



1. Código e título do Projeto

BRA/23/024 – Inovação e inclusão na promoção de direitos humanos e cidadania no Brasil

2. Número e título do Edital

Edital nº 06/2026 – Programa de Privacidade e Segurança da Informação

3. Organismo Internacional

PNUD – Programa das Nações Unidas para o Desenvolvimento

4. Secretaria Demandante

Coordenação-Geral de Tecnologia da Informação (CGTI/SPOA/SE/MDHC)

5. Supervisor técnico

Supervisor Técnico: Belmiro da Graça Soares, Coordenador-Geral de Tecnologia da Informação

Supervisor Técnico (Substituto): Eduardo Schneider Machado, Coordenador-Geral de Tecnologia da Informação Substituto.

6. Antecedentes e justificativa

A implementação das ações previstas no Programa de Privacidade e Segurança da Informação (PPSI), coordenado pelo Ministério da Gestão e da Inovação em Serviços Públicos (MGI), o cumprimento integral da Lei nº 13.709/2018 (LGPD) e a adoção de controles baseados nos frameworks NIST e CIS Controls constituem compromissos legais e administrativos para o Poder Público.

Tais diretrizes exigem que os órgãos da Administração Pública Federal adotem medidas técnicas e organizacionais robustas para assegurar a proteção de dados pessoais, a prevenção de incidentes e a conformidade com os princípios de transparência e governança.

A execução dessas ações demanda um processo técnico contínuo e metodologicamente estruturado para a coleta e sistematização de informações provenientes de diversas áreas e sistemas.

A complexidade do escopo envolve o mapeamento de fluxos de tratamento, a revisão de bases legais, a análise de riscos, a elaboração de normativos internos e a implementação de processos de gestão técnica de segurança e de resposta a incidentes cibernéticos, integrando dados qualitativos e quantitativos para o atingimento das metas do PPSI.



Considerando que a LGPD e o PPSI transversalizam áreas sensíveis no âmbito do MDHC — como atendimento ao público demandante das ações do Ministério, TIC, gestão de pessoas etc., — a articulação interinstitucional e a adoção de metodologias especializadas tornam-se indispensáveis.

A diversidade das fontes de informação e a necessidade de compatibilização entre sistemas internos reforçam a importância de suporte técnico qualificado para garantir a precisão e a completude das entregas.

Nesse cenário, justifica-se a contratação de consultoria técnica especializada com expertise em privacidade, proteção de dados e segurança da informação.

A pessoa consultora apoiará a instituição na identificação de lacunas de conformidade, proposição de metodologias de riscos, revisão de fluxos internos e desenvolvimento de instrumentos de governança alinhados às melhores práticas nacionais e internacionais.

A atuação de especialistas elevará o nível de maturidade institucional, conferindo maior credibilidade aos processos.

Além de assegurar o cumprimento das obrigações legais, a contratação fortalecerá as políticas públicas e a segurança jurídica, garantindo que a instituição cumpra seu papel social com eficiência, transparência e responsabilidade.

Diante do exposto, justifica-se a contratação de consultoria técnica especializada para apoiar a implementação das ações do PPSI e o cumprimento das obrigações previstas na LGPD no âmbito do MDHC.

7. Enquadramento nas ações do Projeto

Produto 1 – Estratégias e metodologias para promoção da inovação e fortalecimento de políticas de promoção e defesa dos Direitos Humanos elaboradas

Atividade 1.2 – desenvolver metodologia para aprimorar ações do MDHC com vistas ao melhor atendimento de grupos sociais beneficiários de políticas.

