POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS MORAIS & ADVOGADOS

I. DA INTRODUÇÃO:

De certo, que a Política de Privacidade é considerada o documento por meio do qual, nosso escritório se propõe explicar à todos os interessados a forma como os dados pessoais dos clientes e usuários da plataforma serão tratados e dessa maneira, busca estar adequado à cultura da proteção de dados, respeitando a observância do que dispõe a legislação vigente, a saber, a Lei 13.709/2018 – Lei Geral de Proteção de Dados - LGPD. Nesse contexto, reafirmamos nosso compromisso e respeito à privacidade e à proteção de dados com a publicação da presente política.

II. DO OBJETIVO DA POLÍTICA DE PRIVACIDADE:

Fica definido que a Política de Privacidade e Proteção de Dados Pessoais, aqui denominada simplesmente de "Política", é tida como sendo, a principal legislação que orienta o Programa Interno de Privacidade e Proteção de Dados do escritório MORAIS & ADVOGADOS e tem como base, as recomendações das normas da ABNT, em especial, as normas NBR ISO/IEC 27.001, 27.002 e 27.701 e, que se aplicam como normas de boas práticas na gestão da privacidade e segurança da informação.

Nosso escritório, realiza operações de gestão administrativa através de um servidor, localizado nas dependências da sua sede, considerando, portanto, imprescindível a criação de uma política que normatize e que direcione os procedimentos que são considerados necessários para garantir a privacidade e os requisitos mínimos estabelecidos pela LGPD.

Desta forma, nossa Política tem como objetivo, o estabelecimento das normas, das diretrizes e dos procedimentos que visam assegurar, sobretudo, a Privacidade e a Proteção dos Dados Pessoais, garantindo assim, que haja por parte dos usuários e clientes, uma total confiabilidade quanto às informações através da preservação da confidencialidade, da integridade e da disponibilidade dos dados que são confiados ao nosso escritório e que conta com a participação ativa de todos os colaboradores, por meio de treinamentos e do cumprimento das regras de segurança aos dados.

Assim, consideramos que estão preservados os pilares que sustentam a segurança da informação, a saber:

1) **Da Confidencialidade**: Considerada o pilar que possibilita que a informação seja acessível apenas para pessoas que estejam devidamente cadastradas ou autorizadas a ter acesso;

2) **Da Integridade**: Considerada o pilar que tem como função primordial, garantir que a informação seja correta, confiável e sem a ocorrência de alterações que não sejam devidamente autorizadas;

3) **Da Disponibilidade**: Considerada o pilar que torna a informação acessível ao uso de maneira legítima para os usuários devidamente autorizados.

III. DA DIVULGAÇÃO DA POLÍTICA DE PRIVACIDADE:

Nós do escritório MORAIS & ADVOGADOS, adotamos por padrão, obedecer e tomar todos os cuidados com a prática efetiva da Privacidade e com a Proteção de Dados Pessoais, passando a ser de todos, a responsabilidade com os dados pessoais dos nossos clientes internos e externos, adotando por meio da governança e, da implementação de um Programa Interno de Privacidade e de Proteção de Dados, incluindo os pessoais, que está pautada no respeito aos procedimentos quer sejam técnicos, quer sejam administrativos, sempre levando em conta a maneira como os colaboradores possam respeitar e contribuir com o uso adequado das tecnologias tornando de maneira efetiva quanto ao objetivo dessa política, em especial, no que se refere à garantia da segurança e proteção dos dados pessoais a nós confiados.

IV. DA EFETIVIDADE DAS CLÁUSULAS DA POLÍTICA DE PRIVACIDADE:

Consideramos essencial que todos os responsáveis pelos processos internos, embasados nessa Política, demonstrem seu comprometimento para o cumprimento efetivo. Assim, desde os colaboradores até a mais alta cúpula diretiva, devem cumpri-la em sua inteireza, pois é dessa maneira que se entende que haverá efetividade no cumprimento da Privacidade e da Proteção de Dados Pessoais que, como se percebe, depende estritamente do comprometimento pessoal de cada um, em especial, da alta direção, como fundamental para o seu real cumprimento, possibilitando assim, que haja:

a) A inexistência de exceções às regras estabelecidas na política;
b) Que a Política tenha a mais ampla divulgação e seja respeitada;
c) Que a Política seja considerada sempre um ativo estratégico;
d) Que por padrão a Política seja adotada desde o processo seletivo;

Desta maneira, fica clara a ideia de que praticamos efetivamente todos os passos para que Política seja cumprida, visando sempre a Privacidade e a Proteção dos Dados Pessoais, pois do contrário, ante o não cumprimento dessa política, o documento escrito passaria a ser apenas um documento sem valor.

