CONSELHO REGIONAL DE CONTABILIDADE DO PARANÁ

RESOLUÇÃO CRCPR Nº 899, DE 30 DE OUTUBRO DE 2026.

Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no CRCPR.

O Plenário do **CONSELHO REGIONAL DE CONTABILIDADE DO PARANÁ (CRCPR)**, no uso de suas atribuições legais e regimentais,

CONSIDERANDO o acelerado desenvolvimento de tecnologias de inteligência artificial, notadamente por meio de algoritmos que utilizam grandes modelos de linguagem, os quais são capazes de interagir com usuários e oferecer soluções geradas automaticamente;

CONSIDERANDO a imprescindibilidade de regulamentação específica para o emprego de técnicas de inteligência artificial generativa no âmbito do CRCPR, com plena transparência e publicidade, de modo a assegurar que sua utilização esteja em consonância com valores éticos fundamentais, incluindo dignidade humana, respeito aos direitos humanos, não discriminação, devido processo, devida motivação e fundamentação da prestação da atividade fiscalizatória, prestação de contas e responsabilização;

CONSIDERANDO os preceitos contidos no Projeto de Lei nº 2.338/2023, que dispõe sobre o desenvolvimento, a implementação e o uso responsável de sistemas de Inteligência Artificial no Brasil;

CONSIDERANDO os preceitos contidos na Resolução CNJ nº 615, de 11 de março de 2025, que estabelece diretrizes para o desenvolvimento, utilização, auditoria e governança de soluções de Inteligência Artificial;

CONSIDERANDO as diretrizes constantes do Guia Unificado de Inteligência Artificial para o Setor Público e dos referenciais de governança de Inteligência Artificial da Administração Pública Federal;

CONSIDERANDO as recomendações do Tribunal de Contas da União relativas à utilização segura de ferramentas de Inteligência Artificial Generativa na Administração Pública;

CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO a necessidade de assegurar a proteção de dados pessoais, a segurança da informação, a mitigação de riscos e a supervisão humana nos processos apoiados por Inteligência Artificial;

CONSIDERANDO a Resolução CFC nº 1.783/2025, que estabelece a Política de Governança no âmbito do Sistema CFC/CRCs;

RESOLVE:

Art. 1º - Aprovar a Política de Inteligência Artificial (IA), com a finalidade de estabelecer princípios, diretrizes, responsabilidades e mecanismos de governança para utilização de sistemas de Inteligência Artificial no âmbito do Conselho Regional de Contabilidade do Paraná, nos termos do Anexo desta Resolução.

Art. 2º - Esta Resolução entrará em vigor na data de sua publicação.

Contador **EVERSON LUIZ BREDA CARLIN**

CO - CRCPR Nº 29.607/O

Presidente

ALBERTO BARBOSA

CO – CRCPR Nº 31.006/O

ANGELITA ROZA

CO – CRCPR Nº 64.278/O

ANTONIO MOACIR POZZOBON

CO – CRCPR Nº 20.423/O

ARIANE YUMI DE ALMEIDA ROCHA

CO - CRCPR Nº 40.667/O

CAROLINA ARAUJO DOS SANTOS FEIJÓ

CO – CRCPR Nº 69033/O

CESAR SOARES ZANIN

CO – CRCPR Nº 33.601/O

DANILO ALVES GRANI

CO – CRCPR Nº 56.387/O

EUNICE MARIA CAVALI DUARTE

CO – CRCPR Nº 34.322/O

FERNANDO ANTONIO BORAZO RIBEIRO

CO - CRCPR Nº 32.263/O

GERVALDO RODRIGUES CAMPOS

CO - CRCPR Nº 31.135/O

GISELE MARTINS MACHIOSKI

CO - CRCPR Nº 53.810/O

GLICÉRIO RAMPAZZO

CO – CRCPR Nº 35.574/O

IVONEL DOMBROSKI

CO - CRCPR Nº 67.529/O

JEFFERSON PAULO MARTINS

CO - CRCPR Nº 35.401/O

JÚLIO RICARDO MORONA

CO – CRCPR Nº 48.431/O

MARCIA OGIDO HOKAMA

CO - CRCPR Nº 34.399/O

MARCIO JOSÉ ASSUMPÇÃO

CO – CRCPR Nº 36.207/O

MICHEL GULIN MELHEM

CO – CRCPR Nº 64.351/O

NELINHO KUKLA

CO - CRCPR Nº 50.194/O

RAFAEL ANTÔNIO DE LORENZO

CO - CRCPR Nº 41.346/O

RODINEI BONFADINI

CO - CRCPR Nº 42.621/O

ROSEMERE KIYOMI HAYASHI

CO – CRCPR Nº 35.176/O

RUBENS RICARDO POLIDO

CO - CRCPR Nº 49.198/O

SÉRGIO AUGUSTO DA PORCIÚNCULA JÚNIOR

CO - CRCRS Nº 69.409/O – TPR

SIMONE VANNI SOARES

CO - CRCPR Nº 36.620/O

TÂNIA TEREZINHA DOBROVOLSKI

TC - CRCPR Nº 51.649/O

Aprovada na 1434ª Reunião Plenária de 2026, realizada em 30 de outubro de 2026.

Documento assinado eletronicamente por **Rafael Antonio de Lorenzo**, **Conselheiro**, em 30/10/2026, às 07:53, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Danilo Alves Grani**, **Vice-Presidente**, em 30/10/2026, às 08:01, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Angelita Roza**, **Conselheira**, em 30/10/2026, às 08:08, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Ariane Yumi de Almeida Rocha**, **Vice-Presidente**, em 30/10/2026, às 08:17, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Gisele Martins Machioski**, **Conselheira**, em 30/10/2026, às 08:18, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Julio Ricardo Morona**, **Conselheiro**, em 30/10/2026, às 08:20, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcio José Assumpção**, **Conselheiro**, em 30/10/2026, às 08:22, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Cesar Soares Zanin**, **Conselheiro**, em 30/10/2026, às 08:27, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Simone Vanni Soares**, **Conselheiro**, em 30/10/2026, às 08:35, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Carolina Araujo Dos Santos Feijó**, **Conselheira**, em 30/10/2026, às 08:38, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcia Ogido Hokama**, **Conselheira**, em 30/10/2026, às 08:47, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Rosemere Kiyomi Hayashi**, **Vice-Presidente**, em 30/10/2026, às 08:48, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Rodinei Bonfadini**, **Vice-Presidente**, em 30/10/2026, às 09:03, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Sérgio Augusto da Porciúncula Júnior**, **Conselheiro**, em 30/10/2026, às 09:05, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Michel Gulin Melhem**, **Vice-Presidente**, em 30/10/2026, às 09:06, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Nelinho Kukla**, **Conselheiro**, em 30/10/2026, às 09:08, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Glicerio Rampazzo**, **Conselheiro**, em 30/10/2026, às 09:09, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Eunice Maria Cavali Duarte**, **Conselheira**, em 30/10/2026, às 09:09, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Fernando Antonio Borazo Ribeiro**, **Conselheiro**, em 30/10/2026, às 09:12, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Ivonel Dombroski**, **Conselheiro Suplente**, em 30/10/2026, às 09:13, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Tânia Terezinha Dobrovolski**, **Conselheira Suplente**, em 30/10/2026, às 09:14, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Rubens Ricardo Polido**, **Conselheiro**, em 30/10/2026, às 09:17, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Gervaldo Rodrigues Campos**, **Conselheiro**, em 30/10/2026, às 09:18, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Antonio Moacir Pozzobon**, **Conselheiro**, em 30/10/2026, às 09:19, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Alberto Barbosa**, **Conselheiro**, em 30/10/2026, às 10:00, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Jefferson Paulo Martins**, **Vice-Presidente**, em 30/10/2026, às 10:52, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Everson Luiz Breda Carlin**, **Presidente**, em 30/10/2026, às 12:43, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1613144** e o código CRC **D45E1F4B**.

ANEXO

POLÍTICA DE INTELIGÊNCIA ARTIFICIAL DO CRCPR

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Política de Inteligência Artificial estabelece os princípios, as diretrizes, as responsabilidades e os mecanismos de governança, gestão de riscos e controles aplicáveis ao desenvolvimento, à aquisição, à contratação, à implementação e ao uso de soluções de Inteligência Artificial – IA no âmbito do Conselho Regional de Contabilidade do Paraná – CRCPR.

§ 1º A utilização de Inteligência Artificial no CRCPR deverá observar a legislação e as regulamentações aplicáveis, os normativos do CFC e os atos normativos internos do Conselho, especialmente aqueles relacionados à governança, gestão de riscos, integridade, proteção de dados pessoais, segurança da informação, transparência, gestão documental e contratações.

§ 2º A utilização de soluções de Inteligência Artificial deverá estar alinhada à missão institucional, ao planejamento estratégico, à geração de valor público e ao interesse público, observadas as competências legais e regimentais do CRCPR.

Artigo 2º - Esta Política aplica-se:

I – aos conselheiros, empregados, estagiários, terceirizados, prestadores de serviços, colaboradores e demais pessoas que, no exercício de suas atividades ou por força de vínculo com o CRCPR, utilizem, desenvolvam, administrem ou tenham acesso a soluções de Inteligência Artificial institucionais;

II – às soluções de Inteligência Artificial desenvolvidas, adquiridas, contratadas, disponibilizadas ou utilizadas pelo CRCPR, independentemente de sua modalidade tecnológica ou de seu local de processamento;

III – aos processos, atividades e serviços administrativos, fiscalizatórios, educacionais, institucionais, de atendimento ao público e demais atividades relacionadas às competências do CRCPR;

IV – aos dados, informações, documentos, conteúdos e demais ativos informacionais utilizados como entrada, processados ou produzidos por soluções de Inteligência Artificial no âmbito institucional; e

V – às soluções de Inteligência Artificial de terceiros utilizadas no exercício das atividades institucionais, inclusive aquelas disponibilizadas como serviço ou por meio de plataformas em nuvem.

Parágrafo único. A utilização de ferramentas de Inteligência Artificial de uso público ou particular para tratamento de informações institucionais deverá observar esta Política, os normativos de segurança da informação, proteção de dados pessoais e demais regras internas aplicáveis.