8. Finalidade da contratação

Contratação de consultor pessoa física, na modalidade produto, para elaborar subsídios técnicos destinados à implementação das ações previstas no Programa de Privacidade e Segurança da Informação (PPSI) versão 2.0 e ao atendimento das obrigações estabelecidas pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

A consultoria apoiará o Ministério na sistematização de informações, identificação de lacunas de conformidade, proposição de metodologias de avaliação de riscos, revisão de fluxos de tratamento de dados pessoais e de segurança da informação e elaboração de instrumentos de



governança necessários ao fortalecimento da proteção de dados e da segurança da informação no âmbito institucional

9. Requisitos

9.1 Requisitos Obrigatórios

- Pós-graduação em Ciência da Computação, Sistemas de Informação, Engenharia da Computação, Engenharia de Software, Segurança da Informação, Gestão de Tecnologia da Informação ou áreas correlatas, em instituição de ensino superior reconhecida pelo Ministério da Educação.
- Experiência profissional de, no mínimo, 5 anos em atividades relacionadas à Segurança da Informação ou Proteção e Privacidade de Dados, ou Arquitetura Organizacional ou Elaboração de normativos sobre segurança cibernética e/ou privacidade e Elaboração de estudos/notas técnicos sobre segurança cibernética e/ou privacidade.
- Experiência com implementação de controles de segurança e privacidade conforme as melhores práticas: NIST Cybersecurity Framework (NIST CSF) ou CIS Critical Security Controls (Controles CIS v8.1) ~~ou~~ ABNT NBR ISO/IEC 27001 ou ABNT NBR ISO/IEC 27557 ou ABNT NBR ISO/IEC 27701 ou LGPD ou controles do PPSI (1.0/2.0) ou normas do GSI/PR

9.2 Requisitos Desejáveis

- Formação Complementar de no mínimo 120 horas, nas áreas de Proteção de Dados Pessoais e LGPD, Segurança da Informação, Cibersegurança, Governança de Tecnologia da Informação, Gestão de Riscos, Compliance ou Governança Pública Digital.
- Experiência profissional em implementação ou apoio à implementação de programas institucionais de segurança da informação, privacidade ou governança de dados, incluindo definição de políticas, processos e estruturas de governança;
- Experiência profissional em elaboração ou coordenação de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), bem como Relatórios de Impacto Algorítmico (RIA) ou instrumentos equivalentes de avaliação de riscos relacionados ao tratamento de dados e uso de tecnologias;
- Experiência profissional em realização de inventário de dados pessoais, mapeamento de fluxos de tratamento e registro de operações de tratamento de dados, abrangendo o ciclo de vida da informação.
- Certificações em proteção e privacidade de dados, tais como: Certified Data Privacy Solutions Engineer (CDPSE), da ISACA, e Privacy & Data Protection Professional (PDPP), da EXIN.
- Certificações em segurança da informação, tais como: Certified Information Security Manager (CISM), da ISACA, e Certified Information Systems Security Professional (CISSP), da ISC².



As hipóteses de inabilitação estão listadas nos itens 4 e 5 das [Diretrizes Gerais para Seleção](#).

Importante: Por exigência do organismo internacional, a contratação ficará condicionada à apresentação dos seguintes documentos:

- Atestado médico que comprove boas condições de saúde; e
- Comprovante de imunização contra a covid-19.

10. Atividades a serem desenvolvidas

- Participar de reuniões, preferencialmente de forma remota, com os supervisores da consultoria, prestando informações sobre o andamento dos trabalhos sempre que solicitado.
- Realizar levantamento e análise de dados e informações;
- Acompanhar, sistematizar e analisar processos de consulta participativa;
- Produzir documentações técnicas.

11. Produtos e resultados esperados

Produtos	Descrição
Produto 1 – Plano de Trabalho	Deverá conter, no mínimo: 1.1 Metodologia e cronograma executivo das atividades para o ciclo PPSI 2.0 1.2 1.2 Marco normativo e institucional relacionado à segurança da informação, proteção de dados e privacidade 1.3 Estimativa de capacidade técnica, matriz de recursos necessários e estratégia contínua de monitoramento e sustentação
Produto 2 – Documento técnico contendo proposta de Governança e Estratégia	Deverá conter, no mínimo: 1. Diagnóstico de Maturidade e Conformidade 1.1. Metodologia e critérios de avaliação de maturidade e conformidade 1.2. Mapeamento e avaliação de maturidade dos processos finalísticos sob a ótica de segurança da informação e privacidade, com identificação de lacunas 1.3. Diagnóstico de controles de segurança cibernética e de infraestrutura baseados em frameworks de referência (CIS Controls v8.1 e NIST CSF)



