Código	POL16	Data	28/08/2024
Assunto	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA ÁGUAS DO NORTE, S.A.		

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA ÁGUAS DO NORTE, S.A.

1. INTRODUÇÃO

A Águas de Norte, S.A, doravante designada por AdNorte está ciente da importância da Segurança da Informação na sua organização como vetor determinante no sucesso da realização da sua missão.

Garantir a confidencialidade, a integridade e a disponibilidade dos seus ativos, é um objetivo estratégico na AdNorte na resiliência operacional e na confiança digital dos serviços por si disponibilizados, bem como no suporte nas decisões de negócio.

A Política de Segurança da Informação implementada pela AdNorte orienta-se por modelos de referência internacionais e nacionais, como a ISO/IEC 27001 e o Quadro Nacional de Referência para a Cibersegurança.

A AdNorte compromete-se com esta Política a disponibilizar todos os recursos necessários à melhoria contínua da Segurança da Informação, permitindo, cumprir os requisitos legais, contratuais, normativos em vigor e aplicáveis à AdNorte, bem como demais requisitos das partes interessadas. Compromete-se ainda a realizar uma gestão adequada dos riscos que se colocam à segurança da informação, através da análise do risco de segurança e da adoção das medidas técnicas e organizativas, de forma a eliminar ou mitigar os riscos que impactem negativamente a normal continuidade da organização, a sua reputação e as suas partes interessadas.

2. OBJETIVO

A presente Política define os princípios e as regras fundamentais de gestão da segurança da Informação da AdNorte.

3. ÂMBITO

Esta política aplica-se aos trabalhadores, aos colaboradores externos, estagiários, aos fornecedores ou qualquer outra entidade que de alguma forma aceda e trate ativos de informação da AdNorte.

4. PRINCÍPIOS ORIENTADORES DA POLÍTICA

A Política da Segurança de Informação da AdNorte assenta nos seguintes pilares:

a) **Confidencialidade** - Garantir de que a informação está acessível apenas por pessoas devidamente autorizadas para o efeito.
b) **Integridade** - Salvaguardar a exatidão da informação e dos métodos de processamento.
c) **Disponibilidade** - Garantir que os utilizadores autorizados têm acesso à informação sempre que necessário.
d) **Auditabilidade** - Os dados e informações corporativas e/ou de negócio e as operações de tratamento de dados pessoais são registados, compilados, analisados, e revelados de modo a permitir que auditores internos ou externos possam atestar a sua veracidade.

e) Rastreabilidade - Assegurar a capacidade de recuperação do histórico das ações concretizadas, através de um registo que deverá estar atualizado e disponível em qualquer momento.

Figura 1: Propriedades básicas da Segurança da Informação

f) Modelo de Governo - Aplicar práticas de segurança da informação de forma transversal nos processos, através da estrutura organizacional, autoridades e responsabilidades.
g) Gestão de identidades e acessos - Gerir identidades e acessos, tendo por base os princípios de menor privilégio e da segregação de funções.
h) Segurança "by design" - As iniciativas ou projetos incluem as medidas técnicas e organizativas adequadas ao risco de segurança de informação associado. As alterações a implementar, referentes a tratamento de dados pessoais e/ou informação, devem ser realizadas sob a gestão do Sistema de Gestão de Segurança de Informação da AdNorte.
i) Proteção da Informação - Implementar as medidas, físicas e/ou digitais, adequadas para garantir a segurança da informação, a sua classificação e o seu manuseamento de acordo com o nível de risco, respeitando os requisitos de identificação, autenticação e não repúdio, com verificações do seu cumprimento e eficácia, procurando proceder à mitigação dos riscos que possam colocar em causa a segurança da informação, a proteção dos dados pessoais e a continuidade do negócio.

j) Gestão e resposta a eventos de segurança da informação - Reportar qualquer evento de segurança da informação, que possa colocar em causa a confidencialidade, a integridade ou a disponibilidade dos ativos. Monitorizar os controlos, físicos e lógicos, de segurança da informação. Aplicar medidas de proteção, mitigação e corretivas, seguindo os procedimentos instituídos na AdNorte.
k) Gestão do Risco – Identificar possíveis ameaças que possam explorar as vulnerabilidades dos ativos e identificar qual o nível de risco associado, avaliando a probabilidade de ocorrência e possíveis impactos.
l) Gestão de Fornecedores – Avaliar fornecedores críticos, rever os requisitos contratuais e procedimentais para conformidade com a Política de Segurança da Empresa.
m) Continuidade de Negócio – Preparar e responder a incidentes disruptivos para assegurar a resiliência das operações.
n) Gestão das Pessoas – Assegurar que os trabalhadores e colaboradores externos compreendem as suas responsabilidades no contexto da segurança da informação, detêm a informação necessária para esse cumprimento e que os interesses da AdNorte são protegidos durante a sua permanência e após a sua saída, de forma transversal em todas as direções.
o) Melhoria Contínua – Realizar a melhoria contínua do Sistema de Gestão de Segurança de Informação de forma cumprir os objetivos definidos pela AdNorte.

