PECB

BEYOND RECOGNITION

NIS 2 DIRECTIVE LEAD IMPLEMENTER

Guida del candidato

PECB

Sommario

PECB

SEZIONE I: INTRODUZIONE

PECB

PECB è un organismo di certificazione che offre educazione[1], certificazione e programmi di certificazione per individui in un'ampia gamma di discipline.

Con la nostra presenza in più di 150 paesi, aiutiamo i professionisti a dimostrare le loro competenze in diverse aree di conoscenza fornendo valutazione, certificazione e programmi di certificazione validi a fronte di standard riconosciuti a livello internazionale.

I nostri obiettivi principali sono:

1. Stabilire i requisiti minimi necessari per certificare i professionisti e organizzazioni e concedere le nomine
2. Revisione verifica delle qualifiche dei richiedenti per accertarsi che siano idonei alla certificazione
3. Mantenere e migliorare costantemente il processo di valutazione per la certificazione degli individui
4. Certificare gli individui qualificati, concedere le nomine e mantenere il rispettivo albo
5. Stabilire requisiti per il rinnovamento periodico delle certificazioni e accertarsi che gli individui certificati siano conformi ai requisiti
6. Accertarsi che i professionisti PECB aderiscano agli standard etici nella pratica professionale
7. Rappresentare le parti interessate in argomenti di interesse comune
8. Promuovere i vantaggi della certificazione e dei programmi di certificazione per i professionisti, le aziende i governi e il pubblico

La nostra missione

Offrire ai clienti servizi di esame, certificazione e programmi di certificazione completi che ispirino fiducia e portino benefici alla società nel suo complesso.

La nostra visione

Diventare il riferimento globale per la fornitura di servizi di certificazione professionale e i programmi di certificazione.

I nostri valori

Integrità, professionalità, equità

[1] Per "educazione" si intendono corsi di formazione ideati da PECB e offerti in tutto il mondo attraverso la nostra rete di partner.

Il valore della certificazione PECB

Riconoscimento globale
Le credenziali PECB sono riconosciute a livello internazionale e sono approvate da molti organismi di accreditamento in modo tale che i professionisti che le ottengono traggono vantaggio dal nostro riconoscimento sui mercati nazionali e internazionali.

Il valore delle certificazioni PECB è confermato dall'accreditamento da parte dell'International Accreditation Service (IAS-PCB-111), dal United Kingdom Accreditation Service (UKAS-No. 21923) e dal Korean Accreditation Board (KAB-PC-08) ai sensi dell'ISO/IEC 17024 – Requisiti generali per gli organismi che operano per la certificazione delle persone. Il valore dei programmi di certificazione PECB è confermato dall'accreditamento da parte dell'ANSI National Accreditation Board (ANAB-Accreditation ID 1003) ai sensi dell'ANSI/ASTM E2659-18, Pratica standard per i programmi di certificazione.

PECB è membro associato dell'Independent Association of Accredited Registrars (IAAR), membro effettivo dell'International Personnel Certification Association (IPC), membro firmatario di IPC MLA e membro di Club EBIOS, CPD Certification Service, CLUSIF, Credential Engine e ITCC. Inoltre, PECB è Licensed Partner Publisher (LPP) del Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) per il Cybersecurity Maturity Model Certification standard (CMMC), è stato approvato da Club EBIOS per EBIOS Risk Manager Skills certification ed è approvato dalla CNIL (Commission Nationale de l'Informatique et des Libertés) per la certificazione DPO. Per ulteriori informazioni, fare clic qui.

Prodotti e servizi di alto livello
Siamo orgogliosi di offrire prodotti e servizi di alto livello che corrispondono alle esigenze e alle richieste dei nostri clienti. Tutti i nostri prodotti sono stati attentamente preparati da un team di esperti e professionisti in base alle buone pratiche e alle metodologie.

Conformità con le norme
Le nostre certificazioni e i programmi di certificazione sono conformi all' ISO/IEC 17024 e all'ASTM E2659. Garantiscono che i requisiti della norma siano stati soddisfatti e convalidati con l'adeguata coerenza, professionalità e imparzialità.

