PECB BEYOND RECOGNITION

Manual do candidato

ISO/IEC 27001
IMPLEMENTADOR LÍDER

Índice

SEÇÃO I: INTRODUÇÃO

Sobre o PECB

O PECB é um órgão de certificação que oferece formação[1] e certificação de acordo com a norma ISO/IEC 17024 a pessoas de uma ampla gama de disciplinas.

Ajudamos os profissionais a demonstrar comprometimento e competência, fornecendo a eles serviços valiosos de avaliação e certificação de acordo com normas reconhecidos internacionalmente. Nossa missão é fornecer serviços que inspirem confiança e melhoria contínua, demonstrem reconhecimento e beneficiem a sociedade como um todo.

Os principais objetivos do PECB são:

1. Estabelecer os requisitos mínimos necessários para a certificação de profissionais.
2. Analisar e verificar as qualificações dos candidatos para garantir que eles sejam elegíveis para solicitar a certificação.
3. Desenvolver e manter avaliações de certificação confiáveis.
4. Conceder certificações a candidatos qualificados, manter registros e publicar um diretório dos detentores de certificações válidas.
5. Estabelecer requisitos para a renovação periódica da certificação e garantir a conformidade com tais requisitos.
6. Garantir que os candidatos cumpram com os padrões éticos em sua prática profissional.
7. Representar seus membros, quando apropriado, em questões de interesse comum.
8. Promover os benefícios da certificação para organizações, empregadores, funcionários públicos, profissionais em campos relacionados e o público geral.

[1] O termo formação refere-se aos cursos de capacitação desenvolvidos pelo PECB e oferecidos globalmente por meio da nossa rede de parceiros.

O valor da certificação PECB

Por que escolher o PECB como seu organismo de certificação?

Reconhecimento global
Nossas certificações são reconhecidas internacionalmente e acreditadas pelo International Accreditation Service (IAS); signatário do Multilateral Recognition Arrangement (MLA) da IAF, que garante o reconhecimento mútuo da certificação acreditada entre os signatários do MLA e a aceitação da certificação acreditada em muitos mercados. Portanto, os profissionais que buscam uma credencial de certificação PECB se beneficiarão do reconhecimento da PECB em mercados nacionais e internacionais.

Equipe competente
A equipe do PECB é composta por profissionais competentes que possuem experiência relevante em diferentes setores. Todos os nossos funcionários possuem credenciais profissionais e estão em constante aperfeiçoamento para prestar serviços altamente satisfatórios aos nossos clientes.

Conformidade com as normas
Nossas certificações são uma demonstração de conformidade com a ISO/IEC 17024. Elas garantem que os requisitos da norma foram cumpridos e validados com a devida consistência, profissionalismo e imparcialidade.

Atendimento ao cliente
Somos uma empresa centrada nos clientes e tratamos todos com valorização, importância, profissionalismo e honestidade. O PECB tem uma equipe de especialistas dedicados a dar suporte às solicitações, problemas, preocupações, necessidades e opiniões dos clientes. Fazemos o possível para manter um tempo máximo de resposta de 24 horas sem comprometer a qualidade do serviço.

Código de Ética do PECB

Os profissionais do PECB devem:

1. Ter uma conduta profissional, com honestidade, acurácia, imparcialidade, responsabilidade e independência.
2. Sempre agir segundo os interesses de seu empregador, clientes, público geral e da profissão, aderindo aos padrões profissionais e às técnicas aplicáveis ao oferecer serviços profissionais.
3. Manter a competência em seus respectivos campos e esforçar-se para aprimorar constantemente suas capacidades profissionais.
4. Oferecer somente serviços profissionais para os quais estejam qualificados e informar adequadamente os clientes sobre a natureza dos serviços propostos, incluindo quaisquer questões ou riscos relevantes.
5. Informar cada empregador ou cliente sobre quaisquer interesses ou afiliações comerciais que possam influenciar seu discernimento ou prejudicar sua imparcialidade.
6. Tratar de maneira confidencial e privada todas as informações adquiridas durante negociações profissionais e comerciais de qualquer empregador ou cliente, atual ou anterior.
7. Respeitar todas as leis e regulamentos das jurisdições onde as atividades profissionais são realizadas.
8. Respeitar a propriedade intelectual e as contribuições de terceiros.
9. Não comunicar, intencionalmente ou não, informações falsas ou falsificadas que possam comprometer a integridade do processo de avaliação de um candidato a uma designação profissional.
10. Não agir de maneira que possa comprometer a reputação do PECB ou de seus programas de certificação.
11. Cooperar integralmente na investigação de uma suposta violação deste Código de Ética.

A versão completa do Código de Ética do PECB pode ser baixada neste link.

Introdução à ISO/IEC 27001 - Implementador Líder

A norma ISO/IEC 27001 especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). As habilidades mais importantes exigidas no mercado são a capacidade de planejar, implementar e gerenciar com eficácia o SGSI, avaliar e tratar os riscos de segurança da informação, selecionar e implementar os controles de segurança da informação e gerenciar (ou fazer parte de) equipes de implementação do SGSI.

A credencial de "Implementador Líder ISO/IEC 27001" é uma certificação profissional para indivíduos que desejam demonstrar a competência para implementar o sistema de gestão de segurança da informação e liderar uma equipe de implementação de SGSI.

Considerando que a função de implementação é uma das profissões mais demandadas, uma certificação reconhecida internacionalmente pode ajudar você a explorar o potencial de sua carreira e a atingir seus objetivos profissionais.

É importante observar que as certificações PECB não são uma licença ou uma simples filiação. Elas representam o reconhecimento por parte dos colegas de que um indivíduo demonstrou proficiência e compreensão de um conjunto de competências. As certificações PECB são concedidas a candidatos capazes de demonstrar sua experiência e que tenham sido aprovados em um exame padronizado na área de certificação.

