iapp

CORPO DE CONHECIMENTO E SUMÁRIO DE CONTEÚDO CIPM

VERSÃO 4.0.0

EM VIGOR A PARTIR DE: 02/10/2023

CORPO DE CONHECIMENTO CIPM DA IAPP

COMO FUNCIONA O CORPO DE CONHECIMENTO DA IAPP

O principal objetivo do corpo de conhecimento é documentar o conhecimento e as habilidades que serão avaliados no exame de certificação. Os domínios refletem o que o profissional de privacidade deve saber e ser capaz de fazer para demonstrar competência nessa certificação.

O corpo de conhecimento também inclui o sumário do conteúdo do exame, que mostra o número mínimo e máximo de questões de cada domínio que serão encontradas no exame.

O corpo de conhecimento é desenvolvido e mantido pelos especialistas que constituem cada conselho de desenvolvimento de exames de certificação e comitê estrutural. O corpo de conhecimento é revisado (e, se necessário, atualizado) todos os anos. As alterações são refletidas nas atualizações anuais do exame e comunicadas aos candidatos pelo menos 90 dias antes de o novo conteúdo aparecer no exame.

COMPETÊNCIAS E INDICADORES DE DESEMPENHO

Em vez do antigo formato que usávamos para nossos corpos de conhecimento, agora representamos o conteúdo como uma série de Competências e Indicadores de desempenho.

As Competências são grupos de tarefas e habilidades conectadas que constituem um domínio geral de conhecimento.

Indicadores de desempenho são as tarefas e habilidades específicas que constituem o grupo mais amplo de competências. As perguntas do exame avaliam a proficiência de um profissional de privacidade nos indicadores de desempenho.

QUE TIPOS DE PERGUNTAS CAIRÃO NO EXAME?

Para candidatos à certificação, os indicadores de desempenho evidenciam a profundidade do conhecimento necessário para demonstrar competência. Os verbos que iniciam as declarações de habilidades e tarefas (identificar, avaliar, implementar, definir) indicam o nível de complexidade das questões do exame e seus corolários são encontrados na Taxonomia de Bloom (consulte a próxima página).

ACREDITAÇÃO DO ANAB

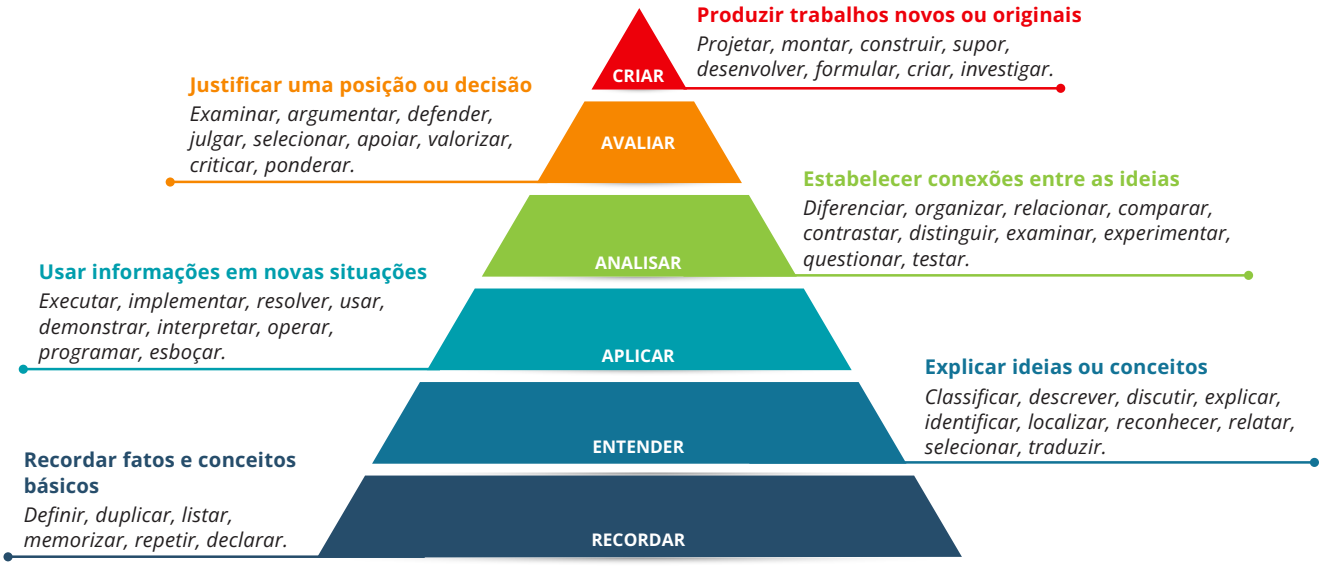
As certificações CIPM, CIPP/E, CIPP/US e CIPT da IAPP são credenciadas pelo **National Accreditation Board (ANAB) do American National Standards Institute (ANSI) sob o padrão 17024:2012 da International Organization for Standardization (ISO).**

O ANAB é um órgão de acreditação reconhecido internacionalmente que avalia e credencia programas de certificação com padrões rigorosos.

