

POLÍTICA DE TI

A Política de Tecnologia da Informação é o documento que orienta e estabelece as diretrizes de **FCB Advogados** para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas do escritório.

1, OBJETIVO

1.1. Estabelecer diretrizes que permitam a todos seguir padrões de comportamento relacionados à segurança da informação adequados às necessidades de trabalho e de proteção legal do escritório e dos indivíduos.

1.2. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

1.3. Preservar as informações de **FCB Advogados, seus Clientes, Advogados, Estagiários, Empregados e Terceiros com quem qualquer indivíduo mantenha relação e utilize dados e ferramentas de TI em nome do escritório** quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2. ABRANGÊNCIA

2.1. As diretrizes aqui estabelecidas deverão ser seguidas por todos, interna e externamente, sejam colaboradores ou prestadores e prestadoras de serviço, e se aplicam à informação em qualquer meio ou suporte.

3. DAS RESPONSABILIDADES

3.1. Dos Colaboradores em Geral

- Entende-se por colaborador toda e qualquer pessoa física, sócia, estagiária, contratada pelo regime CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora do escritório.
- Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a **FCB Advogados** e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

3.2. Dos Gestores de Pessoas e/ou Processos

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.
- Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da política.
- Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações de **FCB Advogados**. Antes de conceder acesso às informações do escritório, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

3.3 Da Área de Tecnologia da Informação

- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta política.
- Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para **FCB Advogados**.
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

- O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.
- Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:
 - os usuários (logins) individuais de funcionários serão de responsabilidade do próprio colaborador.
 - os usuários (logins) de terceiros serão de responsabilidade do gestor da pessoa contratante.
- Proteger continuamente todos os ativos de informação do escritório contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção do escritório em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- Definir as regras formais para instalação de software e hardware em ambiente de produção jurídico, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro do escritório.
- Realizar auditorias periódicas de configurações técnicas e análise de riscos.
- Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos do escritório.
- Monitorar o ambiente de TI, gerando indicadores e históricos de:
 - uso da capacidade instalada da rede e dos equipamentos;
 - tempo de resposta no acesso à internet e aos sistemas críticos;
 - períodos de indisponibilidade no acesso à internet e aos sistemas críticos;
 - incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
 - atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

4. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

4.1. Para garantir as regras mencionadas na presente Política, **FCB Advogados** poderá:

- 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 poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gestor (ou superior) ou por determinação da Sócia Fundadora;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

4.2 Correio eletrônico

- É proibido aos colaboradores o uso do correio eletrônico de **FCB Advogados**:
 - Enviar mensagem por correio eletrônico por endereço genérico de sua área ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
 - Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou **FCB Advogados** vulneráveis a ações civis ou criminais;
 - Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;]
 - Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
 - Apagar mensagens pertinentes de correio eletrônico quando **FCB Advogados** estiver sujeita a algum tipo de investigação.
 - Produzir, transmitir ou divulgar mensagem que: (i) vise a vigiar secretamente ou assediar outro usuário; (ii) vise a acessar informações confidenciais sem explícita autorização do proprietário; (iii) vise a acessar indevidamente informações que possam causar prejuízos a qualquer pessoa; (iv) inclua imagens criptografadas ou de qualquer forma mascaradas; e (v) tenha conteúdo considerado impróprio, obsceno ou ilegal.

5. INTERNET

5.1. Todas as regras atuais de **FCB Advogados** visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional. Embora a conexão direta e permanente da rede corporativa do escritório com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

5.2. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria.

5.3. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do escritório, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

5.4. Ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

6. IDENTIFICAÇÃO

6.1. Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra.

6.2. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 - falsa identidade).

6.3. Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

6.4. Todos os dispositivos de identificação utilizados em **FCB Advogados**, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

6.5. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

6.6. Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

6.7. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

6.8. A periodicidade máxima para troca das senhas é 6 (seis) meses, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 3 (três) meses. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

6.9. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, a Pessoa Responsável por Recursos Humanos deverá imediatamente comunicar tal fato à Pessoa Responsável por Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

6.10. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente ou virtualmente à área técnica responsável para cadastrar uma nova.

7. DISPOSIÇÕES GERAIS

7.1. Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna de **FCB Advogados**. Ou seja, qualquer incidente de segurança decorrente de conduta culposa ou dolosa será entendido como ação contra a ética e os bons costumes regidos pelo escritório.

Esta Política entra em vigor a partir da data de sua divulgação no website de **FCB Advogados** (www.fcbadv.com.br) e vigorará por tempo indeterminado, podendo ser alterada a qualquer tempo, para adequação de suas disposições aos ditames legais e sociais aplicáveis.

u