O presente documento detalha o programa de certificação de Implementador Líder ISO/IEC 27001 do PECB em conformidade com a ISO/IEC 17024:2012. Este manual do candidato também contém informações sobre o processo pelo qual os candidatos podem obter e manter suas credenciais. É muito importante que você leia todas as informações incluídas neste manual do candidato antes de preencher e enviar sua inscrição. Em caso de dúvidas após a leitura, entre em contato com o escritório internacional do PECB pelo e-mail certification@pecb.com.

SEÇÃO II: PROCESSO DE CERTIFICAÇÃO E PREPARAÇÃO PARA EXAMES, REGRAS E POLÍTICAS DO PECB

Descubra qual é a certificação ideal para você

Todas as certificações PECB possuem requisitos específicos de formação e experiência profissional. Para determinar qual é a credencial mais adequada para você, verifique os critérios de elegibilidade para as várias certificações e as suas necessidades profissionais.

Prepare-se e agende o exame

Todos os candidatos são responsáveis pelo seu próprio estudo e preparação para os exames de certificação. Nenhum conjunto específico de cursos de formação ou currículo de estudos é exigido como parte do processo de certificação. No entanto, participar de um curso de formação pode aumentar significativamente as chances de os candidatos serem aprovados em um exame do PECB.

Para agendar um exame, os candidatos têm duas opções:

1. Entrar em contato com um de nossos parceiros que oferecem cursos de formação e exames. Para encontrar um centro de formação em uma determinada região, os candidatos devem acessar o link Parceiros ativos. O cronograma de cursos de formação do PECB também está disponível em Eventos de formação.
2. Fazer um exame do PECB remotamente de sua casa ou de qualquer local que desejar por meio do aplicativo PECB Exam, que pode ser acessado aqui: Eventos de exames.

Para saber mais sobre os exames, domínios de competência e declarações de conhecimento, consulte a Seção III deste documento.

Taxas de inscrição para exames e certificação

O PECB oferece exames diretos, que permitem que o candidato faça a prova sem participar do curso de formação. Os preços correspondentes são os seguintes:

- Exame para Líder: US$ 1000
- Exame para Gerente: US$ 700
- Exame para Fundamentos e Transição US $500

A taxa de inscrição para a certificação é de US$ 500.

Para todos os candidatos que tenham participado do curso de formação e feito o exame com um dos parceiros do PECB, a taxa de inscrição inclui apenas os custos associados ao exame, à inscrição para a certificação e ao primeiro ano da Taxa de Manutenção Anual (AMF).

Domínios de competência

O objetivo do exame "Implementador Líder PECB ISO/IEC 27001" é garantir que o candidato tenha adquirido as competências necessárias para apoiar uma organização no estabelecimento, implementação, gerenciamento e manutenção do sistema de gestão de segurança da informação (SGSI) com base nos requisitos da ISO/IEC 27001.

A certificação de Implementador Líder ISO/IEC 27001 é destinada a:

- Gerentes ou consultores envolvidos e interessados na implementação de um sistema de gestão de segurança da informação em uma organização.
- Gerentes de projetos, consultores ou assessores especializados que buscam dominar a implementação de um sistema de gestão de segurança da informação.
- Indivíduos responsáveis por manter a conformidade com os requisitos da ISO/IEC 27001 em uma organização.
- Membros de uma equipe de implementação de SGSI.

O exame abrange os seguintes domínios de competência:

- **Domínio 1:** Princípios e conceitos fundamentais de um sistema de gestão de segurança da informação (SGSI)
- **Domínio 2:** Sistema de gestão de segurança da informação (SGSI)
- **Domínio 3:** Planejamento da implementação de um SGSI com base na ISO/IEC 27001
- **Domínio 4:** Implementação de um SGSI com base na ISO/IEC 27001
- **Domínio 5:** Monitoramento e medição de um SGSI com base na ISO/IEC 27001
- **Domínio 6:** Melhoria contínua de um SGSI com base na ISO/IEC 27001
- **Domínio 7:** Preparação para uma auditoria de certificação de um SGSI

Domínio 1: Princípios e conceitos fundamentais de um sistema de gestão de segurança da informação (SGSI)

Objetivo principal: Assegurar que o candidato compreenda e seja capaz de interpretar os princípios e conceitos da ISO/IEC 27001

Competências	Declarações de conhecimento
1. Capacidade de entender e explicar os principais conceitos de segurança da informação 2. Capacidade de explicar a diferença e a relação entre informação e ativo 3. Capacidade de entender a diferença entre documentos, especificações e registros 4. Capacidade de entender a relação entre os conceitos de vulnerabilidades, ameaças, riscos e seus impactos 5. Capacidade de entender os conceitos de confidencialidade, integridade e disponibilidade da informação 6. Capacidade de entender e interpretar a classificação dos controles de segurança e seus objetivos 7. Capacidade de entender a relação entre os elementos da segurança da informação	1. Conhecimento das leis, regulamentações, normas internacionais e do setor, contratos, práticas de mercado, políticas internas, melhores práticas etc., que uma organização deve cumprir 2. Conhecimento dos principais conceitos e da terminologia da ISO/IEC 27001 3. Conhecimento dos riscos em segurança da informação e sua importância em um SGSI 4. Conhecimento da confidencialidade, integridade e disponibilidade das informações 5. Conhecimento das vulnerabilidades, ameaças e riscos em segurança da informação 6. Conhecimento dos possíveis impactos que podem afetar a confidencialidade, integridade ou disponibilidade das informações 7. Conhecimento das diferenças entre os tipos de controle de segurança, como controles técnicos, legais, administrativos e gerenciais 8. Conhecimento das diferenças entre os controles de segurança classificados por função, como controles preventivos, corretivos e de detecção

Domínio 2: Sistema de Gestão de Segurança da Informação (SGSI)

