POLÍTICA DE SEGURANÇA CIBERNÉTICA

KOBOLD

Sumário

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Introdução

Este documento de que trata o assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela Kobold.

Objetivos

A Política de Segurança Cibernética da Kobold visa proteger as informações de propriedade e/ou sob guarda da Kobold, 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 da Kobold, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a Kobold, 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 de Compliance, assim definido no Código de Ética da Kobold.

Riscos

As medidas de segurança cibernética utilizadas pela Kobold têm por finalidade preservar as informações comerciais e cadastrais de todos os nossos clientes (cedentes) e seus respectivos sacados, armazenados em banco de dados.

Acesso indevido à essas informações ou mesmo exclusão dos mesmos poderá trazer danos irreparáveis para as operações da Kobold.

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 à esse banco de dados para realização de atividades pontuais de manutenção ou backup.

O backup é feito em fitas LTO armazenadas em ambiente segregado, com acesso apenas à certas pessoas da área de tecnologia.

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.

Resposta a incidentes

Possuímos backups diários do banco de dados, como também backups diferenciais feitos toda hora.
Em caso de indisponibilidade dos dados, temos a possibilidade de restauração imediata dos mesmos a partir desses backups.

Responsáveis

Qualquer incidente que apresente risco à esses dados deverão ser reportados imediatamente ao gerente de área e ao responsável pela área de Compliance.

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.