



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS

Este documento consiste na Política de Segurança da Informação e Privacidade de Dados da Cerizze Sociedade de Advogados, doravante denominada Cerizze, estabelecendo diretrizes para a proteção de ativos e prevenção de responsabilidades.

Cumprе ressaltar que este documento deve ser interpretado em conformidade com qualquer outro documento, contrato ou cláusula de privacidade que o acompanhe, sem prejuízo do sigilo profissional aplicável no relacionamento da Cerizze com seus clientes, observando o Código de Ética e Disciplina da Ordem dos Advogados do Brasil, bem como o Código de Ética da Cerizze.

I - INTRODUÇÃO

A Segurança da Informação deve abranger três propriedades: confidencialidade, integridade e disponibilidade. A **confidencialidade** é a propriedade que estabelece que a informação seja acessível apenas para pessoas autorizadas; a **integridade** implica na preservação da originalidade e confiabilidade, a fim de que a informação mantenha sua consistência e não seja modificada ou eliminada sem autorização; a **disponibilidade** requer que a informação esteja sempre acessível para o uso de pessoas autorizadas, de maneira fluida, segura e eficiente.

A Privacidade de Dados tem como objetivo o tratamento de dados pessoais, observando-se a finalidade almejada, as bases legais, as formas de acesso, coleta, retificação, exclusão, revogação de consentimento, oposição e compartilhamento, em conformidade com a legislação aplicável no Brasil, notadamente a Lei Geral de Proteção de Dados.

Dessa forma, suas diretrizes alcançam os sócios, parceiros, funcionários, estagiários ou qualquer pessoa que, eventualmente, venha a ter ciência ou acesso a dados e informações confidenciais, bem como a sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Cerizze.

Entende-se que houve violação desta Política de Segurança da Informação e Privacidade de Dados quando se verificar:

- Exposição da Cerizze a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança de dados e/ou informações;
- Divulgação ou revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados pessoais ou corporativos, pertencentes a clientes, efetivos ou em potencial, ou à Cerizze;
- Uso de dados para propósitos ilícitos ou em desconformidade com o previamente autorizado pelos clientes, efetivos ou em potencial.



II - OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS

A Política de Segurança da Informação e Privacidade de Dados tem como objetivo estabelecer normas, diretrizes e procedimentos a serem adotados a fim de assegurar a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade de dados e informações pertencentes à Cerizze ou que estejam sob sua guarda.

III - CLASSIFICAÇÃO DA INFORMAÇÃO

Cada setor (empresarial, tributário, trabalhista, societário, administrativo) deve fixar os critérios relativos ao nível de confidencialidade da informação gerada sob sua supervisão ou que lhe seja confiada por cliente, efetivo ou em potencial, de acordo com a classificação abaixo:

1 – Pública: informação que pode ser acessada por usuários da rede do Escritório de Advocacia, clientes, parceiros, prestadores de serviços e público em geral. São exemplos de informação pública: artigos e notícias divulgados no sítio eletrônico da Cerizze, o quadro de sócios e funcionários que compõem a banca.

2 – Interna: informação que só pode ser acessada por sócios e funcionários da Cerizze. Tratam-se de informações utilizadas em tarefas rotineiras e que não se destinam ao uso do público externo. São exemplos de informação interna: políticas e procedimentos internos, e-mails e ramais telefônicos, avisos.

3 – Confidencial: informação que pode ser acessada por usuários da rede da Cerizze. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da Cerizze ou ao negócio do cliente. São exemplos de informação confidencial: processos judiciais, pareceres jurídicos, instrumentos contratuais.

4 – Confidencial restrita: informação que pode ser acessada somente por usuários da rede da Cerizze, explicitamente indicado pelo nome ou por setor a que pertence (empresarial, tributário, trabalhista, societário, administrativo). Todos os integrantes da Cerizze são orientados a não circular informações e/ou mídias consideradas confidenciais e/ou restritas, assim como não deixar relatórios nas impressoras e mídias em locais de fácil acesso. São exemplos de informações confidenciais restritas: resultado de auditorias internas, documentos de clientes, estratégias de negócio.

IV - DADOS E TRATAMENTO

Em consonância com a Lei Geral de Proteção de Dados, dados pessoais são as informações relacionadas a pessoas naturais, identificada ou identificável. Considera-se dado pessoal



sensível, dentre outros, o dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde, dado genético ou biométrico.