Servizio orientato al cliente
Siamo al servizio dei clienti ai quali riserviamo valore, importanza, professionalità e onestà. PECB si avvale di un team di esperti responsabili di gestire le richieste, rispondere alle domande e a qualsiasi esigenza. Ci impegniamo per rispondere alle richieste entro 24 ore al massimo senza compromettere la qualità del servizio.

Flessibilità e comodità
Le opportunità di apprendimento online renderanno il percorso professionale più comodo in quanto potrai programmare le sessioni di apprendimento in base ai tuoi impegni. La flessibilità ti consente di avere più tempo libero e ti dà opportunità di avanzamento di carriera, oltre a ridurre i costi.

Codice etico PECB

Il Codice etico rappresenta i più alti valori che PECB si impegna a seguire, dato che riconosce la loro importanza quando fornisce i servizi e attira i clienti.

La Divisione addetta alla conformità si accerta che i dipendenti, i formatori, gli esaminatori, i sorveglianti, i partner, i distributori, i membri o gli organi e i comitati consultivi, gli individui certificati e i titolari delle certificazioni (qui di seguito "Professionisti PECB") si attengano a questo Codice etico. La Divisione conformità rimarca inoltre l'esigenza di un comportamento professionale e responsabile, competente ed equo nell'erogazione dei servizi alle parti interessate interno ed esterne, come richiedenti, candidati individui certificati e titolari delle certificazioni, autorità di accreditamento e governative.

PECB ritiene che per ottenere successo a livello organizzativo, sia necessario comprendere pienamente i clienti, le esigenze e le aspettative delle parti interessate. Per questo motivo, PECB promuove una cultura basata sui livelli più elevati di integrità, professionalità ed equità, che sono anche i suoi valori. Questi valori sono fondamentali per l'organizzazione e hanno caratterizzato la presenza e la crescita globale nel corso degli anni, oltre alla reputazione di PECB.

PECB crede che valori etici forti siano essenziali per relazioni corrette e stabili. La principale responsabilità di PECB è quindi accertarsi che i professionisti PECB si comportino in base ai suoi principi e valori.

I professionisti PECB hanno la responsabilità di:

1. mantenere un comportamento professionale durante l'erogazione dei servizi, con onestà, precisione, equità e indipendenza
2. agire durante l'erogazione dei servizi nel miglior interesse dei propri datori di lavoro, dei clienti, del pubblico e della professione ai sensi del Codice etico e di altri standard professionali
3. dimostrare e sviluppare le competenze nei rispettivi campi e impegnarsi per migliore costantemente le proprie abilità e le competenze
4. offrire servizi solo per coloro che sono qualificati e competenti e informare i clienti in modo adeguato sulla natura dei servizi proposti, tra cui i problemi o i rischi
5. informare ogni datore di lavoro o cliente degli interessi aziendali o delle affiliazioni che possono influire o alterare il giudizio
6. mantenere la riservatezza delle informazioni dei datori di lavoro o clienti attuali e precedenti durante l'erogazione del servizio
7. essere conformi a tutte le leggi e i regolamenti applicabili della giurisdizione del paese in cui vengono erogati i servizi
8. rispettare la proprietà intellettuale e i contributi di altre parti
9. non comunicare, intenzionalmente informazioni false o contraffatte che possano compromettere l'integrità del processo di valutazione di un candidato per la certificazione o un programma di certificazione PECB
10. non presentarsi in modo falso o scorretto come rappresentanti PECB senza licenza o utilizzare in modo improprio il logo PECB, le certificazioni o i certificati
11. non agire in modo da danneggiare la reputazione, le certificazioni o i programmi di certificazione di PECB
12. dare il proprio contributo alle indagini a seguito di una violazione reclamata del presente Codice etico

Per leggere la versione completa del Codice etico di PECB, andare a Code of Ethics | PECB.

