POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS

CAPÍTULO I – DISPOSIÇÕES GERAIS

Objetivo

Art. 1º. Esta política tem por objetivo organizar o tratamento de dados no âmbito do ICL, visando preservar dados e demais informações quanto à confidencialidade, integridade, disponibilidade e autenticidade, com o propósito de viabilizar a concepção de modelo de governança de dados, bem como assegurar conformidade à legislação de proteção de dados pessoais, com base nos seguintes eixos:

(a) Estabelecimento de diretrizes para disponibilização, controle e uso de recursos de informação, serviços de redes de dados, Internet, telecomunicações e correio eletrônico institucional e definição de regras relativas à Segurança da Informação;

(b) Definição de diretrizes e orientações necessárias para a manutenção da privacidade e proteção dos dados pessoais controlados ou tratados pelo ICL, englobando os principais aspectos da legislação nacional de proteção de dados, os direitos dos titulares de dados pessoais e a forma como tais direitos podem ser exercidos.

Âmbito de aplicação

Art. 2º. Esta Política de Segurança da Informação e Proteção de Dados Pessoais e suas normas complementares abrangem todas as atividades do ICL, incluindo as executadas por seus colaboradores, consultores externos, prestadores de serviço e a quem, de qualquer forma, meio ou suporte, seja afetado ou participe das atividades do ICL.

I - Os princípios e diretrizes gerais desta Política de Segurança da Informação e Proteção de Dados Pessoais também se aplicam às entidades vinculadas ao ICL e a quaisquer relacionamentos com outros órgãos e entidades públicos ou privados, especialmente no que se refere aos dados pessoais.

II - Esta Política de Segurança da Informação e Proteção de Dados Pessoais, suas normas complementares e procedimentos específicos são obrigatórios para todos os usuários, independentemente do tipo de vínculo, nível hierárquico ou função.

III - Cada interessado será devidamente comunicado sobre o teor desta política

Conceitos

Art. 3º. Para os fins desta Política de Segurança da Informação e Proteção de Dados Pessoais, considera-se:

I - *Dados pessoais*: Qualquer informação relacionada a pessoa natural identificada ou identificável;

II - *Dados pessoais sensíveis*: Qualquer dado pessoal que, de alguma maneira, possa gerar discriminação, tais como dados relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, ou, ainda, aqueles referentes à saúde, vida sexual ou informações genéticas e biométricas.

III - *Dado anonimizado*: Dado relativo a qualquer titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - *Dados pessoais utilizados pelo ICL*: Dados pessoais coletados pelo ICL ou de alguma forma submetidos ao seu tratamento, sempre e exclusivamente dentro das hipóteses previstas na legislação. São exemplos de dados pessoais coletados pelo ICL aqueles obtidos em razão da formalização de vínculo empregatício, contratação de consultores externos ou designação de membros para integrar o Conselho Deliberativo e os órgãos internos de fiscalização e controle;

V - *Controlador*: Detentor e responsável pela tomada de decisões referentes ao tratamento de dados pessoais coletados, podendo ser o próprio ICL ou terceiro, que eventualmente venha a compartilhar dados pessoais para tratamento pelo ICL;

VI - *Operador*: Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do ICL;

VII - *Encarregado de dados*: Pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD);

VIII - *Titular de dado pessoal*: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

IX - *Cookies:* Arquivos de dados que são armazenados em dispositivos utilizados ao acessar e navegar em páginas de Internet ou aplicativos, sendo utilizados para viabilizar o funcionamento da página de Internet ou aplicativo (*cookie* essencial); ajudar a aferir o desempenho da página de Internet ou aplicativo (*cookie* de desempenho); melhorar a experiência (*cookie* de funcionalidade); prover publicidade (*cookie* de publicidade); permitir compartilhamento de conteúdo em mídias sociais (*cookie* de mídia social); dentre outros.

X - *Segurança da Informação*: É a proteção dos dados e das informações contra ameaças, com o objetivo de garantir sua confidencialidade, integridade, disponibilidade e autenticidade, preservando a manutenção de suas características contra danos que possam comprometer a entidade ou gerar perdas;

XI - *Sistema de informações*: Todo tratamento sistemático de informações e de dados, inclusive dados pessoais, em meio físico e/ou eletrônico, como os 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.

