FIDELITÀ AI

Política de Riscos Cibernéticos

Maio 2024

CONTATOS

Rodrigo Maciel, CFP®

Telefone: (11) 97687 6893

E-mail: rodrigo.maciel@fidelitaai.com.br

Rogério Tatulli

Telefone: (11) 98122 3843

E-mail: rogerio.tatulli@fidelitaai.com.br

1 - Objetivo:

Estabelecer diretrizes e procedimentos para a gestão eficaz dos riscos cibernéticos da empresa, protegendo seus ativos de informação, sistemas e infraestrutura contra acessos não autorizados, uso indevido, divulgação, alteração ou destruição.

2 - Abrangência:

Aplica-se a todos os colaboradores e sócios da empresa, abrangendo os seguintes aspectos:

- **Segurança da Informação:** Proteção da confidencialidade, integridade e disponibilidade das informações da empresa.
- **Segurança da Rede:** Proteção da rede da empresa contra acessos não autorizados, malware, ataques cibernéticos e outras ameaças.
- **Segurança de Sistemas:** Proteção dos sistemas da empresa contra falhas, vulnerabilidades e softwares maliciosos.
- **Segurança de Dispositivos:** Proteção dos dispositivos utilizados pelos colaboradores da empresa contra acessos não autorizados, perda ou roubo de dados.
- **Conscientização e Treinamento:** Conscientização dos colaboradores sobre os riscos cibernéticos e treinamento sobre boas práticas de segurança da informação.
- **Gerenciamento de Incidentes:** Estabelecimento de procedimentos para a identificação, resposta e recuperação de incidentes de segurança cibernética.

3 - Princípios:

- **Confidencialidade:** As informações da empresa devem ser acessíveis apenas a pessoas autorizadas.
- **Integridade:** As informações da empresa devem ser precisas, completas e confiáveis.
- **Disponibilidade:** As informações da empresa devem estar disponíveis para os usuários autorizados quando necessário.
- **Accountability:** Todos os colaboradores da empresa são responsáveis pela segurança da informação e devem seguir as políticas e procedimentos de segurança cibernética.
- **Melhoria Contínua:** A gestão dos riscos cibernéticos deve ser um processo contínuo, com base em monitoramento, análise e aprendizado com incidentes.

5 - Práticas de Gestão de Riscos Cibernéticos:

- **Análise de Riscos:** Identificação, avaliação e classificação dos riscos cibernéticos que a empresa enfrenta.
- **Tratamento de Riscos:** Implementação de medidas para prevenir, minimizar ou transferir os riscos cibernéticos.

- **Plano de Resposta a Incidentes:** Estabelecimento de procedimentos para a identificação, resposta e recuperação de incidentes de segurança cibernética.

- **Monitoramento e Controle:** Monitoramento contínuo dos sistemas e redes da empresa para detectar e responder a ameaças cibernéticas.

- **Testes de Penetração:** Realização periódica de testes de penetração para avaliar a segurança dos sistemas e redes da empresa.

- **Conscientização e Treinamento:** Conscientização dos colaboradores sobre os riscos cibernéticos e treinamento sobre boas práticas de segurança da informação.

6 - Tecnologia:

Segurança de Sistemas

a. Nossa rede de e-mail possui o pacote da Microsoft Premium que conta com o Microsoft Defender para Office 365 para nossa proteção contra vírus, spam, anexos inseguros, links suspeitos e ataques de *phishing*.
b. Sistema de CRM – Em fase de contratação.
c. Nossa rede de arquivos de carteiras dos gestores, contratos, apresentações e demais documentos são arquivados também na nuvem Microsoft Azure através de nosso pacote business premium
d. Soluções de segurança da informação adequadas aos riscos da empresa, como firewalls, antivírus, sistemas de detecção de intrusão e soluções de criptografia da Microsoft
e. Atualização regular do software e dos sistemas da empresa para corrigir vulnerabilidades de segurança.

7 – Treinamento

- Entendemos que além de uma proteção robusta com os provedores de serviços contratados, entendemos que novas fraudes surgem constantemente e nossa principal vulnerabilidade são os próprios usuários dos sistemas. Por isso, teremos mensalmente vídeos de treinamento em *cybersecurity*, os quais nos manteremos atualizados sobre novas práticas ilegais para mitigarmos ao máximo o risco em nossa empresa.

-

8 – Plano de ação em falhas de segurança cibernética

Embora confiemos em nossos sistemas e nosso plano de constante treinamento contra acessos ilegais em nossa base de dados e informações confidenciais de nossos clientes entendemos que eventuais falhas podem ocorrer.

O plano de ação consiste em:

1- Comunicação imediata ao diretor responsável da empresa

2- Diretor responsável em conjunto com o time Fidelità fará a comunicação com as partes envolvidas relatando em detalhes o ocorrido e potenciais impactos.

3- Concomitante a isso faremos contato com nosso provedor de tecnologia, Microsoft, para solucionar o problema e entender melhor a falha do ocorrido.

4- A área responsável pela falha preencherá o relatório de violação operacional (modelo no Anexo I – da Política de Governança)

5- O comitê de governança se reunirá para avaliar e verificar a falha com todas as partes e sistemas envolvidos, e aprovaremos o relatório do erro relatando todos os passos do início ao fim, bem como as soluções e propostas de alterações em nossos processos, para evitar que o erro ocorra novamente.

9– Plano de ação para extravio de equipamentos com informações da Fidelità:

a) Em caso de perda ou roubo/furto do equipamento o usuário deve comunicar imediatamente o diretor responsável.
b) O diretor responsável entrará no site: https://myaccount.microsoft.com/?ref=OfficePortalSecurityPrivacy
c) Gerenciar dispositivos
d) Excluir dispositivos

10 – Plano de ação para inoperância de servidor de email

Quando o prospect se torna cliente da Fidelità AI ele assinará um termo de relacionamento informando que a movimentação só deve ser considerada realizada, caso ele receba um email da Fidelità informando que a movimentação foi realizada com sucesso. A nossa resposta conterá um comprovante do administrador com o horário e data do lançamento. Caso o cliente envie uma movimentação e fique sem resposta, ele deverá entrar em contato com a Fidelità pelo celular de algum sócio, que estará em nosso site. Um email de continência será compartilhado com o cliente e o email padrão movimentacao@fidelitaai.com.br, deverá ser copiado na mensagem. De todas as formas haverá um registro por escrito do cliente solicitando a movimentação.

11 - Conclusão:

A implementação de uma Política de Riscos Cibernéticos robusta e eficaz é fundamental para proteger a Fidelità contra os crescentes riscos cibernéticos. Ao seguir os princípios e práticas descritos nesta política, a empresa pode minimizar o impacto de incidentes de segurança cibernética e proteger seus ativos de informação, sistemas e infraestrutura.

- A gestão de riscos cibernéticos é um processo contínuo que deve ser adaptado às necessidades específicas da empresa.
- É importante manter a Política de Riscos Cibernéticos atualizada e comunicar seus princípios e práticas a todos os colaboradores da empresa.
- A conscientização e o treinamento dos colaboradores são essenciais para uma cultura de segurança cibernética forte.

8 – Vigência e Revisão:

Esse documento poderá ser revisado e/ou atualizado a qualquer tempo, sempre que necessário independentemente dos avanços regulatórios que revestem as atividades da Fidelità. Esse documento passa a produzir efeitos, **a partir de 16/04/2024**.

Última atualização:

Abril de 2024

São Paulo – SP, 16/04/2024.