A acreditação é um enorme reconhecimento da qualidade e integridade dos programas de certificação da IAPP, pois:

- Demonstra que as credenciais da IAPP seguem referências globais e reconhecidas pelo setor.
- Assegura que as credenciais da IAPP sejam coerentes, comparáveis e confiáveis em todo mundo.
- Protege a integridade e garante a validação do programa de certificação da IAPP.
- Promove junto a empregadores, colegas, clientes e fornecedores a ideia de que profissionais certificados pela IAPP detêm conhecimento e habilidades para desempenharem seu trabalho em qualquer lugar do mundo.

CORPO DE CONHECIMENTO CIPM DA IAPP



Exemplos de questões do tipo Recordar/ Compreender, de várias certificações:

- Qual das alternativas a seguir é a definição correta de tecnologias de melhoria da privacidade?
- A que tipo de atividade se aplica a Carta Canadense dos Direitos?
- Qual instituição da União Europeia tem a competência de propor leis de proteção de dados?
- Quem tem autoridade para regulamentar as leis Fair Credit Reporting Act (FCRA) e a Fair and Accurate Credit Transactions Act (FACTA)?

As respostas a essas questões são um fato e não podem ser contestadas.

Exemplos de questões do tipo Aplicar/Analisar, de várias certificações:

- Qual das seguintes alternativas representa o **maior** desafio para um controlador de dados da União Europeia na ausência de disposições contratuais claramente definidas?
- Qual das seguintes situações constituiria uma violação da privacidade territorial?
- Qual é a **melhor** maneira de garantir que todos os stakeholders tenham o mesmo entendimento básico dos problemas de privacidade enfrentados por uma organização?
- Se os engenheiros de tecnologia da informação definissem originalmente o padrão para as informações de cartão de crédito do cliente como "Não salvar", essa ação estaria de acordo com qual conceito?

A resposta a essa questão depende do conhecimento de fatos e de compreensão que permita a aplicação, análise e/ou avaliação das opções fornecidas para escolher a melhor resposta.

MIN.	MÁX	Domínio I: Programa de Privacidade: desenvolvimento do framework
14	18	**Domínio I – Programa de Privacidade: desenvolvimento do framework** documenta as tarefas preliminares necessárias para criar uma base sólida do programa de privacidade, seus objetivos e seu responsável. O foco é o estabelecimento do modelo de governança do programa de privacidade dentro do contexto da estratégia de privacidade da organização; Como cada organização tem necessidades próprias, o modelo pode variar.

			Competências	Indicadores de desempenho
4	6	I.A	Definir o escopo do programa e desenvolver uma estratégia de privacidade.	Escolher o modelo de governança aplicável.
				Identificar a fonte, tipos e usos das informações pessoais dentro da organização.
				Estruturar a equipe de privacidade.
				Identificar stakeholders e parcerias internas.
4	6	I.B	Comunicar a visão organizacional e a declaração de missão.	Criar consciência do programa de privacidade da organização, interna e externamente.
				Garantir o acesso dos funcionários às políticas e procedimentos e às atualizações relativas às suas funções.
				Adotar o vocabulário do programa de privacidade (por exemplo, incidente ou violação).
5	7	I.C	Indicar leis, regulamentações e normas dentro do escopo e aplicáveis ao programa.	Entender a regulamentação e/ou leis setoriais e industriais.
				Entender as penalidades por descumprimento.
				Entender o escopo e a autoridade dos órgãos de supervisão.
				Entender as implicações de privacidade ao fazer negócios ou operar em países com leis de privacidade inadequadas.