Objetivo principal: Garantir que o candidato compreenda e seja capaz de implementar os controles de segurança listados no Anexo A da ISO/IEC 27001

Competências	Declarações de conhecimento
1. Capacidade de selecionar, projetar e descrever controles de segurança da informação 2. Capacidade de definir a arquitetura de segurança da organização 3. Capacidade de identificar e ilustrar as atividades envolvidas no desenvolvimento e na implantação de sistemas de informação 4. Capacidade de documentar a implementação dos controles de segurança da informação selecionados 5. Capacidade de entender, interpretar e analisar os controles do Anexo A da ISO/IEC 27001 6. Capacidade de implementar os controles do Anexo A com base na ISO/IEC 27001 e nas melhores práticas	1. Conhecimento de serviços de segurança comuns, como serviços de controle de acesso, serviços de controle de perímetro, serviços de integridade, serviços criptográficos e serviços de auditoria e monitoramento 2. Conhecimento das estruturas ou frameworks de arquitetura mais comuns 3. Conhecimento dos 93 controles do Anexo A da ISO/IEC 27001 4. Conhecimento dos quatro grupos de controles do Anexo A, como controles organizacionais, controles de pessoas, controles físicos e controles tecnológicos 5. Conhecimento da seleção e implementação dos controles do Anexo A da ISO/IEC 27001 6. Conhecimento da documentação dos controles de segurança da informação selecionados

PECB

Domínio 3: Planejamento da implementação de um SGSI com base na ISO/IEC 27001

Objetivo principal: Garantir que o candidato seja capaz de planejar a implementação do SGSI com base na ISO/IEC 27001

Competências	Declarações de conhecimento
1. Capacidade de coletar, analisar e interpretar as informações necessárias para planejar a implementação de um SGSI	1. Conhecimento dos principais conceitos, terminologia, processos e melhores práticas de gestão de projetos
2. Capacidade de compreender e definir os objetivos de segurança da informação e do SGSI	2. Conhecimento das principais abordagens e metodologias usadas na implementação de um SGSI
3. Capacidade de identificar e interpretar os riscos do SGSI e seus impactos	3. Conhecimento dos objetivos típicos de segurança da informação e do SGSI, e como alcançar resultados específicos
4. Capacidade de analisar e considerar os contextos interno e externo de uma organização	4. Conhecimento dos aspectos que normalmente constituem os contextos interno e externo de uma organização
5. Capacidade de identificar os recursos necessários para a implementação do SGSI	5. Conhecimento das abordagens usadas para entender o contexto de uma organização
6. Capacidade de gerenciar, estimar e monitorar os recursos necessários para a implementação do SGSI	6. Conhecimento das técnicas usadas para coletar informações sobre uma organização e como realizar uma análise de lacunas de um sistema de gestão
7. Capacidade de identificar as funções e responsabilidades das principais partes interessadas durante e após a implementação e operação de um SGSI	7. Conhecimento de um plano de projeto de SGSI, bem como de uma equipe de projeto de SGSI
8. Capacidade de redigir, arquivar e revisar um plano de projeto de SGSI	8. Conhecimento dos recursos necessários para a implementação de um SGSI
9. Capacidade de realizar uma análise de lacunas e esclarecer os objetivos de gestão da segurança da informação	9. Conhecimento das principais estruturas organizacionais aplicáveis para que uma organização gerencie um SGSI
10. Capacidade de definir e justificar um escopo de SGSI adaptado aos objetivos específicos de segurança da informação da organização	10. Conhecimento das características do escopo de um SGSI em termos de limites organizacionais, tecnológicos e físicos
11. Capacidade de desenvolver e estabelecer uma política de SGSI	11. Conhecimento das melhores práticas e técnicas usadas para redigir e estabelecer políticas e procedimentos de segurança da informação
12. Capacidade de executar as diferentes etapas do processo de avaliação de riscos	12. Conhecimento das diferentes abordagens e metodologias usadas para realizar o processo de avaliação de riscos
13. Capacidade de compreender e redigir o documento de Declaração de Aplicabilidade	13. Conhecimento das características do documento de Declaração de Aplicabilidade

Domínio 4: Implementação de um SGSI com base na ISO/IEC 27001

Objetivo principal: Garantir que o candidato seja capaz de implementar um SGSI com base nos requisitos da ISO/IEC 27001

Competências

1. Capacidade de gerenciar processos de capacitação para a implementação bem-sucedida de um SGSI.
2. Capacidade de estabelecer os processos de documentação e gestão de registros necessários para apoiar a implementação e as operações de um SGSI.
3. Capacidade de definir, projetar e implementar os processos necessários para a operação de um SGSI e documentá-los de forma adequada.
4. Capacidade de compreender, gerenciar e avaliar o conhecimento organizacional.
5. Capacidade de compreender as tendências e tecnologias atuais, como big data, inteligência artificial, aprendizagem de máquina, computação em nuvem e operações terceirizadas.
6. Capacidade de elaborar e implementar programas adequados de formação e conscientização em segurança da informação, bem como planos de comunicação.
7. Capacidade de estabelecer um plano de comunicação de SGSI para auxiliar na compreensão dos problemas, políticas e desempenho da segurança da informação de uma organização, além de fornecer sugestões para melhorar o desempenho do SGSI.
8. Capacidade de estabelecer uma política de gestão de incidentes e uma equipe de resposta a incidentes.
9. Capacidade de compreender a diferença entre continuidade de negócios e recuperação de desastres.

