

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

 FUKUSHIMA
advogados

COM APOIO DE:

keppen
ADVOGADOS

SUMÁRIO

1.	APRESENTAÇÃO.....	02
2.	APLICAÇÃO E VIGÊNCIA.....	02
3.	DEFINIÇÕES.....	02
4.	PRINCÍPIOS.....	05
5.	CLASSIFICAÇÃO QUANTO À CONFIDENCIALIDADE DAS INFORMAÇÕES.....	06
6.	DIRETRIZES DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO.....	07
7.	MEDIDAS DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO.....	08
8.	BOAS PRÁTICAS NA UTILIZAÇÃO DE FERRAMENTAS DE INTELIGÊNCIA ARTIFICIAL.....	10
9.	BOAS PRÁTICAS NA ELABORAÇÃO DE SENHAS.....	10
10.	PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS.....	11
11.	VIOLAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO.....	12

1. APRESENTAÇÃO

1.1. Esta Política de Segurança Cibernética e da Informação (“Política”) tem por objetivo assegurar a confidencialidade, a integridade e a disponibilidade das informações utilizadas nos sistemas de informação adotados pelo escritório Fukushima Advogados na prestação de seus serviços, bem como estabelecer medidas e procedimentos destinados a garantir a privacidade e a proteção dos dados pessoais tratados nas suas atividades.

1.2. A presente Política foi elaborada considerando o porte, o perfil de risco e o modelo de negócio do Fukushima Advogados, bem como a natureza de seus serviços, atividades e processos, além do volume e categoria dos dados pessoais e das demais informações relativas aos clientes do escritório, em estrita observância às disposições da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), em especial ao teor dos arts. 46 e 47.

2. APLICAÇÃO E VIGÊNCIA

2.1 Esta Política se aplica a todos os colaboradores, de qualquer nível hierárquico, incluindo sócios, coordenadores, consultores, advogados, estagiários e colaboradores da área administrativa do escritório, além parceiros comerciais ou terceiros de qualquer natureza que mantenham vínculo com o Fukushima & Advogados, como prestadores de serviços e fornecedores.

2.2 A presente Política deve ser observada no desempenho das atividades realizadas em todos os ambientes do escritório, incluindo de forma presencial, remota ou qualquer outra modalidade de trabalho em que seja acessado o seu banco de dados.

2.3 Esta Política tem vigência por prazo indeterminado, podendo ser atualizada sempre que necessário, sendo que as alterações deverão ser devidamente divulgadas para os colaboradores, parceiros e terceiros do escritório.

3. DEFINIÇÕES



I - CLIENTES

Pessoas físicas e/ou jurídicas contratantes dos serviços prestados pelo Fukushima Advogados;



II - COLABORADORES

Todos os profissionais contratados diretamente pelo Fukushima Advogados para o desempenho de atividades profissionais, independentemente do tipo de vínculo, incluindo advogados associados, prestadores de serviço contratados sob regime PJ, empregados contratados sob regime CLT e estagiários;



III - DADO PESSOAL

Informação relacionada a uma pessoa natural (excluídos, portanto, os dados de pessoas jurídicas) que permite identificá-la de maneira direta ou indireta, como nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, número de conta bancária, entre outros;



IV - DADO PESSOAL SENSÍVEL

Informação relacionada a uma pessoa natural que pode gerar maior risco de discriminação ao titular, como dados relacionados à origem racial ou étnica, crença religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, além de informações relacionadas à saúde, à vida sexual, a dados genéticos ou biométricos;



V - TRATAMENTO DE DADOS PESSOAIS

Toda ação realizada com um dado pessoal por uma pessoa natural ou jurídica, com finalidade econômica, como relativas à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, modificação, comunicação, transferência, difusão ou extração;



VI - TITULAR DE DADOS PESSOAIS

Pessoa natural a quem se referem os dados pessoais que são objeto do tratamento;



VII - SEGURANÇA DA INFORMAÇÃO

Conjunto de práticas, medidas e controles destinados a preservar a confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações, assegurando sua proteção e contribuindo para o alcance dos objetivos estratégicos do Fukushima Advogados;



VIII - USUÁRIO

Toda pessoa autorizada, seja colaborador, terceirizado ou prestador de serviços, a utilizar os recursos tecnológicos e acessar informações do Fukushima Advogados;



