credsystem

Política de Segurança da Informação credsystem

Na **credsystem**, desenvolvemos soluções simples, digitais e seguras para tornarmos novas conquistas possíveis aos nossos parceiros lojistas e consumidores finais.

Valorizamos nossos clientes e entendemos o quanto a segurança das informações é importante para aderirem às nossas soluções com confiança.

A segurança de dados está entre as prioridades da **credsystem**, por isso, disponibilizamos abaixo um resumo da nossa Política de Segurança da Informação para que você possa conhecer brevemente as diretrizes aplicadas internamente para proteger os seus dados.

Objetivos de segurança

O objetivo da nossa Política de Segurança da Informação é garantir que os três pilares fundamentais da segurança sejam aplicados por meio da:

1. Confidencialidade: Apenas usuários autorizados têm permissão para acessar suas informações;
2. Integridade: Apenas alterações autorizadas podem ser realizadas na informação armazenada;
3. Disponibilidade: A informação deve ser disponibilizada apenas para usuários **autorizados** quando solicitado.

Diretrizes

Além dos objetivos principais da nossa Política de Segurança da Informação, há também as diretrizes que norteiam nossa atividade, que são:

1. Classificar dados de acordo com sua criticidade e sensibilidade para o negócio da empresa e seus clientes, considerando os níveis abaixo:

- Informação confidencial;
- Informação restrita ou de uso interno;
- Informação pública.

2. Aplicar a estratégia de defesa em profundidade por meio da implementação de mais de uma camada de segurança, gerando maior garantia em relação a possíveis comprometimentos de alguma das camadas anteriores;

3. Manter a capacidade de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, utilizando-se de registros de rastreabilidade da manipulação de dados da companhia e de seus clientes;

4. Assegurar que os dados da empresa e de seus clientes sejam acessados e manipulados apenas por pessoas autorizadas e de forma segura;

5. Proteger ativos tecnológicos e estabelecer procedimentos de monitoramento das redes da organização e das máquinas de colaboradores para a detecção de intrusões;

6. Conduzir o monitoramento e a resposta de incidentes, seguindo as etapas de detecção, mitigação emergencial e análise de causa raiz;

7. Elaborar cenários de incidentes para a realização periódica de testes de continuidade;

8. Garantir a conscientização do time interno por meio de treinamentos mandatórios e avaliações periódicas.

Importante: A Política de Segurança da Informação da **credsystem** é revisada pelo menos uma vez ao ano a fim de garantir um material atualizado e em linha com as exigências do mercado. Aqui, os seus dados estão seguros!