Declarações de conhecimento

1. Conhecimento das melhores práticas de gestão do ciclo de vida de informações documentadas.
2. Conhecimento das características e das diferenças entre as diversas informações documentadas relacionadas a uma política, procedimento, diretriz, norma, base de referência, planilha, etc., de um SGSI.
3. Conhecimento dos três V's em big data: volume, variedade e velocidade.
4. Conhecimento de inteligência artificial forte e fraca e aprendizagem de máquina.
5. Conhecimento dos serviços de computação em nuvem: infraestrutura como serviço (IaaS), plataforma como serviço (PaaS) e software como serviço (SaaS).
6. Conhecimento do impacto das novas tecnologias na segurança da informação.
7. Conhecimento das características e das melhores práticas de implementação de programas de formação e conscientização em segurança da informação, além de de planos de comunicação.
8. Conhecimento dos objetivos de comunicação, das atividades e das partes interessadas para aumentar seu apoio e confiança.
9. Conhecimento do processo de gestão de incidentes com base nas melhores práticas de segurança da informação.
10. Conhecimento da continuidade dos negócios e da recuperação de desastres.

PECB

Domínio 5: Monitoramento e medição de um SGSI com base na ISO/IEC 27001 **Objetivo principal:** Garantir que o candidato seja capaz de analisar, avaliar, monitorar e medir o desempenho de um SGSI.	
Competências	**Declarações de conhecimento**
1. Capacidade de monitorar e avaliar a eficácia de um SGSI. 2. Capacidade de verificar em que medida os objetivos identificados do SGSI foram alcançados. 3. Capacidade de desenvolver e implementar um programa de auditoria interna de um SGSI. 4. Capacidade de realizar revisões regulares e metódicas para garantir a adequação, eficácia e eficiência de um SGSI com base nas políticas e objetivos da organização. 5. Capacidade de desenvolver e executar um processo de análise crítica pela direção.	1. Conhecimento das melhores práticas e técnicas utilizadas para monitorar e avaliar a eficácia de um SGSI. 2. Conhecimento dos conceitos relacionados à medição e avaliação. 3. Conhecimento dos principais conceitos e componentes relacionados à implementação e operação de um programa de auditoria interna de um SGSI. 4. Conhecimento da diferença entre não conformidades maiores e menores. 5. Conhecimento das diretrizes e melhores práticas para elaborar um relatório de não conformidade. 6. Conhecimento das melhores práticas utilizadas para realizar análises críticas pela direção.

PECB

Domínio 6: Melhoria contínua de um SGSI com base na ISO/IEC 27001 **Objetivo principal:** Garantir que o candidato seja capaz de fornecer orientações sobre a melhoria contínua de um SGSI:	
Competências	**Declarações de conhecimento**
1. Capacidade de rastrear e adotar medidas em relação a não conformidades. 2. Capacidade de identificar e analisar as causas-raiz das não conformidades e propor planos de ação para tratá-las. 3. Capacidade de assessorar uma organização sobre como melhorar continuamente a eficácia e eficiência de um SGSI. 4. Capacidade de implementar processos de melhoria contínua em uma organização. 5. Capacidade de determinar as ferramentas adequadas para apoiar os processos de melhoria contínua de uma organização.	1. Conhecimento dos principais processos, ferramentas e técnicas usadas para identificar as causas básicas das não conformidades. 2. Conhecimento do processo de tratamento de não conformidades. 3. Conhecimento dos principais processos, ferramentas e técnicas utilizados para desenvolver planos de ações corretivas. 4. Conhecimento dos principais conceitos relacionados à melhoria contínua. 5. Conhecimento dos processos relacionados ao monitoramento contínuo de fatores de mudança. 6. Conhecimento da manutenção e melhoria de um SGSI.

Domínio 7: Preparação para uma auditoria de certificação de um SGSI

Objetivo principal: Garantir que o candidato a Implementador Líder ISO/IEC 27001 seja capaz de preparar uma organização para a certificação da ISO/IEC 27001.

Competências	Declarações de conhecimento
1. Capacidade de compreender as principais etapas, processos e atividades relacionados à auditoria de certificação da ISO/IEC 27001. 2. Capacidade de compreender, explicar e ilustrar a abordagem baseada em evidências em uma auditoria de SGSI. 3. Capacidade de assessorar uma organização na identificação e seleção de um organismo de certificação que atenda às suas expectativas. 4. Capacidade de determinar se uma organização está pronta e preparada para a auditoria de certificação da ISO/IEC 27001. 5. Capacidade de treinar e preparar a equipe de uma organização para a auditoria de certificação da ISO/IEC 27001. 6. Capacidade de argumentar e contestar os resultados e conclusões da auditoria com auditores externos.	1. Conhecimento da abordagem de auditoria baseada em evidências. 2. Conhecimento dos tipos de auditoria e suas diferenças. 3. Conhecimento das diferenças entre a Fase 1 e a Fase 2 da auditoria. 4. Conhecimento dos requisitos, etapas e atividades da Fase 1 da auditoria. 5. Conhecimento dos critérios de análise da informação documentada. 6. Conhecimento dos requisitos, etapas e atividades da Fase 2 da auditoria. 7. Conhecimento dos requisitos, etapas e atividades da auditoria de acompanhamento. 8. Conhecimento dos requisitos, etapas e atividades das auditorias de vigilância e recertificação. 9. Conhecimento dos requisitos, diretrizes e melhores práticas para desenvolver planos de ação após uma auditoria de certificação da ISO/IEC 27001.

Com base nos domínios mencionados acima e em sua relevância, o exame é composto 80 questões, conforme resumido na tabela abaixo:

				Nível de compreensão exigido (cognitivo/taxonomia)	
		Número de perguntas/pontos por domínio de competência	% do exame dedicado/pontos para cada domínio de competência	Perguntas que avaliam a compreensão, aplicação e análise	Perguntas que medem a síntese e a avaliação
Domínios de competência	Princípios e conceitos fundamentais de um sistema de gestão de segurança da informação (SGSI)	15	18.75	X	
	Sistema de gestão da segurança da informação (SGSI)	12	15	X	
	Planejamento da implementação de um SGSI com base na ISO/IEC 27001	18	22.5		X
	Implementação de um SGSI com base na ISO/IEC 27001	14	17.5		X
	Monitoramento e medição de um SGSI com base na ISO/IEC 27001	10	12.5	X	
	Melhoria contínua de um SGSI com base na ISO/IEC 27001	6	7.5	X	
	Preparação para uma auditoria de certificação de um SGSI	5	6.25		X
	Total	**80**	**100%**		
	Número de perguntas por nível de compreensão:			**43**	**37**
	% do exame dedicado a cada nível de compreensão (cognitivo/taxonomia):			**53.75%**	**46.25%**

A pontuação mínima para aprovação no exame é de 70%.