Tratamento é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O Tratamento de Dados Pessoais poderá ser realizado pela Cerizze, mediante consentimento prévio e por escrito, ou em virtude de outra base legal, com a finalidade de viabilizar a prestação dos serviços jurídicos para os quais foi contratada, bem como para:

- Identificar e/ou oferecer conteúdo relevante, incluindo, mas não se limitando a pílulas, *newsletter*, eventos, convites, lembretes;
- Compor o banco de dados de fornecedores, prestadores de serviço, parceiros, candidatos a vagas de emprego e estágio da Cerizze, a depender do caso;
- Cumprimento da legislação aplicável.

Deverá ser observada a boa-fé e os seguintes princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

IV.1 - DADOS DE FUNCIONÁRIOS E SÓCIOS

A Cerizze se compromete em não acumular ou manter intencionalmente dados pessoais dos sócios e funcionários, além daqueles relevantes na condução do negócio, os quais não serão utilizados para fins diversos daqueles para os quais foram coletados. Todos os dados pessoais que porventura sejam armazenados serão classificados como confidenciais.

Os dados pessoais não serão transferidos para terceiros, exceto quando exigido por lei ou quando essencial para o desenvolvimento do negócio, desde que as partes firmem cláusula de confidencialidade.

IV.2 - INCLUSÃO OU EXCLUSÃO DE SÓCIOS/ FUNCIONÁRIOS/ ESTAGIÁRIOS

A inclusão/exclusão de sócios e a admissão/demissão de funcionários ou estagiários deverá ser imediatamente informada ao setor administrativo, a fim de que possam ser cadastrados ou excluídos no sistema da Cerizze, notadamente com relação ao registro de usuário e fornecimento de senha para acesso à rede interna, ao *e-mail* corporativo e demais sistemas que sejam utilizados por estes.

Cabe ao setor solicitante da contratação a comunicação ao setor administrativo sobre as pastas eletrônicas e informações a que o novo sócio/ funcionário/ estagiário terá direito de acesso. Em se tratando de estagiário, deverá ser informado o período máximo da



contratação, em consonância com as determinações da Instituição de Ensino a que esteja vinculado.

O responsável pelo setor administrativo dará conhecimento e obterá as devidas assinaturas de concordância do novo sócio/ funcionário/ estagiário em relação à Política de Segurança da Informação e Privacidade de Dados da Cerizze, que é requisito para seja concluída a inclusão ou admissão.

IV.3 - DADOS PESSOAIS DE CLIENTES E TERCEIROS

Em se tratando de dados pessoais de clientes, efetivos ou em potencial, bem como de pessoas a eles relacionadas, a coleta ocorrerá mediante solicitação da Cerizze, formalizada por escrito, em cláusula destacada das demais cláusulas contratuais, acompanhada de justificativa e motivação, com indicação de finalidade determinada.

A título exemplificativo, consideram-se dados pessoais de terceiros: *e-mail*, documento de identidade, endereço, certidão de casamento, dados relativos à saúde.

O consentimento pode ser revogado a qualquer tempo, mediante manifestação expressa do titular, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado.

A Cerizze também poderá realizar o tratamento de dados para as finalidades previstas nos incisos II, V, VI e X do art. 7º da LGPD.

IV.4 - PRAZO DE ARMAZENAMENTO, ALTERAÇÃO E REMOÇÃO DE DADOS

O armazenamento de dados perdurará pelo período necessário para a prestação de serviços advocatícios, conforme contratado entre as partes, e pelo prazo determinado na legislação em vigor, principalmente em se observando os prazos de decadência e prescrição e a necessidade de cumprimento de obrigação legal ou regulatória.

Enquanto estiver no banco de dados da Cerizze, o cliente ou o terceiro interessado poderá solicitar a remoção, alteração ou exclusão dos dados pessoais, pelo e-mail corporativo: contato@cerizze.com. O retorno e a adoção das medidas necessárias ocorrerá em prazo razoável, segundo a viabilidade técnica e operacional da Cerizze.

V - RESPONSABILIDADES

- 1- Será de inteira responsabilidade dos sócios, funcionários, parceiros e colaboradores:
 - Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação e Privacidade de Dados da Cerizze;
 - Adotar postura exemplar em relação à segurança da informação e de dados;



- Consultar o Encarregado de Dados para esclarecimentos de dúvidas referentes à presente Política de Segurança da Informação e Privacidade de Dados;
- Proteger as informações contra acesso, divulgação, modificação ou destruição não autorizados pela Cerizze;
- Garantir que equipamentos e recursos tecnológicos sejam utilizados apenas para as finalidades aprovadas pela Cerizze;
- Devolução ao cliente ou descarte adequado de documentos, em conformidade com seu grau de classificação e as implicações da legislação vigente;
- Informar sobre novas contratações ou adequações no quadro societário;
- Classificar e reclassificar as informações sempre que necessário;