Artigo 3º - Para os fins desta Política, considera-se:

I – Inteligência Artificial – IA: sistema computacional que, a partir de diferentes níveis de autonomia e para objetivos explícitos ou implícitos, é capaz de processar dados e produzir resultados, tais como previsões, recomendações, classificações, conteúdos ou outros resultados que possam influenciar ambientes físicos ou virtuais;

II – Inteligência Artificial Generativa – IA Generativa: sistema de Inteligência Artificial destinado a gerar, a partir de dados de entrada, novos conteúdos, tais como textos, imagens, áudios, vídeos, códigos, documentos ou outras modalidades de conteúdo;

III – Solução de Inteligência Artificial: sistema, aplicação, ferramenta, modelo, serviço ou recurso tecnológico que utilize técnicas ou modelos de Inteligência Artificial para executar, apoiar ou automatizar atividades, processos ou tarefas;

IV – Usuário: pessoa que utilize solução de Inteligência Artificial no exercício de atividades institucionais do CRCPR, independentemente da modalidade de acesso ou disponibilização da ferramenta, observadas as autorizações, restrições, atribuições e responsabilidades estabelecidas nesta Política e nos demais normativos aplicáveis;

V – Supervisão Humana: acompanhamento, análise, avaliação e, quando aplicável, validação ou revisão realizados por pessoa competente sobre os resultados produzidos ou apoiados por uma solução de Inteligência Artificial, especialmente quando possam produzir efeitos relevantes sobre pessoas, processos ou decisões institucionais;

VI – Dados Pessoais: informação relacionada a pessoa natural identificada ou identificável, nos termos da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD;

VII – 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, dados referentes à

saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural, nos termos da LGPD;

VIII – Tratamento de Dados Pessoais: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

IX – Sistema de IA de Alto Risco: solução de Inteligência Artificial cuja utilização, em razão de sua finalidade, contexto, grau de autonomia, natureza dos dados tratados ou potencial de impacto sobre pessoas, direitos, serviços ou atividades institucionais, possa representar riscos relevantes e, por isso, esteja sujeita a controles adicionais definidos nesta Política e em seus instrumentos complementares;

X – Avaliação de Impacto: processo sistemático destinado a identificar, avaliar e tratar riscos decorrentes do desenvolvimento ou uso de uma solução de Inteligência Artificial, considerando, conforme aplicável, aspectos jurídicos, éticos, operacionais, tecnológicos, de segurança da informação e de proteção de dados pessoais;

XI – Relatório de Impacto à Proteção de Dados Pessoais – RIPD: documentação que descreve os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como as medidas, salvaguardas e mecanismos destinados a mitigar esses riscos, nos termos da LGPD e da regulamentação aplicável;

XII – Risco de IA: possibilidade de ocorrência de evento decorrente do desenvolvimento, aquisição, implantação ou utilização de uma solução de Inteligência Artificial capaz de produzir efeitos adversos sobre pessoas, dados, informações, processos, serviços, recursos, conformidade, reputação ou objetivos institucionais;

XIII – Fornecedor de IA: pessoa física ou jurídica, pública ou privada, responsável pelo desenvolvimento, fornecimento, disponibilização, manutenção ou suporte de solução de Inteligência Artificial utilizada pelo CRCPR.

XIV – Ferramenta de IA de Uso Geral: solução de Inteligência Artificial disponibilizada para utilização em diferentes atividades e finalidades, tais como elaboração de textos, pesquisas, análises, geração de conteúdos e apoio a tarefas administrativas, sem desenvolvimento específico para o CRCPR; e

XV – Solução Institucional de IA: solução de Inteligência Artificial desenvolvida, adquirida, contratada, integrada ou formalmente disponibilizada pelo CRCPR para utilização em seus processos, atividades e serviços institucionais.

CAPÍTULO II
DOS OBJETIVOS

Artigo 4º - Esta Política tem por objetivo estabelecer diretrizes para a governança, o desenvolvimento, a aquisição, a contratação, a implementação, a utilização e o monitoramento de soluções de Inteligência Artificial no âmbito do Conselho Regional de Contabilidade do Paraná – CRCPR, visando promover a inovação responsável, de forma ética, segura, transparente e orientada à geração de valor público, em consonância com os princípios da Administração Pública, o planejamento estratégico, a governança institucional, a transformação digital, a proteção de dados pessoais, a segurança da informação, a gestão de riscos e a integridade.

§ 1º A utilização de Inteligência Artificial deverá estar alinhada às competências legais e regimentais do CRCPR e contribuir para o aperfeiçoamento dos processos de trabalho, a melhoria da prestação dos serviços, o fortalecimento da capacidade institucional e a geração de benefícios para a sociedade, os profissionais da contabilidade e as demais partes interessadas.

§ 2º Constituem objetivos específicos desta Política:

I – promover o uso ético, responsável, seguro, confiável e juridicamente adequado da Inteligência Artificial, em conformidade com a legislação vigente, os direitos fundamentais, os princípios da Administração Pública, as boas práticas de governança e os valores institucionais do CRCPR;

II – ampliar a eficiência, a qualidade, a celeridade e a efetividade dos processos e serviços institucionais, mediante a utilização planejada de soluções de Inteligência Artificial que apoiem a automação de atividades, a análise de informações, a gestão do conhecimento e a tomada de decisões baseada em evidências;

III – fortalecer a governança digital, a inovação e a transformação organizacional, promovendo a adoção de tecnologias de Inteligência Artificial de forma planejada, controlada, sustentável e alinhada ao planejamento estratégico e aos objetivos institucionais do CRCPR;

IV – assegurar a proteção dos dados pessoais, das informações institucionais e dos demais ativos de informação, mediante observância da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD, da regulamentação aplicável da Agência Nacional de Proteção de Dados – ANPD e dos normativos internos de proteção de dados e segurança da informação;

V – assegurar níveis adequados de transparência, rastreabilidade, auditabilidade e prestação de contas na utilização de soluções de Inteligência Artificial, de modo a possibilitar o acompanhamento, o controle, a avaliação dos resultados e a responsabilização dos agentes competentes;

VI – garantir que as soluções de Inteligência Artificial sejam utilizadas como instrumentos de apoio às atividades institucionais, preservando a supervisão humana e a competência decisória dos agentes responsáveis, especialmente nos processos que possam produzir efeitos relevantes sobre direitos, interesses ou obrigações de pessoas físicas ou jurídicas;

VII – promover a identificação, avaliação, tratamento, monitoramento e comunicação dos riscos associados à utilização da Inteligência Artificial, considerando, entre outros, riscos tecnológicos, operacionais, jurídicos, de conformidade, de segurança da informação, de proteção de dados pessoais, reputacionais, financeiros e relacionados à confiabilidade dos resultados;

VIII – prevenir e mitigar vieses, discriminações, erros, alucinações, resultados inadequados ou não confiáveis produzidos ou apoiados por soluções de Inteligência Artificial, mediante adoção de controles proporcionais aos riscos e à finalidade de cada solução;

IX – incentivar a utilização de soluções de Inteligência Artificial que apresentem, quando tecnicamente aplicável, transparência, explicabilidade, confiabilidade, proporcionalidade, segurança, robustez e possibilidade de auditoria, observados os limites decorrentes de segredo comercial, propriedade intelectual, segurança institucional e demais hipóteses legais de restrição de acesso;

X – assegurar que a utilização de Inteligência Artificial em processos administrativos, fiscalizatórios, disciplinares, sancionadores ou em outros processos que possam produzir efeitos relevantes não resulte na transferência da responsabilidade decisória para sistemas automatizados, permanecendo a decisão sob responsabilidade do agente competente;

XI – promover a capacitação contínua de conselheiros, empregados, estagiários, terceirizados, prestadores de serviços e demais usuários autorizados, de acordo com suas respectivas atribuições, quanto ao uso seguro, crítico, ético e responsável da Inteligência Artificial;

XII – estabelecer mecanismos para a avaliação prévia e classificação dos riscos das soluções de Inteligência Artificial, especialmente aquelas que envolvam dados pessoais, informações sigilosas, atividades fiscalizatórias, decisões institucionais ou impactos relevantes sobre pessoas e organizações;

XIII – promover a integração da governança de Inteligência Artificial com os mecanismos institucionais de gestão de riscos, controles internos, integridade, proteção de dados, segurança da informação, governança de dados, auditoria e prestação de contas;

XIV – assegurar que a contratação ou utilização de soluções de Inteligência Artificial fornecidas por terceiros observe requisitos adequados de segurança da informação, proteção de dados pessoais, confidencialidade, transparência, rastreabilidade, continuidade, reversibilidade, auditoria e responsabilização, conforme a legislação e os normativos aplicáveis; ainda, garantir que os requisitos relacionados abaixo, constem no Estudo Técnico Preliminar e no Termo de referência: Vedação de uso dos dados para treinamento; Localização dos dados; Acordo de tratamento de dados (DPA); Prazo de notificação de incidentes; Devolução dos dados ao fim do contrato.

XV – estimular o desenvolvimento de uma cultura institucional de inovação responsável, orientada pela ética, pela conformidade, pela segurança, pela transparência, pela proteção dos direitos fundamentais e pela geração de benefícios concretos para o CRCPR e para a sociedade; e

XVI – assegurar a melhoria contínua das soluções de Inteligência Artificial utilizadas pelo CRCPR, mediante monitoramento periódico de seu desempenho, riscos, resultados, impactos e conformidade com esta Política e com a legislação aplicável.

§ 3º A consecução dos objetivos previstos neste artigo deverá observar a proporcionalidade entre os benefícios esperados e os riscos associados à utilização da Inteligência Artificial, considerando a finalidade, o contexto de utilização, a natureza dos dados tratados, o grau de autonomia, a relevância da atividade apoiada e os impactos potenciais de cada solução.

§ 4º A adoção de solução de Inteligência Artificial deverá ser precedida, quando aplicável, de avaliação quanto à sua necessidade, adequação, viabilidade, riscos, impactos e compatibilidade com os objetivos institucionais, não sendo recomendada sua utilização quando os riscos identificados superarem os benefícios esperados ou quando houver alternativa menos arriscada capaz de alcançar o mesmo objetivo.