V. DAS DEFINIÇÕES DA POLÍTICA - LGPD:

A LGPD: Lei Geral de Proteção de Dados;
Os Dados Pessoais: É toda informação relacionada à uma pessoa natural, podendo ser identificada ou identificável;
Os Dados Pessoais Sensíveis: São os dados pessoais que versam, em síntese, sobre origem racial ou étnica, sobre convicções religiosas, opiniões políticas, sobre filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou a vida sexual, além de dados genéticos ou biométricos;
Os Dados Anonimizados: São dados relativos ao titular que, após tratamento pela empresa, impede a identificação do seu titular;
O Controlador: É toda pessoa natural ou jurídica, de direito público ou privado, a quem competem tomar as decisões referentes ao tratamento dos dados pessoais;
O Operador: É toda pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
O Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
O Encarregado - DPO - *Data Protection Officer* – É a pessoa indicada pelo controlador ou pelo operador, para atuar como canal de comunicação entre o controlador e os titulares dos dados ou entre controlador e a Autoridade Nacional de Proteção de Dados – ANPD;
A Autoridade Nacional de Proteção de Dados - ANPD: É o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.
Os Agentes de tratamento de Dados: São considerados agentes de tratamento de dados, o controlador e o operador;
O Consentimento: É a autorização que é dada pelo titular dos dados, que expressa sua manifestação de vontade, de forma livre, específica, informada e explícita, onde ele aceita, de forma declarada e inequívoca, seja eletronicamente ou não, que seus dados pessoais podem ser objeto de tratamento, sendo o objetivo específico;
O Banco de dados: É o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou mesmo físico;
O Tratamento de Dados Pessoais: É toda operação que é realizada com quaisquer dos dados pessoais, por exemplo, a coleta, a produção, a recepção, a classificação, a utilização, o acesso, a reprodução, a transmissão, a distribuição, o processamento, o arquivamento, o armazenamento, a eliminação, a avaliação, a modificação, a comunicação, a transferência nacional ou internacional, a difusão, o armazenamento, a extração ou mesmo a eliminação;
As Bases Legais: São hipóteses de tratamento de dados em que permitidas pela LGPD - Lei Geral de Proteção de Dados Pessoais;
O Compartilhamento de dados: É toda comunicação, difusão, interconexão de dados pessoais ou transferência nacional ou

internacional, tratamento compartilhado de bancos de dados pessoais por órgãos públicos ou por entidades, no cumprimento de suas competências, seja entre esses, ou entre entres privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento, permitidas por esses entes públicos ou entre entes privados;

O Relatório de impacto à proteção de dados pessoais: Documento emitido pelo Controlador, que contém de forma detalhada, a descrição de todo o processo ou processos internos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como, medidas, salvaguardas e mecanismos para mitigação de riscos;

Os Cookies: São pequenos pacotes de arquivos de texto que coletam e armazenam determinadas informações durante a navegação do usuário e que, no primeiro acesso é possível ao usuário (titular de dados) decidir se aceita, recusa ou ainda gerenciar suas escolhas e preferências com a finalidade de otimizar a experiência do usuário em sua navegação pelo site;

Os Banner de Cookies: São uma espécie de recurso visual que é utilizado no design de aplicativos ou em sites na internet, que se utiliza de barras de leitura destacadas, para informar ao usuário, de forma resumida, simples e direta, sobre a utilização dos cookies no site visitado. O banner tem como função, fornecer ferramentas para que o usuário possa ter maior controle sobre o tratamento de seus dados, dando a ele condições de decidir pelo consentimento ou não de determinados cookies.

VI. DOS DIREITOS DOS TITULARES DE DADOS:

Reconhecida na Constituição Federal Brasileira como direito fundamental, a proteção de dados, garante aos titulares de dados, por meio da LGPD, os seguintes direitos:

- **A confirmação** da existência de tratamento de dados;
- **O acesso** aos seus dados;
- **A correção** de dados incompletos, inexatos ou desatualizados;
- **A anonimização**, bloqueio ou eliminação de dados desnecessários;
- **A portabilidade** dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador ou da autoridade nacional, observados os segredos comercial e industrial;
- **A eliminação** dos dados pessoais tratados com o consentimento do titular, após o uso, exceto nas hipóteses previstas no art. 16, da LGPD;
- **A informação** prestada às entidades públicas e privadas com as quais o controlador realizou o compartilhamento dos dados;

- **A informação** presada sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- **A revogação** do consentimento, nos termos do art. 8º, §5º da LGPD.
- **É direito do titular dos dados** apresentar petição do titular à Autoridade Nacional – ANPD, sobre seus dados pessoais, sem qualquer custo, sempre que não conseguir exercer seus direitos perante o controlador;

VII. DOS PRINCÍPIOS PARA TRATAMENTO DE DADOS PESSOAIS:

Na LGPD, são descritos os princípios para o tratamento de dados e o escritório MORAIS & ADVOGADOS observa os princípios no tratamento de dados de pessoa física, a saber:

O Princípio da Finalidade: Que consiste na realização do tratamento de dados pessoais para propósitos legítimos, específicos, explícitos e que deverão ser informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades específicas;
O Princípio da Adequação: Que consiste na compatibilidade entre o tratamento de dados com as finalidades informadas ao titular, de acordo com o contexto do tratamento dos dados;
O Princípio da Necessidade: Que estabelece a limitação do tratamento dos dados ao mínimo necessário para a cumprimento das suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos, em relação às finalidades do tratamento de dados definidos;
O princípio do Livre Acesso: Que consiste na garantia aos titulares dos dados, a consulta facilitada e gratuita sobre a forma e a duração do tratamento dos dados, bem como, sobre a integralidade de seus dados pessoais;
O princípio da Qualidade dos Dados: Que consiste na garantia aos titulares dos dados, quanto a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
O princípio da Transparência: Que consiste na garantia aos titulares, mediante informações claras, precisas e facilmente acessíveis sobre a realização do tratamento de dados e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
O princípio da Segurança: Que consiste na utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
O princípio da Prevenção: Que consiste na aplicação de medidas preventivas para assegurar o tratamento de dados pessoais de acordo com as exigências legais, a fim de evitar a ocorrência de danos aos titulares;

