1. OBJETIVO E PROPÓSITO ESTRATÉGICO

Esta Política estabelece diretrizes, responsabilidades e controles para o uso ético, seguro e legal de sistemas de Inteligência Artificial (IA) e agentes autônomos de IA. Serve como norma-mãe para todas as empresas controladas pela Imagem Tecnologia, prevalecendo sobre qualquer norma local em caso de conflito.

Fundamenta-se nos requisitos da LGPD (Lei 13.709/2018), nos controles de segurança da ISO/IEC 27001 e ISO42001 e nas boas práticas de governança de IA amplamente adotadas pelo mercado de tecnologia.

1.1 Pilares Estratégicos

Pilar	Descrição	Princípio Central
Cooperação Inteligente	Compartilhamento de conhecimento, dados e capacidades entre as controladas, evitando retrabalho e acelerando a inovação conjunta.	Sinergia
Inovação Responsável	Desenvolvimento e adoção de IA com rigor ético, avaliação de impactos e conformidade regulatória.	Responsabilidade
Excelência Operacional	Soluções de IA projetadas para escalar com eficiência, qualidade e segurança, com processos padronizados entre empresas.	Escalabilidade

CÓPIA CONTROLADA

2. DEFINIÇÕES E GLOSSÁRIO

Termo	Definição
Inteligência Artificial (IA)	Sistema que, dado um conjunto de objetivos definidos, realiza previsões, recomendações, decisões ou gera conteúdo que influencia ambientes reais ou virtuais (ISO/IEC 42001:2023).
Agente de IA	Sistema autônomo ou semi-autônomo que percebe o ambiente, processa informações e executa ações para atingir objetivos, podendo interagir com APIs, bancos de dados e outros sistemas.
LLM (Large Language Model)	Modelo de linguagem de grande escala capaz de gerar, resumir, traduzir e raciocinar sobre linguagem natural.
Dado Pessoal Sensível	Categoria especial sob a LGPD: saúde, financeiro, biométrico, racial, religioso, político, sexual e dados de crianças/adolescentes.
AI Officer	Responsável designado por cada empresa controlada pela governança de IA em nível empresarial. Função de negócio/gestão, não necessariamente de TI.
AISP (AI System Profile)	Perfil de risco atribuído a um sistema de IA com base em sua criticidade, autonomia e potencial impacto, conforme ISO 42001.
Descomissionamento	Processo de desativar e retirar de operação um modelo ou sistema de Inteligência Artificial de forma segura, ética e definitiva.
Prompt Engineering	Técnica de formulação de instruções para modelos de linguagem visando obter respostas seguras e alinhadas ao objetivo.
RAG (Retrieval-Augmented Generation)	Arquitetura que combina modelos de linguagem com recuperação de informações de bases de conhecimento externas.

DPO (Data Protection Officer)	Encarregado de Proteção de Dados, conforme exigido pela LGPD (Art. 41).
SGAI	Sistema de Gestão de Inteligência Artificial, conforme estruturado pela ISO/IEC 42001:2023, aqui observada como referência de boa prática.
Diretoria Executiva	Diretoria Executiva — Pessoa responsável pela supervisão do SGAI na respectiva empresa.
DPIA	Avaliação de Impacto à Proteção de Dados (Data Protection Impact Assessment). Obrigatório para sistemas de IA de risco Médio ou superior.
DPA	Data Processing Agreement, contrato com o fornecedor sobre tratamento de dados pessoais (LGPD Art. 39)
Prompt Injection	(injeção de prompt) é uma técnica de manipulação que engana sistemas de Inteligência Artificial (como chatbots ou assistentes).
Jailbreak	Ação de contornar ou remover restrições impostas pelos fabricantes em softwares ou dispositivos eletrônicos
Guardrail	Mecanismo de controle e segurança implementado em sistemas de IA para limitar, filtrar ou supervisionar seus outputs.
Framework de Agentes	Conjunto de políticas, processos, controles e responsabilidades que cada empresa controlada adota para governar o uso e desenvolvimento de agentes de IA.
Permissionamento de IA	Conjunto de regras que define quais colaboradores podem usar quais ferramentas de IA e com qual nível de acesso e capacidade.

3. ESCOPO, EMPRESAS CONTROLADAS E HIERARQUIA NORMATIVA

Esta Política se aplica a todos os colaboradores (CLT, PJ, estagiários e terceiros com acesso a sistemas internos) e a todas as empresas controladas pela **Imagem Tecnologia**.

3.1 Empresas Controladas

Para os fins desta Política, são consideradas Empresas Controladas todas as sociedades nas quais a Imagem Tecnologia detém, direta ou indiretamente, participação majoritária no capital social ou poder de controle sobre as decisões estratégicas.

3.2 Hierarquia Normativa — Holding → Controladas

Esta Política constitui a norma-mãe (primeiro nível) em matéria de IA. Sua observância é obrigatória por todas as controladas.

Nível	Instrumento e Regra
1º — Política Local da Controlada	Cada controlada pode ter política complementar, nunca conflitante. Aprovada pela Diretoria Executiva da controlada.
2º — Instruções Normativas	Procedimentos e frameworks de cada empresa. Respeitam os limites deste documento.
3º — Contratos e Acordos	DPAs, NDAs e contratos com fornecedores de IA. Obrigatoriamente alinhados a esta Política.

