Política de Segurança Cibernética WISEDIGITAL

1. Objetivo e Escopo

1.1. O objetivo desta política é estabelecer diretrizes e práticas de segurança cibernética para proteger ativos de informação críticos da Wisedigital contra ameaças cibernéticas.

1.2. Esta política se aplica a todos os funcionários, contratados, fornecedores e terceiros que tenham acesso aos sistemas de informação da empresa.

2. Classificação de Ativos

2.1. Todos os ativos de informação devem ser classificados de acordo com sua importância para a organização, identificando informações confidenciais, restritas e públicas.

3. Gerenciamento de Acessos

3.1. O acesso aos sistemas e informações da empresa deve ser concedido com base no princípio do menor privilégio, garantindo que os usuários tenham apenas as permissões necessárias para realizar suas funções.

3.2. O controle de acesso deve ser monitorado e revisado periodicamente.

4. Conscientização e Treinamento

4.1. A Wisedigital deve fornecer treinamento regular sobre segurança cibernética a todos os funcionários e terceiros com acesso aos sistemas de informação.

5. Políticas de Senhas

5.1. Senhas fortes devem ser usadas em todos os sistemas, e as senhas devem ser alteradas regularmente.

5.2. A autenticação de dois fatores deve ser implementada sempre que possível.

6. Gerenciamento de Vulnerabilidades

6.1. Deve ser realizado um escaneamento regular de vulnerabilidades em sistemas e redes.

6.2. As vulnerabilidades devem ser avaliadas e abordadas de acordo com sua gravidade.

7. Monitoramento e Detecção de Incidentes

7.1. Deve ser implementado um sistema de monitoramento de segurança cibernética para detectar e responder a incidentes de segurança.

8. Resposta a Incidentes

8.1. A Wisedigital deve ter um plano de resposta a incidentes que detalhe os procedimentos a serem seguidos em caso de violação de segurança.

9. Atualizações e Patches

9.1. Todos os sistemas e software devem ser mantidos atualizados com as últimas correções e patches de segurança.

10. Criptografia

10.1. A criptografia deve ser usada para proteger dados sensíveis em trânsito e em repouso, de acordo com as melhores práticas de segurança.

11. Auditorias de Segurança

11.1. Auditorias de segurança cibernética devem ser realizadas regularmente para avaliar a eficácia das medidas de segurança.

12. Conformidade Legal

12.1. A Wisedigital deve cumprir todas as leis e regulamentações de segurança cibernética aplicáveis.

13. Revisão e Melhoria Contínua

13.1. Esta política será revisada regularmente para garantir sua relevância e eficácia. As melhorias serão implementadas conforme necessário.

14. Responsabilidade

14.1. A alta administração e todos os funcionários têm a responsabilidade de cumprir esta política de segurança cibernética.