CAPÍTULO III
DOS PRINCÍPIOS

Artigo 5º - A governança, o desenvolvimento, a aquisição, a contratação, a implementação e a utilização de soluções de Inteligência Artificial no âmbito do Conselho Regional de Contabilidade do Paraná – CRCPR observarão os princípios da Administração Pública, os direitos e garantias fundamentais e os seguintes princípios específicos:

I – legalidade e conformidade, com observância da Constituição Federal, da legislação e da regulamentação aplicáveis, dos normativos do CFC e dos atos normativos internos do CRCPR;

II – interesse público e geração de valor público, orientando a utilização da Inteligência Artificial para o cumprimento da missão institucional, o fortalecimento das competências legais do CRCPR, a melhoria dos serviços prestados e a geração de benefícios para a sociedade, os profissionais da contabilidade e as demais partes interessadas;

III – ética e integridade, assegurando que a Inteligência Artificial seja utilizada de forma responsável, íntegra, imparcial e compatível com os valores institucionais, com os padrões de conduta e com os princípios éticos aplicáveis;

IV – transparência, promovendo, de forma proporcional aos riscos e à finalidade da solução, informações claras e acessíveis sobre a utilização da Inteligência Artificial, suas finalidades, limitações, responsabilidades e, quando aplicável, seus impactos, observados os direitos à privacidade, os sigilos legais, a segurança da informação, a propriedade intelectual e as demais hipóteses legais de restrição de acesso;

V – explicabilidade e inteligibilidade, buscando assegurar que os resultados produzidos ou apoiados por soluções de Inteligência Artificial possam ser compreendidos e adequadamente avaliados pelos responsáveis, em nível compatível com a finalidade, a complexidade, o grau de risco e a tecnologia empregada;

VI – segurança da informação, mediante a adoção de medidas técnicas, administrativas e organizacionais destinadas à proteção da confidencialidade, integridade, disponibilidade e autenticidade das informações e à prevenção, detecção e resposta a incidentes de segurança;

VII – proteção da privacidade e dos dados pessoais, assegurando o tratamento adequado dos dados pessoais e dos dados pessoais sensíveis, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD, com a regulamentação da Agência Nacional de Proteção de Dados – ANPD e com os normativos institucionais aplicáveis;

VIII – não discriminação, equidade e mitigação de vieses, buscando prevenir resultados discriminatórios, injustificados ou incompatíveis com os direitos e garantias fundamentais, mediante identificação, avaliação

e tratamento dos riscos de vieses associados às soluções de Inteligência Artificial;

IX – supervisão humana, assegurando que as soluções de Inteligência Artificial sejam utilizadas como instrumentos de apoio às atividades institucionais, preservando a capacidade de análise, avaliação crítica, revisão e decisão pelos agentes competentes, especialmente quando estiverem envolvidos direitos, interesses ou obrigações de pessoas físicas ou jurídicas;

X – responsabilização e prestação de contas, assegurando a definição clara de responsabilidades pelos processos, resultados, decisões e atos praticados com apoio de Inteligência Artificial, bem como a adoção de mecanismos de registro, monitoramento, controle e prestação de contas;

XI – gestão de riscos e precaução, determinando que os riscos associados à utilização da Inteligência Artificial sejam identificados, avaliados, tratados, monitorados e comunicados de forma contínua, adotando-se medidas proporcionais ao potencial de impacto da solução;

XII – confiabilidade, qualidade e robustez, buscando assegurar que as soluções de Inteligência Artificial sejam adequadas às finalidades para as quais foram adotadas, apresentem desempenho compatível com os requisitos estabelecidos e sejam submetidas a testes, validações e monitoramento proporcionais aos riscos envolvidos;

XIII – inovação responsável, incentivando a adoção de soluções tecnológicas capazes de contribuir para a modernização, a transformação digital e o aperfeiçoamento institucional, sem afastar os requisitos de governança, conformidade, segurança, proteção de dados e gestão de riscos;

XIV – proporcionalidade e adequação, assegurando que a utilização de Inteligência Artificial seja compatível com a finalidade pretendida e que os controles aplicados sejam proporcionais à natureza, à complexidade, ao grau de autonomia e aos riscos e impactos potenciais da solução;

XV – eficiência e melhoria contínua, promovendo a utilização responsável dos recursos disponíveis, o aperfeiçoamento dos processos de trabalho, a melhoria da qualidade dos serviços e a avaliação contínua dos resultados obtidos; e

XVI – sustentabilidade e responsabilidade institucional, buscando assegurar que a adoção de soluções de Inteligência Artificial considere, sempre que pertinente, sua sustentabilidade tecnológica, econômica, operacional e ambiental, bem como seus impactos sobre a capacidade institucional de longo prazo.

Parágrafo único. A aplicação dos princípios previstos neste artigo deverá considerar a natureza, a finalidade, o contexto de utilização, o grau de autonomia, os dados tratados, o potencial de impacto e o nível de risco de cada solução de Inteligência Artificial, observando-se a proporcionalidade entre os benefícios esperados e os riscos associados à sua utilização.

CAPÍTULO IV
DOS USOS PERMITIDOS

Artigo 6º - A utilização de soluções de Inteligência Artificial no âmbito do Conselho Regional de Contabilidade do Paraná – CRCPR é permitida para apoiar o desempenho de atividades administrativas, técnicas, operacionais, educacionais, fiscalizatórias e gerenciais, desde que compatível com as competências institucionais e observados os princípios, diretrizes, responsabilidades, controles e requisitos estabelecidos nesta Política, na legislação e regulamentação aplicáveis e nos normativos institucionais.

§ 1º A utilização de soluções de Inteligência Artificial poderá ocorrer, entre outras finalidades compatíveis com as atribuições institucionais do CRCPR, para:

I – apoiar a elaboração, revisão, consolidação, padronização e aperfeiçoamento de documentos administrativos, ofícios, comunicações, relatórios, apresentações e demais documentos institucionais, mediante revisão pelo responsável;

II – auxiliar na realização de pesquisas técnicas, normativas, doutrinárias, jurisprudenciais e administrativas, bem como na localização, organização, comparação e sistematização de informações relevantes para as atividades institucionais, observada a necessidade de verificação da atualidade, autenticidade e confiabilidade das fontes;

III – apoiar a elaboração de minutas, estudos, análises preliminares, resumos, consolidações e sistematizações de informações, sem substituir a análise técnica e a responsabilidade do agente competente;

IV – realizar a organização, classificação, categorização, indexação e recuperação de informações e documentos, observados os requisitos de segurança da informação, gestão documental e proteção de dados pessoais;

V – automatizar tarefas repetitivas, operacionais ou de baixo risco, visando à melhoria da eficiência, produtividade, qualidade e padronização dos processos de trabalho;

VI – apoiar atividades de fiscalização profissional, inclusive mediante identificação de padrões, inconsistências, indícios de risco, priorização de ações fiscalizatórias e análise de grandes volumes de informações, vedada a utilização dos resultados da IA como fundamento exclusivo para a adoção de medidas que possam produzir efeitos relevantes sobre fiscalizados ou terceiros, devendo ser assegurada análise e decisão por agente competente;

VII – apoiar análises de dados institucionais, geração de indicadores, identificação de tendências, avaliação de cenários, gestão de riscos e produção de informações destinadas a subsidiar o planejamento e a tomada de decisão;

VIII – auxiliar na elaboração de relatórios gerenciais, painéis de acompanhamento, estudos estatísticos e instrumentos de monitoramento e avaliação institucional;

IX – apoiar ações de educação profissional continuada, capacitação, produção e revisão de conteúdos educacionais, curadoria de conhecimento e disseminação de informações técnicas;

X – apoiar atividades de atendimento ao usuário, inclusive mediante assistentes virtuais e outros recursos de automação, desde que sejam observados requisitos de transparência, qualidade, acessibilidade, proteção de dados pessoais, segurança da informação e possibilidade de encaminhamento para atendimento humano;

XI – apoiar atividades de governança, planejamento estratégico, gestão documental, gestão do conhecimento, auditoria, controle interno, integridade, conformidade e gestão de riscos;

XII – apoiar iniciativas de inovação, transformação digital e modernização dos processos e serviços prestados pelo CRCPR; e

XIII – apoiar atividades de análise e produção de informações para subsidiar a avaliação de políticas, programas, projetos e resultados institucionais, observados os requisitos de governança e validação humana.

§ 2º A utilização de Inteligência Artificial deverá ser adequada à finalidade pretendida e proporcional ao nível de risco, considerando, entre outros aspectos, a natureza da atividade, o grau de autonomia da solução, os dados tratados, a possibilidade de impacto sobre pessoas físicas ou jurídicas e a relevância dos resultados para a tomada de decisão institucional.

§ 3º Os resultados, análises, recomendações, classificações, previsões ou conteúdos produzidos por soluções de Inteligência Artificial deverão ser considerados instrumentos de apoio, não constituindo, por si sós, manifestação institucional definitiva, prova conclusiva ou fundamento suficiente para a prática de atos que dependam de análise ou decisão de agente competente.

§ 4º A utilização de resultado produzido ou apoiado por Inteligência Artificial em manifestação oficial, decisão administrativa, ato fiscalizatório, parecer técnico, comunicação institucional, orientação ao usuário ou documento destinado à produção de efeitos jurídicos deverá ser precedida de análise crítica, verificação de consistência, validação e aprovação pelo agente competente, conforme a natureza do ato.

§ 5º A responsabilidade pelo conteúdo, pelas informações, análises, conclusões, manifestações e decisões decorrentes da utilização de Inteligência Artificial permanecerá com o agente ou unidade competente, não sendo transferida ao sistema, ao modelo de IA ou ao fornecedor da solução.

§ 6º A utilização de Inteligência Artificial não poderá resultar na transferência ou delegação indevida de competências legais, regimentais ou institucionais atribuídas aos empregados, gestores, conselheiros, fiscais, comissões ou órgãos deliberativos do CRCPR, devendo ser preservada a supervisão humana efetiva e compatível com o risco da atividade.

§ 7º Sempre que tecnicamente possível e proporcional aos riscos e à finalidade da solução, deverão ser adotados mecanismos destinados a assegurar a rastreabilidade, auditabilidade, registro, integridade e recuperação das informações relacionadas à utilização da Inteligência Artificial, observados os requisitos de segurança da informação, proteção de dados pessoais e gestão documental.