Em caso de conflito, prevalece a norma de nível superior. As políticas de Segurança da Informação e Políticas de Privacidade são aplicadas em conjunto a esta. Em divergência, aplica-se a norma mais restritiva.

3.3 Deveres de Cada Empresa Controlada

- Adotar integralmente esta Política e comunicá-la a todos os seus colaboradores, garantindo que todos estejam devidamente e formalmente compromissados quanto ao seu cumprimento integral;
- Garantir que Empresa Controlada assuma a responsabilidade integral pela governança de IA na sua empresa;
- Manter inventário atualizado dos sistemas e agentes de IA em uso, registrando o processo em que a IA é usada, onde os dados são armazenados e por quanto tempo, quem tem acesso (interno e externo) e a classificação do dado (pessoal ou sensível); e

- Reportar a Diretoria Executiva, com visibilidade à diretoria da Vunox, toda nova iniciativa de IA de risco Alto ou Crítico antes do início do desenvolvimento ou contratação.

4. PRINCÍPIOS NORTEADORES

Princípio	Descrição
Responsabilidade Humana	Toda decisão crítica apoiada por IA tem revisão humana identificada. A IA auxilia — humanos decidem e respondem.
Transparência	Colaboradores, clientes e titulares são informados sobre o uso de IA que os afete (LGPD Art. 6º, VI).
Equidade e Não-Discriminação	Sistemas de IA não devem gerar resultados que discriminem grupos protegidos por lei.
Privacidade por Design	Proteção de dados incorporada desde a concepção do sistema (LGPD Art. 46).
Minimização de Dados	Apenas dados estritamente necessários são usados no treinamento ou operação (LGPD Art. 6º, III).
Segurança	Controles técnicos e organizacionais protegem integridade, confidencialidade e disponibilidade (ISO 27001).
Rastreabilidade	Ações de sistemas e agentes de IA são registradas e auditáveis.
Proporcionalidade	O nível de automação é proporcional ao risco e ao impacto potencial sobre pessoas e negócios.
Melhoria Contínua	Práticas e soluções de IA são monitoradas e aprimoradas de forma regular.

IMPORTANTE: A responsabilidade pela governança de IA em cada empresa controlada é integralmente da sua Diretoria Executiva. O AI Officer, caso exista, será o delegado operacional da Diretoria. A área de TI é parceira técnica, sem alçada de deliberação autônoma

4.1 Comitê de Tecnologia

Fica formalmente instituído o Comitê de Tecnologia, órgão colegiado multidisciplinar responsável por deliberar sobre a governança de IA no Grupo, revisando e atualizando a estrutura preexistente e centralizando a padronização de IA entre as empresas.

4.2 Auditoria de Conformidade pela Atmis

O cumprimento das diretrizes e dos processos desta Política é auditado pela Atmis Gestão, na condição de segunda linha de defesa. A Atmis verifica a adesão ao processo de aprovação por alçada, a existência de DPIAs e pareceres exigidos, a manutenção do inventário/catálogo de IA, a execução dos controles mínimos por nível de risco e o tratamento tempestivo de incidentes e desvios, registrando não conformidades e reportando-as ao Comitê.

5. CLASSIFICAÇÃO DE RISCO DE SISTEMAS, FERRAMENTAS E AGENTES DE IA

A classificação resulta do cruzamento de duas dimensões: o tipo de ferramenta, medido pelo grau de autonomia de ação efetivamente concedido, e a classe da informação que a ferramenta acessa, processa ou produz.

5.1. Regra de classificação: todo sistema de IA em RH é, no mínimo, risco Médio. O potencial de viés discriminatório eleva o risco independentemente de haver dados sensíveis. Sistemas que tratam código-fonte proprietário e ativos intangíveis do Grupo são classificados como alto ou superior, dada a proteção do segredo de negócio e da propriedade intelectual.

Todo sistema, ferramenta ou agente de IA deve ser classificado antes de ser adquirido, desenvolvido ou adotado, e reclassificado sempre que houver mudança relevante em suas permissões, integrações ou na informação que acessa. A classificação define os controles e as aprovações obrigatórias.

A classificação resulta do cruzamento de duas dimensões: o tipo de ferramenta, medido pelo grau de autonomia de ação efetivamente concedido, e a classe da informação que a ferramenta acessa, processa ou produz.

Papel da Vunox no Nível Crítico: nos cenários de Nível Crítico, o Pentest é executado pela Vunox, que integra formalmente a alçada de aprovação, assinando a aprovação em conjunto com a Diretoria da empresa controlada. Sem o parecer favorável e a assinatura da Diretoria da Vunox, o sistema Crítico não é aprovado para produção (vide Matriz de Alçadas)

CÓPIA CONTROLADA

5.2 Primeira dimensão - tipo de ferramenta e grau de autonomia

Tipo	Definição	Exemplos
T1 — Assistente	Gera sugestões, textos, análises ou código. Não executa ações em sistemas: toda saída depende de ação humana para produzir efeito.	Chat corporativo de LLM; autocomplete de código; resumo de documentos; apoio à redação e à análise de relatórios.
T2 — Agente supervisionado	Executa ações em escopo delimitado (criar e alterar arquivos, rodar comandos, consultar APIs) mediante aprovação humana por etapa ou revisão obrigatória antes do efeito.	Assistentes de desenvolvimento que criam e alteram arquivos e executam comandos no repositório; automações que produzem entregável submetido a aprovação.
T3 — Agente autônomo	Encadeia ações sem aprovação humana por etapa; interage com APIs, bancos de dados e sistemas de terceiros. A supervisão humana é por exceção ou a posteriori.	Agente de atendimento que consulta e altera registros; agente que executa rotinas em produção; orquestrações multiagente.