	1.4. Diagnóstico de conformidade legal e hipóteses de tratamento segundo a LGPD 1.5. Relatório consolidado de maturidade 1.6. Matriz de priorização e análise de impacto Plano de adequação e <i>roadmap</i> de remediação 2. Matriz de Riscos de Privacidade e Segurança da Informação 2.1. Metodologia e critérios para gestão de riscos 2.2. Processo de identificação, mapeamento e avaliação de riscos 2.3. Matriz e catálogo consolidado de riscos institucionais 2.4. Plano de tratamento e estratégias de resposta a riscos 2.5. Plano de mitigação e controles compensatórios aplicados aos processos finalísticos 2.6. Modelo e procedimentos para monitoramento contínuo dos riscos
Produto 3 - Documento técnico contendo proposta de Processos e Dados	Deverá conter, no mínimo: 1. Inventário e Fluxo de Dados 1.1 Levantamento dos processos finalísticos e de suporte que realizam tratamento de dados pessoais 1.2 Mapeamento do ciclo de vida dos dados pessoais (da coleta ao descarte) e validação formal com as unidades gestoras 1.3 Registro das Operações de Tratamento, contemplando: agentes de tratamento, finalidades, categorias de titulares e de dados, bases legais, medidas técnicas/administrativas de segurança e prazos de retenção 1.4 Inventário de bases de dados críticas e sigilosas, contendo critérios de classificação, retenção, segurança e rotinas de restauração 1.5 Fluxo e procedimento operacional padrão para atendimento aos direitos dos titulares 1.6 Mapeamento dos fluxos de dados, contemplando categorias de dados (pessoais e sensíveis), canais de tráfego, locais de processamento e repositórios de armazenamento; 1.7 Mapa do fluxo de dados pessoais por macroprocesso



	organizacional 1.8 Avaliação de riscos e conformidade em segurança e privacidade no processo de tratamento de dados pessoais 2. Gestão e Inventário de Ativos de TI 2.1 Inventário catalogado de ativos de TIC e suas integrações (hardware, software, redes e serviços em nuvem) 2.2 Mapeamento de bibliotecas, APIs e bancos de dados vinculados ao tratamento de dados corporativos 2.3 Aplicação de matriz de vulnerabilidades e riscos sobre os ativos inventariados 2.4 Plano de ação para mitigação de vulnerabilidades e implementação de controles compensatórios em ativos críticos 3. Relatórios de Impacto (RIPD e RIA) 3.1 Metodologia, <i>templates</i>, diretrizes e fluxo operacional para elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) 3.2 Critérios formais para triagem e identificação de tratamentos de dados de alto risco; 3.3 Metodologia, <i>templates</i>, diretrizes e fluxo operacional para elaboração de Relatório de Impacto Algorítmico (RIA) em soluções de Inteligência Artificial 4. Classificação de Dados e Ativos 4.1 Critérios, taxonomia e matriz de classificação da informação por níveis de sigilo, criticidade e sensibilidade 4.2 Diretrizes, controles de segurança e requisitos técnicos e operacionais de proteção por nível de classificação 4.3 Padrões de rotulagem para a informação classificada 4.4 Regras de segurança para interoperabilidade, transferência externa e compartilhamento com outros órgãos, além de diretrizes para custódia segura 4.5 Minuta da Política de Classificação da Informação acompanhada de procedimento operacional padrão do ciclo de vida da informação
--	---