§ 8º A utilização de solução de Inteligência Artificial que envolva dados pessoais, dados pessoais sensíveis, informações sigilosas, informações classificadas ou outros ativos de informação protegidos deverá observar os requisitos específicos estabelecidos nesta Política e nos normativos institucionais aplicáveis, inclusive quanto à autorização, segurança, finalidade, necessidade e controle de acesso.

§ 9º A utilização de solução de Inteligência Artificial por empregado, conselheiro, estagiário, terceirizado, prestador de serviço ou outro usuário autorizado, ainda que realizada por meio de ferramenta disponibilizada gratuitamente ou em conta pessoal, não afasta a aplicação desta Política quando houver utilização para fins institucionais ou tratamento de informações do CRCPR.

CAPÍTULO V
DOS USOS VEDADOS

Artigo 7º - É vedada a utilização de soluções de Inteligência Artificial no âmbito do Conselho Regional de Contabilidade do Paraná – CRCPR quando incompatível com a legislação e a regulamentação aplicáveis, com os princípios da Administração Pública, com os direitos e garantias fundamentais, com a Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD, com as normas de segurança da informação e com os princípios, diretrizes e controles estabelecidos nesta Política.

§ 1º É vedado aos usuários:

I – inserir, compartilhar, processar, armazenar ou submeter, em plataformas públicas, abertas, não homologadas ou não autorizadas pelo CRCPR, informações classificadas como sigilosas, restritas, confidenciais ou protegidas por dever legal ou contratual de sigilo; Quando houver necessidade de utilização de solução de Inteligência Artificial não constante no catálogo de ferramentas homologadas pelo CRCPR, o usuário deverá formalizar solicitação à Divisão de Tecnologia da Informação e Comunicação (TIC), ficando sua utilização condicionada à conclusão do processo de avaliação e homologação institucional.

O processo de homologação deverá observar, no mínimo, as seguintes etapas:

a) TIC faz a análise técnica e de segurança;

b) DPO avalia a LGPD e a transferência internacional;

c) Assessoria Jurídica analisa os termos contratuais;

d) Comitê de Tecnologia e Segurança da Informação aprova.

II – inserir ou submeter a soluções de Inteligência Artificial dados pessoais, dados pessoais sensíveis, informações de processos administrativos não públicos ou outras informações protegidas por sigilo legal, quando inexistente fundamento jurídico, autorização ou controle institucional adequado para o respectivo tratamento;

III – utilizar soluções de Inteligência Artificial para tomada de decisão exclusivamente automatizada em processos disciplinares, fiscalizatórios, sancionadores, de gestão de pessoas ou em outros procedimentos capazes de produzir efeitos relevantes sobre direitos, interesses ou obrigações de pessoas físicas ou jurídicas;

IV – utilizar soluções de Inteligência Artificial para produzir, disseminar ou validar deliberadamente informações falsas, fraudulentas, enganosas ou manipuladas, ou para conferir aparência de autenticidade a conteúdos que não tenham sido devidamente verificados;

V – utilizar soluções, ferramentas, aplicações, plataformas ou serviços de Inteligência Artificial não homologados ou autorizados pelo CRCPR, quando a homologação ou autorização for exigida pelos procedimentos institucionais aplicáveis;

VI – utilizar Inteligência Artificial para produzir ou disseminar conteúdos que violem a legislação, os direitos autorais, a propriedade intelectual, os direitos da personalidade, as normas éticas, os regulamentos institucionais ou as obrigações contratuais assumidas pelo CRCPR;

VII – utilizar Inteligência Artificial para promover, induzir ou apoiar práticas discriminatórias ou que possam resultar em tratamento desigual, injustificado ou incompatível com os direitos e garantias fundamentais;

VIII – utilizar resultados produzidos por Inteligência Artificial como informação definitiva, sem a necessária verificação de precisão, consistência, atualidade, fonte, contexto e adequação à finalidade pretendida, especialmente quando o resultado puder influenciar decisões ou atos institucionais;

IX – atribuir à Inteligência Artificial a responsabilidade por análises, pareceres, manifestações técnicas, atos administrativos ou decisões que dependam de julgamento humano, conhecimento especializado ou competência legalmente atribuída a agente, comissão, unidade do CRCPR;

X – utilizar soluções de Inteligência Artificial com a finalidade de contornar, desabilitar ou comprometer controles internos, mecanismos de segurança, regras de acesso, procedimentos de auditoria ou mecanismos de governança estabelecidos pelo CRCPR;

XI – utilizar Inteligência Artificial para gerar, promover ou disseminar conteúdos ofensivos, difamatórios, discriminatórios, assediadores, fraudulentos ou incompatíveis com os princípios de ética, integridade, respeito e dignidade que orientam a atuação institucional;

XII – utilizar Inteligência Artificial para realizar monitoramento, perfilamento, classificação ou avaliação de pessoas de forma incompatível com a legislação aplicável, com a finalidade do tratamento, com os direitos dos titulares ou com os princípios da necessidade, adequação, finalidade, transparência e proporcionalidade;

XIII – utilizar soluções de Inteligência Artificial para realizar tratamento de dados pessoais em finalidade incompatível com aquela que fundamentou sua coleta ou utilização, ou com a base legal aplicável;

XIV – utilizar soluções de Inteligência Artificial para gerar ou alterar documentos, registros, evidências ou informações institucionais com a finalidade de ocultar, modificar ou comprometer sua autenticidade, integridade, rastreabilidade ou valor probatório;

XV – utilizar conteúdo produzido por Inteligência Artificial como se fosse manifestação, parecer, decisão ou posicionamento oficial do CRCPR sem a devida revisão, validação e aprovação pelo agente ou unidade competente; e

XVI – utilizar soluções de Inteligência Artificial em desacordo com as regras de segurança da informação, proteção de dados pessoais, gestão documental, propriedade intelectual, ética, integridade ou demais normativos internos aplicáveis.

§ 2º É vedada a substituição integral da atuação humana em atividades que, em razão da legislação, da natureza ou do impacto da matéria, exijam avaliação técnica especializada, interpretação normativa, juízo de valor, deliberação institucional ou tomada de decisão por agente ou unidade competente.

§ 3º A utilização de Inteligência Artificial não afasta nem reduz a responsabilidade dos usuários, gestores, unidades, comissões ou órgãos competentes quanto à legalidade, legitimidade, veracidade, integridade, fundamentação e adequação dos atos praticados com apoio da tecnologia.

§ 4º Identificados riscos relevantes ou incidentes relacionados à proteção de dados pessoais, à segurança da informação, aos direitos dos titulares, à confiabilidade ou à integridade dos resultados produzidos por solução de Inteligência Artificial, sua utilização deverá ser imediatamente comunicada à unidade competente e, quando necessário, suspensa ou restringida, até que sejam adotadas as medidas de contenção, avaliação e correção cabíveis.

§ 5º A suspensão prevista no § 4º deverá observar a natureza e a gravidade do risco, podendo ser total ou parcial, sem prejuízo da preservação dos registros e evidências necessários à investigação, auditoria, responsabilização e melhoria dos controles.

§ 6º O descumprimento das disposições deste artigo sujeitará o responsável às medidas administrativas, disciplinares, contratuais e legais cabíveis, observados o devido processo, o contraditório e a ampla defesa, quando aplicáveis, sem prejuízo das responsabilidades civil, administrativa e penal previstas na legislação.

CAPÍTULO VI
DA PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Artigo 8º - O tratamento de dados pessoais realizado por meio de soluções de Inteligência Artificial deverá observar a Constituição Federal, a Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD, a regulamentação aplicável, as políticas e normas internas do CRCPR relacionadas à proteção de dados pessoais, privacidade, segurança da informação e governança de dados.

§ 1º O tratamento de dados pessoais por soluções de Inteligência Artificial deverá observar, conforme aplicável, os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas, previstos na LGPD, devendo a utilização dessas soluções observar, no mínimo:

I – a existência de finalidade legítima, específica e compatível com as atribuições institucionais e com o tratamento realizado;

II – a utilização da base legal adequada ao tratamento dos dados pessoais, conforme a natureza da atividade e as disposições da LGPD;

III – a limitação do tratamento aos dados necessários e pertinentes ao atendimento da finalidade pretendida;

IV – a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

V – a garantia, sempre que aplicável, dos direitos dos titulares de dados pessoais previstos na LGPD;

VI – a manutenção da qualidade, exatidão, clareza e atualização dos dados utilizados, especialmente quando os resultados produzidos pela solução puderem influenciar atividades ou decisões institucionais;

VII – a adoção de medidas destinadas a prevenir tratamentos discriminatórios ou incompatíveis com os direitos e garantias fundamentais; e

VIII – a documentação e demonstração das medidas adotadas para assegurar a conformidade do tratamento com a legislação e os normativos institucionais aplicáveis.

§ 2º A utilização de soluções de Inteligência Artificial deverá observar os princípios de privacidade desde a concepção (privacy by design) e privacidade por padrão (privacy by default), sempre que tecnicamente aplicáveis e compatíveis com a natureza e finalidade da solução.

§ 3º O tratamento de dados pessoais deverá restringir-se ao mínimo necessário para a realização de suas finalidades, sendo vedada a coleta, utilização, retenção ou compartilhamento de dados excessivos, incompatíveis ou desnecessários.

§ 4º Antes da implementação ou utilização de solução de Inteligência Artificial que envolva tratamento de dados pessoais, deverão ser avaliados, de forma proporcional à natureza, finalidade e risco da solução, os impactos relacionados à privacidade, proteção de dados pessoais, segurança da informação, direitos dos titulares e conformidade legal.

§ 5º Quando o tratamento puder resultar em alto risco aos direitos e liberdades dos titulares, deverá ser avaliada a necessidade de elaboração ou atualização de Relatório de Impacto à Proteção de Dados Pessoais – RIPD, sem prejuízo de outras avaliações ou instrumentos de gestão de riscos exigidos pelo CRCPR ou pela legislação aplicável.

§ 6º As soluções institucionais de Inteligência Artificial utilizadas pelo CRCPR deverão, sempre que tecnicamente possível e proporcional ao risco, possibilitar a identificação dos dados tratados, o registro das operações relevantes, a rastreabilidade das atividades e a realização de auditoria e controle; em caso de soluções contratadas, o cumprimento desse levantamento de informações se dará por exigência contratual ao fornecedor.