O princípio da Não Discriminação: Que consiste na impossibilidade de realização do tratamento de dados para fins discriminatórios ilícitos ou abusivos;
O princípio da Responsabilização e da Prestação de Contas: Que consiste na demonstração pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

VIII. DAS BASES LEGAIS - HIPÓTESES PARA O TRATAMENTO DE DADOS PESSOAIS:

O escritório MORAIS & ADVOGADOS, realizou mapeamento de todos os processos internos que utilizam dados pessoais, classificando-os e definindo a "Base Legal" que autoriza o tratamento, de acordo com as hipóteses estabelecidas na LGPD, a saber:

a) DADOS PESSOAIS:

1. Cumprimento de obrigação legal;
2. 2. Execução de Contrato;
3. Estudo por Órgãos de Pesquisa;
4. Proteção de Crédito;
5. Proteção da vida ou da incolumidade física do titular ou de terceiros;
6. Atos da Administração Pública;
7. Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
8. Exercício Regular de Direitos;
9. Interesse Legítimo;
10. Com o consentimento do Titular;

b) DADOS PESSOAIS SENSÍVEIS:

1. Cumprimento de obrigação legal;
2. Estudo por Órgãos de Pesquisa;
3. Atos da Administração Pública;
4. Proteção da vida ou da incolumidade física do titular ou de terceiros;
5. Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
6. Exercício Regular de Direitos;
7. Com o consentimento do Titular;
8. Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Importante: O mapeamento dos processos internos e a coleta dos dados pessoais foi realizado, por meio da aplicação de medidas e

conhecimentos específicos sobre a matéria, restando definido que tal processo deverá ser acompanhado permanentemente e que, deverá ser atualizado pelo Comitê de Privacidade, sob a responsabilidade do Encarregado de Proteção de Dados (DPO).

Periodicamente, serão realizadas auditorias e revisões dos mapeamentos, conforme definição a ser realizada pelo Comitê de Privacidade ou por pessoa indicada para tal.

É dever de todos os colaboradores, gestores e administradores, observarem o cumprimento das Bases Legais – Hipóteses de Tratamento, sendo vedado o uso dos dados pessoais para finalidades outras que não tenham sido mapeadas no processo interno.

Ocorrendo qualquer alteração, exclusão ou inclusão de novos processos internos ou acrescida a necessidade de novos dados pessoais nas atividades do escritório MORAIS & ADVOGADOS, o Encarregado de Proteção de Dados – DPO, deverá ser imediatamente informado para tomada das medidas cabíveis.

IX. DA EXCLUSÃO DE DADOS PESSOAIS:

Todos os dados pessoais coletados pelo escritório MORAIS E ADVOGADOS permanecerão armazenados no banco de dados para fins legítimos e essenciais, tais como:
a. existência de lei ou regulação específica exigindo prazo determinado para retenção de dados;
b. para exercício regular de direitos da MORAIS E ADVOGADOS;
c. para fins segurança, controle de fraudes e prestação de contas para os titulares dos dados e para a ANPD.
A MORAIS E ADVOGADOS permanecerá com o histórico de seus dados, garantindo o uso exclusivo pela organização e pelas outras por ela contratadas para cumprimento das finalidades descritas nesta Política, além da preservação da segurança de tais informações e outros interesses legítimos.
Após a regulamentação deste tema pela ANPD, serão estruturadas Políticas de Retenção de
Dados, a fim de estabelecer critérios e regras para exclusão dos dados pela MORAIS E ADVOGADOS.

X. DOS TREINAMENTOS:

O escritório MORAIS & ADVOGADOS, disponibilizará os recursos necessários para treinamento e realização de campanhas regulares de divulgação para todos os que devam seguir esta Política de Privacidade e Proteção de Dados Pessoais. Os treinamentos serão aplicados presencialmente ou de forma remota.

XI. DOS CONTRATOS COM FORNECEDORES:

Foi necessária a estruturação de uma Política de *Due Diligence* com relação aos Terceiros, que estabelece um novo fluxo, responsabilidades e os modelos de avaliação de riscos que passam a ser adotadas nas contratações do escritório MORAIS & ADVOGADOS, com objetivo de garantir que seus fornecedores e parceiros tenham, pelo menos, o mesmo nível de responsabilidade e compromisso com a Proteção de Dados Pessoais, estabelecidos pela legislação especial.

O escritório MORAIS & ADVOGADOS estabeleceu ainda, cláusulas-padrão para aplicação em todos os contratos com fornecedores e parceiros, em que são compartilhados dados de pessoa física, estabelecendo-se as obrigações básicas para os controladores e para operadores, a fim de que sejam cumpridas as regras estabelecidas pela LGPD.

Todos os novos contratos que envolvam compartilhamento de dados pessoais, passam a ser assinados, obrigatoriamente, com a presença das cláusulas atinentes à Privacidade e Proteção de Dados Pessoais.

Caso o fornecedor não aceite as sugestões de cláusulas, o assunto deverá ser encaminhado ao Encarregado - *Data Protection Officer* - DPO do escritório, para que seja realizada uma análise quanto aos riscos e, se for o caso, para a indicação das medidas cabíveis ao caso.