Após a aprovação no exame, os candidatos poderão solicitar a credencial de "Implementador Líder ISO/IEC 27001Certificado pelo PECB" dependendo do seu nível de experiência.

Como fazer o exame

Informações gerais sobre o exame

Os candidatos devem chegar com pelo menos 30 minutos de antecedência do início do exame. Candidatos que chegarem atrasados não receberão tempo adicional para compensar o atraso e e podem não ser autorizados a fazer o exame.

Os candidatos devem trazer um documento de identidade válido (carteira de identidade nacional, carteira de motorista ou passaporte) e mostrá-lo ao fiscal.

Se solicitado no dia do exame (para exames em papel), poderá ser concedido tempo adicional aos candidatos que fizerem o exame em um idioma que não seja sua língua nativa, da seguinte forma:

- 10 minutos adicionais para exames de Fundamentos
- 20 minutos adicionais para exames de Gestor
- 30 minutos adicionais para exames de Líder

Formato e tipos de exames PECB

1. **Em papel:** Os exames são feitos cópias físicas, e os candidatos não podem usar nada além do caderno de exame e uma caneta. Não é permitido o uso de dispositivos eletrônicos, como laptops, tablets ou telefones. A sessão de exame é supervisionada por um fiscal aprovado pelo PECB no local onde o Parceiro organizou o curso de formação.
2. **Online:** Os exames são realizados eletronicamente via a aplicação de Exames PECB. Não é permitido o uso de dispositivos eletrônicos, como tablets e telefones. A sessão do exame é supervisionada remotamente por um Fiscal PECB via a aplicação de Exames PECB e uma câmera externa/integrada.

Para obter informações mais detalhadas sobre o formato online, consulte o Guia de Exames Online do PECB.

Os exames PECB estão disponíveis em dois tipos:
1. Exame com questões dissertativas
2. Exame com questões de múltipla escolha

Este exame contém questões de múltipla escolha: Este formato foi escolhido por ter se mostrado ser eficaz e eficiente para medir e avaliar os resultados de aprendizagem relacionados aos domínios de competência estabelecidos. O exame de múltipla escolha pode ser usado para avaliar a compreensão de um candidato sobre muitos assuntos, incluindo conceitos simples e complexos. Ao responder a essas questões, os candidatos terão de aplicar diversos princípios, analisar problemas, avaliar alternativas, combinar vários conceitos ou ideias, etc. As questões de múltipla escolha são baseadas em cenários, o que significa que são elaboradas com base em um cenário que os candidatos devem ler e responder a uma ou mais questões relacionadas a esse cenário. Este exame de múltipla escolha é "com consulta", devido à característica dependente de contexto das perguntas: Você encontrará exemplos de perguntas abaixo.

Como o exame é "com consulta", os candidatos estão autorizados a usar os seguintes materiais de referência:
- Uma cópia da norma ISO/IEC 27001
- Materiais do curso de capacitação (acessados pelo aplicativo PECB Exams e/ou impressos)
- Anotações pessoais feitas durante o curso de
- de capacitação (acessadas pelo aplicativo PECB Exams e/ou impressas)
- Um dicionário impresso

Qualquer tentativa de cópia, conluio ou de fraude durante a sessão de exame levará à reprovação automática.

Os exames PECB estão disponíveis em inglês e também em outros idiomas. Para saber se o exame está disponível em um idioma específico, entre em contato com examination@pecb.com.

Observação: O PECB fará uma transição progressiva para exames de múltipla escolha. Eles também serão com consulta e incluirão perguntas baseadas em cenários que permitirão que o PECB avalie o conhecimento, habilidades e competências dos candidatos para usar informações em novas situações (aplicar), estabelecer conexões entre ideias (analisar) e justificar uma posição ou decisão (avaliar). Todos as questões dos exames de múltipla escolha do PECB têm uma pergunta e três alternativas, das quais apenas uma é correta.

Para informações específicas sobre tipos de exame, idiomas disponíveis e outros detalhes, visite o site Lista de exames PECB.

Exemplos de questões de exames

Cenário:

A Empresa A é uma seguradora com sede em Chicago. Ela oferece uma ampla gama de serviços e produtos que envolvem seguros de saúde e de automóveis. Recentemente, a empresa se tornou uma das maiores e mais bem-sucedidas seguradoras, com mais de 70 escritórios em todo os EUA.

Os objetivos da empresa são manter adequadamente seus ativos e proteger a confidencialidade das informações de seus clientes.
A empresa decidiu obter a certificação ISO/IEC 27001, pois isso a ajudaria não apenas a atingir seus objetivos organizacionais e a cumprir as leis e regulamentos internacionais, mas também a aumentar sua reputação. A empresa iniciou a implementação do SGSI com a definição de uma estratégia baseada em uma análise detalhada de seus processos existentes e dos requisitos do SGSI.
A empresa prestou atenção especial à avaliação de riscos de segurança da informação, o que foi crucial para entender as ameaças e vulnerabilidades que enfrentava.
Ela também definiu os critérios de risco com o objetivo de avaliar os riscos identificados.

A Empresa A experimentou um rápido crescimento que resultou em um processamento de dados complexo e intensivo. Com base nos resultados da avaliação de riscos, decidiu inicialmente atualizar seu esquema de classificação de informações existente e, em seguida, implementar os controles de segurança necessários com base no nível de proteção exigido por cada classificação de informações.

