

Políticas e Normas

Inteligência Artificial



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANCA E C. TECNOLOGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

Política de Uso Adequado de Inteligência Artificial

Sumário

Uso de Inteligência Artificial	2
1. Definições Essenciais	2
2. Propósito	3
3. Pilares da Segurança da Informação	3
4. Diretrizes de Uso Responsável	6
5. Consequências de Descumprimento	7

Políticas e Normas

Inteligência Artificial



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANÇA E C. TECNOLÓGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

Uso de Inteligência Artificial

1. Definições Essenciais

Inteligência Artificial (IA): Qualquer sistema computacional capaz de gerar conteúdo, prever padrões, automatizar decisões, analisar dados ou realizar tarefas que imitem capacidades cognitivas humanas.

Alucinação de IA: Fenômeno em que modelos de linguagem geram informações que parecem coerentes, mas são factualmente incorretas, inexistentes ou baseadas em dados falsos.

Anonimização: Processo técnico pelo qual dados são desvinculados de um indivíduo, tornando impossível a sua identificação, direta ou indiretamente, utilizando meios razoáveis e disponíveis na ocasião de seu tratamento.

Pseudonimização: Processo técnico pelo qual o dado perde a capacidade de identificar um indivíduo, substituindo-o por um código ou pseudônimo, desde que utilizado isoladamente, ou seja, a identificação só é possível com a adição de informação suplementar, mantida separadamente e sob medidas técnicas e organizacionais adequadas.

Ativos Informacionais: Conjunto de informações, sistemas, equipamentos e recursos tecnológicos que possuem valor para a SGM e cuja proteção é crucial para suas operações e continuidade.

Dados Confidenciais: Informações estratégicas, financeiras, comerciais, técnicas, operacionais ou quaisquer outros dados que, se divulgados sem autorização, possam causar prejuízo ao SGM, como planos estratégicos, segredos comerciais, códigos-fonte proprietários etc.

Dados Pessoais: Informação relacionada a pessoa natural identificada ou identificável, conforme definido na Lei Geral de Proteção de Dados Pessoais (LGPD).

Dados Pessoais Sensíveis: Dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, conforme Art. 5º, II, da LGPD.

Políticas e Normas

Inteligência Artificial



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANÇA E C. TECNOLÓGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

Decisões Automatizadas: Decisões tomadas exclusivamente com base em tratamento automatizado de dados pessoais, sem qualquer intervenção humana, e que afetem interesses ou direitos dos indivíduos.

Encarregado de Dados (DPO – Data Protection Officer): Profissional indicado para orientar a instituição sobre proteção de dados pessoais e LGPD, atender titulares e atuar como canal de comunicação com a Autoridade Nacional de Proteção de Dados (ANPD). Também participa da avaliação de riscos e da definição de diretrizes para que o tratamento de dados ocorra de forma lícita, transparente e segura.

2. Propósito

A SGM reconhece o potencial transformador das ferramentas de Inteligência Artificial (IA) para otimizar processos, fomentar a inovação e aprimorar a produtividade. Contudo, a adoção dessas tecnologias exige uma abordagem consciente, responsável e compatível com os riscos envolvidos.

Esta política tem por finalidade estabelecer diretrizes para o uso ético, seguro e responsável de ferramentas de IA no âmbito da SGM, aplicando-se a colaboradores, estagiários, prestadores de serviços, fornecedores e terceiros que utilizem tais recursos em atividades relacionadas à instituição.

A presente Política de Inteligência Artificial complementa a Política de Segurança da Informação (PSI) e deve ser interpretada em conjunto com ela. Os pilares de confidencialidade, integridade, disponibilidade e rastreabilidade, bem como os controles gerais de acesso, classificação, uso aceitável, monitoramento, automação e resposta a incidentes previstos na PSI, permanecem integralmente aplicáveis ao uso de IA.

A IA deve ser utilizada como instrumento de apoio cognitivo e operacional, nunca como entidade autônoma de decisão. Nenhum recurso tecnológico substitui a responsabilidade humana pela revisão, validação, aprovação e utilização dos resultados gerados.

3. Diretrizes de Uso Responsável

Sem prejuízo das obrigações estabelecidas na PSI e nas demais normas internas, o uso de ferramentas de IA deverá observar as diretrizes específicas abaixo.

Autorização, acesso e rastreabilidade

Políticas e Normas

Inteligência Artificial



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANÇA E C. TECNOLÓGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

A utilização de ferramentas de IA somente é permitida quando previamente aprovada pela área de Tecnologia da Informação (TI) e pelo Encarregado de Dados (DPO), conforme relação de ferramentas autorizadas divulgada pela instituição.

As ferramentas de IA devem ser acessadas exclusivamente por contas corporativas, gerenciadas ou fornecidas pela SGM. É vedado o uso de contas ou credenciais pessoais para processar informações relacionadas às atividades institucionais.

As interações realizadas em ferramentas aprovadas poderão ser registradas, monitoradas e auditadas para fins de segurança, conformidade, investigação de incidentes e proteção dos ativos informacionais.

Proteção de dados pessoais e informações corporativas

É proibido inserir dados pessoais, informações confidenciais, segredos comerciais, códigos-fonte, documentos internos ou outros ativos informacionais em ferramentas de IA não aprovadas ou que não ofereçam controles adequados de segurança, privacidade e desativação do uso das informações para treinamento de modelos públicos.