Quando a informação inclui operações de tratamento de Dados Pessoais acrescem os princípios previstos no Regulamento Geral de Proteção de Dados:

- Licitude;
- Lealdade;
- Transparência;
- Minimização;
- Finalidades determinadas, explícitas e legítimas, sendo vedada a possibilidade de um tratamento posterior de forma incompatível com essas finalidades;
- Princípio da adequação, pertinência e limitação às finalidades para os quais os dados são tratados;
- Os dados deverão ser exatos e atualizados sempre que necessário;
- Conservados apenas pelo período necessário à execução da finalidade para o qual são tratados.

5. RESPONSABILIDADES

Todos os colaboradores / utilizadores da AdNorte têm a responsabilidade de conhecer e cumprir os documentos do sistema de gestão, nomeadamente a presente Política, o Manual de Acolhimento, o Código de Conduta e Ética, Política de privacidade para colaboradores da AdNorte, Política de Cookies, entre outros, assim como a legislação e os requisitos estatutários e regulamentares em vigor.

As Autoridades e responsabilidades no contexto de segurança da informação são descritas de forma macro, nos próximos parágrafos.

Administração, comunica e faz executar esta Política e a sua melhoria contínua.

Responsável de segurança, assegura a definição, implementação e manutenção da estratégia de segurança da informação de forma holística e estruturada. Garante a implementação de boas práticas de Segurança da Informação e cibersegurança, como o "Quadro Nacional de Referência para a Cibersegurança" e a ISO/IEC 27001. Coordena a identificação de requisitos e medidas de segurança da informação, incluindo na gestão de risco, deteção e resposta a incidentes e resiliência operacional.

Responsável de privacidade de dados (DPO), supervisiona, apoia na implementação e manutenção da estratégia de proteção de dados de forma holística e estruturada.

Direção de Recursos Humanos, supervisiona e assegura que a entrada, permanência e saída de funcionários e colaboradores externos é concretizada de acordo com a política de segurança da informação no acesso a ativos físicos e lógicos.

Cargos de direção, têm responsabilidade ao nível da sensibilização e cumprimento das regras instituídas, assegurando a integração da segurança da informação em todos os processos organizacionais, incluindo a gestão de risco de segurança da informação.

Direção de tecnologias de informação e inovação, assegura a implementação e controlo das medidas de segurança da informação nos ativos de informação em alinhamento com as direções da empresa.

6. CONFORMIDADES LEGAIS

Sendo a AdNorte, um operador de serviços essenciais, tem o dever de cumprir com o Decreto-Lei n.º 65/2021 e com o regulamento Geral sobre a Proteção de Dados (RGPD) (Regulamento (EU) 2016/679 do Parlamento Europeu do Conselho).

Conforme o exposto no D.L. n.º 46/2018, deverá notificar o Centro Nacional de Cibersegurança dos incidentes com um impacto relevante na continuidade dos serviços essenciais por si prestados.

7. MELHORIA CONTÍNUA

A Política de Segurança da Informação da AdNorte não se limita a este documento nem é estática, é acente num processo de melhoria contínua com vista a aumentar o nível de maturidade de segurança da empresa consubstanciado outras políticas e processos, de acordo com a ISO/IEC 27002, tais como:

- Inventário e classificação da Informação.
- Gestão de Identidades e Acessos.
- Gestão de eventos e incidentes de segurança.
- Gestão de Risco de Segurança da Informação.
- Resiliência na continuidade de operações.
- Manual de uso aceitável da Informação.
- Gestão de vulnerabilidades técnicas.
- Privacidade e proteção de informações de dados pessoais.

8. FORMAÇÃO E SENSIBILIZAÇÃO EM CIBERSEGURANÇA

Anualmente são agendadas ações de formação e sensibilização para a temática da Segurança da Informação.

9. VIOLAÇÃO/DESVIO

O colaborador que detetar uma violação/desvio a esta política deverá informar prontamente a AdNorte.

Estas violações/desvios de segurança devem ser remetidas ao DTII, por SICO, para que sejam analisadas as causas da sua ocorrência e sejam definidas e implementadas as ações necessárias.

Os colaboradores que deliberadamente violem esta ou outras políticas ficam sujeitos a ações disciplinares, que podem ir até à cessação do seu vínculo contratual e participação às autoridades judiciais das situações que indiciem a prática de crime. Exemplos de violações/desvios:

a) Uso ilegal de software;
b) Introdução (intencional ou não) de vírus informático;
c) Tentativas de acesso não autorizado a dados e sistemas;
d) Partilha de informações sensíveis do negócio;
e) Divulgação de informações e das operações contratadas;
f) Partilha de palavras-chave.

Em caso de dúvidas quantos aos princípios e responsabilidades descritas nesta política, o colaborador deve contactar a DTII.

10. PROPRIEDADE INTELECTUAL

A informação desenvolvida e produzida pela AdNorte pelos seus trabalhadores ou em projetos da responsabilidade da empresa são propriedade da AdNorte.

Os direitos de propriedade intelectual incluem direitos autorais de software ou de documentos, direitos de design, marcas registadas, patentes, licenças de código-fonte.

11. MANUTENÇÃO E COMUNICAÇÃO DA POLÍTICA DE SEGURANÇA

A Política de Segurança da Informação é regularmente revista, avaliada e aprovada pela Administração, de forma a garantir que continua a ser adequada à AdNorte. A Política deve ser divulgada por toda a instituição através das normas e canais de comunicação definidos internamente.