Observação: o enquadramento segue a capacidade efetivamente concedida no ambiente, não o nome comercial do produto. Uma mesma ferramenta pode ser T1, T2 ou T3 conforme as permissões, integrações e credenciais que lhe forem atribuídas; na dúvida entre dois tipos, aplica-se o mais restritivo.

CÓPIA CONTROLADA

5.3 Segunda dimensão - classe da informação acessada

As classes de informação e seus critérios são os definidos na Política de Classificação da Informação do Grupo, documento de referência primário para este fim. Esta Política não cria nem redefine classes: apenas determina os controles de IA aplicáveis a cada uma.

A Política de Classificação da Informação deve tratar, de forma integrada, tanto os requisitos da LGPD — dados pessoais e dados pessoais sensíveis — quanto a sensibilidade de negócio, que independe de haver dado pessoal envolvido: contratos, precificação, código-fonte proprietário, dados e evidências técnicas de clientes, resultados de testes de segurança ofensiva e informações estratégicas do Grupo.

Consideram-se informações confidenciais, para fins de uso de ferramentas de Inteligência Artificial, todos os dados que possam causar impactos financeiros, legais, estratégicos, reputacionais ou de privacidade caso sejam divulgados indevidamente. Isso inclui, mas não se limita a:

- Dados pessoais de colaboradores, clientes e terceiros;
- Informações financeiras e contábeis não públicas;

- Contratos, propostas e informações comerciais;
- Planejamento estratégico e projetos internos;
- Propriedade intelectual, metodologias e know-how da empresa;
- Informações de segurança da informação, acessos e vulnerabilidades;
- Denúncias, investigações, auditorias e informações de compliance.

Essas informações somente poderão ser utilizadas em soluções de IA aprovadas pela empresa e que possuam controles adequados de segurança, privacidade e proteção de dados. Quando houver dúvida sobre a classificação da informação, ela deverá ser tratada como confidencial.

Classe da informação	Tratamento nesta Política
Pública / Interna	Uso permitido em ferramentas aprovadas (Anexo A), observadas as regras gerais da Seção 7.
Restrita	Exige ferramenta homologada para a classe, registro de uso e controle de acesso nominal. Inclui, entre outros, dados pessoais não sensíveis, código-fonte proprietário, contratos e informações comerciais.
Confidencial	Exige ferramenta homologada para a classe e aprovação formal prévia. Inclui, entre outros, dados pessoais sensíveis (LGPD, Art. 5º, II), dados e evidências técnicas de clientes, resultados de testes de segurança ofensiva e informações estratégicas do Grupo.

5.4 Matriz de classificação de risco

O nível de risco do sistema, ferramenta ou agente resulta do cruzamento das duas dimensões:

Tipo de ferramenta ↓ / Classe da informação →	Pública / Interna	Restrita	Confidencial
T1 — Assistente	**Baixo**	**Médio**	**● Alto**
T2 — Agente supervisionado	**Médio**	**● Alto**	**● Alto**
T3 — Agente autônomo	**● Alto**	**⛔ Crítico**	**⛔ Crítico**

CÓPIA NÃO CONTROLADA

5.5 Regras de elevação de nível

O nível obtido na matriz é elevado quando presente qualquer das condições abaixo. Em caso de dúvida entre dois níveis, aplica-se sempre o mais restritivo.

- Ação com efeito irreversível ou sem trilha de reversão — nível mínimo Alto; em produção com dados reais de clientes, Crítico.
- Tratamento de dados pessoais sensíveis (LGPD, Art. 5º, II) — nível mínimo Alto.
- Decisões com efeito sobre pessoas — seleção, avaliação, promoção, desligamento, concessão de crédito ou benefício — nível mínimo Alto, observada a Seção 10.
- Operação em ambiente de produção com dados reais de clientes — nível mínimo Alto; se agente autônomo (T3), Crítico.
- Uso cross-empresa entre controladas ou fine-tuning com dados do Grupo — aprovação obrigatória da Holding.
- Ferramentas que tratam código-fonte proprietário e ativos intangíveis
- Ferramenta não constante do Anexo A — uso vedado até aprovação formal, independentemente do nível.

5.6 Controles mínimos

Nível	Controles mínimos
▯ **Baixo**	Registro no Inventário de Sistemas de IA; treinamento básico; revisão humana crítica da saída.
▯ **Médio**	Controles do nível Baixo + DPIA (Anexo C); logs com retenção mínima de 90 dias; acesso por conta nominal; revisão humana definida.
● **Alto**	Controles do nível Médio + ferramenta homologada (5.7); parecer formal do DPO; revisão humana obrigatória; privilégio mínimo com conta própria do agente; testes de prompt injection; guardrails e circuit breaker.
⛔ **Crítico**	Controles do nível Alto + DPA vigente; teste de intrusão; relatório de conformidade; plano de contingência e de descomissionamento documentados.