IX - AMBIENTE EM NUVEM

Modelo de armazenamento de arquivos e disponibilização de recursos de tecnologia da informação através da internet, como plataformas ou softwares, fornecidos por provedores externos e caracterizados por elevada escalabilidade, flexibilidade e disponibilidade ao usuário;



X - ANTIVÍRUS/ANTIMALWARE

Ferramenta instalada em dispositivos com a finalidade de identificar, bloquear e eliminar softwares maliciosos, contribuindo para a proteção dos sistemas e das informações do Fukushima Advogados;



XI - ATIVO DE INFORMAÇÃO

Todo recurso que armazene, processe ou viabilize o tratamento de dados pelo Fukushima Advogados, abrangendo arquivos, sistemas, equipamentos físicos (como notebooks e servidores) e documentos em meio físico;



XII - INCIDENTE DE SEGURANÇA

Qualquer situação que viole ou comprometa a confidencialidade, integridade ou disponibilidade das informações ou dos dados pessoais tratados pelo escritório;



XIII - RISCOS CIBERNÉTICOS

São os riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede, fraudes externas, entre outros, que possam expor dados, redes e sistemas do Fukushima Advogados, causando danos;



XIV - BACKUP

Cópia de segurança das informações corporativas, mantida em ambiente protegido, destinada à restauração dos dados em caso de perda, falha operacional ou incidente de segurança;



XV - CRIPTOGAFIA

Método de transformação de dados em formato codificado, destinado a impedir o acesso ou a compreensão dessas informações por pessoas não autorizadas;



XVI - FIREWALL

Mecanismo, implementado por meio de dispositivo ou software, destinado a monitorar e controlar o tráfego de rede, autorizando ou bloqueando conexões conforme regras e políticas de segurança previamente estabelecidas; e



XVII - VULNERABILIDADE

Deficiência existente em sistemas, processos ou configurações que pode ser explorada por agentes externos, resultando em danos ou no acesso indevido às informações.

4. PRINCÍPIOS

4.1 Confidencialidade: proteção dos dados pessoais e demais informações contra acessos não autorizados e demais formas de tratamento indevido;

4.2 Integridade: garantia da inviolabilidade e da exatidão dos dados pessoais, das demais informações e dos sistemas e serviços do escritório;

4.3 Acesso Controlado: limitação e controle de acesso aos dados pessoais, às demais informações e aos sistemas do escritório, assegurando que colaboradores e terceiros acessem apenas o que for estritamente necessário ao desempenho de suas atividades; e

4.4 Prevenção: adoção de medidas prévias à ocorrência de incidentes de segurança, contribuindo para a mitigação de riscos cibernéticos e de tratamento indevido de dados pessoais sob a responsabilidade do escritório.

5. CLASSIFICAÇÃO QUANTO À CONFIDENCIALIDADE DAS INFORMAÇÕES

5.1 Os dados e as informações devem ser classificados conforme seu grau de relevância ao escritório e aos riscos que podem decorrer do seu tratamento, com o objetivo de adotar medidas de proteção compatíveis com essa classificação, dividida da seguinte forma:

5.1.1 Confidencial: informações de acesso extremamente restrito, cujo vazamento, alteração ou uso indevido pode causar danos graves ao escritório, a clientes ou parceiros, incluindo dados pessoais sensíveis, peças processuais, estratégias jurídicas, segredos profissionais e demais informações protegidas por dever legal de sigilo;

5.1.2 Restrito: informações de acesso limitado a grupos específicos de colaboradores ou terceiros autorizados, cujo uso indevido pode gerar prejuízos relevantes ao escritório, a seus clientes ou parceiros, como contratos, dados pessoais comuns não públicos e documentos com informações particulares;

5.1.3 Interno: informações destinadas ao uso interno do escritório, que não devem ser divulgadas externamente, mas cujo eventual vazamento tende a gerar impacto moderado, como comunicações internas, procedimentos administrativos, materiais de consulta exclusivos do escritório e relatórios de atividades que contenham apenas informações operacionais; e

5.1.4 Público: informações que podem ser divulgadas ao público sem restrição, por não apresentarem risco ao escritório, a titulares de dados ou a terceiros, como conteúdos institucionais autorizados, materiais de divulgação e informações publicadas em canais oficiais.



