



Política de Segurança da Informação para Fornecedores

1. OBJETIVO

Orientar e apresentar diretrizes no relacionamento com fornecedores e parceiros, de modo a garantir a segurança das informações e mitigar os riscos associados com o acesso de fornecedores as informações, aos ativos e as instalações da Almaviva Experience.

2. CAMPO DE APLICAÇÃO

As diretrizes estabelecidas nesta política aplicam-se a todos os fornecedores que executem serviços que tenham impacto direto sobre os negócios ou sobre questões relacionadas com a Segurança da Informação e Privacidade.

3. REFERÊNCIAS

- PSI-002 – Política de Segurança da Informação – Pública
- PPD-001 - Política Externa de Privacidade
- NBR ISO/IEC 27001:2022 – Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos
- NBR ISO/IEC 27002:2022 – Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação
- NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes
- Lei nº 13.709/2018 – LGPD (Lei Geral de Proteção de Dados Pessoais).

4. DEFINIÇÕES

Não se aplica.

5. RESPONSABILIDADES

Compete a todos os Fornecedores:

- seguir todas as diretrizes definidas nesta política e demais políticas aplicáveis.

Compete a área de Segurança da Informação e Privacidade Almaviva:

- definir e manter as diretrizes desta política atualizadas e disponíveis
- realizar o levantamento e o apoio ao tratamento de riscos
- realizar e apoiar auditorias, quando aplicável.

Compete ao Jurídico Almaviva:

- estabelecer cláusulas para a preservação da confidencialidade, propriedade intelectual, o sigilo das informações e a proteção de dados pessoais (LGPD) que devem ser respeitadas e cumpridas antes, durante e após a prestação dos serviços dos fornecedores através de acordos entre as partes envolvidas.

6. DIRETRIZES

O acesso aos ativos de informação da Almaviva Experience só pode ser feito em condições controladas e monitoradas. A concessão dos acessos físicos e lógicos seguirá as premissas estabelecidas pelas políticas de segurança da informação, não sendo permitido que terceiros acessem informações confidenciais sem a devida autorização.

As diretrizes, programas, códigos de conduta, normas internas e políticas estabelecidas pela Almaviva Experience devem ser cumpridas integralmente.

Os fornecedores deverão garantir, no mínimo, que todos os seus colaboradores associados ao serviço prestado tomaram conhecimento e se comprometem a obedecer ao descrito na presente política. A Almaviva Experience poderá solicitar, em qualquer momento, evidências do processo de divulgação destas informações.

O fornecedor deve garantir o repasse de todas as informações necessárias, para que o gestor do contrato controle os processos, produtos e serviços de forma a assegurar que todos os requisitos especificados, acordos de níveis de serviços e obrigações contratuais pactuadas sejam cumpridas.

Convém que, boas práticas para garantir a gestão de riscos sejam adotadas e monitoradas em toda cadeia de suprimento.

Requisitos legais e regulamentares, quando aplicáveis, devem ser atendidos e monitorados. É obrigatória a proteção e preservação dos ativos de informação da Almaviva Experience, para assegurar a confidencialidade, integridade e disponibilidade das informações.

Todos os acordos para a preservação da confidencialidade, propriedade intelectual e o sigilo das informações acessadas antes, durante e após a prestação dos serviços devem ser respeitados e cumpridos.

O gestor do contrato deve ser comunicado na identificação de quaisquer riscos ou incidentes que possam causar impacto à segurança e a privacidade das informações.

Documentos e registros que demonstrem e evidenciem o atendimento dos requisitos definidos em contrato e das diretrizes estabelecidas em políticas internas da Almaviva Experience devem ser apresentados sempre que necessário.

Ao utilizar os bens e as instalações da Almaviva Experience os cuidados necessários para a conservação do patrimônio devem ser adotados. É dever de todos zelar pela proteção dos ativos e ter hábitos que evitam os desperdícios de forma geral.

Na identificação de riscos, incidentes e não conformidades, o gestor do contrato deve ser comunicado, e ações corretivas e preventivas devem ser adotadas, de modo a eliminar a causa raiz e prover o tratamento adequado dos riscos associados.