Ao elaborar comandos (prompts), o colaborador deverá aplicar os princípios da necessidade e da minimização, utilizando termos genéricos e, sempre que possível, dados anonimizados ou pseudonimizados, evitando nomes de clientes, identificadores exclusivos ou informações desnecessárias.

É proibido inserir dados pessoais sensíveis em ferramentas externas de uso geral, ainda que aprovadas para atividades comuns. Qualquer exceção dependerá de avaliação formal de riscos, finalidade específica e autorização prévia da TI e do DPO.

O processamento de contratos, planilhas de clientes ou leads, documentos jurídicos, informações financeiras, dados estratégicos ou materiais equivalentes somente poderá ocorrer em solução corporativa formalmente aprovada e de acordo com a classificação e os controles definidos na PSI.

Supervisão humana, integridade e validação

Políticas e Normas

Inteligência Artificial



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANÇA E C. TECNOLÓGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

O colaborador permanece integralmente responsável pelo trabalho realizado com auxílio de IA, inclusive pela precisão, adequação, licitude e finalidade do conteúdo gerado, resumido, traduzido, analisado ou aprimorado.

Todo resultado produzido por IA deverá ser revisado criticamente antes de ser utilizado, compartilhado ou incorporado a documento, processo ou decisão institucional.

Fatos, números, referências bibliográficas, jurisprudenciais, normativas ou técnicas geradas por IA deverão ser conferidos em fontes confiáveis e, quando aplicável, em fontes oficiais primárias.

É proibido utilizar IA como fundamento exclusivo para decisões que afetem direitos de pessoas naturais, especialmente em contextos trabalhistas, financeiros, comerciais ou comportamentais. Tais decisões exigem revisão humana estruturada e autorização do DPO quando envolverem dados pessoais.

É vedado utilizar ferramentas de IA para produzir ou disseminar desinformação, conteúdo enganoso, plágio ou material incompatível com a legislação, os princípios éticos e as normas internas da instituição.

Ética e direitos de terceiros

Não utilize ferramentas de IA para criar, reproduzir ou ampliar conteúdos discriminatórios, preconceituosos, ofensivos, ilícitos ou que promovam discurso de ódio.

É proibido inserir, reproduzir ou transformar material protegido por direitos autorais, segredo de negócio, confidencialidade ou outros direitos de terceiros sem autorização ou fundamento jurídico adequado.

Conteúdos destinados ao público externo deverão ser submetidos aos fluxos internos de revisão e aprovação aplicáveis, ainda que tenham sido produzidos apenas parcialmente com auxílio de IA.

Agentes, automações e integrações

É proibida a criação ou ativação autônoma de agentes, automações ou integrações de IA que acessem e-mails institucionais, sistemas de comunicação, documentos em nuvem, CRM, ERP, bancos de dados ou informações de clientes.

Políticas e Normas

Inteligência Artificial



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANÇA E C. TECNOLÓGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

Qualquer implementação dessa natureza dependerá de aprovação técnica formal da TI e do DPO, definição de finalidade e escopo, avaliação de riscos, controle de acessos, registro de atividades, supervisão humana e possibilidade de interrupção imediata.

As credenciais, tokens e chaves utilizados em integrações deverão ser protegidos conforme os controles previstos na PSI, sendo vedada sua inserção direta em prompts, códigos, scripts ou documentos desprotegidos.

Incidentes, comunicação e capacitação

Qualquer suspeita de vazamento, exposição indevida, uso não autorizado, resposta anômala ou falha relacionada à IA deverá ser comunicada imediatamente ao DPO e à área responsável pela Segurança da Informação.

A utilização da ferramenta ou integração envolvida deverá ser interrompida quando houver risco relevante, permanecendo suspensa até a conclusão da análise e a adoção das medidas corretivas necessárias.

Os usuários deverão participar dos treinamentos e observar as orientações emitidas pela SGM sobre uso seguro, responsável e eficaz de IA, considerando a evolução contínua dessas tecnologias e de seus riscos.

4. Propriedade Intelectual

Os conteúdos, documentos, códigos-fonte, materiais técnicos e demais resultados produzidos, aprimorados ou processados com auxílio de IA no exercício das atividades profissionais integram o patrimônio intelectual da SGM, observados os direitos de terceiros, os termos de uso das ferramentas e a legislação aplicável.

A utilização de IA não autoriza a apropriação, reprodução ou divulgação de conteúdo protegido, nem afasta a responsabilidade do colaborador por verificar a origem, a licença, as restrições de uso e a possibilidade de utilização do material gerado

Políticas e Normas

Inteligência Artificial



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANÇA E C. TECNOLÓGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

5. Consequências do Descumprimento

O descumprimento desta política será analisado de acordo com a gravidade, a natureza, a frequência e o impacto da conduta, sem prejuízo das medidas previstas na PSI, nos contratos, no regimento interno e na legislação aplicável.

As medidas poderão incluir orientação formal, treinamento adicional, advertência, restrição ou suspensão de acessos, responsabilização contratual, rescisão do contrato de trabalho ou de prestação de serviços e adoção das medidas administrativas, civis ou judiciais cabíveis, sempre de forma proporcional ao risco e aos danos potenciais