Princípios

Art. 4º. São princípios aplicáveis a esta Política de Segurança da Informação e Proteção de Dados Pessoais:

Confidencialidade

I - As informações e dados do ICL, quando não forem expressamente classificadas, são presumidamente confidenciais e não poderão ser fornecidas para terceiros, exceto no interesse do ICL e mediante expressa autorização da Diretoria ou do Conselho Deliberativo, quando pertinente;

Integridade

II - Os dados e as informações do ICL deverão ser verídicos e completos;

Controle

III - Deverão ser criados e mantidos controles internos, incluindo rotinas, métodos e procedimentos, especialmente para os processos e/ou sistemas relevantes, visando assegurar que os objetivos institucionais sejam atingidos e de modo que as ocorrências significantes sejam rastreáveis até o evento inicial, permitindo a identificação dos responsáveis, o melhor gerenciamento dos riscos associados e o aprimoramento contínuo da gestão;

Responsabilidade

IV - Cada usuário é individualmente responsável pela segurança dos dados e das informações no âmbito do ICL, principalmente daqueles que estejam sob sua guarda ou responsabilidade direta;

Acesso controlado

V - O acesso à informação deverá ser restrito às pessoas que tenham real necessidade de conhecê-la, limitando-se, portanto, às pessoas autorizadas;

Accountability de dados

VI - Os sistemas, recursos e aplicações informacionais e comunicacionais do ICL deverão ser utilizados mediante controle de acessos gerenciados e monitorados com apoio de ferramentas tecnológicas adequadas e mediante processos suficientemente definidos com vistas a assegurar a devida proteção dos

ativos de informação e da infraestrutura computacional do instituto. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Identificação de riscos

VII - Os requisitos associados à segurança da informação deverão ser identificados na fase de levantamento do escopo de um projeto ou sistema, e avaliados, tratados, documentados e testados durante a fase de execução.

Cláusulas contratuais

VIII - Quando o objeto for pertinente, deverão constar nos contratos celebrados pelo instituto cláusulas de confidencialidade, de obediência às normas internas de Segurança da Informação e/ou de proteção de dados pessoais, a serem observadas pelos colaboradores, associados, prestadores de serviço e por todos os profissionais que vierem a desempenhar atividades no âmbito dos respectivos contratos celebrados com o ICL.

CAPÍTULO II –TRATAMENTO E SEGURANÇA DA INFORMAÇÃO, DIRETRIZES E CONTROLES

Tratamento da informação

Art. 5º. As diretrizes específicas e os procedimentos próprios de tratamento das informações institucionais serão regulamentados em norma complementar, a ser elaborada pela área de tecnologia da informação, considerando as seguintes diretrizes gerais:

(a) Documentos, dados e informações institucionais imprescindíveis às atividades deverão ser armazenados em dispositivos de rede. Arquivos armazenados localmente, nos computadores de usuários, não serão cobertos pelo serviço de *backup* (cópias de segurança), estando sujeitos à perda e a não recuperação.

(b) Arquivos pessoais e/ou não pertinentes às atividades (fotos, músicas, vídeos etc.) não deverão ser armazenados ou movidos para os dispositivos de rede, pois podem sobrecarregar a capacidade de armazenamento e conter vulnerabilidades, oferecendo riscos de segurança. Na hipótese de identificação, esses arquivos serão excluídos, de forma imediata e definitiva, sem necessidade de comunicação prévia ao usuário.

Controles e perfis de acesso

Art. 6º. Os controles e perfis de acesso devem obedecer às seguintes diretrizes gerais:

(a) Para a concessão de acesso aos ativos de informação, o usuário deve firmar termo de declaração de ciência das normas contidas nesta Política de Segurança da Informação e Proteção de Dados Pessoais.

(b) Na configuração das contas e concessão de perfis de acesso, deve ser garantida a adequada segregação e alinhamento às boas práticas de segurança da informação.

(c) As credenciais de acesso (usuário e senha) fornecidas aos colaboradores e usuários para acesso e/ou uso das instalações, informações e recursos de tecnologia da informação no ICL são pessoais e intransferíveis, não devendo ser compartilhadas em qualquer hipótese.

