



POLÍTICA DE SEGURANÇA CIBERNÉTICA



Sumário

1. Introdução	3
2. Objetivos.....	3
3. Riscos	3
4. Proteção e Prevenção	4
5. Supervisão	4
6. Resposta a incidentes	5
7. Responsáveis.....	5
8. Vigência e Atualização	5



POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. Introdução

Este documento trata de assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela KOBOLD INSTITUICAO DE PAGAMENTO S.A ("KOB").

2. Objetivos

A Política de Segurança Cibernética do KOB visa proteger as informações de propriedade e/ou sob guarda do KOB, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora do KOB, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a KOB, ou de qualquer natureza relativa às atividades da empresa e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor Presidente, assim definido no Código de Ética e Conduta do KOB.

3. Riscos

As medidas de segurança cibernética utilizadas pelo KOB têm por finalidade preservar as informações comerciais e cadastrais de todos os nossos clientes e demais stakeholders, armazenados em banco de dados.

Acesso indevido a essas informações ou mesmo exclusão das mesmas poderá trazer danos irreparáveis para as operações do KOB.



4. Proteção e Prevenção

Estas informações são armazenadas em banco de dados relacional, com acesso restrito, disponível para consulta apenas através de aplicações especificamente escritas para isso. Nenhum tipo de escrita, alteração, leitura e deleção é feita fora dos sistemas conectados ao banco de dados.

Apenas colaboradores do Departamento de Tecnologia da Informação possuem acesso completo a esse banco de dados para realização de atividades pontuais de manutenção.

O backup das informações nos bancos de dados é feito diariamente de maneira automática, em nuvem, e permanece disponível para recuperação imediata durante 30 (trinta) dias. Após esse período, são arquivadas e permanecem disponíveis, mas a recuperação poderá levar algumas horas. O backup permanece disponível por período de 10 anos, podendo ser removido após esse período. Uma vez ao dia, o backup anterior é restaurado e testado, garantindo a disponibilidade das informações.

A manipulação das informações nos bancos de dados, feita por aplicações que utilizam essas informações de maneira exclusiva, é limitada também aos profissionais de Tecnologia. O acesso é limitado, pessoal e intransferível. Toda mudança feita é gravada, salva em nova versão e armazenada de maneira distribuída, em nuvem e nos computadores de todos os colaboradores de tecnologia. Toda mudança nos sistemas é aplicada de maneira automática, após aprovação de ao menos um colaborador além do autor da mudança.

5. Supervisão

O ambiente possui acesso restrito aos dados. Mesmo para os casos de acesso aos dados via aplicação, controles de logs registram quais usuários (clientes e colaboradores) fizeram operações significativas em transações no sistema.



6. Resposta a incidentes

Possuímos backups diários do banco de dados, restaurados ao menos 1 (uma) vez, os quais garantem a segurança de disponibilidade das informações no caso de perda catastrófica.

Acessos às informações ou mudança na forma como elas são disponibilizadas, são gravadas e podem ser observadas caso haja necessidade.

7. Responsáveis

Qualquer incidente que apresente risco a esses dados devem ser reportados imediatamente ao responsável pela área de tecnologia e ao responsável pela área de Compliance.

8. Vigência e Atualização

Esta política será revisada periodicamente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo.

Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.