MIN.	MÁX		Domínio II: Programa de Privacidade: estabelecimento da governança do programa	
12	16		**Domínio II - Programa de Privacidade: estabelecimento da governança do programa** identifica como os requisitos de privacidade serão implementados em toda a organização ao longo de todos os estágios do ciclo de vida da privacidade. O Domínio se concentra nas funções, responsabilidades e requisitos de treinamento dos diversos stakeholders, além das políticas e procedimentos que serão seguidos para garantir a conformidade contínua.	
			Competências	**Indicadores de desempenho**
6	8	II.A	Criar políticas e processos a serem seguidos ao longo de todos os estágios do ciclo de vida do programa de privacidade.	Estabelecer modelo organizacional, responsabilidades e estrutura hierárquica adequados ao tamanho da organização.
				Definir políticas bem elaboradas relacionadas ao tratamento dos acervos e compartilhamento de dados da organização, considerando requisitos legais e éticos.
				Identificar pontos de coleta, considerando as limitações de transparência e integridade da coleta de dados.
				Criar um plano para o gerenciamento de violações.
				Criar um plano para gestão de reclamações.
1	3	II.B	Esclarecer funções e responsabilidades.	Definir funções e responsabilidades para gerenciar o compartilhamento e a divulgação de dados para uso interno e externo.
				Definir papéis e responsabilidades para respostas a violações por função, incluindo stakeholders e sua responsabilidade perante os órgãos reguladores, coordenando equipes de detecção (por exemplo, TI, segurança física, RH, equipes de investigação, fornecedores) e estabelecendo equipes de supervisão.
2	4	II.C	Definir métricas de privacidade para supervisão e governança.	Criar métricas por público-alvo e/ou identificar o público-alvo das métricas com processos claros que descrevam a finalidade, o valor e o reporte das métricas.
				Entender as finalidades, os tipos e os ciclos de vida das auditorias na avaliação da eficácia dos controles em todas as operações, sistemas e processos da organização.
				Estabelecer sistemas de monitoramento e aplicação para rastrear mudanças na lei de privacidade em diversas jurisdições a fim de garantir o alinhamento contínuo.
1	3	II.D	Estabelecer atividades de treinamento e conscientização.	Desenvolver treinamentos direcionados para funcionários, gerentes e prestadores de serviços em todos os estágios do ciclo de vida da privacidade.
				Criar atividades contínuas do programa de privacidade (por exemplo, educação e conscientização, monitoramento da conformidade interna, garantia do programa, incluindo auditorias e procedimentos de tratamento de reclamações).

MIN.	MÁX	Domínio III: Ciclo de vida operacional do programa de privacidade: avaliação de dados		
12	16	**Domínio III - Ciclo de vida operacional do programa de privacidade: avaliação de dados** define como identificar e minimizar os riscos à privacidade e avaliar os impactos à privacidade associados aos sistemas, processos e produtos de uma organização. Tratar possíveis problemas desde o início ajuda a estabelecer um programa de privacidade mais robusto.		
			Competências	**Indicadores de desempenho**
3	5	III.A	Documentar os sistemas de governança de dados.	Mapear inventários de dados, mapear fluxos de dados, mapear o ciclo de vida dos dados e as integrações de sistemas.
				Avaliar a conformidade da política em relação aos requisitos internos e externos.
				Determinar o estado desejado e fazer análise de gaps em relação a uma norma ou lei aceita.
1	3	III.B	Avaliar operadores e fornecedores terceirizados.	Identificar os riscos de internalização e terceirização de dados, inclusive requisitos contratuais e regras de transferências internacionais de dados.
				Realizar avaliações no nível funcional mais apropriado dentro da organização (por exemplo, compras, auditoria interna, segurança da informação, segurança física, autoridade de proteção de dados).
0	2	III.C	Avaliar controles físicos e ambientais.	Identificar riscos operacionais de locais físicos (como data centers e escritórios) e controles físicos (como retenção e destruição de documentos, limpeza e descarte de mídia, análise forense de dispositivos e segurança de dispositivos).
3	5	III.D	Avaliar controles técnicos.	Identificar riscos operacionais do processamento digital (por exemplo, servidores, armazenamento, infraestrutura e nuvem).
				Revisar e definir limites para o uso de dados pessoais (por exemplo, acesso baseado em função).
				Revisar e definir limites para a retenção de registros.
				Determinar a localização dos dados, incluindo os fluxos internacionais de dados.
2	4	III.E	Avaliar os riscos associados aos dados compartilhados em fusões, aquisições e desinvestimentos.	Concluir procedimentos de due dilligence.
				Avaliar as obrigações contratuais e de compartilhamento de dados, inclusive leis, regulamentação e normas.
				Conduzir alinhamento de riscos e controles.

MIN.	MÁX	Domínio IV: Ciclo de vida operacional do programa de privacidade: proteção de dados pessoais		
9	13	**Domínio IV - Ciclo de vida operacional do programa de privacidade: proteção de dados pessoais** descreve como proteger os ativos de dados durante o uso por meio da implementação de controles e tecnologia eficazes de privacidade e segurança. Independentemente do tamanho, da localização geográfica ou do setor, os dados devem estar física e virtualmente seguros em todos os níveis da organização.		
		Competências		**Indicadores de desempenho**
4	6	IV.A	Aplicar práticas e políticas de segurança da informação.	Classificar os dados segundo o esquema de classificação aplicável (por exemplo, público, confidencial, restrito).
				Entender as finalidades e limitações dos diferentes controles.
				Identificar riscos e implementar controles de acesso aplicáveis.
				Usar medidas organizacionais adequadas para mitigar qualquer risco residual.
1	3	IV.B	Integrar os princípios básicos da Privacidade desde a concepção (PbD).	Integrar a privacidade por meio do ciclo de vida de desenvolvimento do sistema.
				Integrar a privacidade por meio de processos de negócios.
3	5	IV.C	Aplicar diretrizes organizacionais para o uso de dados e garantir a aplicação dos controles técnicos.	Verificar se as diretrizes para usos secundários de dados estão sendo seguidas.
				Verificar se as salvaguardas administrativas, como políticas, procedimentos e contratos de fornecedores e do RH, estão sendo aplicadas.
				Garantir que os controles de acesso de funcionários e as classificações de dados aplicáveis estejam ativados.
				Colaborar com tecnólogos de privacidade para habilitar controles técnicos de ofuscação, minimização de dados, segurança e outras tecnologias de aprimoramento da privacidade.