XII. DO COMITÊ DE PRIVACIDADE:

Definiu-se que o Comitê de Proteção de Dados Pessoais, reúne os principais interessados no tema da Proteção de Dados e que são responsáveis pelas atividades de tratamento de dados pessoais relevantes do MORAIS & ADVOGADOS.

O Comitê ficou responsável pela estruturação e por colocar em prática o Programa de Governança em Privacidade e Proteção de Dados Pessoais a partir das diretrizes que forem definidas por ele próprio e pela Política de Privacidade.

Além disso, o Comitê de Privacidade realizará reuniões periódicas sendo: ordinariamente, 01 (uma) vez por mês e, extraordinariamente, sempre que for necessário deliberar sobre algum incidente grave ou definição relevante do MORAIS & ADVOGADOS.

Cabe ao Comitê de Privacidade:

1) Definir estratégias, políticas, instruções de trabalho, boas práticas e regras de governança, privacidade e segurança de dados de pessoa física;
2) Disseminar a cultura de Proteção, Privacidade e Segurança de Dados;

3) Conduzir Auditorias Internas que monitorem o Programa de Privacidade e Proteção de Dados;
4) Propor, formatar e aprovar de treinamentos a todos os colaboradores do MORAIS E ADVOGADOS;
5) Fiscalizar o cumprimento das normas de governança de dados pessoais e respectivos treinamentos, todos relacionados ao cumprimento da Lei Geral de Proteção de Dados - LGPD;
6) Analisar, classificar, investigar a violação da Política de Privacidade e Proteção de Dados do MORAIS & ADVOGADOS;
7) Zelar pela aplicação dos modelos de cláusulas-padrão definidos para contratação de fornecedores, exigindo e fiscalizando que todos os contratos, de todas as áreas, contenham as referidas cláusulas;
8) Sugerir investimentos quanto à segurança da informação com o intuito de minimizar os riscos na área de Tecnologia da Informação.

De certo que, um dos pilares do comitê é o Encarregado de Proteção de Dados. Foi elaborado um Guia Orientativo para nortear e trazer maior segurança ao Encarregado, norteando suas principais funções dentro do cargo, baseado nas exigências legais e particulares do MORAIS & ADVOGADOS.

XIII. DO ENCARREGADO DE PROTEÇÃO DE DADOS *(DATA PROTECTION OFFICER* – DPO):

O Encarregado de Proteção de Dados, é a figura de natureza obrigatória em instituições, conforme dispõe a exigência do artigo 41, da LGPD. Ele deve estar envolvido em todas as questões de proteção de dados pessoais do escritório MORAIS & ADVOGADOS e necessita ter suporte e acesso a recursos adequados para cumprir suas funções de trabalho e para manter suas habilidades e conhecimentos técnicos.

Cabe ao Encarregado de Proteção de Dados Pessoais:

a) Orientar e sanar dúvidas jurídicas acionadas pelo Comitê de Privacidade, relacionadas a aplicação da Lei Geral de Proteção de Dados (LGPD);
b) Conscientizar e capacitar os Colaboradores do MORAIS & ADVOGADOS acerca de suas responsabilidades e, enquanto controladores e operadores de dados pessoais, bem com as boas práticas que devem ser seguidas para garantir conformidade e segurança os processos de tratamento;
c) Revisar os processos que envolvem o tratamento de dados pessoais, para garantir a melhoria contínua das medidas de segurança e atualização do processamento de acordo com as atualizações legais no que tange a Proteção de Dados Pessoais;

d) Fiscalizar a conformidade dos processos de tratamento de dados pessoais com a LGPD - Lei Geral de Proteção de Dados, regulamentos, atos normativos e políticas internas, sugerindo sanções quando necessárias;
e) Cooperar com a ANPD - Autoridade Nacional de Proteção de Dados, servindo como ponto de contato para questões relacionadas ao processamento e tratamento de dados pessoais pelo MORAIS & ADVOGADOS;
f) Servir como ponto de contato com os titulares dos dados, para garantir que estes, caso queiram, tenham acesso facilitado a informações relacionadas à coleta, processamento e tratamento dos seus dados pessoais.

XIV. DOS CANAIS DE COMUNICAÇÃO:

O escritório MORAIS & ADVOGADOS disponibiliza dados de contato e recebimento de solicitações dos titulares de dados, para eventuais dúvidas ou informações acerca da Política de Privacidade:

1) DADOS DO CONTROLADOR:

Razão Social:
MORAIS SOCIEADADE INDIVIDUAL DE ADVOCACIA
CNPJ/MF Nº 22.685.463/0001-77
Endereço: Av. Tancredo Neves, nº 620, Edifício Mundo Plaza, Sala 519, Caminho das Árvores - Salvador – BA, CEP: 41.820-020.