Introduzione a NIS 2 Directive Lead Implementer

La Direttiva NIS 2 specifica i requisiti per aumentare la sicurezza della rete e dei sistemi informativi in tutta l'Unione europea (UE). Un programma di cybersicurezza conforme ai requisiti della Direttiva NIS 2 consente alle organizzazioni di rafforzare le proprie misure di cybersicurezza, proteggere l'infrastruttura critica ed essere conformi ai requisiti legali nell'UE. La Direttiva NIS 2 si applica a diverse organizzazioni, definite come enti essenziali o importanti dalla direttiva, con soglie dimensionali specifiche per ogni settore, tra cui quelli che forniscono servizi essenziali o importanti per l'economia e la società europea, oltre a organizzazioni che sono fornitori esclusivi di un servizio fondamentale in uno Stato membro.

La credenziale "NIS 2 Directive Lead Implementer" è una certificazione professionale per individui che aspirano a dimostrare la competenza relativa alla conformità ai requisiti della Direttiva NIS 2 e a guidare un team di attuazione.

Considerando che le professioni correlate all'attuazione sono molto ricercate, la certificazione riconosciuta può aumentare in modo significativo le possibilità di carriera e consentire il raggiungimento degli obiettivi professionali.

In questo documento è specificato lo schema di certificazione PECB NIS 2 Directive Lead Implementer ai sensi dell'ISO/IEC 17024:2012. Indica anche i passi che i candidati devono intraprendere per ottenere e mantenere le credenziali. È molto importante leggere tutte le informazioni di questo documento prima di completare e presentare la domanda. In caso di domande o per ulteriori informazioni, contattare l'ufficio internazionale di PECB all'indirizzo certification.team@pecb.com.

PECB

SEZIONE II: ESAME, PREPARAZIONE, REGOLE E POLITICHE

Preparazione e programmazione dell'esame

Tutti i candidati hanno la responsabilità dello studio e della preparazione per gli esami di certificazione. Anche se ai candidati non è richiesto di frequentare il corso di formazione per sostenere l'esame, la frequenza può migliorare notevolmente le possibilità di superare l'esame.

Per fissare la data di esame i candidati hanno due opzioni:

1. Contattare uno dei nostri partner autorizzati. Per trovare un partner autorizzato nella tua area, consultare Active Partners. Il corso di formazione è anche disponibile online accedendo a Training Events.
2. Sostenere l'esame da remoto tramite PECB Exams application. Per programmare un esame da remoto, seguire il link qui di seguito: Exam Events.

Per altre informazioni su esami, aree di competenza e dichiarazioni di conoscenza consultare la *Sezione III* di questo documento.

Riprogrammazione dell'esame

Per qualsiasi variazione relativa alla data, all'ora al luogo dell'esame o per altri dettagli, contattare online.exams@pecb.com.

Tasse di iscrizione per l'esame e la certificazione

I candidati possono sostenere l'esame senza frequentare il corso di formazione. Qui di seguito sono indicati i prezzi:

- Esame Lead: 1000 dollari[2]
- Esame Manager: 700 dollari
- Esame Foundation: 500 dollari
- Esame Transition: 500 dollari

La tassa per la domanda di certificazione è di 500 dollari.

Per tutti i candidati che hanno seguito il corso di formazione e sostenuto l'esame con uno dei nostri partner PECB, la tassa di iscrizione comprende il costo dell'esame (primo tentativo e prima ripetizione), la richiesta di certificazione e il primo anno di tassa annuale di mantenimento (Annual Maintenance Fee, AMF).

[2] Tutti i prezzi sono in dollari USA.

Aree di competenza

L'obiettivo dell'esame "PECB NIS 2 Directive Lead Implementer" è accertarsi che il candidato abbia acquisito le competenze necessarie per supportare un'organizzazione a definire, attuare, gestire e mantenere un programma di conformità alla Direttiva NIS 2.