	de manuseio a descarte seguro
Produto 4 - Documento técnico contendo proposta de Gestão Técnica e de Segurança	Deverá conter, no mínimo: 1. Plano de Gestão de Identidades e Acessos (IAM) 1.1 Inventário de identidades e contas (usuários internos, privilégios administrativos em SO/nuvem/rede, contas de serviço, identidades não humanas/máquinas, integrações de APIs, terceiros, convênios e parceiros institucionais) 1.2 Diagnóstico de lacunas e vulnerabilidades em autenticação e autorização (ex.: contas inativas/órfãs, credenciais compartilhadas, políticas de senhas fracas, concessões sem expiração e acúmulo indevido de permissões) 1.3 Processo unificado do ciclo de vida de acessos e procedimento operacional padrão associados: concessão/admissão, movimentação/transferência, revogação/desligamento e recertificação periódica 1.4 Definição de arquitetura e modelo para centralização do ciclo de identidades e federação de acessos 1.5 Processo de centralização técnica e operacional da gestão de contas de rede e sistemas 1.6 Processo de centralização dos fluxos de solicitação, aprovação e provisionamento de acessos 1.7 Processo para concessão, revisão periódica, trilhas de auditoria e revogação de privilégios 1.8 Diretrizes para menor privilégio, segregação de funções, gestão de credenciais privilegiadas e autenticação multifator 1.9 Requisitos técnicos de proteção e controle de acesso a dados pessoais e dados pessoais sensíveis. 2. Arquitetura de Rede Segura 2.1 Definição de padrões de configuração segura para ativos de rede, conectividade, segurança, processamento e armazenamento



	2.2 Diretrizes de arquitetura de rede: segmentação, microssegmentação e proteção de perímetro (ambientes locais e em nuvem) 2.3 Minuta da Política de Gestão de Logs e Trilhas de Auditoria (requisitos de geração, sincronismo de tempo, retenção, integridade, correlação de eventos, monitoramento e guarda legal)
Produto 5 - Documento técnico contendo proposta de Gestão de Terceiros	Deverá conter, no mínimo: 1. Inventário e Avaliação de Provedores de Serviços 1.1 Mapeamento de prestadores de serviços que realizam operações de tratamento de dados em nome do MDHC 1.2 Classificação de fornecedores por criticidade e risco considerando volume e sensibilidade dos dados, privilégios de acesso concedidos e impacto operacional em caso de incidente) 1.3 Diretrizes operacionais para gestão e fiscalização de riscos de terceiros que realizam o tratamento de dados pessoais nas etapas de pré-contratação, contratação, execução/fiscalização técnica e encerramento contratual. 2. Cláusulas Padronizadas de Privacidade e Segurança 2.1 Cláusulas-padrão de privacidade, proteção de dados e segurança da informação aplicáveis ao processo de contratação (ETP, Termo de Referência, Editais e Contratos) 2.2 Cláusulas-padrão aditivos contratuais com disposições de segurança privacidade, proteção de dados para adequação dos contratos vigentes 2.3 Procedimentos para verificação de conformidade em terceiros, obrigações de resposta e notificação de incidentes, e protocolos seguros para devolução ou descarte de dados ao fim do contrato.
Produto 6 - Documento técnico contendo proposta de Pessoas e Cultura	Deverá conter, no mínimo: 1. Portal Unificado de Segurança e Privacidade 1.1 Arquitetura de informação e estrutura de navegação do portal 1.2 Definição de catálogo de conteúdos, cartilhas educativas e orientações corporativas 1.3 Fluxos e regras de governança para atualização e gestão de dados no portal



	1.4 Canal integrado e fluxo operacional para atendimento aos direitos dos titulares de dados 2. Boas Práticas em Segurança da Informação e Privacidade 2.1 Manual de Boas Práticas e Conduta Segura em Segurança da Informação 2.2 Guia Operacional para Tratamento de Dados Pessoais 2.3 Guia de Diretrizes para uso seguro de Soluções de Inteligência Artificial 3. Trilhas de Capacitação Específicas 3.1 Matriz de capacitação temática em Privacidade, Proteção de Dados, Segurança da Informação e IA 3.2 Definição da metodologia pedagógica e formatos de aplicação 3.3 Ementas customizadas por perfis de atuação (equipe de TIC/Segurança, Alta Gestão/Fiscais de Contratos, Consultoria Jurídica e Encarregado/Rede de Pontos Focais) 3.4 Plano de execução e realização de pelo menos um treinamento prático para cada perfil de atuação 3.5 Transferência de Conhecimento dos produtos da Consultoria a equipe do MDHC
--	---

Observação: Os documentos técnicos previstos deverão ser entregues em formato editável (DOCX ou ODT e XLSX ou ODS) e em PDF.