2- Será de inteira responsabilidade do setor administrativo, atuando em conjunto com a área de informática:

- Exigir de sócios, funcionários, parceiros e colaboradores a assinatura de termo de confidencialidade com relação às informações e aos dados a que terão acesso;
- Avaliar incidentes e descumprimentos, propondo ações corretivas;
- Definir regras para a instalação de *software* e *hardware*;
- Homologar os equipamentos pessoais (*smartphones* e *notebooks*) para acesso a wi-fi, e-mail institucional e documentos da rede interna;
- Monitorar os acessos às informações e aos ativos da Cerizze, em conformidade com a Política de Segurança da Informação e Privacidade de Dados.

3 – Será de inteira responsabilidade dos Sócios de Capital:

- Aprovar a Política de Segurança da Informação e suas atualizações;
- Aprovar investimentos relacionados à segurança da informação.

VI - ESTAÇÕES DE TRABALHO

As estações de trabalho devem permanecer operáveis, adotando-se algumas medidas de segurança. Por exemplo, devem permanecer bloqueadas (*logoff*) nos períodos de ausência do usuário.

Os documentos e os arquivos que têm relação com a atividade desempenhada pelo colaborador deverão ser armazenados em local próprio, no servidor da rede interna da Cerizze, que possui rotinas de *backup* e controle de acesso. Em especial, os documentos



críticos e confidenciais somente deverão ser armazenados no servidor da rede, nunca no disco local da máquina dos usuários.

Os documentos e os arquivos físicos de clientes deverão ser digitalizados, armazenados no servidor da rede interna da Cerizze e devolvidos, mediante protocolo de entrega, ou destinados para a finalidade para a qual foram entregues ou ainda descartados, em conformidade com sua natureza, seu grau de classificação e as implicações da legislação vigente. Os documentos que devam permanecer no Escritório, em via física, deverão ser armazenados em local próprio, sempre observando a política do *clean desk* (mesa limpa).

VII - PROGRAMAS ILEGAIS

A Cerizze respeita os direitos de propriedade intelectual inerentes aos programas que utiliza e reconhece que deve pagar o justo valor por eles, sendo terminantemente proibido o uso de programas ilegais ou sem prévio licenciamento ou autorização na Cerizze.

Os usuários não podem, em hipótese alguma, instalar *software* não autorizado nos equipamentos pertencentes à Cerizze ou nos equipamentos pessoais que sejam conectados à rede da Cerizze. Caso o sócio ou funcionário utilize computador ou outro equipamento pessoal para acessar a rede interna da Cerizze ou o *e-mail* corporativo, deverá respeitar as precauções determinadas pelo setor de informática, notadamente com relação à instalação de programa antivírus avançado.

Periodicamente, a área de informática verificará a conformidade dos computadores e outros equipamentos pessoais utilizados pelos sócios/ funcionários/ estagiários, visando garantir a correta aplicação desta diretriz.

O descumprimento implicará na responsabilização do usuário perante a Cerizze, por quaisquer problemas ou prejuízos ocasionados, sujeitando-se às sanções previstas neste documento, sem prejuízo da adoção das medidas judiciais cabíveis.

VIII - PERMISSÕES E SENHAS

O acesso à rede interna do Escritório de Advocacia requer o prévio cadastro de usuário e senha, pessoais e intransferíveis, junto ao setor administrativo.

Havendo necessidade de cadastramento de novo usuário para utilização da rede, sistemas ou equipamentos de informática da Cerizze, o setor que efetuou a contratação deverá comunicar esta necessidade ao setor administrativo, via e-mail, informando as pastas e os programas a que o novo usuário terá direito de acesso e quais serão restritos.

A área de informática efetuará o cadastramento e informará ao novo usuário qual será a sua primeira senha, que deverá ser, obrigatoriamente, alterada logo após o primeiro *login*. A



área de informática recomenda que as senhas tenham um critério mínimo de segurança para que não sejam facilmente copiadas e não possam ser repetidas.

Todos os usuários responsáveis pela aprovação eletrônica de documentos deverão comunicar ao setor administrativo qual será seu substituto em caso de ausência, para que as permissões possam ser alteradas.

O acesso do usuário deverá ser imediatamente cancelado em caso de desligamento, mudança de setor ou quando, por qualquer razão, cessar a necessidade de acesso ao sistema ou à informação.

Usuários externos somente terão acesso à rede visitantes, que permite conexão à internet. Jamais terão acesso à rede interna da Cerizze.