E-mail institucional

Art. 7º. As diretrizes específicas e procedimentos próprios ao serviço de correio eletrônico institucional (*e-mail*) serão regulamentados em norma complementar, a ser elaborada pela área de tecnologia da informação, considerando as seguintes diretrizes gerais:

(a) O correio eletrônico institucional é uma ferramenta comunicacional de trabalho, de uso obrigatório no âmbito do ICL.

(b) O correio eletrônico institucional é destinado para uso exclusivo em serviço e relacionado estritamente às atividades profissionais do usuário no âmbito do ICL.

(c) O uso do correio eletrônico institucional para fins pessoais será tolerado, desde que eventual e restrito ao tratamento de temas que não afrontem os princípios, valores e interesses do ICL e, ainda, a cultura moral vigente.

(d) O correio eletrônico institucional pode ser monitorado a qualquer tempo pela Administração e, sobretudo, pela Diretoria de *Compliance*, não havendo ofensa ao sigilo das comunicações telemáticas, nem expectativa de privacidade.

Uso de recursos e informações

Art. 8º. As informações e recursos do ICL serão usados apenas para fins profissionais pré-estabelecidos e em atendimento aos objetivos institucionais.

§1º. Não é permitida, em nenhuma hipótese, a alteração de configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança, sem autorização prévia, por escrito, da área responsável.

§2º. O uso de recursos como computadores e telefones para fins pessoais será tolerado, desde que eventual e restrito ao tratamento de temas que não afrontem os princípios, valores e interesses do ICL e, ainda, a cultura moral vigente.

Tratamento de dados

Art. 9º. O ICL determina os fins e meios de tratamento dos dados sob seu controle, coletando informações de forma ética e legal e as armazenando em ambiente seguro e controlado.

Classificação e tratamento da informação

Art. 10. No ICL, toda informação criada ou adquirida deve ser classificada segundo sua especificidade e seu grau de confidencialidade, devendo ser armazenada, transportada, divulgada e descartada com segurança física e lógica compatível com sua classificação.

§1º. O acesso às informações institucionais, conforme o seu nível de proteção, deve ser restrito às pessoas que tenham real necessidade de conhecê-las, a fim de que possam executar suas atividades adequadamente, de acordo com os padrões do ICL.

§2º. A informação será classificada como pública quando puder ser publicamente divulgada, sem provocar impactos nas atividades do ICL.

§3º. A informação será classificada como interna quando puder ser acessada exclusivamente por colaboradores, associados ou parceiros.

§4º. A informação será classificada como confidencial quando for estratégica para o ICL e não puder ser divulgada para terceiros sem prévia autorização.

§5º. A classificação da informação compete ao seu gestor, podendo ser revista e alterada a qualquer tempo, em alinhamento aos objetivos estratégicos do Instituto.

§6º. Na ausência de classificação prévia, a informação deverá ser presumidamente considerada confidencial.

CAPÍTULO III – TRATAMENTO DE DADOS PESSOAIS

Art. 11. O ICL poderá atuar como controlador dos dados pessoais coletados no âmbito das relações estabelecidas com qualquer titular de dados pessoais com o qual venha a interagir.

§1º. São exemplos de dados pessoais passíveis de coleta e controle pelo ICL aqueles obtidos em razão da formalização de vínculo empregatício, contratação de consultores externos, designação de membros para compor o Conselho Deliberativo e os órgãos internos de fiscalização e controle etc.

§2º. Enquanto Controlador, compete ao ICL as decisões referentes ao tratamento dos dados pessoais coletados.

Art. 12. Nos termos da legislação vigente, o ICL poderá tratar dados pessoais como dados de identificação, qualificação, cadastro, histórico, dentre outros.

Art. 13. Independente da origem e forma de coleta dos dados pessoais, o tratamento se dará exclusivamente nos limites estabelecidos na legislação e nesta Política.

Finalidade

Art. 14. Os dados pessoais serão coletados e mantidos de acordo com as necessidades do Instituto, seja para manutenção de sua regularidade, alcance de objetivos, desenvolvimento de atividades, incluindo a realização de estudos, ou, ainda, exercício regular de direito em processos judiciais, administrativos ou arbitrais e proteção de crédito.

Parágrafo único. Os dados pessoais ainda poderão ser coletados e mantidos de acordo com as demais hipóteses previstas na legislação vigente.