12. Cronograma de entrega e pagamento dos produtos

Produto	Prazo de entrega após assinatura do contrato	Valor	Percentual
Produto 1 – Plano de Trabalho	20 dias	6.000,00	5%
Produto 2 - Documento técnico contendo proposta de Governança e Estratégia	60 dias	15.000,00	12,5 %



Produto 3 - Documento técnico contendo proposta de Processos e Dados	120 dias	30.000,00	25 %
Produto 4 - Documento técnico contendo proposta de Gestão Técnica e de Segurança	180 dias	30.000,00	25 %
Produto 5 - Documento técnico contendo proposta de Gestão de Terceiros	210 dias	15.000,00	12,5 %
Produto 6 - Documento técnico contendo proposta de Pessoas e Cultura	255 dias	24.000,00	20 %
Total		R\$ 120.000,00	100%

13. Valor total do contrato

R\$ 120.000,00 (cento e vinte mil reais)

14. Duração do contrato

A duração do contrato é de 255 dias a partir da data de assinatura do termo

15. Insumos

Para a execução das atividades e elaboração dos produtos previstos neste Termo de Referência, a pessoa consultora deverá analisar, entre outros, os seguintes documentos e materiais de referência:

1. Lei 12.527/2011 - Lei de Acesso à Informação
2. Lei nº 13.709/2018 - Lei Geral de Proteção de Dados
3. Lei nº 14.129/2021 - Governo Digital
4. Decreto nº 7.845/2012 - Procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo
5. Decreto nº 9.203/2017 - Governança na Administração Pública Federal
6. Decreto nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas
7. Decreto nº 10.569/2020 - Estratégia Nacional de Segurança de Infraestruturas Críticas
8. Decreto nº 10.748/2021 - Rede Federal de Gestão de Incidentes Cibernéticos



9. Decreto nº 11.341/2023 – Estrutura Regimental do Ministério dos Direitos Humanos e da Cidadania
10. Decreto nº 11.856/2023 - Política Nacional de Cibersegurança
11. Decreto nº 12.572/2025 - Política Nacional de Segurança da Informação
12. Decreto nº 12.573/2025 - Estratégia Nacional de Cibersegurança
13. Portaria SGD/MGI nº 9.511/2025 - PPSI 2.0
14. Coletânea de publicações do PPSI 2.0 - <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0>
15. Instrução Normativa SGD/MGI nº 4, de 14 de janeiro de 2026 - Ciclo de implementação de 2026 do PPSI 2.0
16. Portaria nº 1.522, de 1º de setembro de 2025 – Diretrizes de soluções de IA no MDHC
17. Coletânea de Normas de Segurança da Informação da GSI - https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/nucleo/legislacao-de-interesse/coletanea_normas_seguranca_informacao_classificada.pdf
18. ABNT NBR ISO/IEC 27036:2016 - Segurança da informação para relacionamento com fornecedores
19. ABNT NBR ISO/IEC 29101:2018 – Arquitetura de Privacidade em Sistemas de TIC
20. ABNT NBR ISO/IEC 29100:2020 – Estrutura de privacidade
21. ABNT NBR ISO/IEC 27008:2020 - Diretrizes para a avaliação de controles de segurança
22. ABNT NBR ISO/IEC 20889:2020 - Técnicas de desidentificação e anonimização de dados
23. ABNT NBR ISO/IEC 27000:2020 - Visão geral e vocabulário de SGSI
24. ABNT NBR ISO/IEC 27007:2021 - Diretrizes para auditoria de SGSI
25. ABNT NBR ISO/IEC 27014:2021 – Governança de Segurança da Informação
26. ABNT NBR ISO/IEC 27018:2021 – Proteção de informação em cloud
27. ABNT NBR ISO/IEC 27001:2022 – Sistema de Gestão de segurança da informação
28. ABNT NBR ISO/IEC 27017:2022 - Controles de segurança da informação para serviços em nuvem
29. ABNT NBR ISO/IEC 27004:2022 - Monitoramento, medição, análise e avaliação da segurança
30. ABNT NBR ISO/IEC 27002:2022 - Controles de segurança da informação
31. ABNT NBR ISO/IEC 27032:2023 – Segurança Cibernética
32. ABNT NBR ISO/IEC 27557:2023 - Gestão de riscos de privacidade
33. ABNT NBR ISO/IEC 16167:2023 - Classificação, rotulação e tratamento da informação
34. ABNT NBR ISO/IEC 27005:2023 - Gestão de Riscos de Segurança da Informação
35. ABNT NBR ISO/IEC 27555:2023 – Gestão de Dados pessoais
36. ABNT NBR ISO/IEC 22989:2023 – Conceitos e terminologia de inteligência artificial
37. ABNT NBR ISO/IEC 23894:2023 - Gestão de riscos em inteligência artificial
38. ABNT NBR ISO/IEC 42001:2024 – Sistema de gestão da inteligência artificial