Quando necessário, auditorias, inspeções e avaliações podem ser realizadas pela Almaviva Experience para garantir que todos os requisitos para a segurança da informação estão sendo atendidos. Os resultados das inspeções e avaliações, bem como recomendações de melhorias serão registradas e encaminhadas para providências pelo fornecedor.

Os fornecedores devem respeitar e cumprir todas as medidas, procedimentos e instruções para o registro e controle de acessos físicos e lógicos estabelecidos pela Almaviva Experience.

Sempre que necessário, os fornecedores fornecerão a Almaviva Experience uma lista de pessoas, sua descrição de perfil, funções e responsabilidades associados ao serviço prestado, comunicando todas as eventuais alterações realizadas referentes à relação com a Companhia (admissão, demissão, substituição ou alteração de funções ou cargos).

Os fornecedores deverão garantir que todos os seus colaboradores possuam a instrução adequada e estejam devidamente capacitados para executar o serviço prestado, seja especificamente em relação aos campos que correspondam às atuações associadas com a prestação de serviço ou com referência à segurança da informação e a privacidade.

Assegurar que os ativos de informação sejam utilizados apenas para as finalidades estabelecidas e aprovadas pela Almaviva Experience, estando sujeitos à monitoração, rastreabilidade e auditoria.

O fornecedor somente poderá subcontratar se o contrato permitir, devendo divulgar para a Almaviva Experience qualquer uso ou alteração de subcontratados para tratar informação de cliente, incluindo dados pessoais, antes do uso.

Os fornecedores deverão possuir Plano de Contingência e Plano de Recuperação de Desastres para garantir a continuidade dos serviços contratados, com a mesma qualidade e dentro dos prazos acordados, com a Almaviva Experience, revisados e testados anualmente.

Quando e onde aplicável, os fornecedores deverão possuir Política de Backup bem como procedimentos de monitoramento e restauração, incluindo testes periódicos para avaliação de integridade, devendo ser apresentados sempre que solicitados pela Almaviva para fins de auditoria.

Os backups do fornecedor devem estar logicamente desconectados do ambiente de rede da organização sendo acessíveis somente pela(s) ferramenta(s) de backup, com acesso restrito e monitorado. Adicionalmente, deve ser mantida cópia (backup) adicional offsite (em local distinto ao principal) com distância mínima de 10 km.

Quando e onde aplicável, os fornecedores de serviços deverão realizar testes de segurança das suas aplicações, tais como pentests e scan de vulnerabilidades, corrigindo onde necessário, assim como efetuar a revisão periódica de acessos, devendo ser apresentados os resultados, sempre que solicitados pela Almaviva para fins de auditoria.

Ao participar de projeto envolvendo clientes contratantes Almaviva, o fornecedor deve estar de acordo, e cumprir com os mesmos compromissos assumidos pela Almaviva.

Qualquer mudança nos produtos ou serviços prestados deve ser previamente comunicada ao gestor do contrato, de modo a garantir a continuidade, a conformidade e o adequado acompanhamento das obrigações assumidas.

6.1. Uso de solução de tratamento automatizado

É expressamente vedado ao fornecedor tratar dados pessoais para quaisquer finalidades diversas das previstas em contrato. Em especial, quando não for necessário para a execução do Contrato, fica proibido à título de exemplificativo e não exaustivo, realizar a extração massiva de dados pessoais, inclusive mediante o uso de ferramentas de automação, tais como “RPA – Robotic Process Automation”, salvo se houver prévia e expressa autorização, por escrito, da Almaviva.

Nos casos em que ocorrer o tratamento de dados pessoais de forma automatizada, ao fornecedor deverá assegurar que:

- nenhuma decisão que produza efeitos jurídicos ou que afete de maneira relevante os interesses da Almaviva ou de titulares de dados seja tomada exclusivamente com base em tratamento automatizado, sem a possibilidade de revisão humana
- exista sempre a intervenção de pessoa natural apta a revisar, validar ou contestar os resultados advindos de processos decisórios automatizados
- os mecanismos de revisão sejam transparentes, documentados e disponibilizados à Almaviva, sempre que solicitado.