6. DIRETRIZES DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

6.1 O escritório Fukushima Advogados compromete-se a observar as diretrizes legais e as boas práticas técnicas aplicáveis à privacidade e proteção de dados pessoais e demais informações que são tratadas em suas atividades, bem como prevenir, detectar e mitigar vulnerabilidades e incidentes de segurança que possam gerar danos relevantes aos titulares ou ao próprio escritório.

6.2 O escritório utiliza ferramentas seguras e atualizadas para a gestão de seu ambiente digital, com apoio de empresas especializadas em armazenamento em nuvem e consultoria de TI responsável pela infraestrutura e pela realização de backups periódicos, assegurando a disponibilidade contínua das informações.

6.3 É de integral responsabilidade dos colaboradores e terceiros relacionados ao Fukushima Advogados a observância das seguintes diretrizes no exercício das suas atividades profissionais:

6.3.1 Resguardar os dados pessoais e demais informações tratadas pelo escritório contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas, em observância às disposições desta Política;

6.3.2 Identificar o nível de sigilo das informações e a categoria dos dados pessoais tratados, adotando as medidas adequadas para assegurar proteção compatível com os riscos decorrentes do seu tratamento;

6.3.3 Assegurar que os sistemas e os dados sob sua responsabilidade estejam devidamente protegidos contra acessos não autorizados, garantindo que sua utilização ocorra exclusivamente para o exercício das atividades profissionais no Fukushima Advogados;

6.3.4 Realizar, ou assegurar que seja realizada, a manutenção periódica e a atualização constante dos softwares, antivírus e firewall utilizados pelo Fukushima Advogados, garantindo sua eficácia na proteção dos ativos de informação;

6.3.5 Manter o sigilo das credenciais de acesso, sendo expressamente proibido o compartilhamento de contas e senhas, ainda que com outros colaboradores do Fukushima Advogados;

6.3.6 Adotar mecanismos de autenticação multifator para controle de acesso a dispositivos móveis utilizados no desempenho das atividades do Fukushima Advogados, tais como smartphones e laptops;

6.3.7 Sempre que possível, manter separados os dispositivos móveis de uso pessoal daqueles destinados às atividades institucionais do Fukushima Advogados;

6.3.8 Bloquear o computador e demais dispositivos de acesso sempre que se ausentar do posto de trabalho, ainda que por curto período;

6.3.9 Comunicar imediatamente ao superior hierárquico sempre que tiver acesso indevido a informações ou receber, por equívoco, conteúdo ao qual não deveria ter acesso;

6.3.10 Comunicar imediatamente ao setor administrativo do Fukushima Advogados, ou ao suporte técnico de TI, qualquer incidente de segurança da informação que contrarie as diretrizes estabelecidas nesta Política e não envolva dados pessoais, sendo que o procedimento adequado para comunicar incidentes neste último caso observará o disposto no item 10.2 desta Política.

7. MEDIDAS DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

7.1 O Fukushima Advogados exige a adoção das seguintes medidas e controles por seus colaboradores e terceiros relacionados às suas atividades, com o objetivo de reduzir vulnerabilidades relacionadas à cyberssegurança e ao tratamento de dados pessoais, bem como assegurar a continuidade dos negócios pela excelência e segurança no atendimento aos clientes:

7.1.1. O acesso aos dados pessoais e às informações classificadas como confidenciais, restritas ou internas do Fukushima Advogados (conforme item 5 desta Política) será concedido exclusivamente mediante autenticação individual no sistema, por meio de login e senha pessoal, sigilosa e intransferível;

7.1.2. Caso o terceiro não possua, por força contratual, acesso direto aos ambientes virtuais internos do Fukushima Advogados, o compartilhamento de informações ficará restrito ao mínimo necessário para a adequada execução do contrato, devendo ocorrer, preferencialmente, por meio de conexão privada, segura e devidamente controlada;

7.1.3. Informações confidenciais e/ou dados pessoais sensíveis deverão ser compartilhados exclusivamente de forma criptografada e protegida por mecanismos adicionais de segurança, como senha ou outro método de anonimização ou pseudonimização de dados;

7.1.4 O Fukushima Advogados promoverá treinamentos e avaliações periódicas com a finalidade de assegurar a conscientização e capacitação contínua de colaboradores e terceiros relacionados ao escritório em relação às boas práticas de segurança da informação e proteção de dados;