- 39. ABNT NBR ISO/IEC 29134:2023 - Avaliação de impacto sobre a privacidade
- 40. ABNT NBR ISO/IEC 22301:2024 - Sistema de gestão de continuidade de negócios
- 41. ABNT NBR ISO/IEC 27701:2026 - Sistema de Gestão de Privacidade da Informação
- 42. NIST Cybersecurity Framework (CSF v2.0): Estrutura focada em identificar, proteger, detectar, responder e recuperar de ataques cibernéticos.
- 43. CIS Controls (Center for Internet Security v8.1): Conjunto de ações de cibersegurança.
- 44. MITRE ATT&CK.

16. Previsão de viagem

A pessoa consultora deverá ter disponibilidade para participar de eventuais reuniões na Coordenação-Geral de Tecnologia da Informação, Assessoria Especial de Controle Interno ou outras unidades internas do Ministério, a serem realizadas, preferencialmente, por videoconferência. Caso haja necessidade de reuniões presenciais e a pessoa selecionada não resida no Distrito Federal, as despesas com passagens e diárias serão custeadas pelo Projeto.

Poderão ser realizadas, ao longo do contrato, viagens para o cumprimento do objetivo da consultoria e elaboração dos produtos. Nesses casos, as despesas com passagens e diárias também serão custeadas pelo Projeto.

17. Localidade do trabalho

Local de Trabalho: Território Nacional

18. Número de vagas

Número de Vagas: 1 vaga

19. Critérios de Seleção

Fase I: Até 80 pontos (nota máxima da fase de análise curricular)

Requisitos obrigatórios	Até 40 pontos
Pós-graduação em Ciência da Computação, Sistemas de Informação, Engenharia da Computação, Engenharia de Software, Segurança da Informação, Gestão de Tecnologia da Informação ou áreas correlatas, em instituição de ensino superior reconhecida pelo Ministério da Educação	Até 10 pontos Pós-Graduação (Obrigatória) 5 pontos por Pós-Graduação adicional