Art. 9º Sempre que tecnicamente possível, adequado e proporcional à finalidade do tratamento, deverão ser adotadas medidas destinadas a reduzir os riscos à privacidade, à proteção de dados pessoais e à segurança da informação.

§ 1º Na concepção, desenvolvimento, aquisição ou utilização de soluções de Inteligência Artificial, deverão ser consideradas, conforme a finalidade e a necessidade do tratamento:

I – a utilização de dados anonimizados quando a finalidade puder ser alcançada sem a identificação dos titulares;

II – a pseudonimização ou outras técnicas de redução de identificabilidade quando a utilização de dados pessoais identificáveis não for necessária à finalidade pretendida;

III – a utilização de ambientes computacionais protegidos, homologados ou autorizados pelo CRCPR;

IV – a utilização de bases de dados avaliadas quanto à qualidade, integridade, confiabilidade, origem e conformidade jurídica;

V – mecanismos de controle de acesso, autenticação, criptografia, registro de eventos, monitoramento e demais controles de segurança compatíveis com a natureza e o nível de risco das informações tratadas; e

VI – mecanismos destinados à eliminação, anonimização ou descarte seguro dos dados quando cessada a necessidade de sua utilização, observadas as obrigações legais e institucionais de retenção.

§ 2º A utilização de plataformas ou serviços externos de Inteligência Artificial que envolvam tratamento de dados ou informações institucionais deverá ser precedida de avaliação quanto, no mínimo:

I – às condições de segurança e confidencialidade;

II – à finalidade e às condições de tratamento dos dados;

III – à existência de mecanismos de retenção, exclusão e descarte das informações;

IV – à possibilidade de utilização dos dados fornecidos para treinamento ou aperfeiçoamento dos modelos;

V – à localização e às condições de transferência internacional de dados, quando aplicável;

VI – às responsabilidades do fornecedor e do CRCPR;

VII – às condições de auditoria, rastreabilidade e resposta a incidentes; e

VIII – aos requisitos contratuais, legais e regulatórios aplicáveis.

§ 3º É vedada a utilização de dados pessoais ou informações institucionais para treinamento, aperfeiçoamento ou alimentação de modelos de Inteligência Artificial de terceiros quando essa utilização não estiver autorizada pelo CRCPR ou não estiver amparada por fundamento jurídico, contratual e institucional adequado.

§ 4º A autorização prevista no § 3º não dispensa a avaliação dos riscos relacionados à proteção de dados pessoais, segurança da informação, confidencialidade, propriedade intelectual e demais ativos informacionais envolvidos.

§ 5º Os usuários deverão adotar as medidas de segurança e proteção estabelecidas pelo CRCPR para prevenir acesso não autorizado, uso indevido, alteração, perda, destruição, divulgação ou qualquer outra forma de comprometimento dos dados e informações utilizados em soluções de Inteligência Artificial.

§ 6º A ocorrência ou suspeita de incidente de segurança envolvendo dados pessoais ou informações institucionais no contexto da utilização de Inteligência Artificial deverá ser comunicada imediatamente às

unidades competentes, observados os procedimentos institucionais de gestão de incidentes de segurança da informação e proteção de dados pessoais.

CAPÍTULO VII
DA SEGURANÇA DA INFORMAÇÃO

Artigo 10º - A utilização, o desenvolvimento, a aquisição, a contratação, a implementação, a operação, a alteração e a descontinuidade de soluções de Inteligência Artificial no âmbito do Conselho Regional de Contabilidade do Paraná – CRCPR deverão observar processo de governança e gestão de riscos, integrado ao modelo institucional de governança, gestão de riscos, integridade, segurança da informação e proteção de dados pessoais.

§ 1º A gestão de riscos deverá ocorrer durante todo o ciclo de vida da solução de Inteligência Artificial, desde sua concepção ou contratação até sua descontinuidade, considerando a natureza, a finalidade, o contexto de utilização, o grau de autonomia, os dados tratados, a criticidade e os potenciais impactos da solução.

§ 2º A avaliação de riscos deverá considerar, no mínimo, quando aplicável:

I – riscos relacionados à segurança da informação, incluindo acesso não autorizado, vazamento, perda, alteração ou comprometimento da confidencialidade, integridade, disponibilidade e autenticidade das informações;

II – riscos relacionados à proteção de dados pessoais e à privacidade dos titulares;

III – riscos de indisponibilidade, interrupção ou comprometimento da continuidade dos serviços, processos e atividades institucionais que dependam da solução;

IV – riscos de desconformidade com a legislação, regulamentação, normas técnicas, contratos, políticas institucionais e demais requisitos aplicáveis;

V – riscos relacionados à reputação, à credibilidade e à confiança da sociedade e das partes interessadas no CRCPR;

VI – riscos decorrentes de erros, imprecisões, resultados não confiáveis, informações falsas ou inadequadas, limitações técnicas, alucinações de modelos e vieses algorítmicos;

VII – riscos relacionados à dependência tecnológica, à concentração de fornecedores, à descontinuidade de serviços e à utilização de ambientes ou serviços externos;

VIII – riscos relacionados à qualidade, origem, integridade e representatividade dos dados utilizados no desenvolvimento, treinamento, validação ou operação da solução;

IX – riscos relacionados à propriedade intelectual, aos direitos autorais, ao sigilo profissional e à utilização indevida de informações protegidas; e

X – potenciais impactos sobre direitos, interesses legítimos, segurança, igualdade e demais direitos fundamentais de profissionais da contabilidade, cidadãos, empregados, colaboradores e demais partes interessadas.

§ 3º As soluções de Inteligência Artificial deverão ser classificadas conforme níveis de risco e criticidade definidos em metodologia institucional, considerando, entre outros fatores:

I – a finalidade e a relevância da solução para as atividades institucionais;

II – o grau de autonomia da solução;

III – a natureza e a sensibilidade dos dados tratados;

IV – o potencial de impacto sobre direitos, interesses ou obrigações de pessoas físicas ou jurídicas;

V – a possibilidade de utilização dos resultados para fundamentar decisões administrativas ou fiscalizatórias;

VI – o impacto potencial sobre a continuidade dos serviços; e

VII – a extensão dos impactos decorrentes de falhas, erros ou uso indevido da solução.

§ 4º O nível de risco e criticidade da solução deverá determinar, de forma proporcional, os requisitos de:

I – avaliação e aprovação;

II – supervisão humana;

III – segurança da informação;

IV – proteção de dados pessoais;

V – testes e validação;

VI – documentação e rastreabilidade;

VII – monitoramento;

VIII – auditoria; e

IX – revisão ou reavaliação da solução.

§ 5º A identificação de risco elevado ou inaceitável deverá ensejar a adoção de medidas de mitigação, restrição, suspensão ou não utilização da solução, conforme a natureza e a gravidade do risco, antes de sua implantação ou continuidade.

§ 6º Quando os riscos identificados não puderem ser adequadamente tratados ou permanecerem incompatíveis com a finalidade institucional, os benefícios esperados ou os requisitos legais aplicáveis, a solução não deverá ser implantada ou deverá ter sua utilização descontinuada.

§ 7º A avaliação de riscos deverá ser revisada periodicamente e sempre que ocorrer alteração relevante na finalidade, tecnologia, modelo, fornecedor, dados tratados, ambiente de utilização ou contexto operacional da solução, bem como quando forem identificados incidentes ou alterações significativas em seu perfil de risco.

§ 8º O CRCPR deverá manter, conforme definido em regulamentação interna, registro atualizado das soluções de Inteligência Artificial utilizadas institucionalmente, contendo informações suficientes para sua identificação, classificação, responsabilização, monitoramento e controle.

Artigo 11º - O acesso às soluções, plataformas e ferramentas de Inteligência Artificial utilizadas pelo CRCPR deverá observar os princípios do menor privilégio, necessidade de acesso, segregação de funções, rastreabilidade e responsabilização, em conformidade com as normas institucionais de segurança da informação.

§ 1º Os acessos deverão ser concedidos de acordo com as atribuições e necessidades funcionais dos usuários, observados os respectivos níveis de autorização.

§ 2º As soluções deverão utilizar mecanismos de autenticação e controle de acesso compatíveis com seu nível de risco e criticidade, sempre que tecnicamente aplicável.

§ 3º Deverão ser mantidos registros de auditoria (*logs*) das soluções institucionais suficientes para permitir a rastreabilidade das operações relevantes, observados os requisitos legais e institucionais de proteção de dados pessoais; em caso de soluções contratadas, a manutenção desses registros se dará por exigência contratual ao fornecedor.

§ 4º Os registros de auditoria deverão ser protegidos contra alteração, exclusão, acesso ou utilização não autorizados e mantidos pelo período definido nos normativos institucionais aplicáveis.

§ 5º Os registros poderão contemplar, conforme a natureza e o risco da solução:

I – identificação do usuário ou serviço responsável;

II – data e horário das operações;

III – operações relevantes realizadas;

IV – alterações de configuração ou permissões;

V – eventos de segurança;

VI – incidentes e falhas; e

VII – demais informações necessárias à auditoria e à rastreabilidade.

§ 6º O monitoramento da utilização das soluções de Inteligência Artificial poderá ser realizado pelas áreas competentes do CRCPR, exclusivamente para finalidades legítimas relacionadas à segurança, conformidade, gestão de riscos, proteção dos ativos institucionais e adequada utilização dos recursos tecnológicos, observada a legislação aplicável.

§ 7º A identificação de uso indevido, acesso não autorizado, vulnerabilidade, incidente de segurança ou descumprimento desta Política deverá ser comunicada imediatamente às áreas competentes, conforme os procedimentos institucionais estabelecidos.

§ 8º As soluções de Inteligência Artificial deverão dispor, sempre que tecnicamente possível e proporcional ao risco, de mecanismos de auditoria, rastreabilidade, monitoramento, registro e verificação de conformidade.

CAPÍTULO VIII
DA SUPERVISÃO HUMANA

Artigo 12º - A utilização de soluções de Inteligência Artificial no âmbito do Conselho Regional de Contabilidade do Paraná – CRCPR deverá ocorrer sob **supervisão humana efetiva, adequada e proporcional** à finalidade, à complexidade, ao grau de autonomia, ao potencial de impacto e ao nível de risco da atividade desenvolvida.

