POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ABRIL 2017

REVISADO EM SETEMBRO 2020

Política de Segurança da Informação

A Tecnologia da Informação, TI, está cada dia mais presente nas empresas, mudando radicalmente os hábitos e a maneira de comunicação, sendo de vital importância a definição de normas de segurança que visem disciplinar o uso da tecnologia da informação.

A **AFMFO – AF MULTI FAMILY OFFICE CONSULTORIA FINANCEIRA LTDA** definiu sua Política de Segurança da Informação, conscientizando e definindo as normas e procedimentos necessários para proteger a confidencialidade das informações e a continuidade dos negócios.

A Política de segurança da Informação tem como principal objetivo documentar e proteger as informações consideradas importantes para a continuidade e manutenção dos objetivos de negócios da AFMFO, padronizando e estabelecendo requisitos mínimos de segurança.

A AFMFO, trabalha com um conjunto de controles e mecanismos que garantem a integridade e segurança de uma estrutura de rede na qual exista o tráfego de informações e dados comuns e/ou restritos, e nela incluídos os equipamentos que armazenam tais informações.

Garante a proteção das informações entre clientes e empresa nos aspectos de confidencialidade, integridade e disponibilidade.

- **Confidencialidade** – Garantia de que o acesso à informação seja obtido, apenas, por pessoas autorizadas. A quebra desse sigilo pode acarretar danos inestimáveis para a empresa ou até mesmo para uma pessoa física;

- **Integridade** – Garantia de que a informação não seja adulterada falsificada ou furtada;

- **Disponibilidade** – Garantia de que a informação esteja disponível sempre que requisitada pelos usuários autorizados mesmo com as interrupções involuntárias de sistemas, ou seja, não intencionais.

A Política de Segurança da Informação aplica-se a todos os usuários da empresa e a qualquer colaborador ou pessoa custodiante de informações da AFMFO ou de seus clientes.

Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade intelectual, industrial (Lei nº 9279) e de direitos autorais, (Lei nº 9610).

A AFMFO entende que o sistema de segurança da informação somente será eficaz com o comprometimento de TODOS!

Comprometimento dos Usuários

- Respeitar esta Política de Segurança da Informação
- Responder pela guarda e proteção dos recursos computacionais colocados á sua disposição para o trabalho;
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- Ativar suas senhas de proteção para Correio Eletrônico e Sistema Operacional, sob orientação do Gestor de Liberações da área de TI;
- Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software.

- Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc;
- Assegurar que as informações e dados de propriedade da AFMFO não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico.
- Comprometer-se em não auxiliar terceiro ou não provocar invasão dos computadores ou da rede de dados, conforme artigo 154-A do Código Penal Brasileiro.
- Relatar para o seu responsável hierárquico e à Gerência de TI, o surgimento da necessidade de um novo software para suas atividades.
- Responder pelo prejuízo ou dano que vier a provocar a AFMFO ou a terceiros, em decorrência da não obediência as diretrizes e normas aqui referidas.

Comprometimento dos Responsáveis Hierárquicos

- Apoiar e zelar pelo cumprimento desta Política de Segurança da Informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.
- Atribuir na fase de contratação e de formalização dos contratos individuais de trabalho CLT, prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança da Informação.
- Autorizar o acesso e definir o perfil do usuário junto ao gestor de liberações da área de TI,
- Autorizar as mudanças no perfil do usuário junto ao gestor de liberações da área de TI,
- Educar os usuários sobre os princípios e procedimentos de Segurança da Informação,
- Notificar imediatamente ao gestor de liberações da área de TI quaisquer vulnerabilidades e ameaças a quebra de segurança;
- Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação;
- Advertir formalmente o usuário e aplicar sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente o fato ao gestor de liberações da área de TI.
- Obter aprovação técnica do gestor de liberações da área de TI antes de solicitar a compra de hardware, software ou serviços de informática.
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

Comprometimento da Área de TI

- Configurar os equipamentos e sistemas para cumprir os requerimentos desta Política de Segurança da Informação,
- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
- Restringir a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança do acesso público e manter evidências que permitam a rastreabilidade para auditoria ou investigação.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.
- Administrar, proteger e testar as cópias de segurança dos programas e dados ao negócio da AFMFO.
- Gerenciar o descarte de informações a pedido dos custodiantes.
- Garantir que as informações de um usuário sejam removidas antes do descarte ou mudança de usuário.

- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários garantindo a segurança por área do negócio.
- Criar a identidade lógica dos colaboradores na empresa.
- Atribuir contas e senhas identificáveis a pessoa física para uso de computadores, sistemas, bases de dados e qualquer outro ativo de informação.
- Proteger todos os ativos de informação da empresa contra códigos maliciosos e ou vírus.
- Garantir que processos de mudança não permitam vulnerabilidades ou fragilidades no ambiente de produção.
- Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro da empresa.
- Realizar inspeções periódicas de configurações técnicas e análise de riscos.
- Gerenciar o uso, manuseio e guarda de assinaturas e certificados digitais.
- Garantir assim que solicitado o bloqueio de acesso de usuários por motivo de desligamento da empresa,
- Propor as metodologias sistemas e processos específicos que visem aumentar a segurança da informação,
- Promover a conscientização dos colaboradores em relação a relevância da segurança da informação,
- Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços.
- Buscar alinhamento com as diretrizes corporativas da empresa.
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.
- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas pode ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Monitorar o ambiente de TI a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso a internet e aos sistemas críticos da AFMFO, indisponibilidade aos sistemas críticos, incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); atividade de todos os colaboradores durante os acessos as redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior), conforme procedimento publicado na matriz de responsabilidade.
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

A segurança da informação depende de pessoas comprometidas, processos gerenciais de controle e sistemas de segurança da informação.