2) DADOS DO ENCARREGADO - DPO

Contato:
contato@moraiseadvogados.adv.br

3) CANAL DE SOLICITAÇÕES/RECLAMAÇÕES

Requisição de Titulares:
contato@moraiseadvogados.adv.br

XV. DAS RESPONSABILIDADES:

Esta política reafirma a responsabilidade do MORAIS & ADVOGADOS com a Proteção de Dados Pessoais dos seus colaboradores, parceiros e fornecedores. Por este motivo, serão adotadas diretrizes e orientações específicas, de acordo com norma ABNT NBR ISO/IEC 27701, a fim de que o Programa de Privacidade de Proteção de Dados Pessoais se mantenha de forma íntegra:

Dos Controles dos Documentos Físicos:

Será de inteira responsabilidade dos empregados, fornecedores e terceirizados do MORAIS & ADVOGADOS o cumprimento das seguintes obrigações:

a) As informações classificadas como confidencial ou confidencial restrita não poderão ser deixadas sobre a mesa de trabalho, dentro de gaveta ou em armários que não possuam chave;
b) Os documentos armazenados em armários físicos deverão ser acessados – preferencialmente, por uma única chave - exclusivamente aos colaboradores e às áreas que necessitarem dos mesmos para execução dos seus processos internos;
c) As informações confidenciais ou confidenciais restritas, devem ser totalmente destruídas quando não mais necessárias, de forma segura e seguindo as orientações do escritório MORAIS & ADVOGADOS, mediante uso de uma fragmentadora de papel;
d) Não é permitido realizar cópias, divulgar ou compartilhar informações confidenciais, para uso pessoal ou de terceiros, exceto para os casos estritamente necessários para execução das atividades.

Do Acesso e utilização da Rede Interna Corporativa:

O acesso à rede interna corporativa do MORAIS & ADVOGADOS é controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam minimizados.

Assim, foi preciso que fossem instauradas algumas regras, listadas a seguir:

a) A Internet cabeada deve ser disponibilizada apenas para máquinas e equipamentos de propriedade do escritório MORAIS & ADVOGADOS, com a finalidade restrita à realização de atividades inerentes ao desempenho de tarefas laborais;
b) O uso da internet para visitantes ou mesmo para os equipamentos smartphones da empresa e, especialmente, os equipamentos pessoais, é segregada, em rede própria diversa daquela que em são utilizados os equipamentos que terão acesso à internet e rede de acesso ao servidor de arquivos, garantindo o isolamento da rede interna do MORAIS & ADVOGADOS, com o objetivo de fornecer acesso a sistemas e dados internos apenas para os colaboradores desempenharem suas tarefas; Ainda, foi criada outra ter outras redes com acesso apenas à Internet para disponibilizar a visitantes e usuários que não precisam ou podem ter acesso aos dados internos;

c) Os ativos de TIC, tecnologias e serviços fornecidos para o acesso à Internet, são de propriedade do MORAIS & ADVOGADOS, que pode analisar e, se necessário, bloquear em nível de rede firewall ou sistema de intrusão, usuários, qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Privacidade e Proteção de Dados;
d) A Internet disponibilizada pelo MORAIS & ADVOGADOS aos seus colaboradores, poderá ser utilizada para fins pessoais, desde que seja autorizada pela respectiva liderança e não prejudique o andamento dos trabalhos;
e) É terminantemente proibida a divulgação e/ou o compartilhamento indevido de informações internas, confidenciais e confidenciais restritas em listas de discussão, sites, armazenamento em nuvem pública, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata que use a internet com via, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer penalidades previstas nos procedimentos internos e/ou na forma da lei;
f) Os Colaboradores com acesso à Internet só poderão fazer o download de programas necessários às suas atividades no MORAIS & ADVOGADOS quando autorizados pelo gestor ou pela Alta Direção;
g) O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos;
h) Os colaboradores não poderão, em hipótese alguma, utilizar os recursos do MORAIS & ADVOGADOS para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;
i) Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso do MORAIS & ADVOGADOS;
j) Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;
k) Os empregados não poderão usar os recursos do MORAIS & ADVOGADOS para deliberada ou inadvertidamente propagar qualquer tipo vírus, worms, cavalos de troia, spam, ou programas de controle remoto de outros computadores;
l) Não serão permitidos os acessos a softwares peer-to-peer (Kazaa, BitTorrent, utorrent e afins);
m) Não serão permitidos os acessos a sites de compartilhamento de arquivos, tais como: mega, uploaded, bitshare, depositfiles, etc;
n) Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos e estratégias de bypass de firewall;

o) Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego (Sniffers), ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar auditorias de segurança;
p) Os arquivos do MORAIS & ADVOGADOS, obrigatoriamente, deverão ser armazenados na pasta compartilhada de cada setor, localizada no servidor de arquivos, para a garantia de backup destes documentos. É terminantemente proibido armazenar estes tipos de arquivos em equipamentos pessoais;
q) Não será permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro.

XVI. DA POLÍTICA DO USO DE SENHA:

Ficou estabelecido que a senha é o método mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra. O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 - falsa identidade). Assim, com o objetivo de orientar a criação de senhas seguras, define-se as seguintes regras:

a) A senha é de responsabilidade pessoal, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma, ser imediatamente alterada, no caso de suspeita de sua divulgação;
b) A senha inicial só será fornecida à pessoa durante a sua integração na organização. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador;
c) É proibido o compartilhamento de login para funções de administração de sistemas;
d) As senhas não devem ser anotadas e deixadas próximo ao computador, como por exemplo, embaixo do teclado, colada nos monitores, etc.);
e) Sugere-se, que sigam os seguintes pré-requisitos:
    (i) Senha com número mínimo de 08 (oito) caracteres;
    (ii) Caracteres com pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais;
    (iii) As senhas não devem ser baseadas em informações pessoais de fácil dedução, tais como, data de aniversário, nome do cônjuge, etc);
f) O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:
    I. Desligamento do Colaborador;
    II. Mudança de função do Colaborador;

III. Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.

