ÍNDICE

1. OBJETIVOS

São objetivos desta Política de Segurança da Informação:

- Declarar a importância da Segurança da Informação para a organização.
- Definir as diretrizes gerais para elaboração de normas e procedimentos de Segurança da Informação.
- Descrever como a Segurança da Informação está organizada, por meio da definição de papéis e atribuição de responsabilidades.

2. APLICAÇÃO

Esta Política aplica-se a todos os colaboradores próprios e terceirizados, fornecedores e demais parceiros comerciais da FK Grupo S/A. (Empresa), incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de TI ou que acessem informações de propriedade ou sob custódia da Empresa.

3. ENUNCIADO

A FK Grupo S/A. afirma o seu compromisso com a proteção das informações de sua propriedade e/ou sob sua custódia, por meio de diretrizes e práticas de segurança orientadas para a preservação da sua confidencialidade, integridade, disponibilidade e privacidade.

Esta Política está suportada por um conjunto de normas, procedimentos e demais documentos que integram o Sistema de Gestão de Segurança da Informação, e aplica-se a todos os colaboradores da Empresa e suas subsidiárias, seus sistemas, serviços e ativos de tecnologia da informação.

4. TERMOS E DEFINIÇÕES

Os termos e definições utilizados no contexto da Segurança da Informação podem ser consultados no MSI - Manual de Segurança da Informação.

5. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

5.1. Sistema de Gestão da Segurança da Informação

O Sistema de Gestão de Segurança da Informação (SGSI) consiste em um conjunto de documentos (políticas, normas, manuais, procedimentos, registros) definidos de acordo com o nível de maturidade (atual e desejado), considerando as capacidades técnicas e operacionais para mantê-los. Desta forma, a abordagem da Empresa para implantação do SGSI consiste em melhorias contínuas e sucessivas, com o objetivo de assegurar a sustentabilidade das diretrizes implementadas.

5.2. Responsabilidade e Comprometimento

Todos os colaboradores, em qualquer vínculo, função ou cargo, são responsáveis pela proteção e salvaguarda dos ativos de informação sob sua responsabilidade, dos ambientes físicos e computacionais a que tenham acesso, independente das medidas de segurança existentes.

5.3. Gestão de Riscos

As diretrizes dessa política, das normas que a suportam e as decisões de segurança da informação são determinadas conforme a percepção de risco aos objetivos e negócios da Empresa, visando atingir o grau de segurança necessário, dentro dos limites orçamentários e padrões de qualidade estabelecidos.

5.4. Classificação e Tratamento da Informação

As informações de propriedade da Empresa ou sob sua custódia devem ser classificadas de acordo com seu grau de sigilo e receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida.

5.5. Gestão de acessos

O acesso às instalações, sistemas, redes, dados e informações de propriedade ou sob responsabilidade da Empresa deve ser monitorado, controlado e restrito às necessidades profissionais de cada colaborador. O acesso de terceiros (clientes, fornecedores e demais parceiros comerciais) aos ativos de informação da Empresa deve seguir as normas, procedimentos e critérios definidos, com a finalidade de mitigar os riscos de violação dos requisitos de segurança da informação.

5.6. Aquisição de hardware e software

Toda aquisição de hardware e software necessária para o desempenho das atividades dos colaboradores deverá ser coordenada pela área de TI, para garantir a aderência aos requisitos técnicos e funcionais de tecnologia e segurança da informação.

5.7. Utilização dos recursos de TI

Os recursos de TI e comunicação disponibilizados aos colaboradores devem ser utilizados para as finalidades determinadas, sempre em harmonia com os interesses da Empresa.

5.8. Gestão da Continuidade de Negócios

A Empresa deve identificar as ameaças potenciais e os impactos operacionais e estratégicos aos seus negócios, e desta forma desenvolver e manter mecanismos que garantam a continuidade de seus processos críticos.

5.9. Aquisição, desenvolvimento e manutenção de sistemas

Com o objetivo de promover a redução de riscos e manutenção dos níveis de segurança já existentes, o desenvolvimento de sistemas de informação por equipe própria ou por terceiros deve levar em conta as diretrizes e normas de segurança da informação. De forma similar, a aquisição de sistemas e os contratos de suporte e manutenção das aplicações utilizadas na Empresa estão também sujeitos aos mesmos controles.

5.10. Gerenciamento de Projetos

Todos os projetos iniciados e em andamento na Empresa devem levar em conta os aspectos relevantes em segurança da informação. A confidencialidade, disponibilidade e integridade dos ativos de informação devem ser preservadas pelas equipes envolvidas no projeto, independentemente de serem os colaboradores próprios ou terceirizados.

5.11. Notificação, Registro e Tratamento de Incidentes

Os colaboradores devem reportar quaisquer incidentes que possam comprometer a segurança das informações corporativas. A Equipe de TI é responsável por avaliar e tratar os incidentes de segurança da informação, implantando as medidas necessárias para evitar a sua recorrência. Quando necessário, contatos apropriados com autoridades relevantes devem ser mantidos.

5.12. Auditoria e Conformidade

As práticas de segurança da informação adotadas pelos colaboradores serão auditadas periodicamente, de forma a avaliar a conformidade das ações executadas em relação ao estabelecido nesta Política e demais normas e procedimentos que suportam o SGSI.

5.13. Monitoramento

A Empresa reserva-se o direito de monitorar os acessos físicos, bem como a utilização de seus equipamentos, sistemas e demais recursos de TI, para que ameaças ou ações não autorizadas sejam detectadas e tratadas tempestivamente.