5.7 Homologação de ferramentas para agentes com informação Confidencial ou Restrita

Agentes supervisionados (T2) e agentes autônomos (T3) que acessem, processem ou produzam informação classificada como Confidencial ou Restrita somente podem operar em ferramentas, modelos e ambientes expressamente homologados pela área de Segurança da Informação do Grupo.

São critérios mínimos de homologação:

CÓPIA CONTROLADA

- Vedação contratual ao uso dos dados do Grupo e de seus clientes para treinamento de modelos;
- Contratação em modalidade corporativa, em conta de titularidade do Grupo — vedado o uso de contas pessoais ou de planos gratuitos com informação Confidencial ou Restrita;
- Isolamento lógico, criptografia em trânsito e em repouso e documentação de residência e transferência internacional de dados (LGPD, Art. 33);
- Registro auditável e exportável de prompts, acessos e ações executadas, com retenção mínima de 90 dias;
- Controle granular de permissões, compatível com o princípio do privilégio mínimo;
- DPA vigente e política de privacidade publicada;
- Capacidade de revogação imediata de acesso e de interrupção da operação do agente.

A relação de ferramentas, modelos e capacidades homologadas, consta do Anexo A, mantido e atualizado pela Segurança da Informação do Grupo com ciência da Diretoria Executiva e do DPO. A atualização do Anexo A não depende de revisão desta Política — a evolução do mercado de ferramentas de IA não deve exigir alteração da norma-mãe a cada novo produto ou versão.

São exemplos de arranjos elegíveis à homologação, a título ilustrativo e sujeitos a avaliação caso a caso: **(a)** modelo executado na infraestrutura do Grupo ou de provedor sob controle contratual do Grupo; **(b)** provedor de IA acessado exclusivamente por conta corporativa em plano Enterprise, com opt-out de treinamento e DPA assinado; **(c)** acesso por API corporativa, com chaves em cofre de segredos e registro centralizado. O enquadramento concreto de cada fornecedor é decidido na homologação, não nesta Política.

5.8 Não-ampliação de privilégio de acesso por IA

> Princípio: sistemas, ferramentas e agentes de IA herdam o perfil de acesso do usuário ou do processo que os aciona. Nenhuma ferramenta de IA pode se sobrepor ao controle de acesso vigente nem dar a um usuário visibilidade sobre informação a que ele não teria acesso pelos meios convencionais.

Decorrem desse princípio as seguintes regras:

- Agentes operam com identidade própria, nominal e rastreável, com privilégio mínimo e escopo temporal definido; é vedado o compartilhamento de credenciais e o uso de contas de serviço com privilégio superior ao do usuário solicitante;
- Bases de conhecimento, arquiteturas RAG e índices vetoriais devem replicar, na camada de recuperação, os controles de acesso do repositório de origem; repositório cujo controle de acesso não possa ser replicado não pode ser indexado;
- É vedado utilizar IA para contornar segregação de funções, need-to-know, controles de prevenção de vazamento ou guardrails de segurança, inclusive por meio de prompts, automações, exportações ou agregação de informações isoladamente acessíveis;
- Toda ação executada por agente é registrada de forma atribuível ao usuário ou processo solicitante;
- A concessão de acesso a um agente segue o mesmo rito de concessão de acesso a pessoas, com revisão periódica e revogação imediata em caso de desligamento, mudança de função ou descomissionamento do agente.

CÓPIA CONTROLADA

A tentativa de obter, por meio de IA, acesso a informação não autorizada, ainda que sem êxito, constitui violação desta Política e da Política de Segurança da Informação, sujeitando o colaborador às penalidades nelas previstas.

5.9 Exemplos de aplicação

Os exemplos abaixo são ilustrativos e não exaustivos; prevalece a classificação formal registrada no Inventário de Sistemas de IA.

Situação	Tipo	Classe	Nível
Chat corporativo usado para redigir comunicado interno	T1	Interna	Baixo
Autocomplete de código com leitura de repositório proprietário	T1	Restrita	● Alto
Assistente de desenvolvimento que cria e altera arquivos e executa comandos sobre repositório proprietário	T2	Restrita	● Alto
Agente de teste em ambiente isolado, sem dados reais e sem credenciais no contexto	T2	Interna	Médio
Relatório ou evidência técnica de teste de intrusão de cliente submetido a ferramenta de IA	T1	Confidencial	● Alto
Agente que consulta e altera registros de clientes em sistema de atendimento em produção	T3	Confidencial	⛔ Crítico

CÓPIA CONTROLADA

5.10 Correspondência com os níveis de permissionamento (Seção 6.3)

Tipo (Seção 5.2)	Nível de permissionamento (Seção 6.3)	Observação
T1 — Assistente	N1 — Consulta / N2 — Produção assistida	N1 para dado público/interno genérico; N2 quando há dado interno de trabalho.
T2 — Agente supervisionado	N3 — Integração de sistemas	Inclui automações, RAG corporativo e assistentes de desenvolvimento com execução.
T3 — Agente autônomo	N4 — Agentes autônomos	Sempre sujeito ao Checklist do Anexo B.

CÓPIA CONTROLADA

6. CONTRATAÇÃO E PERMISSIONAMENTO DE FERRAMENTAS DE IA

Toda ferramenta de IA requer aprovação formal da Diretoria Executiva de cada empresa antes de ser adotada. Ferramentas não listadas no Anexo A são proibidas sem aprovação prévia.