XVII. DO USO DO E-MAIL:

O e-mail é um dos principais meios de comunicação. No entanto, é, também, uma das principais vias de disseminação de malwares, por isso, urge a necessidade de normatização da utilização deste recurso, assim:

a) O e-mail corporativo é destinado para fins profissionais, relacionados às atividades dos empregados; Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem esta Política;
b) É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo "corrente", campanhas ou promoções;
c) É proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;
d) É proibido enviar qualquer mensagem por meios eletrônicos que torne a MORAIS E ADVOGADOS vulnerável a ações civis ou criminais;
e) É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
f) Proibido produzir, transmitir ou divulgar mensagem que:
    (i) contenha ameaças eletrônicas, como: spam, phishing, mail bombing, malwares;
    (ii) contenha arquivos com código executável (.exe, cmd, pif, js, .hta, src, cpl, reg, dl, .inf) ou qualquer outra extensão que represente um risco à segurança;
    (iii) vise obter acesso não autorizado a outro computador, servidor ou rede;
    (iv) vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

XVIII. DO USO DE ESTAÇÕES DE TRABALHO:

As estações de trabalho devem permanecer disponíveis e operáveis durante o maior tempo possível para que os empregados não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas, são elas:

a) É vedada a abertura de computadores para qualquer tipo de reparo pelos empregados. Caso seja necessário, o reparo deverá ser feito pela equipe de TI;

b) É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe de TI;
c) É proibida a instalação de softwares que não possuam licença;
d) As estações de trabalho devem permanecer bloqueadas (logoff) nos períodos de ausência do Colaborador;
e) Os documentos e arquivos relativos à atividade desempenhada pelo empregado deverão, sempre que possível, serem armazenados em local próprio no servidor de arquivo da rede, o qual possui rotinas de backup e controle de acesso adequado;
f) É proibido o uso de estações de trabalho para:

    (i) tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
    (ii) burlar quaisquer sistemas de segurança;
    interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    (iii) cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
    (iv) hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;

g) É proibido o uso dos notebooks corporativos para fins de lazer, a exemplo de: Jogos ou entretenimento em sites não confiáveis, downloads de filmes, músicas etc;
h) Os acessos aos sistemas e recursos de redes, utilizando os notebooks corporativos, poderá ser realizado por meio de VPN, para garantia da segurança da rede corporativa;
i) Deve-se evitar o acesso a redes WI-FI públicas, não seguras, em qualquer lugar ou estabelecimento.

XIX. DO TRABALHO EM HOME OFFICE – TELETRABALHO:

Em caso de teletrabalho, os colaboradores, gestores e administradores deverão observar todas as orientações de segurança para realizar o acesso remoto aos sistemas e as informações do MORAIS & ADVOGADOS, em especial, observar as questões abaixo:

a) O equipamento eventualmente disponibilizado pela MORAIS E ADVOGADOS deverá ser de uso exclusivo do Colaborador, sendo expressamente vedado o acesso à terceiros;
b) É expressamente proibido o compartilhamento à terceiros, fora do domínio da organização, dos dados pessoais que o colaborador eventualmente tenha acesso, exceto com a expressa anuência da organização;

c) Sugere-se que o empregado evite a impressão de documentos onde contenham dados pessoais, a fim de evitar a circulação e o acesso indevido por terceiros;
d) É proibida a impressão de documentos que contenham dados pessoais por meio de impressoras públicas de locais (gráficas, lan houses, loja de impressão e similares);
e) Caso sejam impressos documentos com dados pessoais, os mesmos deverão ser devidamente descartados após o uso, conforme orientações do Empregador;
f) É proibido o acesso do notebook do Empregado com algum Wi-Fi público não seguro, seja em qualquer lugar;
g) O acesso aos sistemas da organização deve preferencialmente ser através de software de VPN (Virtual Private Network), que, devidamente configurado, estabelece uma conexão direta com o servidor da organização, de forma privativa e segura, sem o uso da internet pública.

O escritório MORAIS & ADVOGADOS poderá implementar outros mecanismos de controle de segurança e de vulnerabilidades nos equipamentos que serão utilizados pelo colaborador, a fim de assegurar o cumprimento das regras estabelecidas na Lei Geral de Proteção de Dados.

XX. DO USO DE EQUIPAMENTOS PESSOAIS E DISPOSITIVOS MÓVEIS:

O objetivo do MORAIS & ADVOGADOS é maximizar a agilidade e a eficiência na realização das atividades e tarefas dos colaboradores contando com todos os recursos de equipamentos disponíveis. Mas, não pode deixar de considerar os requisitos de segurança da informação. Por isso, estabelece algumas regras para o uso de equipamentos de propriedade particular e de dispositivos móveis. Estas regras serão especialmente fiscalizadas pela área de TIC do MORAIS & ADVOGADOS.

Caracteriza-se por dispositivo móvel qualquer equipamento eletrônico com atribuições de mobilidade, seja de propriedade do MORAIS & ADVOGADOS ou particular como: notebooks, smartphones, HD's Externos e pendrives.