As solicitações médicas de seus clientes, classificadas como informações confidenciais, foram criptografadas usando a criptografia AES e então transferidas para a nuvem privada. A Empresa A utilizou o armazenamento em nuvem pela facilidade de acesso. Devido ao acesso frequente de seus funcionários a esse serviço, a empresa também decidiu utilizar o processo de registro de logs. O serviço foi configurado para conceder o acesso automático ao armazenamento em nuvem para todos os funcionários responsáveis pelo processamento de solicitações médicas.

Devido ao fato de que os serviços de armazenamento em nuvem sofreram violações de segurança, seja por erro humano ou ataques deliberados, o departamento de TI da empresa decidiu restringir o acesso a informações confidenciais armazenadas na nuvem se não fossem usados e-mails profissionais corporativos. Além disso, eles utilizaram um software de gestão de senhas para esses endereços de e-mail e foram geradas senhas mais fortes.

Com base nesse cenário, responda às seguintes questões:

1. **O departamento de TI não restringiu o acesso ao armazenamento em nuvem. Qual das ameaças abaixo pode explorar essa vulnerabilidade?**
   A. Alteração do hardware
   B. **Uso não autorizado de informações confidenciais**
   C. Treinamento insuficiente em armazenamento em nuvem

2. **A Empresa A criptografa informações confidenciais antes de transferi-las para a nuvem. Qual princípio de segurança da informação é seguido nesse caso?**
   A. **Confidencialidade, porque a criptografia garante que somente usuários autorizados possam acessar as informações criptografadas.**
   B. Disponibilidade, porque a criptografia garante que as informações estejam protegidas tanto em repouso quanto em trânsito, portanto acessíveis quando necessário.
   C. Integridade, porque a criptografia garante que somente modificações autorizadas sejam feitas nas informações criptografadas.

3. **A Empresa A decidiu restringir o acesso a informações confidenciais armazenadas na nuvem se não fossem usados e-mails profissionais corporativos. Qual controle de segurança foi implementado nesse caso?**
   A. Controle de detecção
   B. **Controle preventivo**
   C. Controle corretivo

4. **A Empresa A definiu os critérios de risco ao avaliar seus riscos. Isso é necessário?**
   A. **Sim, porque a empresa deve estabelecer e manter os critérios de risco ao avaliar os riscos de segurança da informação.**
   B. Não, porque os critérios de risco devem ser estabelecidos somente quando as opções de tratamento de risco forem definidas.
   C. Não, porque os critérios de risco são estabelecidos quando os riscos residuais de segurança da informação são aceitos.

Resultados de exames

Os resultados dos exames serão comunicados via e-mail.

- O prazo para a divulgação começa a partir da data do exame e é de duas a quatro semanas para exames de múltipla escolha em papel.

- Para exames de múltipla escolha online, os candidatos recebem seus resultados instantaneamente.

Os candidatos que forem bem-sucedidos no exame poderão se candidatar a uma das credenciais do respectivo esquema de certificação.

Para os candidatos reprovados no exame, será incluída no e-mail uma lista dos domínios em que o desempenho foi insatisfatório para ajudá-los a se preparar melhor em uma nova tentativa.

Política de reaplicação de exames

Não há limite para o número de vezes que um candidato pode refazer um exame. Entretanto, há certas limitações quanto ao de intervalo entre as novas tentativas de exame.

- Se um candidato não for aprovado no exame na primeira tentativa, ele/ela deverá aguardar 15 dias após a data inicial do exame para a próxima tentativa (primeira repetição).

  Nota: Candidatos que completaram o curso de formação com um de nossos parceiros e não passaram na primeira tentativa do exame têm direito a refazer o exame gratuitamente em um período de 12 meses a partir da data de recebimento do código do cupom, pois a taxa paga pelo curso inclui duas tentativas de exame. Caso contrário, serão cobradas taxas de reaplicação de exame.

Para os candidatos que não passarem na segunda tentativa, o PECB recomenda que participem de um curso de formação para se prepararem melhor para o exame.

Para agendar a segunda tentativa, com base no formato do exame, os candidatos que completaram um curso de formação devem seguir os seguintes passos:

1. Exame on-line: ao agendar a segunda tentativa do exame, use o código de cupom inicial para isentar-se da taxa.
2. Exame em papel: os candidatos precisam entrar em contato com o parceiro/distribuidor do PECB que inicialmente organizou a sessão para agendar a repetição do exame (data, hora, local, custos).

Os candidatos que não concluíram um curso de formação com um parceiro, mas fizeram o exame on-line diretamente com o PECB, não se enquadram nessa política. O processo para agendar a repetição do exame é o mesmo que para o exame inicial.

Segurança do exame

Um componente importante de uma credencial de certificação profissional é a manutenção da segurança e da confidencialidade do exame. O PECB confia no comportamento ético dos titulares de certificações e candidatos para manter a segurança e a confidencialidade dos exames do PECB. Qualquer divulgação de informações sobre o conteúdo dos exames do PECB é uma violação direta do Código de Ética do PECB. O PECB tomará medidas contra quaisquer indivíduos que violem tais regras e políticas, incluindo a proibição permanente de buscar credenciais do PECB e a revogação de quaisquer credenciais anteriores. O PECB também tomará medidas legais contra indivíduos ou organizações que infringirem seus direitos autorais, direitos proprietários e propriedade intelectual.

Reagendamento do exame

Para quaisquer alterações relativas à data, hora, local ou outros detalhes do exame, favor entrar em contato com examination@pecb.com.