Experiência profissional de, no mínimo, 5 anos em atividades relacionadas à Segurança da Informação ou Proteção e Privacidade de Dados, ou Arquitetura Organizacional ou Elaboração de normativos sobre segurança cibernética e/ou privacidade e Elaboração de estudos/notas técnicos sobre segurança cibernética e/ou privacidade	Até 15 pontos 5 anos (Obrigatório) 2,5 pontos por ano adicional
Experiência com implementação de controles de segurança e privacidade conforme as melhores práticas: NIST Cybersecurity Framework (NIST CSF) ou CIS Critical Security Controls (Controles CIS v8.1), ou ABNT NBR ISO/IEC 27001 ou ABNT NBR ISO/IEC 27557 ou ABNT NBR ISO/IEC 27701 ou LGPD ou controles do PPSI (1.0/2.0) ou normas do GSI/PR	Até 15 pontos 1 guia/normas (framework) de melhores práticas (Obrigatório) 2,5 pontos por guia/normas (framework) de melhores práticas, adicional. A pontuação valerá por Atestado ou documento similar emitido pela entidade no qual foi implementado
Requisitos desejáveis	Até 40 pontos
Formação Complementar de no mínimo 120 horas, nas áreas de Proteção e Privacidade de Dados Pessoais ou Segurança da Informação ou Cibersegurança ou Governança de Tecnologia da Informação ou Gestão de Riscos ou Governança Digital.	Até 8 pontos 2 pontos por curso
Experiência profissional em implementação ou apoio à implementação de programas institucionais de segurança da informação ou proteção e privacidade de dados ou governança de dados, incluindo definição de políticas, processos e estruturas de governança	Até 8 pontos 2 pontos por ano de experiência
Experiência profissional em elaboração ou coordenação de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) ou Relatórios de Impacto Algorítmico (RIA) ou instrumentos equivalentes de avaliação de riscos relacionados ao tratamento de dados pessoais e uso de tecnologias emergentes	Até 8 pontos 2 pontos por ano de experiência
Experiência profissional em realização de inventário de dados pessoais, mapeamento de fluxos de tratamento e registro de operações de tratamento de dados, abrangendo o ciclo de vida da informação	Até 08 pontos 2 pontos por ano de experiência



Certificações em proteção e privacidade de dados, tais como: Certified Data Privacy Solutions Engineer (CDPSE), da ISACA, e Privacy & Data Protection Professional (PDPP), da EXIN.	Até 4 pontos 2 pontos por certificação
Certificações em segurança da informação, tais como: Certified Information Security Manager (CISM), da ISACA, e Certified Information Systems Security Professional (CISSP), da ISC.	Até 4 pontos 2 pontos por certificação

Fase II: Até 20 pontos (nota máxima da fase de entrevista)

Habilidades e competências	Até 20 pontos
Deverá demonstrar domínio dos temas relacionados ao objeto da contratação, com fluência verbal e postura profissional, evidenciando cordialidade, polidez e assertividade, bem como atenção, clareza e objetividade na exposição de ideias e argumentos, além de capacidade de análise e síntese.	A pontuação será atribuída proporcionalmente ao número de perguntas, conforme o nível de atendimento a cada requisito.

20. Inscrições

As pessoas interessadas em participar do processo seletivo deverão encaminhar currículo no modelo padrão disponível em: https://www.gov.br/mdh/pt-br/navegue-por-temas/cooperacao-internacional/editais-2025/2025_CV_padrao.docx, para o endereço eletrônico cgti@mdh.gov.br

O currículo deverá ser enviado em PDF, em português, e conforme o modelo padrão. Currículos que não observem esse padrão, assim como arquivos corrompidos, ilegíveis ou inviáveis de visualizar, serão desconsiderados.

No campo “Assunto” do e-mail, deverá constar obrigatoriamente: Projeto PNUD/BRA-23/024 – Edital 06/2026, a fim de identificar a vaga pretendida.

O não atendimento aos subitens acima implicará o indeferimento da candidatura.

21. Disposições Finais

Leia atentamente o documento “Critérios Gerais de Seleção 2026 – Projetos de Cooperação Internacional/MDHC”, disponível em:



https://www.gov.br/mdh/pt-br/navegue-por-temas/cooperacao-internacional/editais-2025/2025_Criterios_consultorias_PF.pdf

O documento reúne as regras gerais do processo seletivo, incluindo requisitos, inscrições, previsão de viagens, hipóteses de inabilitação, critérios de classificação e divulgação de resultados. Apresenta, ainda, orientações sobre contratação, entrega, avaliação e pagamento dos produtos, bem como os critérios de seleção e a pontuação máxima por etapa.