponibilidade), protegendo os dados contra ameaças internas e externas.
- **Educação:** Promoção constante de conscientização e treinamento dos colaboradores sobre práticas seguras.
- **Legalidade:** Aderência estrita a leis, regulamentos e obrigações contratuais relacionadas à segurança da informação.
- **Gestão de Incidentes:** Tratamento completo de incidentes, incluindo registro, investigação, correção e documentação, com o apoio de todas as áreas e comunicação às autoridades quando necessário.
- **Continuidade de Negócios:** Manutenção e testes periódicos de planos de recuperação de desastres para garantir a operação contínua da empresa.
- **Melhoria Contínua:** Revisão sistemática dos objetivos de segurança em todos os níveis, garantindo que sejam mensuráveis, monitorados e documentados.
- **Gestão de Mudanças:** Planejamento cuidadoso de alterações no sistema de gestão para manter sua eficácia e pertinência.

5. Diretrizes

A NewB estabelece diretrizes para fomentar um comportamento seguro, prevenir incidentes e responsabilidades legais, além de assegurar a proteção das informações e o cumprimento regulatório.

- **5.1 Controle da Informação:** As informações devem ser classificadas adequadamente. Sendo ativos vitais, elas devem ser protegidas conforme as leis e normas internas.
- **5.2 Proteção de Dados:** Compromisso com a legislação de proteção de dados para manter a segurança das informações. O armazenamento de dados

privados ou confidenciais deve seguir estritamente as regras de retenção e finalidade.

- **5.3 Arquitetura de Segurança:** Adoção de modelos de referência e tecnologias de segurança proporcionais à criticidade das informações tratadas pelos sistemas da NewB.
- **5.4 Gestão de Ativos Tecnológicos:** Definição de responsabilidades e regras para o gerenciamento do ciclo de vida de todo hardware e software, incluindo equipamentos que circulam fora da empresa.
- **5.5 Conscientização:** Disseminação de uma cultura sólida de segurança através de programas de capacitação contínua.
- **5.6 Plano de Continuidade de Negócio:** Gestão da capacidade de manter processos, tecnologias e pessoas essenciais operando mesmo em cenários de crise.
- **5.7 Gestão de Identidades e Acessos:** Controle rigoroso de acessos para evitar privilégios excessivos, fraudes ou vazamentos, garantindo a segregação de funções conforme as normas da empresa.
- **5.8 Resposta a Incidentes:** Atuação focada na redução de danos causados por ações indevidas ou violações de política.
- **5.9 Segurança de Redes:** Monitoramento e gestão de vulnerabilidades para prevenir acessos não autorizados e garantir a disponibilidade da rede corporativa.
- **5.10 Privacidade:** Proteção de dados pessoais de forma a garantir sua confidencialidade e integridade em todos os canais e processos da companhia.
- **5.11 Monitoramento:** Análise e correlação de eventos para detectar desvios de conduta ou ameaças, visando a proteção de todos os envolvidos no negócio.
- **5.12 Segurança de Software:** Aplicação de diretrizes de segurança desde o desenvolvimento até a manutenção de sistemas e aplicativos, exigindo o mesmo padrão de fornecedores de software.
- **5.13 Gestão de Terceiros:** Estabelecimento de requisitos de segurança em contratos com fornecedores, assegurando que eles possuam políticas documentadas para proteger os dados da NewB.
- **5.14 Gestão de Vulnerabilidades:** Gerenciamento preventivo de falhas de segurança em ativos locais ou em nuvem para mitigar riscos tecnológicos.
- **5.15 Segurança Física:** Manutenção de diretrizes para a proteção física dos perímetros onde dados e informações são armazenados.