6.1 Processo de Avaliação e Aprovação

Etapa	Ação	Responsável
1. Solicitação	Colaborador ou gestor solicita avaliação com justificativa de negócio.	Solicitante → Diretor da área
2. Avaliação Técnica	TI do Grupo avalia: segurança, DPA, certificações do fornecedor, controles de acesso.	TI do Grupo (suporte técnico)
3. Avaliação Jurídica/Privacidade	DPO avalia conformidade com LGPD, DPA e transferência internacional.	DPO do Grupo e Juridico
4. Decisão e Aprovação	Diretoria Executiva delibera e aprova ou rejeita a ferramenta.	Diretoria Executiva ou pessoa delegada.
5. Parametrização	TI define perfis de acesso, restrições técnicas e logs.	TI do Grupo

6. Inclusão no Anexo A	Ferramenta aprovada entra na lista com permissões formalizadas.	Diretoria Executiva

6.2 Matriz de Alçadas de Aprovação por Nível de Risco

A Matriz de Alçadas define quem aprova e quem se responsabiliza, distribuindo as decisões entre Gerências, Diretorias e Comitê de Tecnologia conforme o caso, e deve ser lida em conjunto com a classificação de risco (Seção 5).

Nível	Aprovação (alçada)	Pareceres obrigatórios	Instância que se responsabiliza	Reporte
▯ **Baixo**	Gestor imediato / Gerência da área	N/A	Gestor da área (Dono do uso)	Registro no inventário
▯ **Médio**	Diretoria Executiva da empresa controlada	DPO (privacidade); TI (segurança)	Diretoria Executiva da controlada	Comitê de Tecnologia (informativo)
● **Alto**	Diretoria executiva da controlada + Comitê de Tecnologia	DPO (parecer formal); TI (Atmis+Vunox) + Jurídico (riscos contratuais e legais)	Diretoria Executiva + Comitê de Tecnologia	Comitê de Tecnologia (deliberativo)
⛔ **Crítico**	Diretoria Executiva da controlada + Diretoria da Vunox + Comitê de Tecnologia	DPO + DPA + Pentest/parecer Vunox (artefato de aprovação)	Diretorias signatárias	Comitê de Tecnologia + Presidência da Imagem Tecnologia

CÓPIA CONTROLADA

6.3 Níveis de Permissionamento — Tipos de Acesso

Nível	Capacidades	Quem Pode Ter	Como Obtém
N1 — Consulta	Chat com dados públicos ou internos genéricos. Sem integração de sistemas.	Todos os colaboradores.	Após módulo de integração de IA (30 dias).
N2 — Produção Assistida	Geração de código, conteúdo, análises com dados internos não sensíveis.	Colaboradores com necessidade justificada.	Solicitação ao Diretor da área. Aprovação do gestor.
N3 — Integração de Sistemas	APIs, automações low-code, RAG com dados corporativos.	Times técnicos com treinamento específico.	Aprovação da Diretoria Executiva + TI do Grupo.
N4 — Agentes Autônomos	Agentes com ações em sistemas externos, dados de clientes.	Times de desenvolvimento.	Aprovação obrigatória da Diretoria Executiva via Checklist (Anexo B).

7. DIRETRIZES DE USO DE IA

7.1 Regras para Todos os Colaboradores

As ferramentas de IA corporativas destinam-se exclusivamente às atividades profissionais do colaborador. O colaborador responde pelo conteúdo que usa, quanto à qualidade, integridade, veracidade e legitimidade.

7.1.1 São Obrigações de todos os Colaboradores:

- Se comprometer, formalmente, ao cumprimento integral de todas as diretrizes, normas, regras e Políticas vigentes estabelecidas pela Empresa;
- Adotar condutas que preservem a integridade, confidencialidade e disponibilidade dos sistemas de IA corporativos e das informações tratadas por eles;
- Utilizar exclusivamente ferramentas de IA constantes da Lista de Ferramentas Aprovadas, requerendo aprovação prévia da Diretoria Executiva para aquisição de qualquer ferramenta não listada;

- Nunca armazenar chaves de API, tokens de acesso, credenciais ou segredos em código-fonte, mensagens, e-mails ou quaisquer meios não protegidos;
- Relatar imediatamente à área de Tecnologia da Informação qualquer comportamento anômalo, falha de segurança, suspeita de vazamento de dados ou acesso não autorizado por sistemas de IA;
- Não instalar, configurar ou integrar ferramentas de IA de terceiros aos sistemas corporativos sem aprovação formal do processo de Aprovação de Novo Sistema de IA (Checklist — Anexo B da desta Política);
- Não utilizar ferramentas de IA externas em ambientes de produção ou que processem dados reais de clientes sem autorização formal da Diretoria Executiva da Empresa Controlada.
- Revisar criticamente conteúdos gerados por IA antes de serem entregues a clientes ou publicados, sendo o COLABORADOR responsável pelo conteúdo que utiliza em seu trabalho, não só quanto à qualidade técnica, mas quanto a integridade e veracidade e legitimidade de todo o conteúdo.
- Comunicar ao seu gestor imediato e à área de TI do Grupo sempre que identificar novas ferramentas, funcionalidades ou práticas de IA que possam ser relevantes para as atividades do Grupo ou que apresentem riscos de segurança, privacidade ou conformidade ainda não mapeados nesta Política.