Todas as regras do tópico "Estações de Trabalho" se enquadram nesta seção, acrescentando-se:
a) Fica autorizado o uso de notebooks e dispositivos móveis para acesso à rede interna da MORAIS E ADVOGADOS mediante autorização do líder imediato e prévio cadastro e liberação da TIC;
b) A TIC deverá verificar as configurações de rede, do aplicativo de antivírus e demais aplicativos instalados para que o acesso à rede interna seja concedido. Aplicativos peer to peer, farejadores de tráfego, softwares que possam gerar carga excessiva na rede, que

não estejam de acordo com a legislação vigente ou que possam trazer prejuízos à infraestrutura ou à imagem do MORAIS & ADVOGADOS não serão permitidos. Caso o equipamento não obedeça aos requisitos mínimos de segurança, o acesso não será concedido;

c) A TIC tem o direito de, periodicamente, auditar os equipamentos utilizados no MORAIS & ADVOGADOS, visando proteger suas informações bem como garantir que aplicativos ilegais não estejam sendo usados no MORAIS & ADVOGADOS;
d) É de responsabilidade do proprietário a instalação do Sistema Operacional que será utilizado, bem como dos aplicativos a serem utilizados no notebook e smartphone, salvo exceções de aplicativos específicos autorizados pela TIC;
e) É de responsabilidade do proprietário usar somente aplicativos legalizados em seu notebook e smartphone;
f) Não podem ser executados nos notebooks aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede, acesso a informações sem a devida permissão ou informações confidenciais;
g) É proibido o armazenamento de informações que não sejam de uso pessoal do proprietário do notebook. Todos os arquivos que pertençam a MORAIS E ADVOGADOS não podem ser armazenados no disco rígido do notebook ou em dispositivos de armazenamento móvel (ex: pendrive e HD Externo. Estes arquivos devem sempre ser armazenados no servidor de arquivos de compartilhamento destinado para tal;
h) Mesmo nos computadores portáteis fornecidos pelo MORAIS & ADVOGADOS, é proibido o armazenamento de informações confidenciais e confidenciais restritas no disco rígido do equipamento.

XXI. DO USO DE IMPRESSORAS CORPORATIVAS:

O uso de impressoras no MORAIS & ADVOGADOS deve seguir algumas regras conforme abaixo:

a) É proibida a impressão de documentos de cunho pessoal e/ou ilegal;
b) A configuração e manutenção das impressoras só podem ser realizadas pela equipe técnica da Tl e/ou parceiro do outsourcing de impressão;
c) A instalação das impressoras deverá ser realizada através do servidor de impressão pela equipe de TIC.

XXII. DA POLÍTICA DE BACKUP:

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança). Uma organização tem que estar preparada para recuperar (restaurar) todos

os seus dados de forma íntegra caso um incidente ou problema de perda de dados venha a ocorrer.

Assim, estabelecem-se as regras:

a) Todo sistema ou informação relevante para a operação dos negócios do MORAIS & ADVOGADOS deve possuir cópia dos seus dados de produção para que, em eventual incidente ou problema de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição;
b) Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, períodos de pouco ou nenhum acesso de usuários;
c) As mídias de backup devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo, segundo as normas da ABNT) e, preferencialmente, distantes o máximo possível do Datacenter;
d) Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento;
e) A TIC deve preparar semestralmente um plano para execução de testes de restauração de dados, que deve ter escopo definido em conjunto com as áreas de negócio. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos;
f) Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser executados apenas mediante justificativa de necessidade.

XXIII. DA VIOLAÇÃO DA POLÍTICA:

1. Das Disposições Gerais:

As penalidades em caso de violação da presente Política aplicar-se-ão a todos os colaboradores, gestores e administradores do MORAIS & ADVOGADOS, sendo que, todos possuem o compromisso de informar qualquer irregularidade ou descumprimento das normas de segurança.

A presente Política será disponibilizada nos canais de comunicação internos do MORAIS & ADVOGADOS, sendo obrigatória a assinatura por todos empregados, gestores e administradores do TERMO CIÊNCIA E COMPROMISSO DE CUMPRIMENTO DA POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS (ANEXO I).

Para eventuais denúncias ou quaisquer assuntos relativos às possíveis violações desta e de qualquer outra Política, o informante deverá contatar pelo Canal de Denúncia contato@moraiseadvogados.adv.br o qual avaliará os fatos narrados, fazendo uma classificação das violações operadas, seguindo o fluxo abaixo:
Recebida a denúncia ou Identificada a Violação:

- Análise do Caso e identificação dos dados afetados

Caso envolva dados pessoais (**o DPO analisará o caso, conforme critérios abaixo, e sugere aplicação de medidas disciplinares**.)

Caso não envolva dados Pessoais (**DPO deve reportar o incidente à Alta Direção**.)

2. Da Aplicação Das Penalidades:

O DPO e o Comitê de Privacidade do MORAIS & ADVOGADOS, conforme fluxo acima, assim que cientificados da violação às Políticas deverão tomar providências cabíveis (em especial a aplicação das penalidades desta Política), avaliando o incidente de forma individual, aplicando as sanções com bom senso e discernimento, considerando os seguintes critérios:

a) Quais pessoas estão envolvidas no evento;
b) Qual a classificação do risco envolvido no descumprimento da Política pelo empregado ou administradores (BAIXO, MEDIO OU ALTO);
c) Qual o impacto gerado pelo descumprimento;
d) Qual a quantidade, natureza e classificação dos dados pessoais impactados;
e) Qual era intenção das pessoas envolvidas;
f) Se as pessoas envolvidas receberam treinamento;
g) Se é reincidente do descumprimento da Política.

Para análise dos critérios acima, o DPO ou o Comitê deverão investigar o ocorrido, incluindo, mas não se limitando a:

a) analisar as evidências e provas que demonstram o descumprimento;
b) realizar oitiva das pessoas envolvidas (quando necessário);
c) coletar informações sobre o investigado junto ao Gestor da área responsável.