7.1.5. Os acessos aos dados pessoais tratados pelo Fukushima Advogados serão concedidos em estrita observância ao princípio da necessidade, previsto no art. 6º, III, da LGPD, devendo ser limitados ao mínimo necessário para o desempenho das atividades profissionais, os quais estarão sujeitos a medidas contínuas de controle, monitoramento e restrição, de modo a assegurar a adequada proteção dessas informações e prevenir tratamentos irregulares;

7.1.6. Os acessos concedidos às pastas e sistemas internos do Fukushima Advogados serão revistos periodicamente e serão imediatamente revogados quando o colaborador for desligado ou ocorrer o término da relação contratual com o terceiro, ou sempre que houver alteração das atribuições que justifique a modificação ou revogação das permissões;

7.1.7. A utilização dos e-mails corporativos vinculados ao Fukushima Advogados deve ocorrer exclusivamente para fins profissionais, sendo expressamente proibido seu uso para finalidades particulares ou em desacordo com as demais diretrizes estabelecidas nesta Política de Segurança Cibernética e da Informação;

7.1.8. O uso de telefone celular corporativo do Fukushima Advogados será restrito aos colaboradores cuja atividade justifique sua disponibilização, durante a vigência do vínculo profissional, sendo vedada a utilização do equipamento para fins particulares, bem como a instalação de softwares, programas ou aplicativos que não sejam previamente autorizados pelo escritório;

7.1.9. O acesso remoto aos ambientes virtuais do Fukushima Advogados, incluindo pastas compartilhadas e sistemas de armazenamento em nuvem, será restrito a colaboradores em regime de home office e a terceiros devidamente autorizados, os quais deverão observar integralmente as medidas de segurança cibernética e da informação previstas nesta Política;

7.1.10. É expressamente proibida a instalação de softwares ou aplicativos nos equipamentos de titularidade do Fukushima Advogados sem a prévia e formal autorização do setor administrativo do escritório;

7.1.11. É vedada, em qualquer hipótese, a transferência de dados pessoais e demais informações das estações de trabalho do Fukushima Advogados para dispositivos de armazenamento externo, tais como pen drives, discos rígidos externos ou quaisquer mídias removíveis não autorizadas;

7.1.12. Ao utilizar a rede cabeada ou wi-fi do Fukushima Advogados, é vedado o acesso a sites ou aplicativos estranhos às atividades profissionais que possam comprometer a segurança cibernética e da informação;

7.1.13. É vedado aos colaboradores do Fukushima Advogados divulgar, de forma intencional ou acidental, informações sob resguardo do escritório por meio de filmagens ou fotografias realizadas nas suas dependências internas, devendo agir com cautela na produção desses registros, cuja eventual divulgação dependerá de autorização prévia do gestor responsável; e

7.1.14. Todas as medidas de segurança cibernética e da informação previstas nesta Política aplicam-se integralmente aos ativos informacionais em formato físico do Fukushima Advogados que contenham dados pessoais ou informações classificadas como sendo confidenciais, restritas ou internas, tal como documentos impressos.

8. BOAS PRÁTICAS NA UTILIZAÇÃO DE FERRAMENTAS DE INTELIGÊNCIA ARTIFICIAL

8.1 O Fukushima Advogados não veda a utilização de ferramentas de inteligência artificial em todas as situações, por reconhecer que podem proporcionar maior eficiência e otimização das atividades profissionais, contudo, em razão dos riscos inerentes à segurança das informações do escritório, sua utilização somente será permitida mediante a estrita observância das seguintes diretrizes:

8.1.1. Apenas será autorizada a utilização da ferramenta Adobe, já instalada nos computadores dos colaboradores, para a conversão do formato de documentos, sendo vedada a utilização de outras ferramentas para essa finalidade, como o a plataforma / *Love PDF*;

8.1.2. Na utilização de ferramentas de inteligência artificial destinadas à elaboração de textos, como o ChatGPT, é expressamente proibida a inserção de dados pessoais ou informações classificadas como sendo confidenciais, restritas ou interna, sob tutela do Fukushima Advogados, sendo admitido seu uso nessas hipóteses apenas quando essas informações forem previamente tarjadas; e

8.1.3. Na utilização de ferramentas de inteligência artificial para elaboração de materiais visuais e apresentações, é proibida a inserção da logomarca ou de quaisquer elementos que identifiquem o Fukushima Advogados, seus clientes ou parceiros, devendo tais informações serem incluídas apenas após a utilização da ferramenta.