§ 1º A supervisão humana deverá assegurar que o agente responsável possua competência, autoridade e informações suficientes para compreender, avaliar e, quando necessário, corrigir, rejeitar, restringir ou interromper a utilização dos resultados produzidos pela solução de Inteligência Artificial.

§ 2º Nenhuma decisão institucional, manifestação técnica, ato administrativo, procedimento fiscalizatório, deliberação ou outra atividade capaz de produzir efeitos relevantes sobre direitos, interesses ou obrigações de pessoas físicas ou jurídicas poderá ser fundamentada exclusivamente em resultados, recomendações, inferências, classificações ou conteúdos produzidos por solução de Inteligência Artificial.

§ 3º As soluções de Inteligência Artificial deverão atuar como instrumentos de apoio às atividades institucionais, cabendo aos agentes legalmente competentes realizar a análise crítica, a validação dos resultados e a tomada da decisão final, quando aplicável.

§ 4º A intensidade e a forma de supervisão humana deverão ser definidas de acordo com o nível de risco da solução, podendo compreender, conforme o caso:

I – supervisão prévia, mediante análise e validação dos resultados antes de sua utilização;

II – supervisão durante a execução da atividade, mediante acompanhamento do funcionamento e dos resultados produzidos;

III – supervisão posterior, mediante revisão, auditoria e avaliação dos resultados e impactos; ou

IV – combinação das modalidades previstas nos incisos anteriores.

§ 5º A supervisão humana deverá abranger, quando aplicável:

I – a avaliação da adequação da solução à finalidade institucional pretendida;

II – a verificação da qualidade, consistência, confiabilidade, atualidade e pertinência dos resultados produzidos;

III – a identificação de erros, inconsistências, imprecisões, alucinações, vieses ou outras limitações da solução;

IV – a avaliação dos impactos relacionados à proteção de dados pessoais, à segurança da informação, à equidade e aos direitos e interesses dos envolvidos;

V – a revisão e validação dos conteúdos, análises, recomendações ou classificações produzidas pela solução;

VI – a possibilidade de rejeição ou desconsideração dos resultados produzidos pela Inteligência Artificial; e

VII – a adoção de medidas para interromper ou restringir a utilização da solução quando identificados riscos incompatíveis com sua finalidade ou nível de autorização.

§ 6º A utilização de Inteligência Artificial não afasta, reduz ou transfere a responsabilidade funcional, técnica, administrativa ou institucional dos agentes competentes pelas atividades desempenhadas e pelas decisões adotadas.

Artigo 13º - Caberá ao responsável pelo processo, atividade ou decisão apoiada por solução de Inteligência Artificial, observadas suas atribuições e competências:

I – verificar a consistência, confiabilidade, pertinência e adequação dos resultados produzidos em relação à finalidade pretendida;

II – validar as informações, análises, recomendações, classificações e conteúdos produzidos pela Inteligência Artificial antes de sua utilização, divulgação ou incorporação a documentos ou processos institucionais, quando aplicável;

III – identificar, corrigir ou determinar a correção de erros, inconsistências, vieses, distorções ou informações inadequadas produzidas pela solução;

IV – confrontar, quando necessário, os resultados produzidos pela Inteligência Artificial com fontes oficiais, normativas, técnicas, jurídicas ou outras fontes confiáveis;

V – assegurar que a utilização da solução observe esta Política e os demais normativos institucionais aplicáveis;

VI – rejeitar ou impedir a utilização de resultados quando houver dúvida relevante quanto à sua precisão, confiabilidade, segurança, legalidade ou adequação à finalidade pretendida;

VII – comunicar às áreas competentes falhas, incidentes, vulnerabilidades, comportamentos inadequados ou riscos identificados;

VIII – assegurar a observância das normas de proteção de dados pessoais, segurança da informação e classificação da informação;

IX – manter, quando exigido pelo nível de risco ou pelos procedimentos institucionais, registros das validações, revisões, intervenções e decisões realizadas com apoio da Inteligência Artificial; e

X – responder, no âmbito de suas atribuições, pelas conclusões, manifestações, análises e decisões decorrentes da atividade desempenhada.

Parágrafo único. Os resultados produzidos por soluções de Inteligência Artificial constituem subsídios para a atuação institucional e não substituem o conhecimento técnico, o julgamento profissional, a interpretação normativa, a avaliação de mérito ou a decisão dos agentes legalmente competentes.

CAPÍTULO IX
DA GOVERNANÇA DA INTELIGÊNCIA ARTIFICIAL

Artigo 14º - Compete ao Comitê de Tecnologia e Segurança da Informação – CTI, sem prejuízo das competências atribuídas à Alta Administração e às demais unidades organizacionais do CRCPR, coordenar, orientar, acompanhar e propor diretrizes relacionadas à governança da Inteligência Artificial no âmbito institucional.

§ 1º A atuação do CTI deverá observar, entre outros, os princípios da legalidade, interesse público, ética, integridade, transparência, segurança da informação, proteção de dados pessoais, gestão de riscos, inovação responsável, responsabilização e prestação de contas.

§ 2º Compete ao Comitê de Tecnologia e Segurança da Informação – CTI, no âmbito de suas atribuições:

I – acompanhar a implementação e a efetividade desta Política, promovendo o alinhamento das iniciativas de Inteligência Artificial aos objetivos estratégicos e às diretrizes institucionais;

II – propor padrões, diretrizes, critérios, procedimentos e controles para a utilização, desenvolvimento, aquisição, contratação, implementação, monitoramento e descontinuidade de soluções de Inteligência Artificial;

III – acompanhar a identificação, avaliação, tratamento e monitoramento dos riscos relacionados à utilização de Inteligência Artificial, observada a metodologia institucional de gestão de riscos;

IV – propor critérios para classificação das soluções de Inteligência Artificial segundo seu nível de risco e criticidade;

V – acompanhar a adoção dos controles proporcionais ao nível de risco e criticidade das soluções;

VI – avaliar, no âmbito de suas competências, riscos, oportunidades, impactos e benefícios decorrentes da adoção de soluções de Inteligência Artificial;

VII – acompanhar indicadores de desempenho, utilização, segurança, confiabilidade, conformidade e efetividade das soluções de Inteligência Artificial;

VIII – propor o aperfeiçoamento desta Política e de seus instrumentos complementares, considerando alterações legislativas e regulamentares, evolução tecnológica, riscos emergentes, boas práticas e necessidades institucionais;

IX – promover a integração entre as áreas responsáveis por tecnologia da informação, segurança da informação, proteção de dados pessoais, gestão de riscos, governança, integridade, fiscalização, gestão e demais áreas relacionadas ao tema;

X – acompanhar, no âmbito de suas competências, incidentes, vulnerabilidades, riscos emergentes e eventos relevantes relacionados à utilização de Inteligência Artificial, propondo medidas preventivas ou corretivas;

XI – fomentar a utilização ética, segura, responsável e eficiente da Inteligência Artificial no âmbito do CRCPR;

XII – propor ações de capacitação, conscientização e desenvolvimento de competências relacionadas ao uso crítico, ético e seguro da Inteligência Artificial;

XIII – acompanhar a evolução da legislação, regulamentação, normas técnicas e boas práticas nacionais e internacionais relacionadas à Inteligência Artificial e propor as adequações institucionais necessárias;

XIV – propor orientações, procedimentos, manuais, padrões técnicos e demais instrumentos necessários à implementação desta Política; e

XV – exercer outras competências relacionadas à governança da Inteligência Artificial que lhe sejam atribuídas pelos normativos institucionais.

§ 3º O exercício das competências previstas neste artigo não implica transferência ou substituição das atribuições legal ou regimentalmente conferidas às demais unidades organizacionais do CRCPR.

§ 4º As decisões que envolvam matéria de competência da Alta Administração, dos órgãos deliberativos ou de outras instâncias institucionais deverão ser submetidas à autoridade ou órgão competente, na forma dos normativos internos.

§ 5º O CTI poderá solicitar às unidades organizacionais do CRCPR informações, estudos, avaliações técnicas, jurídicas, de segurança da informação, proteção de dados ou gestão de riscos necessários ao exercício de suas competências.

Artigo 15º - A Presidência do CRCPR poderá instituir, mediante proposta do Comitê de Tecnologia e Segurança da Informação (CTI), **Grupo de Trabalho de Inteligência Artificial**, de caráter permanente ou temporário, para subsidiar estudos, avaliações, implementação e aperfeiçoamento das iniciativas relacionadas à utilização da tecnologia no CRCPR.

§ 1º O Grupo de Trabalho poderá ser composto por representantes das áreas de tecnologia da informação, segurança da informação, proteção de dados pessoais, gestão de riscos, governança, integridade, jurídico, fiscalização, gestão de pessoas e demais unidades cuja participação seja pertinente à matéria.

§ 2º Compete ao Grupo de Trabalho, conforme ato de sua instituição:

I – realizar estudos técnicos e institucionais sobre a utilização de Inteligência Artificial;

II – apoiar a elaboração de procedimentos, padrões, guias, manuais e orientações;

III – subsidiar a avaliação de riscos, impactos, oportunidades e benefícios;

IV – acompanhar a evolução tecnológica, normativa e regulatória relacionada à Inteligência Artificial;

V – propor ações de capacitação e conscientização;

VI – elaborar estudos, relatórios e recomendações para subsidiar o CTI e as demais instâncias competentes; e

VII – exercer outras atividades que lhe sejam atribuídas no ato de sua instituição.

§ 3º O Grupo de Trabalho não terá competência para substituir as atribuições das unidades organizacionais ou das instâncias decisórias estabelecidas nos normativos institucionais.

§ 4º A criação do Grupo de Trabalho não transfere ao grupo a responsabilidade pela execução dos processos ou pela tomada de decisões que competem às unidades responsáveis.

CAPÍTULO X
DA GESTÃO DE RISCOS

Artigo 16º - As soluções de Inteligência Artificial utilizadas, desenvolvidas, adquiridas, contratadas, customizadas ou disponibilizadas no âmbito do Conselho Regional de Contabilidade do Paraná – CRCPR deverão ser submetidas à identificação, avaliação, tratamento, monitoramento e revisão dos riscos, de forma proporcional à sua finalidade, contexto de utilização, grau de autonomia, natureza dos dados e informações tratados, criticidade, potencial de impacto e consequências decorrentes de falhas, uso indevido ou resultados inadequados.