Cookies

Art. 15. O ICL poderá fazer uso de *cookies* em sua página de Internet ou aplicativos, para fornecer conteúdo personalizado ao usuário.

§1º. A coleta de informações de dados de utilização de usuário, obtida por meio de *cookies*, será devidamente informada na página de Internet ou aplicativos do instituto.

§2º. A critério do usuário, os *cookies* poderão ser permitidos ou bloqueados, excepcionando aqueles de natureza essencial, indispensáveis para o funcionamento das páginas de Internet e aplicativos.

Compartilhamento e armazenamento de dados pessoais

Art. 16. O ICL poderá compartilhar os dados pessoais de titulares com terceiros, sempre de acordo com as regras estabelecidas nesta política e na legislação vigente.

§1º. O compartilhamento de dados de titulares poderá ocorrer quando for necessário para alcance das finalidades descritas no artigo 14 desta política como, por exemplo, no relacionamento com prestadores

de serviços de benefícios, suporte administrativo ou de serviços de infraestrutura de tecnologia necessária para a condução de atividades.

§2º. O compartilhamento de dados de titulares com terceiros será resguardado por cláusulas contratuais prevendo obrigações específicas de confidencialidade, segurança e privacidade.

Art. 17. O ICL poderá transferir os dados pessoais para prestadores de serviços de armazenamento de dados ou para soluções de tecnologia da informação, como servidores externos ou nuvens, observando as medidas e salvaguardas cabíveis, com o objetivo de garantir a proteção dos dados pessoais, em observância aos preceitos estabelecidos na legislação vigente.

Prazo de armazenamento

Art. 18. O ICL manterá o armazenamento dos dados pessoais pelo tempo exigido por lei, até o término do tratamento dos dados pessoais ou, ainda, pelo tempo que se fizer necessário para preservar legítimo interesse ou exercício regular de direito.

Parágrafo único. Os dados pessoais serão eliminados após o término do tratamento, ressalvadas as hipóteses legais ou as previstas nesta Política.

Encarregado de dados

Art. 19. A função de encarregado de dados do instituto será atribuída ao titular da Diretoria de *Compliance*, que acumulará a atribuição de atuar como responsável pelo canal de comunicação entre o ICL, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

Direitos do titular dos dados

Art. 20. O titular de dados pessoais poderá contatar o ICL com o objetivo de exercer qualquer dos seguintes direitos: (i) confirmar o tratamento de seus dados pessoais; (ii) obter acesso aos dados tratados; (iii) requerer atualização ou retificação de dados incompletos, inexatos ou desatualizados; (iv) solicitar anonimização, bloqueio ou eliminação; (v) requerer informações acerca de compartilhamento; (vi) solicitar informações e/ou revogar o consentimento à ICL para tratamento dos dados.

§1º. O titular poderá ainda exercer qualquer outro direito previsto na legislação vigente e não especificado nesta Política, incluindo o direito de peticionar em relação aos seus dados contra o controlador perante a Autoridade Nacional de Proteção de Dados (ANPD).

§2º. O contato com o ICL poderá ser realizado por meio do correio eletrônico dpo@combustivellegal.com.br.

§3º. Ao contatar o ICL, o titular deverá se identificar, informando seu nome completo, CPF e meios de contato; e indicar o direito que pretende exercer, descrevendo a solicitação.

§4º. Os dados pessoais fornecidos por ocasião de contato com o encarregado de dados do ICL serão utilizados exclusivamente com a finalidade de registrar e atender à demanda formulada pelo titular.

Art. 21. O exercício dos direitos referidos no artigo anterior poderá ser restringido pelo ICL em certas situações, como, por exemplo, quando a providência solicitada pelo titular não puder ser cumprida em razão de obrigação legal ou quando o atendimento impedir ou de qualquer forma embaraçar legítimo interesse ou exercício regular de direito do Instituto.

Obrigações comuns a todos os colaboradores

Art. 22. Todos os colaboradores, consultores externos e a quem, de qualquer forma ou meio, esteja afeto às atividades do instituto, devem:

I - Restringir a coleta, utilização, armazenamento ou processamento de dados pessoais ao estritamente necessário para a execução dos processos e atividades do Instituto.

II - Ser diligentes no tratamento de quaisquer dados pessoais, promovendo a segurança, integridade e o uso adequado daqueles que estejam sob sua responsabilidade.

