



SEMENTES DIGITAL
PRESTAÇÃO DE SERVIÇOS
NIF: 5002955466

Talatona, Distrito Urbano de Talatona,
Bairro Futungo de Belas,
Rua Rua A, Travessa 3,
Casa n.º Casa Nº 46.

Plataforma Sementes

Versão: 1.0

Data: Julho de 2026

Política de Segurança da Informação e Segurança Cibernética

1. Objectivo

A presente Política de Segurança da Informação e Segurança Cibernética estabelece os princípios, responsabilidades e medidas adoptadas pela **Sementes (SEMENTES DIGITAL, NIF: 5002955466)** para assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações sob sua responsabilidade, bem como proteger os activos tecnológicos que suportam a plataforma.

Esta política aplica-se a todos os colaboradores, administradores, prestadores de serviços, parceiros, investidores, produtores, fornecedores e demais utilizadores que, de forma directa ou indirecta, tenham acesso aos sistemas, dados ou infra-estruturas da organização.

2. Princípios Gerais

A **Sementes (SEMENTES DIGITAL, NIF: 5002955466)** compromete-se a:

- Proteger as informações e os dados pessoais tratados na plataforma;
- Assegurar a disponibilidade dos seus serviços digitais;
- Preservar a integridade das informações contra alterações não autorizadas;
- Garantir que apenas pessoas autorizadas tenham acesso às informações;
- Adoptar medidas preventivas contra ameaças cibernéticas;
- Cumprir a legislação angolana aplicável e as boas práticas internacionais de segurança da informação.

3. Âmbito

Esta política aplica-se a:

- Plataforma Web;
- Aplicações móveis;
- Infra-estrutura tecnológica;
- Servidores e serviços em nuvem;
- Bases de dados;
- Redes de comunicação;
- Equipamentos utilizados pela organização;
- Serviços contratados a terceiros que tratem informações da organização.

4. Classificação da Informação

As informações tratadas pela **Sementes (SEMENTES DIGITAL, NIF: 5002955466)** são classificadas da seguinte forma:

- **Informação Pública**
 - Pode ser divulgada ao público sem causar prejuízo à organização.
- **Informação Interna**
 - Destina-se exclusivamente aos colaboradores e parceiros autorizados.
- **Informação Confidencial**
 - Inclui informações financeiras, comerciais, operacionais, estratégicas, contratos, relatórios internos e dados dos utilizadores.
- **Informação Restrita**
 - Inclui palavras-passe, chaves criptográficas, credenciais administrativas, informação bancária, documentação crítica e demais activos cuja divulgação possa comprometer a segurança da organização.

5. Controlo de Acessos

O acesso aos sistemas da organização deve obedecer aos seguintes princípios:

- Cada utilizador possuirá uma conta individual;
- Os acessos serão concedidos apenas de acordo com as funções desempenhadas;
- É proibida a partilha de credenciais;
- As permissões serão revistas periodicamente;
- Contas inactivas ou desnecessárias serão imediatamente desactivadas;
- Contas administrativas devem utilizar mecanismos adicionais de autenticação, sempre que tecnicamente possível.

6. Gestão de Credenciais

Todos os utilizadores devem:

- Criar palavras-passe fortes;
- Manter as credenciais em absoluto sigilo;
- Alterar imediatamente a palavra-passe quando existir suspeita de comprometimento;
- Nunca reutilizar palavras-passe críticas em serviços externos.

7. Protecção dos Dados

A **Sementes (SEMENTES DIGITAL, NIF: 5002955466)** implementa medidas técnicas e organizacionais para proteger as informações tratadas, incluindo:

- Encriptação das comunicações;
- Cópias de segurança periódicas;
- Monitorização contínua dos sistemas;
- Registo de eventos de segurança;
- Gestão de vulnerabilidades;
- Actualizações regulares dos sistemas;
- Controlo de acessos baseado em perfis.

8. Segurança da Infra-estrutura Tecnológica

Todos os sistemas deverão manter:

- Sistemas operativos actualizados;
- Correções de segurança aplicadas;
- Protecção contra software malicioso;
- Firewalls e mecanismos de monitorização;
- Separação entre ambientes de desenvolvimento, testes e produção.

9. Utilização Aceitável dos Recursos

Os recursos tecnológicos disponibilizados pela organização destinam-se exclusivamente ao exercício das actividades autorizadas.