§ 1º A gestão de riscos de Inteligência Artificial deverá integrar-se à metodologia institucional de gestão de riscos do CRCPR e observar, no que couber, os processos de governança, segurança da informação, proteção de dados pessoais, integridade, continuidade de negócios e controle interno.

§ 2º A classificação de risco tem por finalidade estabelecer controles proporcionais ao nível de risco e criticidade da solução, orientando os processos de avaliação, autorização, implementação, supervisão humana, monitoramento, auditoria, revisão e eventual descontinuidade.

Artigo 17º Para fins desta Política, as soluções de Inteligência Artificial serão classificadas, conforme metodologia institucional, em **baixo, médio, alto ou extremo**, considerando, no mínimo:

I – a finalidade e o contexto de utilização da solução;

II – o grau de autonomia da solução e sua capacidade de produzir ou recomendar resultados;

III – a natureza, quantidade, sensibilidade e criticidade dos dados e informações tratados;

IV – o potencial de impacto sobre direitos, interesses, obrigações ou expectativas legítimas de pessoas físicas ou jurídicas;

V – a utilização dos resultados para subsidiar decisões administrativas, fiscalizatórias, disciplinares ou sancionatórias;

VI – os impactos potenciais sobre a continuidade, segurança, eficiência e reputação institucional;

VII – a possibilidade e a efetividade da intervenção humana;

VIII – a dependência de fornecedores, modelos, plataformas ou serviços externos;

IX – a possibilidade de ocorrência de discriminação, vieses, erros sistemáticos ou resultados inadequados; e

X – a magnitude dos danos potenciais decorrentes de falhas, uso indevido ou funcionamento inadequado da solução.

I – Soluções de Baixo Risco

§ 1º Consideram-se de **baixo risco** as soluções destinadas predominantemente ao apoio de atividades acessórias, operacionais ou administrativas, cujo funcionamento não apresente potencial relevante de produzir efeitos sobre direitos, obrigações ou interesses de pessoas físicas ou jurídicas.

§ 2º Podem enquadrar-se nessa categoria, entre outras:

I – pesquisas e consultas de informações públicas;

II – apoio à elaboração, revisão e aperfeiçoamento textual;

III – organização, classificação e indexação de documentos;

IV – apoio à gestão do conhecimento;

V – automação de tarefas administrativas de baixa complexidade; e

VI – consolidação ou sumarização de informações sem caráter decisório.

§ 3º As soluções de baixo risco estarão sujeitas aos controles básicos de segurança da informação, proteção de dados pessoais, supervisão humana e conformidade estabelecidos nesta Política e nos normativos institucionais aplicáveis.

II – Soluções de Risco Médio

§ 4º Consideram-se de **risco médio** as soluções que apoiem processos institucionais relevantes, realizem análises ou tratamento de informações significativas ou possam influenciar atividades administrativas, sem produzir, de forma autônoma, efeitos relevantes sobre direitos, obrigações ou interesses de terceiros.

§ 5º Podem enquadrar-se nessa categoria, entre outras:

I – análise de dados institucionais;

II – geração de relatórios analíticos e gerenciais;

III – identificação de padrões, tendências ou inconsistências;

IV – apoio ao planejamento institucional e à gestão de riscos;

V – apoio à tomada de decisão administrativa, desde que preservada a decisão humana;

VI – sistemas de atendimento assistido ao usuário; e

VII – soluções de apoio às atividades fiscalizatórias que não determinem ou produzam autonomamente atos ou efeitos sobre terceiros.

§ 6º As soluções de risco médio deverão ser submetidas, previamente à sua utilização, à avaliação de riscos, à definição de finalidade e responsabilidades e à implementação de mecanismos de monitoramento e supervisão compatíveis com o nível de risco identificado.

III – Soluções de Alto Risco

§ 7º Consideram-se de **alto risco** as soluções cuja utilização possa produzir impactos relevantes sobre direitos, interesses ou obrigações de pessoas físicas ou jurídicas, sobre atividades fiscalizatórias ou sancionatórias, sobre dados pessoais ou informações de elevada criticidade, ou sobre processos institucionais essenciais.

§ 8º Podem enquadrar-se nessa categoria, entre outras:

I – soluções que realizem tratamento de dados pessoais sensíveis em contexto de elevado impacto ou risco;

II – soluções cujos resultados possam influenciar significativamente direitos, obrigações ou interesses de pessoas físicas ou jurídicas;

III – soluções utilizadas como apoio relevante a processos fiscalizatórios, disciplinares ou sancionadores;

IV – soluções utilizadas para classificação, priorização, avaliação ou recomendação que possam produzir impactos significativos sobre terceiros;

V – soluções que tratem informações estratégicas, confidenciais, sigilosas ou de elevada criticidade institucional;

VI – soluções cuja falha, indisponibilidade ou funcionamento inadequado possa comprometer significativamente a continuidade de atividades, a segurança ou a reputação do CRCPR; e

VII – soluções cuja complexidade, autonomia ou opacidade dificulte significativamente a compreensão, validação ou contestação de seus resultados.

§ 9º A utilização de soluções classificadas como de alto risco deverá ser precedida de avaliação específica de riscos e impactos, contemplando, conforme aplicável:

I – riscos à proteção de dados pessoais e à privacidade;

II – riscos à segurança da informação;

III – impactos operacionais, institucionais e reputacionais;

IV – avaliação da qualidade e confiabilidade dos dados utilizados;

V – identificação e mitigação de vieses, discriminações, erros e resultados inadequados;

VI – definição de mecanismos de supervisão humana reforçada;

VII – definição de mecanismos de rastreabilidade e auditabilidade;

VIII – procedimentos de monitoramento e revisão periódica; e

IX – medidas de prevenção, mitigação e resposta aos riscos identificados.

IV – Soluções de Risco Extremo

§ 10. Consideram-se de **risco extremo** as soluções cujo funcionamento, utilização ou resultados possam representar risco incompatível com os princípios desta Política, produzir impactos graves sobre direitos fundamentais, comprometer significativamente a atuação institucional ou envolver grau de autonomia incompatível com a supervisão humana exigida.

§ 11. A utilização de solução classificada como de risco crítico dependerá de avaliação específica e de aprovação pela instância competente, podendo ser restringida, condicionada ou vedada, conforme a natureza dos riscos identificados e a legislação aplicável.

§ 12. A classificação de risco extremo deverá ser objeto de análise específica quanto à necessidade, proporcionalidade e efetiva possibilidade de utilização segura da solução, devendo prevalecer a alternativa que ofereça menor risco para o alcance da finalidade institucional.

CAPÍTULO XI
DA TRANSPARÊNCIA

Artigo 18º - O CRCPR promoverá a transparência, a rastreabilidade e a prestação de contas relacionadas à utilização institucional de soluções de Inteligência Artificial, observados a legislação aplicável, o direito de acesso à informação, a proteção de dados pessoais, a segurança da informação, os deveres de sigilo e as demais hipóteses legais de restrição de acesso.

§ 1º A transparência deverá ser promovida de forma clara, acessível, proporcional à finalidade e ao nível de risco da solução, permitindo que usuários, agentes públicos, profissionais da contabilidade e demais partes interessadas, quando aplicável, a compreensão sobre:

I – a existência e a finalidade da utilização da Inteligência Artificial;

II – a natureza do apoio prestado pela solução;

III – as limitações e os riscos relevantes associados à sua utilização;

IV – a existência de supervisão e validação humana;

V – os mecanismos de controle, monitoramento e responsabilização adotados; e

VI – os canais institucionais destinados ao esclarecimento de dúvidas, exercício de direitos ou apresentação de solicitações e reclamações, quando aplicável.

§ 2º O CRCPR poderá divulgar, em transparência ativa, informações sobre as soluções de Inteligência Artificial utilizadas institucionalmente, observadas a legislação aplicável e as restrições decorrentes da proteção de dados pessoais, da segurança da informação, do sigilo e demais hipóteses legais, não implicando tal dever na divulgação de informações cuja publicidade possa comprometer a segurança institucional ou o adequado funcionamento dos sistemas utilizados pelo Conselho.

Artigo 19º - A utilização de Inteligência Artificial na elaboração de documentos, estudos, relatórios, manifestações, análises, conteúdos ou outros produtos institucionais deverá ser registrada quando sua participação tiver influência relevante na elaboração ou no resultado do conteúdo, conforme critérios estabelecidos em regulamentação própria.

§ 1º O registro poderá ocorrer por meio de nota, identificação no sistema, metadado, campo específico, registro de atividade ou outro mecanismo institucionalmente definido.

§ 2º A identificação da utilização de Inteligência Artificial deverá ser realizada de forma compatível com a natureza do documento, sua finalidade, o nível de risco e as exigências legais aplicáveis.

§ 3º A utilização de Inteligência Artificial não afasta a responsabilidade do agente ou da unidade competente pela revisão, validação, aprovação e utilização do conteúdo produzido.

§ 4º A utilização meramente acessória da Inteligência Artificial, sem influência relevante sobre o conteúdo ou resultado, poderá dispensar o registro específico, conforme critérios estabelecidos em regulamentação complementar.

§ 5º A identificação da utilização de Inteligência Artificial não substitui nem reduz a obrigatoriedade de revisão, validação e supervisão humana estabelecida nesta Política.

CAPÍTULO XII
DA CAPACITAÇÃO E DO DESENVOLVIMENTO DE COMPETÊNCIAS

Artigo 20º - O CRCPR promoverá ações permanentes de capacitação, conscientização e desenvolvimento de competências relacionadas à utilização da Inteligência Artificial, com o objetivo de assegurar seu uso ético, seguro, responsável, crítico e alinhado aos interesses institucionais.

§ 1º As ações de capacitação deverão contribuir para o fortalecimento da governança da Inteligência Artificial, da proteção de dados pessoais, da segurança da informação e da cultura de inovação responsável no âmbito do Conselho.

§ 2º Os programas de capacitação poderão ser destinados a conselheiros, empregados, estagiários, terceirizados, colaboradores e demais usuários autorizados a utilizar soluções de Inteligência Artificial no exercício de suas atividades institucionais.