6.2. Inteligência Artificial

Ao assumir projetos ou soluções envolvendo Inteligência Artificial, o fornecedor deve:

- garantir que quaisquer dados utilizados no treinamento de modelos de IA, quando autorizado e aplicável, serão obtidos exclusivamente de fontes éticas, com base em

permissões válidas, licenças ou bancos de dados publicamente disponíveis, sempre em conformidade com a legislação vigente e com os direitos de propriedade intelectual

- assegurar que todos os seus fornecedores, parceiros de tecnologia, provedores de infraestrutura e prestadores de serviços que, direta ou indiretamente, participem do processamento de dados ou da operação das soluções de Inteligência Artificial:
 - cumprirão contratualmente as mesmas obrigações de confidencialidade, segurança, compliance e proteção de dados estabelecidas nesta política
 - terão firmados instrumentos jurídicos equivalentes a DPA (Data Processing Agreement) quando aplicável, garantindo a plena observância da legislação vigente.
- Utilizar somente plataformas de Inteligência Artificial confiáveis que sigam padrões de segurança confiáveis, não públicas, para processar, armazenar, analisar ou de qualquer forma manipular dados, informações, documentos ou conteúdos confidenciais pertencentes à Almaviva, ou de seus clientes, salvo mediante prévia e expressa autorização por escrito desta.

É expressamente vedado inserir, compartilhar, ou realizar upload de dados pessoais, confidenciais, estratégicos ou sensíveis da Almaviva em sistemas de IA que:

- possam reter ou reutilizar os dados enviados para treinamento ou melhoria de modelos
- não ofereçam garantias técnicas e contratuais adequadas de confidencialidade, segurança e conformidade com a LGPD e normas correlatas
- operem em infraestrutura e/ou jurisdição que não assegurem proteção legal equivalente à legislação brasileira de proteção de dados.

Caso seja necessária a utilização de soluções de Inteligência Artificial, a CONTRATADA deverá:

- submeter previamente à Almaviva, por escrito, a relação das ferramentas pretendidas, incluindo fornecedor, modelo de operação (público, privado, on-premise ou cloud), local de armazenamento e termos de uso, detalhes sobre a utilização pretendida da IA, o tipo de conteúdo que irá gerar e os potenciais riscos e benefícios associados.
- garantir que a solução de IA utilizada possua controles técnicos e contratuais que impeçam o uso indevido, o treinamento não autorizado ou a exposição de dados da Almaviva e de seus clientes;
- obter aprovação formal e por escrito da Almaviva antes de qualquer uso

- utilizar apenas serviços de IA oferecidos por fornecedores confiáveis e reconhecidos no setor, que ofereçam garantias de qualidade, originalidade, legalidade e conformidade com todas as leis e regulamentos aplicáveis, incluindo aqueles sobre proteção de dados e privacidade. A autorização da Almaviva não isenta a Almaviva de responsabilidade por quaisquer perdas e danos decorrentes de tais atos.

A Almaviva poderá, a qualquer tempo, solicitar evidências de conformidade ou realizar auditoria sobre o uso de tais soluções.

O descumprimento de qualquer obrigação prevista em cláusulas contratuais configura falha grave, passível a rescisão imediata do contrato, sem prejuízo das demais responsabilidades civis, regulatórias e indenizatórias cabíveis do fornecedor por eventuais perdas, danos diretos, indiretos, lucros cessantes e sanções administrativas impostas por autoridades competentes.

7. DISPOSIÇÕES FINAIS

Qualquer necessidade de ação em desacordo com as regras estabelecidas na Política de Segurança da Informação, na Política de Privacidade e suas políticas complementares devem ser direcionadas à Segurança da Informação para análise do risco, seu registro, e envio para a apreciação pela alçada competente e/ou Comitê de Segurança da Informação e Privacidade.

O colaborador que fizer uso indevido ou não autorizado dos recursos das empresas, violar controle de segurança, ou de qualquer modo agir em desacordo com os termos dessa política, fica sujeito à aplicação de medidas disciplinares legalmente previstas, podendo haver responsabilização penal, civil e/ou administrativa, na forma da legislação em vigor.

Política revisada em 02/10/2025