La certificazione NIS 2 Directive Lead Implementer si rivolge a:

- professionisti della cybersicurezza che cercano di avere una comprensione globale dei requisiti della Direttiva NIS 2 e di apprendere le strategie pratiche per l'attuazione di solide misure di cybersicurezza
- responsabili e professionisti IT che vogliono avere ulteriori informazioni per l'attuazione dei sistemi di sicurezza e migliorare la resilienza dei sistemi critici
- funzionari governativi e della regolamentazione responsabili dell'applicazione della Direttiva NIS 2

Il contenuto dell'esame è suddiviso come riportato qui di seguito:

- **Area 1:** Concetti e definizioni fondamentali relativi alla Direttiva NIS 2
- **Area 2:** Pianificazione dell'attuazione dei requisiti della Direttiva NIS 2
- **Area 3:** Ruoli e responsabilità della cybersicurezza e gestione del rischio
- **Area 4:** Controlli di cybersicurezza, gestione degli incidenti e gestione della crisi
- **Area 5:** Comunicazione e consapevolezza
- **Area 6:** Test e monitoraggio di un programma di cybersicurezza

Area 1: Concetti e definizioni fondamentali relativi alla Direttiva NIS 2

Obiettivo principale: Accertarsi che il candidato sia in grado di interpretare i concetti e le definizioni della Direttiva NIS 2.

Competenze	Dichiarazioni di conoscenza
1. Capacità di spiegare i concetti principali della Direttiva NIS 2 2. Capacità di sviluppare una conoscenza globale delle norme ISO correlate alla sicurezza delle informazioni 3. Capacità di identificare altre buone pratiche del settore della cybersicurezza, tra cui i controlli e il Quadro di riferimento NIST sulla cybersicurezza 4. Capacità di identificare le pubblicazioni ENISA (European Network and European Security Agency, Agenzia dell'Unione europea per la cybersicurezza) per la cybersicurezza 5. Capacità di confrontare la Direttiva NIS 2 con la precedente Direttiva NIS 6. Capacità di analizzare la struttura, gli obiettivi e l'oggetto della Direttiva NIS 2 7. Capacità di valutare il potenziale impatto della Direttiva NIS 2 sulle parti interessate, tra cui enti essenziali e importanti 8. Capacità di descrivere le ammende amministrative associate alla non conformità per la Direttiva NIS 2 9. Capacità di riconoscere e descrivere le organizzazioni importanti dell'UE coinvolte nell'applicazione e nel regolamento della cybersicurezza nell'Unione europea	1. Conoscenza dei concetti e della terminologia principali della Direttiva NIS 2 2. Conoscenze delle norme ISO relative alla sicurezza delle informazioni, tra cui ISO/IEC 27001 e ISO/IEC 27002 3. Conoscenza di quadri di riferimento legali e dei regolamenti relativi alla sicurezza delle informazioni e alla cybersicurezza tra cui, Legge sui mercati digitali, Legge sui servizi digitali, Regolamento in materia di resilienza operativa digitale, Regolamento UE sulla cybersicurezza, Legge europea sulla resilienza informatica, Legge sulla governance dei dati, GDPR e Direttiva 2 servizi di pagamento 4. Conoscenza del campo di applicazione della Direttiva NIS 2 e confronto con la Direttiva NIS 5. Conoscenza della relazione tra la Direttiva NIS 2 e le serie ISO/IEC 27000 6. Conoscenza della struttura, degli obiettivi e dell'oggetto della Direttiva NIS 2 e suoi effetti per le organizzazioni e i settori delle infrastrutture critiche 7. Conoscenza dell'impatto della Direttiva NIS 2 8. Conoscenza delle ammende amministrative associate alla non conformità alla Direttiva NIS 2 e ai criteri per la determinazione delle ammende 9. Conoscenza delle organizzazioni UE responsabili della governance della cybersicurezza, regolamenti e supervisione, oltre ai loro ruoli per l'applicazione della Direttiva NIS 2

Area 2: Pianificazione dell'attuazione dei requisiti della Direttiva NIS 2

Obiettivo principale: Accertarsi che il candidato sia in grado di identificare e spiegare i requisiti principali della Direttiva NIS 2 e pianificarne l'attuazione.