§ 3º As ações de capacitação deverão contemplar, sempre que possível e de forma compatível com as atribuições dos participantes:

I - uso responsável, seguro, ético e transparente da Inteligência Artificial;

II - princípios, direitos, deveres e boas práticas relacionados à Lei Geral de Proteção de Dados Pessoais (LGPD);

III - segurança da informação, proteção de ativos informacionais e classificação da informação;

IV - ética digital, integridade, prevenção de vieses e utilização responsável de tecnologias emergentes;

V - técnicas de formulação de comandos, instruções e interações com soluções de Inteligência Artificial, incluindo práticas de engenharia de prompts;

VI - avaliação crítica, validação e verificação dos resultados produzidos por soluções de Inteligência Artificial;

VII - identificação de limitações, riscos, inconsistências, alucinações e possíveis vieses presentes nos resultados gerados por ferramentas de Inteligência Artificial;

VIII - governança, gestão de riscos e conformidade aplicadas ao uso da Inteligência Artificial;

IX - utilização adequada de ferramentas institucionais de Inteligência Artificial e dos ambientes autorizados pelo CRCPR;

X - direitos fundamentais, privacidade, transparência, supervisão humana e responsabilização no contexto da utilização da Inteligência Artificial.

§ 4º O CRCPR incentivará a formação continuada dos usuários e a disseminação de boas práticas relacionadas ao uso da Inteligência Artificial, promovendo a atualização periódica dos conteúdos em razão da evolução tecnológica, regulatória e institucional.

§ 5º As ações de capacitação deverão buscar desenvolver nos usuários uma postura crítica e reflexiva em relação aos resultados produzidos pela Inteligência Artificial, reforçando que tais resultados constituem instrumentos de apoio e não substituem a análise técnica, o julgamento profissional ou a tomada de decisão humana.

§ 6º O Comitê de Tecnologia e Segurança da Informação (CTI) poderá propor diretrizes, conteúdos mínimos e ações específicas de capacitação relacionadas à utilização de soluções de Inteligência Artificial, observadas as necessidades institucionais e o grau de risco das soluções utilizadas pelo CRCPR.

CAPÍTULO XIII
DAS RESPONSABILIDADES

Artigo 21º - Os usuários de soluções de Inteligência Artificial no âmbito do Conselho Regional de Contabilidade do Paraná – CRCPR são responsáveis pela utilização ética, segura, diligente, crítica e compatível com suas atribuições, observando a legislação vigente, os normativos institucionais e as disposições desta Política.

§ 1º Constituem responsabilidades dos usuários:

I - conhecer e observar esta Política e os demais normativos institucionais aplicáveis à utilização de Inteligência Artificial, à proteção de dados pessoais, à segurança da informação, à gestão de riscos e ao uso dos recursos tecnológicos;

II - utilizar as soluções de Inteligência Artificial exclusivamente para finalidades legítimas, institucionais e compatíveis com suas atribuições e autorizações de acesso;

III - proteger os dados pessoais, as informações institucionais e os demais ativos de informação sob sua responsabilidade, observando as regras de classificação, tratamento, armazenamento, compartilhamento e descarte estabelecidas pelo CRCPR;

IV - avaliar criticamente, revisar e validar os resultados produzidos por soluções de Inteligência Artificial antes de sua utilização, divulgação ou incorporação a documentos, processos ou atividades institucionais;

V - verificar a consistência, a confiabilidade, a atualidade, a pertinência e a adequação das informações geradas por soluções de Inteligência Artificial, especialmente quando utilizadas para subsidiar manifestações técnicas, relatórios, pareceres ou decisões;

VI - adotar medidas para prevenir o uso inadequado, o compartilhamento indevido ou a exposição não autorizada de dados e informações institucionais;

VII - comunicar imediatamente às áreas competentes a ocorrência de incidentes de segurança da informação, violações de dados, falhas operacionais, resultados inadequados ou quaisquer situações que possam representar riscos decorrentes da utilização de Inteligência Artificial;

VIII - reportar às áreas competentes erros, inconsistências, vieses, limitações ou comportamentos inesperados identificados nas soluções de Inteligência Artificial;

IX - cooperar com as atividades de auditoria, monitoramento, avaliação de conformidade e gestão de riscos relacionadas à utilização da Inteligência Artificial;

X - participar das ações de capacitação e conscientização promovidas pelo CRCPR quando exigidas para a utilização das ferramentas disponibilizadas;

XI - observar os procedimentos institucionais de registro, rastreabilidade e transparência aplicáveis à utilização de Inteligência Artificial; e

XII - atuar com prudência, senso crítico e responsabilidade profissional, reconhecendo que os resultados produzidos pela Inteligência Artificial constituem instrumentos de apoio e não substituem a análise humana.

§ 2º Os gestores das unidades organizacionais deverão promover e estimular a utilização responsável da Inteligência Artificial, garantindo que os empregados sob sua supervisão observem as disposições desta Política e os procedimentos institucionais aplicáveis.

§ 3º As responsabilidades previstas neste artigo não afastam outras obrigações legais, regulamentares, funcionais, contratuais ou éticas aplicáveis em razão do vínculo do usuário com o CRCPR.

Artigo 22º - descumprimento das disposições desta Política ou a utilização inadequada, negligente, imprudente ou dolosa de soluções de Inteligência Artificial poderá ensejar a adoção das medidas administrativas, disciplinares, contratuais ou outras cabíveis, observada a legislação e os normativos aplicáveis.

§ 1º A apuração de eventual irregularidade observará o devido processo legal, o contraditório e a ampla defesa, quando aplicáveis, bem como as normas que disciplinam o vínculo do responsável com o CRCPR.

§ 2º Poderão ser objeto de apuração, entre outras condutas:

I - o descumprimento das regras de proteção de dados pessoais ou de segurança da informação;

II - a utilização de ferramentas de Inteligência Artificial não autorizadas, quando exigida homologação institucional;

III - o compartilhamento ou tratamento indevido de informações pessoais, sigilosas, restritas ou confidenciais em ambientes não autorizados;

IV - a utilização deliberada de Inteligência Artificial para produção ou disseminação de informações fraudulentas, enganosas ou incompatíveis com as finalidades institucionais;

V - a prática de condutas vedadas por esta Política;

VI - a omissão injustificada na comunicação de incidentes, falhas ou riscos relevantes;

VII - a utilização de resultados produzidos por Inteligência Artificial sem a devida revisão e validação humana, quando exigidas por esta Política.

§ 3º Verificada a existência de riscos relevantes à segurança da informação, à proteção de dados pessoais ou ao interesse institucional, o CRCPR poderá determinar a suspensão temporária ou definitiva da utilização de determinada ferramenta, solução ou funcionalidade de Inteligência Artificial, sem prejuízo das demais medidas cabíveis.

§ 4º As infrações relacionadas à utilização de Inteligência Artificial deverão ser registradas e tratadas de acordo com os procedimentos institucionais de gestão de riscos, segurança da informação, proteção de dados pessoais e integridade organizacional.

§ 5º A responsabilização decorrente do uso de Inteligência Artificial observará o princípio de que a decisão, o ato praticado e os resultados produzidos permanecem sob responsabilidade dos agentes humanos competentes, ainda que tenham sido apoiados por soluções automatizados.

CAPÍTULO XIV
DISPOSIÇÕES FINAIS

Artigo 23º - Os casos omissos, as situações excepcionais e as dúvidas relacionadas à interpretação, aplicação ou execução desta Política serão submetidas à deliberação da Presidência do CRCPR, mediante manifestação técnica das áreas competentes, especialmente das unidades responsáveis, Tecnologia da Informação, Segurança da Informação, Assessoria Jurídica e Encarregado pelo Tratamento de Dados Pessoais.

§ 1º Sempre que a matéria envolver riscos relevantes à proteção de dados pessoais, à segurança da informação, à conformidade regulatória ou à utilização de soluções de Inteligência Artificial classificados como de alto risco, a Presidência poderá solicitar manifestação adicional do Comitê de Tecnologia e Segurança da Informação (CTI) ou de Grupo de Trabalho instituído para essa finalidade.

§ 2º As decisões relacionadas aos casos omissos deverão observar os princípios, objetivos e diretrizes previstos nesta Política, bem como a legislação vigente, as normas de governança digital, proteção de dados pessoais, segurança da informação e gestão de riscos aplicáveis à Administração Pública.

§ 3º A interpretação desta Política deverá privilegiar a utilização ética, transparente, segura, responsável e supervisionada da Inteligência Artificial, preservando os direitos fundamentais, o interesse público e a finalidade institucional do CRCPR.

Artigo 24º - Esta Política deverá ser objeto de monitoramento e revisão periódica, com a finalidade de assegurar sua aderência à evolução tecnológica, às mudanças regulatórias, às boas práticas de governança e às necessidades institucionais do CRCPR.

§ 1º A revisão desta Política ocorrerá, no mínimo, a cada dois anos, ou em prazo inferior quando houver:

I - alteração legislativa ou regulamentar relacionada à Inteligência Artificial, proteção de dados pessoais, segurança da informação ou governança digital;

II - publicação de normas, recomendações ou orientações relevantes por órgãos de controle, regulação ou supervisão;

III - identificação de riscos, vulnerabilidades ou incidentes que justifiquem o aperfeiçoamento dos controles estabelecidos;

IV - mudanças significativas no ambiente tecnológico ou nas soluções de Inteligência Artificial adotadas pelo CRCPR;

V - necessidade de atualização decorrente da estratégia institucional, da transformação digital ou da evolução das boas práticas aplicáveis à Administração Pública.

§ 2º As propostas de alteração desta Política poderão ser apresentadas pelo Comitê de Tecnologia e Segurança da Informação (CTI), pelas áreas técnicas competentes ou pela Presidência do Conselho.

§ 3º As revisões deverão observar os princípios da melhoria contínua, da gestão de riscos, da transparência, da proteção de dados pessoais e da supervisão humana.

Artigo 25º - Esta Política entra em vigor na data de sua aprovação.

Parágrafo único - As unidades organizacionais do CRCPR deverão adotar as medidas necessárias para sua implementação, observados os prazos, procedimentos e orientações definidos pela Presidência e pelo Comitê de Tecnologia e Segurança da Informação (CTI), garantindo a adequação gradual dos processos, sistemas e práticas institucionais às disposições estabelecidas nesta Política.

Referência: Processo nº 9079623110000646.000004/2026-08 SEI nº 1613144