7.1.2. São expressamente VEDADOS:

- Inserir dados pessoais de clientes, colaboradores ou parceiros em ferramentas de IA externas sem anonimização prévia;
- Inserir informações Confidenciais ou Restritas em ferramentas não homologadas para tal nível;
- Criar deepfakes, desinformação ou conteúdos fraudulentos; contornar guardrails de segurança;
- Compartilhar credenciais de acesso a ferramentas de IA com terceiros não autorizados;
- Aceitar acriticamente saídas de IA sem verificação humana em decisões que afetam pessoas ou negócios;
- Apresentar ou publicar conteúdo gerado com auxílio de Inteligência Artificial como de autoria própria, sem indicar o uso da ferramenta e sem revisão crítica prévia, quando tal conteúdo puder induzir colaboradores, clientes ou terceiros a erro sobre sua origem ou fidedignidade;
- Compartilhar transcrições de conversas, logs de atendimento, históricos de projetos ou outputs de sistemas de IA que contenham dados pessoais de clientes, colaboradores ou

CÓPIA CONTROLADA

terceiros com pessoas, empresas ou sistemas não expressamente autorizados — salvo mediante validação prévia do DPO;

- Utilizar ferramentas de IA para elaborar, auxiliar ou facilitar fraudes, desvios de qualquer natureza, falsificação de documentos, adulteração de registros ou qualquer conduta ilegal ou antiética — independentemente do destinatário ou da finalidade declarada
- Usar sistemas de IA para monitorar, rastrear, gravar ou perfilar, de forma não autorizada, as atividades, comunicações ou comportamentos de outros colaboradores, clientes ou parceiros — inclusive por meio de automações, agentes ou ferramentas de análise de dados;
- Tentar extrair, exportar, copiar ou reproduzir, para uso pessoal ou externo, modelos de IA, pesos de modelos, datasets de treinamento, system prompts proprietários ou qualquer propriedade intelectual relacionada a sistemas de IA desenvolvidos, customizados ou operados pelas empresas
- Usar IA para discriminar com base em raça, gênero, origem, religião, orientação sexual, deficiência ou atributo protegido.

7.2 APIs de LLMs Externos e Automações

- Uso de APIs externas deve ser aprovado pela Diretoria Executiva da empresa controlada, com DPA do fornecedor verificado pelo DPO;
- Dados pessoais ou sensíveis só trafegam em APIs externas para cumprimento de obrigação legal sem anonimização ou com anonimização e validação do tratamento com DPO;
- Chaves de API em cofres de segredos (ex.: HashiCorp Vault, AWS Secrets Manager) — nunca hardcoded;
- Acesso remoto a ferramentas corporativas de IA: MFA obrigatório e VPN ativa em redes públicas.

CÓPIA CONTROLADA

8. DESENVOLVIMENTO, AQUISIÇÃO E OPERAÇÃO DE FERRAMENTAS E AGENTES DE IA

8.1 Papéis e Responsabilidades

Papel	Responsabilidade	Quem Ocupa
Diretoria Executiva Controladas	Aprovação de aquisição e utilização de IA's, todos os agentes, assunção de riscos, governança geral de IA na empresa.	Diretoria Executiva da empresa controlada.
Dono do Agente (Owner)	Define finalidade, aprova casos de uso, responde pelos resultados do agente específico.	Diretor Funcional ou Gestor da área que usa o agente.
Desenvolvimento	Implementação técnica, segurança, testes e documentação.	Desenvolvedor
TI do Grupo	Suporte técnico: avaliação de segurança do ambiente e verificação de logs de segurança destes ambientes. Gestão da lista de IA adquiridas com aprovação da diretoria	Área de TI da Atmis (suporte a todas as controladas).
DPO	Parecer em DPIAs; bases legais; conformidade LGPD para agentes com dados pessoais.	DPO do Grupo.
Monitor do Agente	Monitoramento contínuo em produção: alertas, logs, anomalias.	Desenvolvedor ou Dono do Agente
Todos os colaboradores	Usar IA de forma ética. Não expor dados sensíveis, confidencias e de propriedade intelectual da empresa. Reportar comportamentos anômalos. Cumprir esta Política e o TCRIAU-001 (Anexo G).	Toda a empresa
Fornecedores de IA	Manter Contrato e Compromisso de Confidencialidade válidos. Notificar	Empresas contratadas

	incidentes. Respeitar limites de uso de dados.	

Nota — TI do Grupo o termo "TI do Grupo" é usado de forma genérica e abrange duas frentes complementares: a Atmis (infraestrutura, ambiente, governança de dados e auditoria de conformidade) e a Vunox (segurança da informação, cibersegurança e Pentest, em papel complementar ao da Atmis). Quando a atividade for específica de uma delas, o texto identifica a empresa responsável.

⚠ Ao encerrar vínculo profissional com o criador de um Agente de IA, a empresa permanece responsável integral pelo destino do agente, incluindo a definição de sua continuidade, encerramento seguro e a proteção dos dados nele inseridos.