Solicitação de certificação

Todos os candidatos aprovados no exame (ou equivalente aceito pelo PECB) têm o direito de solicitar as credenciais do PECB para as quais foram examinados. É necessário atender a requisitos educacionais e profissionais específicos para obter uma certificação PECB. Os candidatos devem preencher o formulário de solicitação de certificação on-line (que pode ser acessado por meio do perfil on-line do PECB), incluindo os detalhes de referências que serão contatadas para validar a experiência profissional do candidato. Os candidatos podem enviar sua solicitação em vários idiomas. Os candidatos podem optar por pagar on-line ou receber uma fatura. Para obter mais informações, entre em contato com certification@pecb.com.

O processo de solicitação da certificação on-line é muito simples e leva apenas alguns minutos, conforme descrito a seguir:

- Registro de conta
- Verificar o link de confirmação em seu e-mail
- Fazer log in para solicitar a certificação

Para mais informações sobre o processo de solicitação, siga as instruções do seguinte manual: Solicitação de certificação.

A solicitação é aprovada assim que o Departamento de Certificação validar que o candidato atende a todos os requisitos de certificação relativos à respectiva credencial. Será enviado um e-mail ao endereço eletrônico fornecido durante o processo de solicitação para comunicar o status da solicitação. Se aprovado, os candidatos poderão fazer o download da certificação em sua Conta PECB.

O PECB oferece suporte tanto em inglês quanto em francês.

Renovação da certificação

As certificações do PECB são válidas por três anos. Para mantê-las, os candidatos devem demonstrar a cada ano que ainda estão realizando tarefas relacionadas à certificação. Os profissionais certificados pelo PECB devem fornecer anualmente créditos de Desenvolvimento Profissional Contínuo (CPD) e pagar a Taxa de Manutenção Anual (AMF) de US$ 100 para manter a certificação. Para mais informações, visite a página de Manutenção da Certificação no site do PECB.

Encerramento de um caso

Se os candidatos não solicitarem a certificação dentro de três anos, seu caso será encerrado. Mesmo que o período de certificação expire, os candidatos têm o direito de reabrir seu caso. No entanto, o PECB não será mais responsável por quaisquer alterações relativas às condições, normas, políticas e manual do candidato que eram aplicáveis antes do encerramento do caso. O candidato que solicitar a reabertura de seu caso deverá fazê-lo por escrito e pagar a respectiva taxa.

SEÇÃO III: REQUISITOS DE CERTIFICAÇÃO

Implementador Líder ISO/IEC 27001

Os requisitos para as certificações Implementador ISO/IEC 27001do PECB são:

Credencial	Exame	Experiência profissional	Experiência em projetos SG	Outros requisitos
Implementador Provisório ISO/IEC 2700 Certificado pelo PECB	Exame de Implementador Líder ISO/IEC 27001 certificado pelo PECB ou equivalente	Não há	Não há	Assinatura do Código de Ética do PECB
Implementador ISO/IEC 27001 certificado pelo PECB	Exame de Implementador Líder ISO/IEC 27001 certificado pelo PECB ou equivalente	Dois anos: Um ano de experiência profissional em gestão de segurança da informação	Atividades de projetos: total de 200 horas	Assinatura do Código de Ética do PECB
Implementador Líder ISO/IEC 27001 certificado pelo PECB	Exame de Implementador Líder ISO/IEC 27001 certificado pelo PECB ou equivalente	Cinco anos: Dois anos de experiência profissional em gestão de segurança da informação	Atividades de projetos: total de 300 horas	Assinatura do Código de Ética do PECB
Implementador Líder Senior ISO/IEC 27001 certificado pelo PECB	Exame de Implementador Líder ISO/IEC 27001 certificado pelo PECB ou equivalente	Dez anos: Sete anos de experiência profissional em gestão de segurança da informação	Atividades de projetos: total de 1.000 horas	Assinatura do Código de Ética do PECB

Para serem consideradas válidas, as atividades de implementação devem seguir as melhores práticas de implementação e gestão e incluir:

1. Elaboração do plano de SGSI
2. Iniciação da implementação do SGSI
3. Implementação do SGSI
4. Gestão, monitoramento e manutenção do SGSI
5. Identificação e atuação sobre oportunidades de melhoria contínua

SEÇÃO IV: REGRAS E POLÍTICAS DE CERTIFICAÇÃO

Referências profissionais

São necessárias duas referências profissionais para cada solicitação. Elas devem ser de indivíduos que tenham trabalhado com o candidato em um ambiente profissional e possam validar sua experiência em projetos de segurança da informação, bem como seu histórico de trabalho atual e anterior. Não são válidas referências profissionais de pessoas que estejam sob a supervisão do candidato ou que sejam seus parentes.

Experiência profissional

Os candidatos devem fornecer informações completas e corretas sobre sua experiência profissional, incluindo cargo(s), data(s) de início e término, descrição(ões) do cargo, entre outras. Recomenda-se que os candidatos façam um resumo de suas atribuições anteriores ou atuais, fornecendo detalhes suficientes para descrever a natureza das responsabilidades de cada cargo. As informações mais detalhadas podem ser incluídas no currículo.

Experiência em projetos de SGSI

O histórico de projetos de SGSI do candidato será verificado para garantir que ele tenha a quantidade necessária de horas de implementação.

Avaliação das solicitações de certificação

O Departamento de Certificação irá avaliar cada solicitação para validar a elegibilidade do candidato para a certificação. Os candidatos cujas inscrições estiverem sendo analisadas serão notificados por escrito e, se necessário, receberão um prazo razoável para fornecer documentação adicional. Se o candidato não responder até o prazo final ou não fornecer a documentação necessária dentro do prazo determinado, o Departamento de Certificação irá validar a solicitação com base nas informações iniciais fornecidas, o que pode resultar no rebaixamento para uma credencial inferior.

Indeferimento da certificação

O PECB pode negar a certificação se os candidatos:

- Falsificarem a inscrição
- Violarem os procedimentos do exame
- Violarem o Código de Ética do PECB
- Falharem no exame

Para mais informações detalhadas, consulte a seção “Reclamações e Recursos”.