Competenze	Dichiarazioni di conoscenza
1. Capacità di spiegare gli elementi della Direttiva NIS 2, tra cui governance, gestione della crisi, misure di rischio e obblighi di segnalazione 2. Capacità di definire l'approccio per l'attuazione dei requisiti della Direttiva NIS 2 3. Capacità di raccogliere, analizzare e interpretare le informazioni necessarie per pianificare l'attuazione dei requisiti della Direttiva NIS 2 4. Capacità di interpretare e definire gli obiettivi di conformità alla Direttiva NIS 2 5. Capacità di analizzare e considerare il contesto interno ed esterno di un'organizzazione 6. Capacità di identificare i ruoli e le responsabilità delle principali parti interessate durante e dopo l'attuazione dei requisiti della Direttiva NIS 2 7. Capacità di eseguire un'analisi del gap e di chiarire gli obiettivi di conformità della Direttiva NIS 2 8. Capacità di definire e giustificare il campo di applicazione del programma di attuazione della Direttiva NIS 2 adatto agli obiettivi di compliance per la Direttiva NIS 2 specifici per l'organizzazione 9. Capacità di spiegare i requisiti della Direttiva NIS 2 correlati alla governance e alla strategia di cybersicurezza 10. Capacità di sviluppare un programma di conformità alla cybersicurezza 11. Capacità di identificare i tipi di politiche e definire una politica di cybersicurezza	1. Conoscenza dei componenti e dei requisiti della Direttiva NIS 2, tra cui le definizioni, la governance, la gestione della crisi, la gestione del rischio e gli obblighi di segnalazione 2. Conoscenza dei principali approcci e metodologie utilizzati per attuare i requisiti della Direttiva NIS 2 3. Conoscenza degli obiettivi specifici di conformità della Direttiva NIS 2 e modalità per conseguirli 4. Conoscenza di che cosa costituisce tipicamente il contesto interno ed esterno di un'organizzazione 5. Conoscenza degli approcci usati per comprendere il contesto di un'organizzazione 6. Conoscenza delle tecniche usate per raccogliere informazioni su un'organizzazione e per eseguire un'analisi del gap 7. Conoscenza del piano di progetto dell'attuazione della Direttiva NIS 2 e del team di progetto dell'attuazione della Direttiva NIS 2 8. Conoscenza delle principali strutture organizzative che un'organizzazione può applicare per gestire l'attuazione della Direttiva NIS 2 9. Conoscenza delle caratteristiche del campo di applicazione della Direttiva NIS 2 in termini di confini organizzativi, tecnologici e fisici 10. Conoscenza degli articoli della Direttiva NIS 2 che trattano la governance e la strategia nazionale per la cybersicurezza 11. Conoscenza della attività necessarie per sviluppare un programma di conformità alla cybersicurezza 12. Conoscenza delle buone pratiche e delle tecniche usate per redigere e stabilire politiche e procedure di cybersicurezza

Area 3: Ruoli e responsabilità della cybersicurezza e gestione del rischio

Obiettivo principale: Accertarsi che il candidato sia in grado di definire i ruoli e le responsabilità della cybersicurezza e attuare la gestione del rischio

Competenze	Dichiarazioni di conoscenza
1. Capacità di analizzare la struttura organizzativa e assegnare ruoli e responsabilità chiave correlati alla cybersicurezza 2. Capacità di definire i ruoli e le responsabilità nell'organizzazione 3. Capacità di creare un team efficace per la cybersicurezza nell'organizzazione 4. Capacità di gestire in modo efficace gli asset di cybersicurezza 5. Capacità di identificare i rischi di cybersicurezza valutando le minacce, le vulnerabilità e le possibili ripercussioni 6. Capacità di analizzare i rischi di cybersicurezza per determinarne la probabilità e le possibili conseguenze 7. Capacità di valutare i rischi di cybersicurezza per stabilirne le priorità in base al loro significato e possibili ripercussioni sull'organizzazione 8. Capacità di attuare strategie di trattamento del rischio per attenuare i rischi di sicurezza identificati 9. Capacità di comunicare in modo efficace e consultarsi con le parti interessate in relazione ai rischi di cybersicurezza e alle strategie di attenuazione 10. Capacità di mantenere i registri e la segnalazione sui rischi della cybersicurezza e controllo e revisione costante dell'efficacia delle azioni intraprese per la gestione del rischio della cybersicurezza	1. Conoscenza della struttura organizzativa 2. Conoscenza dei ruoli e delle responsabilità correlati alla cybersicurezza 3. Conoscenza dei requisiti della Direttiva NIS 2 relativi alla gestione degli asset 4. Conoscenza della gestione degli asset di cybersicurezza 5. Conoscenza dei requisiti della Direttiva NIS 2 relativi alla gestione del rischio 6. Conoscenza delle linee guida sulla gestione del rischio, come ISO 31000, ISO/IEC 27005 e le pubblicazioni ENISA 7. Conoscenza dell'identificazione del rischio di cybersicurezza e analisi per determinarne la probabilità e le possibili conseguenze 8. Conoscenza della valutazione del rischio di cybersicurezza per attuare strategie efficaci di trattamento del rischio 9. Conoscenza della comunicazione e della consultazione con le parti interessate sui rischi della cybersicurezza 10. Conoscenza del mantenimento dei registri e della segnalazione sui rischi e sui trattamenti della cybersicurezza e sul loro stato 11. Conoscenza del monitoraggio e della revisione della procedura per determinare l'efficacia delle azioni di gestione del rischio di cybersicurezza