9. CONFORMIDADE COM A LGPD E SEGURANÇA DA INFORMAÇÃO

i Esta seção é complementar à Política de Segurança da Informação da Empresa, que é o documento de referência primário para controles de segurança. Em caso de conflito entre as políticas, aplica-se a norma mais restritiva.

9.1 Bases Legais e DPIA

Todo tratamento de dados pessoais por sistemas de IA deve ter base legal identificada (LGPD Art. 7º: consentimento, execução de contrato, legítimo interesse ou obrigação legal). DPIA é obrigatório para sistemas classificados como Médio, Alto ou Crítico. O template está no Anexo C.

9.2 Controles Obrigatórios de Privacidade

- Criptografia ou mascaramento de dados em repouso e em trânsito para dados sensíveis processados por IA;
- Segregação de ambientes: dados sensíveis de produção nunca usados em desenvolvimento sem anonimização;
- Contrato de subprocessamento com fornecedores externos que processem dados sensíveis de clientes;
- Avaliação reforçada, pela TI do Grupo, da maturidade de segurança da informação dos fornecedores — em especial os de RH que tratam dados de colaboradores (ex.: Senior) e os que desenvolvem soluções de IA para o Grupo;
- Mecanismos para exercício de direitos dos titulares: acesso, correção, eliminação e oposição (LGPD Arts. 17-22);

- Conteúdo, código, agentes e automações produzidos com ferramentas corporativas de IA são ativos intelectuais do Grupo — o colaborador não possui titularidade exclusiva;

O colaborador é individualmente responsável pela conformidade com a LGPD no âmbito das atividades profissionais que realiza com auxílio de Inteligência Artificial. Nos termos do Art. 42 da Lei 13.709/2018, o agente de tratamento e as pessoas naturais que atuam sob sua autoridade, respondem pelos danos decorrentes do tratamento inadequado de dados pessoais. O desconhecimento desta Política não exime o colaborador dessa responsabilidade, conforme política de privacidade de cada empresa.
Todo colaborador que usa ferramentas de IA deve conhecer e cumprir tanto esta Política quanto a Política de Segurança Informação. O desconhecimento de uma não isenta de responsabilidades pela outra.

10. IA EM RH, MARKETING E COMUNICAÇÃO EXTERNA

Estas áreas envolvem riscos regulatórios e reputacionais específicos. O art. 20 da LGPD veda decisões automatizadas com efeitos jurídicos sobre pessoas sem revisão humana.

- Triagem de candidatos com IA: permitida como auxiliar, com revisão humana obrigatória e transparência ao candidato (LGPD Art. 6º, VI);
- Vedada eliminação automática por atributos protegidos (raça, gênero, idade, deficiência), direta ou via proxies;
- Decisões sobre promoção, rebaixamento ou desligamento exigem decisão final de gestor humano;
- Monitoramento comportamental de colaboradores por IA sem consentimento explícito é proibido;
- Todo sistema de IA em RH é automaticamente risco Médio ou superior — DPIA obrigatório;
- Conteúdo gerado por IA para publicação externa exige revisão e aprovação humana prévia;
- É vedado criar deepfakes, simular depoimentos de clientes ou produzir conteúdo enganoso;

11. GESTÃO DE INCIDENTES DE IA

São considerados incidentes de IA: vazamento de dados por sistema de IA; comportamento inesperado ou perigoso de agente; uso indevido por colaborador; ataque de prompt injection bem-sucedido; decisão automatizada incorreta com impacto sobre titulares; e falha de fornecedor com repercussão nos dados do Grupo.

CÓPIA CONTROLADA

Procedimento de Resposta

Etapa	Ação e Prazo	Responsável
1. Contenção	Desativar ou isolar o sistema afetado imediatamente.	Dono do Agente ou Desenvolvedor
2. Notificação Interna	Acionar Diretoria Executiva, DPO e TI do Grupo em até 2 horas, via chamado formal nomeado como "Incidente".	Dono do Agente ou Desenvolvedor
3. Avaliação de Impacto	Verificar dados pessoais envolvidos e titulares afetados.	Dono do Agente ou Desenvolvedor + DPO
4. Notificação ANPD	Se dados pessoais sensíveis envolvidos: notificar ANPD em até 72h (LGPD Art. 48).	DPO
5. Comunicação a Titulares	Se houver risco relevante: notificar os titulares afetados.	Diretoria Executiva + DPO
6. Causa Raiz e Correção	Documentar, apresentar plano de correção à Diretoria e registrar o incidente.	Dono do Agente ou Desenvolvedor + Qualidade + TI do Grupo

O colaborador que tomar ciência de um incidente de IA, ou de situação que configure risco iminente e não efetuar o reporte imediato nos termos desta Seção poderá ser responsabilizado por omissão culposa, sujeitando-se às penalidades previstas na Seção 12.2, sem prejuízo das responsabilidades civis e criminais aplicáveis.

12. TREINAMENTO, PENALIDADES E VIGÊNCIA

12.1 Treinamento e Conscientização

12.1.1 Cada empresa controlada é responsável por avaliar e decidir, de forma autônoma, quais conhecimentos são necessários para que suas equipes utilizem agentes e ferramentas de IA de maneira segura, ética e em conformidade com a legislação aplicável e esta Política. Nessa avaliação, recomenda-se considerar, entre outros aspectos: as ferramentas e os agentes efetivamente em uso; as funções e os perfis profissionais que interagem com IA; o grau de exposição a dados pessoais e a informações sensíveis; e os riscos específicos da sua atividade.