5.14. Treinamento e Conscientização

Todos os colaboradores devem receber treinamento relativo às diretrizes, normas e procedimentos da Empresa em segurança da informação, além de contínua conscientização sobre os riscos emergentes, precauções e boas práticas para a utilização adequada dos recursos de TI.

Os profissionais envolvidos com tecnologia e segurança da informação devem assegurar a participação em grupos especializados, associações profissionais ou fóruns especializados, com a finalidade de se manter continuamente atualizados.

5.15. Revisão e análise crítica

O conjunto de documentos que compõe a Política de Segurança da Informação deve passar por revisões e análises críticas a cada dois anos, ou sempre que ocorrer algum fato ou evento relevante que justifique a sua revisão ou adequação.

5.16. Penalidades

O descumprimento ou inobservância das diretrizes estabelecidas nesta Política e em seus documentos complementares constitui conduta inadequada do colaborador.

É importante ressaltar que condutas inadequadas podem resultar em prejuízos financeiros, operacionais, além de impactos legais, regulatórios, de reputação e imagem para a Empresa.

Sendo assim, eventuais medidas administrativas, cíveis e judiciais aplicáveis em cada situação serão definidas pelo Comitê de Segurança da Informação e Privacidade - CSIP.

6. ATIVIDADES E RESPONSABILIDADES

6.1. Diretoria

Composta pelos membros da Alta Direção. Responsável por:

- Fornecer apoio organizacional e prover os recursos humanos, materiais e financeiros necessários para implementar e manter os mecanismos de segurança da informação.
- Designar os representantes do Comitê de Segurança da Informação.

6.2. Comitê de Segurança da Informação e Privacidade - CSIP

Equipe multidisciplinar, constituída por representantes (titulares e suplentes) de áreas-chave para o desenvolvimento e manutenção da cultura de segurança da informação. Responsável por:

- Definir e/ou aprovar as diretrizes para preservar a confidencialidade, integridade e disponibilidade dos ativos de informação da Empresa.
- Avaliar eventuais solicitações de exceção a essa política e demais normas e procedimentos de segurança da informação, considerando a real necessidade e possíveis riscos ao negócio.

6.3. Gerencia/Coordenação de Tecnologia da Informação (TI)

Constituída por profissionais que fornecem soluções de infraestrutura de TI e automação, sistemas departamentais e corporativos para suportar as operações do negócio. Responsável por:

- Prover tecnologia e serviços de TI dentro dos padrões e normas de segurança estabelecidos.
- Definir e implementar mecanismos de monitoramento e controle, com a finalidade de assegurar adequada gestão de tecnologia e segurança da informação.

6.4. Responsável da área de Segurança da Informação (SI)

Área da Coordenação de TI dedicada à definição, implantação e acompanhamento de controles relacionados à segurança da informação. Responsável por:

- Desenvolver e manter toda a documentação relativa ao sistema de gestão de segurança da informação (SGSI) na Empresa.
- Promover campanhas de treinamento e conscientização aos colaboradores da Empresa, em tópicos relacionados à segurança da informação.
- Avaliar a aderência dos colaboradores às diretrizes, normas e procedimentos de segurança da informação e propor ações preventivas ou corretivas, sempre que necessário.

6.5. Departamento de Recursos Humanos

Área dedicada ao recrutamento, seleção, contratação, desenvolvimento e administração de pessoal. Responsável por:

- Assegurar o cumprimento das diretrizes de segurança da informação na administração de pessoal próprio ou terceirizado sob sua responsabilidade.
- Manter registros de treinamento de forma a assegurar que todos os colaboradores sejam orientados em relação às práticas de segurança da informação.

6.6. Gestores

Líderes (Gerentes, Coordenadores e Supervisores) que gerenciam equipes de colaboradores próprios ou terceiros. Responsáveis por:

- Assegurar que os colaboradores sob sua responsabilidade conheçam e cumpram as normas de segurança da informação.
- Zelar pelo cumprimento das normas e diretrizes de segurança da informação nas atividades desempenhadas dentro da sua área de atuação.
- Avaliar as solicitações abertas pelos colaboradores sob sua responsabilidade, e emitir parecer baseado na real necessidade dos colaboradores.
- Identificar os requisitos de segurança da informação que sejam específicos à sua área de atuação e informá-los ao Comitê de Segurança da Informação e Privacidade - CSIP.

6.7. Colaboradores

Integrantes do Conselho de Acionistas, diretores, funcionários, estagiários, jovens aprendizes da Empresa, bem como funcionários temporários que, por contrato, atuem em horário integral nas unidades da Empresa e indivíduos e/ou empresas que atuem em nome da Empresa como consultores, despachantes e agentes. Responsáveis por:

- Conhecer e cumprir as diretrizes estabelecidas na política, normas e procedimentos de Segurança da Informação, participando de treinamentos, campanhas de conscientização e outras atividades relacionadas promovidas pela Empresa.
- Zelar pela segurança dos ativos de informação que lhe forem disponibilizados pela Empresa para desempenhar suas atividades.
- Reportar qualquer indício ou falha de segurança que possa colocar em risco a confidencialidade, integridade ou disponibilidade dos ativos de informação da Empresa.

7. REGISTROS

TCOM - Termo de Compromisso (deve ser assinado pelos colaboradores após o treinamento)

8. DOCUMENTOS DE REFERÊNCIA

MSI - Manual de Segurança da Informação