Area 4: Controlli di cybersicurezza, gestione degli incidenti e gestione della crisi

Obiettivo principale: Accertarsi che il candidato sia in grado di attuare i processi di cybersicurezza richiesti per la conformità alla Direttiva NIS 2, tra cui controlli di cybersicurezza, sicurezza della filiera di fornitura, gestione degli incidenti e gestione della crisi.

Competenze	Dichiarazioni di conoscenza
1. Capacità di interpretare i requisiti della Direttiva NIS 2 relativi alle misure di gestione del rischio di cybersicurezza 2. Capacità di spiegare le misure di sicurezza delle risorse umane in base alle buone pratiche del settore 3. Capacità di spiegare le buone pratiche per un controllo efficace degli accessi per tutelare la rete e i sistemi informativi 4. Capacità di utilizzare le tecniche di crittografia per migliorare la sicurezza dei dati 5. Capacità di identificare e attuare le misure necessarie per proteggere i sistemi e i servizi di rete 6. Capacità di selezionare e attuare i processi di gestione del rischio della filiera di fornitura, stabilire i processi di gestione delle vulnerabilità e aumentare la sicurezza delle informazioni nelle relazioni con i fornitori 7. Capacità di preparare, identificare, segnalare, valutare, rispondere e apprendere dagli incidenti di cybersicurezza 8. Capacità di creare un piano di gestione della crisi, piani di comunicazione della crisi e sistemi di comunicazione di emergenza per affrontare situazioni critiche 9. Capacità di sviluppare piani di continuità operativa completi e piani di ripristino di emergenza per garantire la continuità operativa	1. Conoscenza dei requisiti della Direttiva NIS 2 relativi alle misure tecniche, operative e organizzative 2. Conoscenza dei controlli di cybersicurezza necessari per gestire i rischi, come sicurezza delle risorse umane, controlli degli accessi, crittografia e sicurezza della rete 3. Conoscenza dei requisiti della Direttiva NIS 2 che trattano le misure per garantire la sicurezza della filiera di fornitura 4. Conoscenza della gestione del rischio della filiera di fornitura, gestione delle vulnerabilità e pratiche di sicurezza delle informazioni nelle relazioni con i fornitori 5. Conoscenza delle procedure di preparazione, identificazione, segnalazione, valutazione, risposta e apprendimento dagli incidenti di cybersicurezza 6. Conoscenza del ruolo e delle responsabilità dei CSIRT (Computer Security Incident Response Team, Team di risposta agli incidenti di sicurezza informatica) nel processo di gestione degli incidenti come definito dalla Direttiva NIS 2 7. Conoscenza degli obblighi di segnalazione degli incidenti imposti dalla Direttiva NIS 2 alle parti coinvolte nella gestione di un incidente 8. Conoscenza dei requisiti della Direttiva NIS 2 per gli Stati membri e i CSIRT relativi alla gestione della crisi informatica 9. Conoscenza della gestione della crisi e caratteristica e importanza della comunicazione della crisi 10. Conoscenza della gestione della continuità operativa, tra cui la pianificazione delle strategie e del ripristino

Area 5: Comunicazione e consapevolezza

Obiettivo principale: Accertarsi che il candidato sia in grado di sviluppare e attuare una comunicazione efficace, lo sviluppo delle competenze e i programmi di consapevolezza per supportare la cybersicurezza, gli obiettivi dell'organizzazione e la conformità ai requisiti della Direttiva NIS 2.

