POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

OBJETIVO

A Política de Segurança da Informação tem como objetivo garantir a proteção e confidencialidade dos dados e informações da empresa Megaluzz Negócios, inscrita no CNPJ n°: 10.374.179/0001-09, bem como dos clientes e fornecedores, por meio da adoção de práticas de segurança eficazes.

RESPONSABILIDADES

2.1. A diretoria da empresa é responsável por garantir que a política de segurança da informação seja estabelecida, implementada, monitorada e atualizada regularmente.

2.2. Todos os funcionários da empresa são responsáveis por seguir as diretrizes estabelecidas nesta política e tomar as medidas necessárias para proteger a informação confidencial e sensível da empresa e de seus clientes e fornecedores.

DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

3.1. Senhas fortes: Todos os funcionários devem utilizar senhas fortes, com pelo menos 10 caracteres, contendo letras maiúsculas, minúsculas, números e caracteres especiais. Além disso, as senhas devem ser alteradas a cada 90 dias ou menos, e os funcionários não devem usar a mesma senha em mais de uma conta, software ou aplicativo.

3.2. Segurança da rede: A empresa deve garantir que sua rede esteja protegida por um firewall e que o acesso à internet esteja limitado aos sites necessários para os negócios. Além disso, a rede Wi-Fi deve ser protegida por uma senha forte e deve ser atualizada regularmente para garantir a segurança.

3.3. Gerenciamento de dispositivos: Todos os dispositivos, como laptops, desktops e smartphones, que contêm informações sensíveis devem ser gerenciados corretamente. Isso inclui a atualização do software e a proteção por senha. Além disso, os dispositivos devem ser criptografados para evitar o acesso não autorizado.

3.4. Política de Backup: A empresa deve ter um sistema de backup eficaz para garantir que os dados sejam recuperados em caso de perda de informações. Os backups devem ser realizados regularmente e armazenados em um local seguro.

3.5. Acesso aos dados: A empresa deve garantir que apenas funcionários autorizados tenham acesso a informações confidenciais. As senhas devem ser alteradas regularmente e os funcionários devem ser orientados a nunca compartilhar informações confidenciais com pessoas não autorizadas.

3.6. Educação e conscientização: A empresa deve fornecer treinamentos e orientações regulares sobre segurança da informação aos funcionários. Isso inclui a importância de não compartilhar informações confidenciais com pessoas não autorizadas e de relatar quaisquer incidentes de segurança imediatamente.

3.7. Identificação e gestão de riscos: A empresa deve identificar e gerenciar os riscos associados à segurança da informação. Isso inclui a criação de planos de contingência e gerenciamento de riscos em caso de vazamento de informações.

3.8. Atualização de softwares: A empresa deve ter políticas para garantir que o software utilizado seja atualizado regularmente para evitar vulnerabilidades de segurança.

3.9. Conformidade regulatória: A empresa deve cumprir as normas regulatórias aplicáveis em relação à segurança da informação.

3.10. Monitoramento e auditoria: A empresa deve monitorar a conformidade com as diretrizes de segurança da informação e realizar auditorias regulares de segurança.