8.2. Na utilização de ferramentas de inteligência artificial, deverão ser rigorosamente observadas todas as demais diretrizes relativas à privacidade e à proteção de dados pessoais, além das relativas à segurança cibernética e das informações sob tutela do Fukushima Advogados, conforme estabelecido nesta Política.

9. BOAS PRÁTICAS NA ELABORAÇÃO DE SENHAS

9.1. As senhas para acesso aos ativos informacionais do Fukushima Advogados são pessoais, sigilosas e intransferíveis, sendo expressamente proibido seu compartilhamento, anotação em locais acessíveis a terceiros, divulgação ou fornecimento a qualquer outro colaborador.

9.2. As senhas deverão observar os seguintes requisitos mínimos de complexidade:

9.2.1. Conter, no mínimo, 8 (oito) caracteres;

- 9.2.2. Incluir ao menos uma letra maiúscula;
- 9.2.3. Incluir ao menos uma letra minúscula;
- 9.2.4. Conter ao menos um número (0 a 9) ou caractere especial (como \$, @, *, #).

9.3. É vedada a utilização de senhas que:

- 9.3.1. Contenham o ID ou nome de usuário;
- 9.3.2. Repitam mais de 4 (quatro) caracteres contínuos na mesma posição em relação à senha anterior;
- 9.3.3. Incluam informações pessoais de fácil obtenção, tais como nomes, sobrenomes e datas de nascimento;
- 9.3.4. Apresentem repetições ou sequências óbvias de letras, números ou caracteres;
- 9.3.5. Contenham o nome do escritório ou qualquer de suas variações, inclusive por duplicação, inversão ou combinação evidente.

9.4 As senhas deverão ser alteradas, no máximo, a cada 180 (cento e oitenta) dias, sendo que, após esse período, o acesso aos sistemas do Fukushima Advogados ficará condicionado à sua atualização.

9.5. O acesso à rede será automaticamente bloqueado após 5 (cinco) tentativas consecutivas de login malsucedidas, como medida preventiva contra acessos indevidos.

10. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

10.1. Todos os colaboradores e terceiros do Fukushima Advogados deverão observar as medidas necessárias à garantia da privacidade e da proteção de dados pessoais sempre que tiverem acesso a tais informações por meio dos seus ativos informacionais, em observância às diretrizes desta Política de Segurança Cibernética e da Informação e da Política de Privacidade do escritório.

10.2. Em caso de dúvidas relacionadas ao tratamento de dados pessoais, ou para comunicar incidentes de segurança que envolvam essas informações, os colaboradores e terceiros poderão contatar o Encarregado de Dados do Fukushima Advogados por meio do seguinte e-mail privacidade@fukushima.adv.br.

Encarregado Titular: Ademir Nodari.
Encarregado Substituto: William Hosaka.

11. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

11.1 O descumprimento das diretrizes estabelecidas nesta Política sujeitará o infrator a medidas disciplinares, aplicadas de acordo com a natureza e a gravidade da infração, sem prejuízo das penalidades previstas na legislação aplicável.

11.2. Conforme a gravidade dos fatos, o Fukushima Advogados poderá determinar o encerramento da relação de trabalho, parceria ou contrato, bem como a extinção da relação comercial mantida com o infrator.

11.3. Na hipótese de haver prejuízo suportado pelo escritório em decorrência do descumprimento desta Política, poderá o Fukushima Advogados adotar as medidas judiciais cabíveis, inclusive o ajuizamento de ação regressiva para ressarcimento de danos.

11.4. Compete à Equipe de Compliance conduzir as apurações internas relativas a eventuais desvios de conduta envolvendo dados pessoais e segurança das informações, os quais deverão ser comunicados através do Canal de Denúncias do Fukushima Advogados, conforme diretrizes do Regimento Interno do seu Canal de Denúncias. Atualmente, a Equipe de Compliance é composta pelo escritório Keppen Advogados.

CONTROLE DE VERSÃO

Versão 002 (Março/2026)	POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO DO FUKUSHIMA ADVOGADOS	Data da aprovação: 06/03/2026
Elaborador: Keppen Advogados	Revisor: Ademir Nodari	Aprovador: Emerson Fukushima



 FUKUSHIMA
advogados

COM APOIO DE:

keppen
ADVOGADOS