Competenze	Dichiarazioni di conoscenza
1. Capacità di pianificare e fornire attività di sviluppo delle competenze, tra cui programmi di formazione e consapevolezza 2. Capacità di definire la struttura e il tipo di programmi di sviluppo delle competenze allineati con gli obiettivi dell'organizzazione 3. Capacità di erogare programmi di formazione e consapevolezza in modo efficace per rispondere alle esigenze identificate 4. Capacità di determinare e valutare gli esiti e l'efficacia dei programmi di formazione e consapevolezza 5. Capacità di pianificare, eseguire e valutare le attività di comunicazione per raggiungere gli obiettivi di comunicazione 6. Capacità di identificare i requisiti della Direttiva NIS 2 relativi alla consapevolezza sulla cybersicurezza e alla condivisione delle informazioni 7. Capacità di applicare i principi di una strategia di comunicazione efficace	1. Conoscenza dei requisiti della Direttiva NIS 2 per la consapevolezza sulla cybersicurezza nell'Unione europea 2. Conoscenza delle attività e dei programmi di sviluppo delle competenze 3. Conoscenza della progettazione del programma per rispondere agli obiettivi aziendali 4. Conoscenza del processo per erogare programmi di formazione e consapevolezza efficaci 5. Conoscenza della valutazione degli esiti e dell'efficacia dei programmi di formazione e consapevolezza 6. Conoscenza della comunicazione strategica e dei suoi principi: trasparenza, adeguatezza, credibilità, capacità di risposta e chiarezza 7. Conoscenza delle strategie di comunicazione efficaci 8. Conoscenza degli accordi di condivisione delle informazioni sulla cybersicurezza e notifica volontaria di informazioni pertinenti come definito nella Direttiva NIS 2

Area 6: Test e monitoraggio di un programma di cybersicurezza

Obiettivo principale: Accertarsi che il candidato sia in grado di verificare, misurare, monitorare e migliorare costantemente un programma di cybersicurezza secondo la Direttiva NIS 2

Competenze	Dichiarazioni di conoscenza
1. Capacità di comprendere e spiegare il test di cybersicurezza	1. Conoscenza delle tecniche di test della cybersicurezza
2. Capacità di identificare i requisiti della Direttiva NIS 2 sulla sicurezza degli audit e le autovalutazioni	2. Conoscenza dei requisiti della Direttiva NIS relativi alle autovalutazioni e al ruolo di tale valutazione per garantire la conformità alla Direttiva NIS 2
3. Capacità di eseguire audit interni, risolvere i problemi di non conformità e comprendere i principi fondamentali dell'audit	3. Conoscenza dell'audit di conformità interno e delle attività di audit interno
4. Capacità di eseguire le autovalutazioni usando i quadri di riferimento come il quadro di riferimento ENISA per l'autovalutazione	4. Conoscenza del quadro di riferimento ENISA per l'autovalutazione e altri strumenti per la valutazione della cybersicurezza
5. Capacità di definire gli obiettivi di misurazione, stabilire gli indicatori di prestazione e stabilire i metodi di monitoraggio	5. Conoscenza degli obiettivi di misurazione, degli indicatori di prestazione e dei metodi di monitoraggio per valutare l'efficacia dei programmi di cybersicurezza
6. Capacità di identificare il ruolo dei CSIRT e delle autorità competente nel monitoraggio delle minacce informatiche come definito dalla Direttiva NIS 2	6. Conoscenza dei requisiti della Direttiva NIS 2 per i CSIRT sul monitoraggio e l'analisi delle minacce, delle vulnerabilità e degli incidenti a livello nazionale.
7. Capacità di determinare cosa è necessario monitorare, segnalare i risultati del monitoraggio in modo efficace e selezionare i metodi di monitoraggio adeguati	7. Conoscenza della segnalazione dei risultati di monitoraggio alle parti interessate e selezione dei metodi di monitoraggio adeguati
8. Capacità di monitorare i fattori di cambiamento, mantenere e migliorare le misure di cybersicurezza e documentare i miglioramenti	8. Conoscenza del monitoraggio dei fattori di cambiamento, mantenimento e miglioramento delle misure di cybersicurezza e documentazione dei miglioramenti