12.1.2 A partir dessa avaliação, cabe a cada empresa controlada definir o conteúdo, a profundidade, o formato e a periodicidade das ações de capacitação que julgar pertinentes, podendo adotar desde treinamentos formais até abordagens mais rotineiras, materiais de referência, orientações internas, comunicados ou capacitação no próprio fluxo de trabalho.

12.1.3 Recomenda-se que cada empresa controlada mantenha registro da avaliação realizada e das decisões adotadas quanto à capacitação de suas equipes, de modo a demonstrar, quando necessário, que o tema foi devidamente considerado e treinado, em linha com o princípio da utilização consciente da Inteligência Artificial no âmbito de suas atividades.

12.2 Descumprimento e Penalidades

O descumprimento das diretrizes estabelecidas nesta Política poderá resultar em medidas proporcionais à gravidade da infração, incluindo:

i. Advertência formal registrada, ou Notificação extrajudicial, conforme violação;
ii. Suspensão de acesso a ferramentas de IA corporativas;
iii. Processo disciplinar, podendo culminar em rescisão contratual por justa causa, nos termos do art. 482 da CLT;
iv. Responsabilização civil por danos causados a empresa, a clientes ou a terceiros;
v. Responsabilidade criminal, nos termos da LGPD (art. 47 e seguintes), do Código Penal e da legislação aplicável, especialmente em casos de vazamento doloso de dados ou fraude;
vi. Comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e demais órgãos competentes, quando a infração envolver dados pessoais.

12.3 Vigência e Revisão

Esta Política entra em vigor na data de aprovação e tem validade por termo indeterminado, devendo ser revisada: após incidente relevante ou em caso de novas exigências da ANPD.

CÓPIA CONTROLADA

ANEXO A — CHECKLIST DE APROVAÇÃO DE NOVO SISTEMA OU AGENTE DE IA

Verificação	Obrigatório para
☐ **Classificação de risco realizada (Baixo / Médio / Alto / Crítico)**	Todos
☐ **Dono do Agente (Diretor ou Gestor da área) identificado e ciente**	Todos
☐ **Diretoria Executiva informada e aprovação formalmente registrada**	Todos — obrigatório
☐ **Registro no Inventário de Sistemas de IA preenchido**	Todos
☐ **DPIA realizado (template Anexo C)**	Médio, Alto, Crítico
☐ **Bases legais LGPD identificadas e documentadas**	Médio, Alto, Crítico
☐ **DPA com fornecedor de IA externo verificado e assinado**	Quando há fornecedor externo
☐ **Chaves de API em cofre de segredos (não hardcoded)**	N3, N4
☐ **Testes de prompt injection e segurança realizados**	Agentes (todos os níveis)
☐ **System prompts documentados e versionados em repositório**	Agentes (todos os níveis)
☐ **Logs e auditabilidade implementados (retenção mínima 90 dias)**	Todos em produção
☐ **Revisão humana definida para decisões sobre pessoas**	Alto, Crítico
☐ **Escalada humana implementada (agentes de atendimento)**	Agentes de atendimento
☐ **Guardrails de conteúdo configurados**	Agentes e LLMs em produção

☐ **Circuit breaker implementado**	Alto, Crítico
☐ **Plano de contingência documentado**	Alto, Crítico
☐ **Parecer formal do DPO obtido**	Alto, Crítico
☐ **Aprovação da Holding obrigatória para risco Crítico cross-empresa ou fine-tuning com dados do Grupo**	Quando aplicável
☐ **Plano de descomissionamento documentado**	Todos em produção

ANEXO B — TEMPLATE DE DPIA SIMPLIFICADO PARA SISTEMAS DE IA

Campo	Orientação de Preenchimento
1. Identificação do Sistema	Nome, versão, Dono do Agente (Diretor/Gestor responsável)
2. Descrição e Finalidade	O que o sistema faz, qual problema resolve e qual é a finalidade específica do tratamento de dados.
3. Dados Pessoais Tratados	Tipos (nome, CPF, saúde, financeiros etc.), origem, volume estimado e titulares afetados.
4. Base Legal (LGPD Art. 7º)	Qual base legal fundamenta o tratamento. Se consentimento: como é obtido e como pode ser revogado.
5. Necessidade e Proporcionalidade	Justificativa de que os dados tratados são os mínimos necessários para a finalidade declarada.
6. Nível de Risco	Classificação: Baixo / Médio / Alto / Crítico — com justificativa.
7. Riscos à Privacidade	Vazamento, acesso indevido, decisão discriminatória, re-identificação etc.
8. Medidas de Mitigação	Para cada risco: medida técnica e/ou organizacional e responsável pela implementação.
9. Transferência Internacional	Há envio de dados fora do Brasil? País, base legal (LGPD Art. 33), medidas de proteção.

10. Direitos dos Titulares	Como exercer acesso, correção, eliminação, portabilidade e oposição ao tratamento automatizado.
11. Parecer do DPO	Aprovado / Aprovado com ressalvas / Não aprovado — justificativa obrigatória.
12. Data e Próxima Revisão	Data de emissão. Próxima revisão: máximo 1 ano ou após mudança relevante.

CÓPIA CONTROLADA