III - Utilizar os dados pessoais de acordo com a finalidade para a qual a coleta foi realizada.

IV - Utilizar controles para ajudar a proteger os dados pessoais contra perda, destruição, acesso não autorizado, utilização indevida, alteração ou divulgação.

V - Respeitar a privacidade dos demais colaboradores, não publicando informações ou imagens sem o seu prévio consentimento.

Incidente de segurança ou vazamento de dados

Art. 23. Na hipótese de incidente de segurança ou vazamento de dados, o ICL deve:

I - Promover a identificação dos dados, documentando-a;

II - Avaliar o risco e a extensão do dano;

III - Elaborar parecer técnico, com relato da ocorrência e descrição das medidas de tratamento adotadas;

IV - Notificar a Autoridade Nacional de Proteção de Dados (ANPD) e terceiros interessados, em hipóteses de configuração de condutas ilícitas ou violação ética;

V - Monitorar a implementação das medidas de tratamento do risco e elaborar reporte ao Comitê de Integridade e Conduta, indicando a aprendizagem institucional.

§1º. As rotinas descritas nos incisos I, II e III serão executadas pela área responsável pela ocorrência, com a supervisão do encarregado de dados. As rotinas descritas dos incisos IV e V serão executadas pelo encarregado de dados, com o apoio da área responsável pela ocorrência e das demais áreas internas envolvidas.

§2º. Em caso de vazamento de credenciais de acesso, haverá imediata substituição das senhas, além da ativação de todos os mecanismos disponíveis para analisar os registros de acesso e apurar eventuais incidentes.

CAPÍTULO IV – CONDUTAS

Art. 24. As seguintes condutas devem ser observadas no âmbito do ICL, por seus colaboradores, consultores externos e a quem, de qualquer forma ou meio, esteja afeto às atividades do instituto:

I - Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos institucionais de informação e comunicação, utilizando-os sempre de forma ética, legal e consciente;

II - Manter-se atualizado em relação a esta Política de Segurança da Informação e Proteção de Dados Pessoais e às suas normas complementares e procedimentos relacionados, buscando informação junto à área de tecnologia da informação e à Diretoria de *Compliance*, sempre que não estiver absolutamente seguro quanto à obtenção, tratamento, uso e/ou descarte de dados ou informações;

III - Comunicar a área de tecnologia da informação ou à Diretoria de *Compliance*, conforme a situação, qualquer ocorrência relevante e que possa expor a segurança da informação do ICL a risco, ou qualquer outra conduta suspeita com relação à obtenção, tratamento e vazamento dos dados;

IV - Reportar ao titular da Diretoria de *Compliance*, na qualidade de encarregado de dados, qualquer incidente ou suspeita de incidente envolvendo dados pessoais com a maior brevidade possível.

CAPÍTULO IV – DISPOSIÇÕES FINAIS

Art. 25. Para uniformização da informação institucional, esta Política de Segurança da Informação e Proteção de Dados Pessoais deverá ser comunicada a todos os colaboradores, consultores externos e a quem, de qualquer forma ou meio, esteja afeto às atividades do ICL, a fim de que seja cumprida interna e externamente.

Parágrafo único. O não cumprimento dos preceitos e requisitos previstos nesta política e em seus complementos constitui violação às regras internas do ICL e sujeitará o usuário às medidas disciplinares e legais cabíveis.

Art. 26. A Diretoria de *Compliance*, com supervisão do Comitê de Integridade e Conduta, poderá difundir orientações técnicas e esclarecimentos complementares, inclusive por meio de cartilhas, especialmente no que se refere ao tratamento de dados pessoais.

Art. 27. A área de tecnologia da informação, com aprovação da diretoria responsável, deverá conceber normas complementares regulando os temas de sua responsabilidade tratados na presente política.

Art. 28. Está política deverá ser analisada anualmente e revista sempre que necessário.

Esta Política de Segurança da Informação e Proteção de Dados Pessoais foi aprovada pelo Conselho Deliberativo do Instituto Combustível Legal (ICL) em 05 de maio de 2023, com imediata entrada em vigor.

INSTITUTO COMBUSTÍVEL LEGAL - CONSELHO DELIBERATIVO

ÍNDICE