MIN.	MÁX	Domínio V: Ciclo de vida operacional do programa de privacidade: manutenção do desempenho do programa
7	9	**Domínio V - Ciclo de vida operacional do programa de privacidade: manutenção do desempenho do programa** detalha como o programa de privacidade é mantido, pela aplicação de métricas e procedimentos de auditoria pertinentes. Conforme a organização passa pelos ciclos de gerenciamento do programa de privacidade, é importante garantir que todos os processos e procedimentos estejam funcionando de forma eficaz e possam ser replicados no futuro.

			Competências	Indicadores de desempenho
1	3	V.A	Usar métricas para medir o desempenho do programa de privacidade.	Determinar métricas apropriadas para diversos objetivos e analisar os dados coletados por meio de métricas (por exemplo, tendências, ROI, resiliência comercial, modelo de maturidade em privacidade).
				Coletar métricas para vincular as atividades de treinamento e conscientização às reduções nos eventos de privacidade e melhorar continuamente o programa de privacidade com base nas métricas coletadas.
1	3	V.B	Auditar o programa de privacidade.	Entender os tipos, as finalidades e os ciclos de vida das auditorias na avaliação da eficácia dos controles em todas as operações, sistemas e processos da organização.
				Selecionar as formas aplicáveis de monitoramento com base nas metas do programa (por exemplo, auditorias, controles, terceirizados) e concluir o monitoramento da conformidade por meio de auditoria das políticas, dos controles e dos padrões de privacidade, inclusive em relação às normas do setor e às alterações de regulamentações e/ou leis.
3	5	V.C	Gerenciar a avaliação contínua do programa de privacidade.	Realizar avaliações de risco em sistemas, aplicativos, processos e atividades.
				Entender a finalidade e o ciclo de vida de cada tipo de avaliação (por exemplo, PIA, AIPD, TIA, LIA, PTA).
				Implementar mitigação de riscos e comunicações com stakeholders internos e externos após fusões, aquisições e desinvestimentos.
				Garantir que o uso da IA seja ético, imparcial, atenda às expectativas de minimização de dados e limitação de finalidade e esteja em conformidade com quaisquer regulamentos e/ou leis de privacidade.

MIN.	MÁX	Domínio VI: Ciclo de vida operacional do programa de privacidade: resposta a requisições e incidentes		
10	14	**Domínio VI - Ciclo de vida operacional do programa de privacidade: resposta a requisições e incidentes** documenta as atividades envolvidas na resposta a incidentes de privacidade e os direitos dos titulares de dados. Com base nas leis e normas territoriais, setoriais e da indústria aplicáveis, as organizações devem garantir processos adequados para requisições de informações, direitos de privacidade e respostas a incidentes.		
		Competências		**Indicadores de desempenho**
5	7	VI.A	Responder às requisições de acesso do titular de dados e aos direitos de privacidade.	Garantir que os avisos e as políticas de privacidade sejam transparentes e articulem claramente os direitos do titular de dados.
				Cumprir as políticas de privacidade da organização relativas ao consentimento (por exemplo, retiradas de consentimento, requisições de retificação, objeções ao tratamento, acesso a dados e reclamações).
				Entender e cumprir as legislações internacionais, federais e estaduais estabelecidas em relação aos direitos de controle do titular de dados sobre suas informações pessoais (por exemplo, RGPD, HIPAA, CAN-SPAM, FOIA, CCPA/CPRA).
3	5	VI.B	Seguir os procedimentos organizacionais de tratamento e resposta a incidentes.	Realizar uma avaliação de risco sobre o incidente.
				Realizar atividades de contenção.
				Identificar e implementar medidas de remediação.
				Comunicar-se com stakeholders em conformidade com os requisitos de negócios, jurisdicionais e globais.
				Mobilizar a equipe de privacidade para revisar os fatos, determinar ações e executar planos.
				Manter um registro de incidentes e registros associados do incidente.
1	3	VI.C	Avaliar e modificar o atual plano de resposta a incidentes.	Realizar revisões pós-incidente para melhorar a eficácia do plano.
				Implementar mudanças para reduzir a probabilidade de novas violações.