IX - COMPARTILHAMENTO DE DADOS

O compartilhamento de pastas na rede interna do Escritório de Advocacia será possível através da pasta “Público”, cujo acesso é permitido a todos os sócios e funcionários da Cerizze, desde que não envolva documento classificado como de acesso confidencial restrito.

Esse compartilhamento perdurará por, no máximo, 24 (vinte quatro) horas, de modo que, não havendo exclusão pelo próprio usuário, o responsável pelo setor administrativo excluirá, diariamente, todos os documentos inseridos na pasta “público”.

Com relação ao compartilhamento externo de dados, somente será permitido nos limites do o estritamente necessário para cumprir adequadamente as finalidades enumeradas no Contrato de Prestação de Serviços Advocatícios, assim como em virtude de ordem judicial ou decisão de qualquer outra autoridade competente, segundo legislação aplicável.

X - BACKUP

Todos os dados da Cerizze deverão ser protegidos através de rotinas sistemáticas de *backup* em mídias removíveis e soluções em nuvem. As mídias removíveis serão protegidas por controles de segurança para evitar que pessoas não autorizadas tenham acesso aos dados e serão armazenadas em local seguro, fora do prédio da Cerizze, em local seco, climatizado e seguro.

Deverá haver, permanentemente, um conjunto completo de *backup* capaz de restaurar todos os dados da Cerizze em caso de sinistro. Em eventual incidente de indisponibilidade, deve ser possível a recuperação ou minimização dos impactos nas operações negociais. Dessa forma, o conjunto de *backup* armazenado externamente deverá se submeter a rodízio semanal com um dos conjuntos de *backup* ativo.



A validação mensal deverá ser realizada pelo setor de informática, voltando-se parte ou todo o conteúdo do *backup* em um HD previamente definido para esse fim.

XI - SEGURANÇA E INTEGRIDADE DOS DADOS

A Cerizze adota medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

O gerenciamento do banco de dados é responsabilidade exclusiva do setor administrativo, conjuntamente com a área de informática, assim como a manutenção, alteração e atualização de equipamentos e programas.

XII - E-MAIL INSTITUCIONAL

O correio eletrônico fornecido pela Cerizze é instrumento de comunicação interna e externa que deve ser utilizado na prestação de serviços advocatícios e atividades correlatas.

Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear *spams*, *malwares* ou outros conteúdos que violem esta Política. Também é proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas.

As mensagens devem ser escritas em linguagem profissional e conter assinatura institucional com o *design* desenvolvido pela Cerizze.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem e/ou anexo enviados pelo seu endereço, sendo terminantemente proibido o envio de mensagens que contenham declarações difamatórias e linguagem ofensiva; possam trazer prejuízos a outras pessoas; possam prejudicar a imagem da Cerizze; possam prejudicar a imagem de clientes ou outras empresas parceiras; tenham fim ou conteúdo ilícito; sejam incoerentes com a missão, a visão e os valores da Cerizze.

A inclusão de um novo usuário no correio eletrônico deverá ser solicitada junto ao setor administrativo, que encaminhará o pedido formal ao Setor de Informática.

Não será permitido o uso de *e-mail* gratuito nos computadores da Cerizze ou nos computadores pessoais conectados à rede interna da Cerizze. O Setor de Informática poderá, visando evitar a entrada de vírus, bloquear o recebimento de *e-mail* proveniente de sites gratuitos.



XIII - NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS

O setor administrativo é responsável pela aplicação da Política de Segurança da Informação da Cerizze em relação a definição de compra e substituição de *software* e *hardware*.

XIV - SISTEMAS DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da Cerizze, assim como o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do setor administrativo.

XV - USO DE ANTIVÍRUS E FIREWALL

Todo arquivo em mídia proveniente de entidade externa ou da Internet deve ser verificado por programa antivírus, instalado em todas as estações de trabalho, com atualizações periódicas. O usuário não poderá, em hipótese alguma, desabilitar o programa antivírus instalado em sua máquina, ainda que seja pessoal.

Todos os hardwares de propriedade da Cerizze ou conectados em sua rede interna terão o Firewall Guardião instalados e periodicamente atualizados.

XVI - PENALIDADES

O não cumprimento desta Política de Segurança da Informação e Privacidade de Dados implica em falta grave e poderá resultar nas seguintes penalidades: advertência verbal, advertência formal, exclusão do quadro societário ou desligamento, sem prejuízo da adoção das medidas judiciais cabíveis.

XVII - ENCARREGADO DE DADOS

O gestor responsável pela contradoria da Cerizze é nomeado o Encarregado de Dados.

XVIII - VIGÊNCIA

Essa Política entra em vigor em 1º de julho de 2020, podendo ser revisada periodicamente.