É expressamente proibido:

- Instalar software sem autorização;
- Partilhar contas de utilizador;
- Divulgar informação confidencial;
- Utilizar os sistemas para fins ilícitos;
- Tentar obter acesso não autorizado a sistemas ou informações.

10. Gestão de Incidentes de Segurança

Qualquer colaborador, parceiro ou prestador de serviços deverá comunicar imediatamente qualquer incidente ou suspeita de incidente de segurança.

São considerados incidentes, entre outros:

- Acessos não autorizados;
- Perda ou roubo de equipamentos;
- Divulgação indevida de informação;
- Ataques informáticos;
- Infecção por software malicioso;
- Interrupção dos serviços críticos.

Todos os incidentes serão registados, analisados e tratados de acordo com os procedimentos internos da organização.

11. Protecção de Dados Pessoais

A **Sementes (SEMENTES DIGITAL, NIF: 5002955466)** compromete-se a tratar os dados pessoais de forma lícita, transparente e segura.

Os titulares dos dados poderão exercer os direitos legalmente previstos, nomeadamente:

- Direito de acesso;
- Direito de rectificação;
- Direito de actualização;
- Direito de eliminação, quando aplicável;
- Direito de oposição ao tratamento nos casos previstos na legislação.

12. Prestadores de Serviços

Todos os prestadores de serviços que tenham acesso às informações ou sistemas da **Sementes (SEMENTES DIGITAL, NIF: 5002955466)** deverão:

- Cumprir integralmente esta política;
- Garantir a confidencialidade das informações;
- Adoptar medidas equivalentes de segurança;
- Comunicar imediatamente qualquer incidente relacionado com os serviços prestados.

13. Formação e Sensibilização

A organização promoverá regularmente acções de sensibilização e formação sobre:

- Segurança da informação;
- Engenharia social;
- Phishing;
- Gestão segura de palavras-passe;
- Protecção de dados pessoais;
- Boas práticas de utilização dos sistemas.

14. Continuidade do Negócio

A **Sementes (SEMENTES DIGITAL, NIF: 5002955466)** manterá mecanismos destinados a assegurar a continuidade das operações, incluindo:

- Cópias de segurança;
- Planos de recuperação de desastres;
- Redundância dos serviços críticos;
- Testes periódicos aos mecanismos de recuperação.

15. Responsabilidades

Administração

Compete à Administração:

- Aprovar esta política;
- Disponibilizar os recursos necessários à sua implementação;
- Promover uma cultura de segurança da informação.

Equipa Técnica

Compete à equipa técnica:

- Implementar os controlos de segurança;
- Monitorizar continuamente os sistemas;
- Corrigir vulnerabilidades;
- Responder a incidentes de segurança.

Colaboradores

Compete aos colaboradores:

- Cumprir esta política;
- Proteger as credenciais de acesso;
- Reportar incidentes;
- Utilizar os recursos tecnológicos de forma responsável.

Prestadores de Serviços

Compete aos prestadores de serviços cumprir todas as obrigações de segurança previstas contratualmente e nesta política.

16. Incumprimento

O incumprimento das disposições constantes desta política poderá dar origem à aplicação de medidas disciplinares, civis, administrativas ou criminais, nos termos da legislação aplicável e dos contratos celebrados.

17. Revisão

A presente política será revista:

- Anualmente;
- Sempre que ocorram alterações legislativas;
- Após incidentes significativos de segurança;
- Sempre que existam alterações relevantes na infra-estrutura tecnológica.

18. Divulgação

Em cumprimento do disposto no Artigo 5.º relativo ao dever de divulgação das políticas de segurança, a presente política será disponibilizada aos colaboradores, prestadores de serviços, parceiros e demais partes interessadas, utilizando linguagem clara, objectiva e adequada às funções desempenhadas e ao nível de sensibilidade das informações.

19. Entrada em Vigor

A presente Política de Segurança da Informação e Segurança Cibernética entra em vigor na data da sua aprovação pela Administração da **Sementes (SEMENTES DIGITAL, NIF: 5002955466)**, sendo de cumprimento obrigatório por todos os colaboradores, parceiros, prestadores de serviços e utilizadores que tenham acesso aos seus sistemas ou informações.



João Manuel Correia Cabanga