O pagamento da solicitação para a certificação não é reembolsável.

Suspensão da certificação

O PECB pode suspender temporariamente a certificação se o candidato não atender aos requisitos. Os motivos para a suspensão da certificação incluem:

- O PECB receber grandes quantidades de reclamações sérias das partes interessadas (a suspensão será aplicada até que uma investigação seja concluída).
- Os logotipos do PECB ou dos organismos de acreditação serem intencionalmente usados de forma indevida.
- O candidato não corrigir o uso indevido de uma marca de certificação dentro do prazo determinado pelo PECB.
- O indivíduo certificado solicitar voluntariamente uma suspensão.
- O PECB considerar apropriadas outras condições para a suspensão da certificação.

Revogação da certificação

O PECB pode revogar a certificação se o candidato não cumprir os requisitos do PECB. Os candidatos não poderão mais se apresentar como profissionais certificados pelo PECB. Os motivos para a revogação da certificação incluem:

- Violação do Código de Ética do PECB.

- Distorção e fornecimento de informações falsas sobre o escopo da certificação.
- Infração de quaisquer outras regras do PECB.

Upgrade de credenciais

Os profissionais podem solicitar o upgrade para uma credencial superior assim que demonstrarem que cumprem os requisitos.

Para solicitar um upgrade, os candidatos precisam fazer login na sua Conta PECB, visitar a aba “Minhas Certificações” e clicar no link “Upgrade”. A taxa de solicitação de upgrade é de US$ 100.

Downgrade de credenciais

Uma Certificação PECB pode ser rebaixada para uma credencial inferior devido aos seguintes motivos:

- A Taxa Anual de Manutenção (AMF) não foi paga.
- As horas de Desenvolvimento Profissional Contínuo (CPD) não foram submetidas.
- Foram apresentadas horas de CPD insuficientes.
- A comprovação das horas de CPD não foi apresentada quando solicitada.

Observação: *Os profissionais certificados pelo PECB que possuírem Certificações Líder e não fornecerem evidências dos requisitos de manutenção da certificação terão suas credenciais rebaixadas. Por outro lado, os titulares de Certificação Master que não apresentarem CPDs e não pagarem AMFs terão suas certificações revogadas.*

Outros status

Além de estar ativa, suspensa ou revogada, uma certificação pode ser voluntariamente retirada ou designada como Emérita. Para mais informações sobre esses status e o status de interrupção permanente, e como solicitá-los, visite Opções de status de certificações.

SEÇÃO V: POLÍTICAS GERAIS DO PECB

Código de Ética do PECB

A adesão ao Código de Ética do PECB é um compromisso voluntário. É importante que os profissionais certificados pelo PECB não apenas sigam os princípios deste Código, mas também incentivem e apoiem a adesão de outras pessoas. Mais informações podem ser encontradas aqui.

Outros exames e certificações

O PECB aceita certificações e exames de outros organismos de certificação acreditados e reconhecidos. O PECB avaliará as solicitações por meio do seu processo de equivalência para decidir se as respectivas certificações ou exames podem ser aceitos como equivalentes à respectiva certificação do PECB (por exemplo, a certificação Auditor Líder ISO/IEC 27001).

Não discriminação e adaptações especiais

Todas as solicitações de candidatos serão avaliadas objetivamente, independentemente da idade, gênero, etnia, religião, nacionalidade ou estado civil do candidato.

Para garantir igualdade de oportunidades para todas as pessoas qualificadas, o PECB fará adaptações razoáveis para os candidatos, quando apropriado. Se os candidatos precisarem de adaptações especiais devido a uma deficiência ou condição física específica, eles devem informar o Parceiro/Distribuidor para que possam fazer os arranjos adequados. Todas as informações que os candidatos fornecerem sobre sua deficiência/necessidade serão tratadas com total confidencialidade.

Clique aqui para baixar o Formulário de Candidatos com Deficiências.

Reclamações e recursos

Qualquer reclamação deve ser feita no máximo 30 dias após receber a decisão de certificação. O PECB fornecerá uma resposta por escrito ao candidato dentro de 30 dias úteis após o recebimento da reclamação. Se o candidato não estiver satisfeito com a resposta, ele tem o direito de apresentar um recurso. Para mais informações sobre os procedimentos de reclamações e apelações, clique aqui.

(1) De acordo com a ADA, o termo "adaptação razoável" pode incluir: (A) tornar as instalações existentes utilizadas pelos funcionários prontamente acessíveis e utilizáveis por indivíduos com deficiência; e

(B) reestruturação do trabalho, horários de trabalho em tempo parcial ou modificados, reatribuição para uma posição vaga, aquisição ou modificação de equipamentos ou dispositivos, ajuste ou modificações apropriadas de exames, materiais de formação ou políticas, fornecimento de leitores ou intérpretes qualificados e outras adaptações semelhantes para indivíduos com deficiência.

(2) Lei de Emendas da ADA de 2008 (P.L. 110-325) Seção 12189. Exames e cursos. [Seção 309]: Qualquer pessoa que ofereça exames ou cursos relacionados a candidaturas, licenciamento, certificação ou credenciamento para educação secundária ou pós-secundária, profissional ou de comércio, deve oferecer tais exames ou cursos em um local e de maneira acessível a pessoas com deficiência ou oferecer arranjos alternativos acessíveis para tais indivíduos.

Endereço:
Sede da empresa
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax.
T: +1-844-426-7322
F: +1-844-329-7322

Centro de Ajuda PECB
Visite nosso Centro de Ajuda para consultar as Perguntas Frequentes (FAQ), visualizar manuais de uso do site e das aplicações PECB, ler documentos relacionados aos processos do PECB ou entrar em contato conosco por meio do sistema de acompanhamento on-line da Central de Suporte.

E-mail:
Exame: examination.team@pecb.com
Certificação: certification.team@pecb.com
Serviço ao cliente: support@pecb.com