O DPO e/ou o Comitê emitirão um Relatório com os critérios acima avaliados, incluindo como anexo todas as evidências que comprovam o descumprimento da Política.

Com base nestes critérios o Comitê ou DPO deliberará acerca da gravidade da violação, classificando-a como baixa, média ou alta, podendo ser aplicado as seguintes medidas disciplinares:

a) Advertência (verbal e formal);
b) Treinamento;
c) Suspensão;
d) Demissão (com ou sem justa causa);
e) Outras providências jurídicas.

As medidas disciplinares serão indicadas pelo Comitê ou pelo DPO, mediante envio de e-mail para a Alta Direção, para que tome as providências conforme abaixo:

3. Da Advertência Verbal:

a) O empregado será comunicado verbalmente que está infringindo uma das normas o treinamento.
b) O gestor imediato do empregado realizará o registro da aplicação da advertência empregado, a data e a descrição do incidente.
c) O Comitê ou o DPO avaliarão os casos em que será necessário o colaborador refazer o treinamento, definindo qual será o formato, duração e conteúdo a ser abordado.

4. Da Advertência Escrita:

A primeira notificação será enviada pelo DPO ou Comitê, ao gestor imediato do Colaborador, informando o descumprimento da norma, com a indicação precisa da violação cometida, o qual coletará a assinatura confirmando o recebimento pelo colaborador.

Em caso de negativa de assinatura, o Gestor aplicará a advertência na presença de 02 (duas) testemunhas, coletando a assinatura destas.

a) A segunda notificação seguirá o mesmo procedimento acima;
b) O Comitê ou DPO avaliarão os casos em que será obrigatório refazer o treinamento de segurança da informação.

Imediatamente após a aplicação da advertência, o Gestor deverá entregar a notificação original assinada ao Comitê ou DPO.

5. **Da Suspensão:**

A suspensão será aplicada pelo gestor imediato de acordo com o prazo definido pelo Comitê ou DPO.

a) O Comitê ou o DPO avaliarão os casos em que será obrigatório refazer o treinamento;
b) Após aplicação da medida disciplinar, será realizado o registro da suspensão em sistema próprio, contendo as seguintes informações: a identificação do empregado, a data e a descrição do incidente.

6. Da Demissão Sem Justa Causa:

A demissão será aplicada pelo gestor imediato, seguindo todo o procedimento para realizar o desligamento do empregado.

Para aplicação desta penalidade o MORAIS & ADVOGADOS deverá manter as evidências que demonstram o descumprimento da Política de Privacidade e Proteção de Dados Pessoais.

7. **Da Demissão Por Justa Causa**:

A demissão será aplicada pelo gestor imediato, seguindo todo o procedimento para realizar o desligamento do empregado.
Para aplicação desta penalidade a MORAIS E ADVOGADOS deverá manter as evidências que demonstram o descumprimento da Política de Privacidade e Proteção de Dados Pessoais.

8. **Das Outras Medidas Jurídicas:**

A aplicação das penalidades acima não limita a possibilidade do MORAIS & ADVOGADOS tomar outras medidas judiciais e administrativas cabíveis, no que tange responsabilização criminal e ressarcimento dos prejuízos suportados pelo MORAIS & ADVOGADOS em razão do ato cometido pelos colaboradores e administradores, de acordo com a gravidade da violação.

9. **Da Violação Por Terceiros (Fornecedores)**:

Quando o descumprimento for oriundo de terceiros, as penalidades estarão previstas nos contratos mantidos com os fornecedores, cabendo ao Comitê ou DPO avaliar os riscos e a sugestão de rescisão do contrato.

XXIV. DAS CONSIDERAÇÕES FINAIS:

As dúvidas decorrentes de fatos não descritos nesta Política de Privacidade e Proteção de Dados Pessoais deverão ser encaminhadas ao Comitê de Privacidade e/ou DPO.

Esta Política entra em vigor a partir da data de publicação, e pode ser alterada a qualquer tempo, por decisão do Comitê ou Alta Direção, mediante a ocorrência de fatos relevantes que apareçam ou não tenham sido contemplados neste documento.

ANEXO I
TERMO DE CIÊNCIA E COMPROMISSO DE CUMPRIMENTO DA POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS

NOME:
CPF:
E-MAIL:
CARGO:
MATRÍCULA:
SETOR:
TELEFONE:

Declaro que tive acesso a Política de Privacidade e Proteção de Dados Pessoais e me comprometo a executar minhas tarefas de forma a cumprir com as orientações das referidas políticas, bem como quaisquer outras normas e instruções de trabalho disponibilizadas pelo MORAIS & ADVOGADOS.

Comprometo-me a:

a. Utilizar adequadamente os equipamentos de organização, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações.

b. Não revelar, fora do âmbito profissional, fatos ou informações de qualquer natureza que tenha conhecimento devido as minhas atribuições;

c. Acessar as informações somente por necessidade de serviço e por determinação expressa do líder imediato;

d. Manter cautela quanto à exibição de informações sigilosas e confidenciais, em tela de impressoras ou outros meios eletrônicos;

e. Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade de minha senha;

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação de sanções disciplinares cabíveis.

Salvador, Ba ___ de _____ de _____.

_____
NOME DO COLABORADOR