In base alle aree indicate sopra e alla loro rilevanza, l'esame comprende 80 a scelta multipla, come riepilogato nella tabella riportata qui di seguito:

				Livello di comprensione (cognizione/classificazione) richiesto	
		Numero di domande/punti per area di competenza	% dell'esame dedicato a/punti per/per ogni area di competenza	Domande che misurano la comprensione, l'applicazione e l'analisi	Domande che misurano la valutazione
Aree di competenza	Concetti e definizioni fondamentali della Direttiva NIS 2	10	12.5	X	
	Pianificazione dell'attuazione dei requisiti della Direttiva NIS 2	20	25	X	
	Ruoli e responsabilità della cybersicurezza e gestione del rischio	15	18.75		X
	Controlli di cybersicurezza, gestione degli incidenti e gestione della crisi	15	18.75		X
	Comunicazione e consapevolezza	10	12.5	X	
	Test e monitoraggio di un programma di cybersicurezza	10	12.5		X
	Totale	**80**	**100%**		
	Numero di domande per livello di comprensione			**40**	**40**
	% dell'esame dedicata a ogni livello di comprensione (cognizione/classificazione)			**50%**	**50%**

Il punteggio minimo per superare l'esame è pari al **70%**.

Dopo aver superato l'esame, i candidati potranno richiedere la credenziale "PECB Certified NIS 2 Directive Lead Implementer"

Procedura di esame

Informazioni generali sull'esame
I candidati sono tenuti ad arrivare/presentarsi almeno 30 minuti prima dell'inizio dell'esame.

I candidati che arrivano in ritardo non avranno più tempo per compensare il ritardo e potrebbero non essere ammessi all'esame.

I candidati sono tenuti a portare con sé un documento di identità valido (carta d'identità, patente di guida o passaporto nazionali) da mostrare al sorvegliante.

Se richiesto il giorno dell'esame (per gli esami in forma cartacea), si potrà concedere ulteriore tempo ai candidati che sostengono l'esame in una lingua diversa dalla loro lingua madre, come segue:
- 10 minuti in più per esami Foundation
- 20 minuti in più per esami Manager
- 30 minuti in più per esami Lead

Formato e tipo degli esami PECB
1. **Cartaceo:** Gli esami sono in formato cartaceo e ai candidati è consentito solo l'uso del foglio di esame e di una penna. È proibito l'uso di dispositivi elettronici come computer portatili, tablet o telefoni. La sessione d'esame si svolge sotto il controllo di un sorvegliante approvato da PECB nella località in cui il Partner ha organizzato il corso di formazione.
2. **Online:** Gli esami vengono forniti elettronicamente tramite l'applicazione PECB Exams. È proibito l'uso di dispositivi elettronici come tablet e telefoni cellulari. La sessione d'esame viene controllata da remoto da un sorvegliante di PECB tramite l'applicazione PECB Exams e una fotocamera esterna/integrata.

Per ulteriori informazioni sugli esami online, consultare PECB Online Exam Guide.

Sono disponibili due tipi di esami PECB:
1. Esame con domande modello
2. Esame con domande a scelta multipla

Questo esame comprende domande a scelta multipla: L'esame a scelta multipla può essere utilizzato per valutare la comprensione dei candidati di concetti semplici e complessi. Comprende domande indipendenti e basate su scenari Le domande indipendenti rientrano nell'esame e non dipendono da un contesto, mentre le domande basate su scenari sono dipendenti dal contesto, vale a dire sono stati ideate in base a uno scenario che il candidato deve leggere e quindi rispondere a cinque domande relative allo scenario. Quando i candidati rispondono alle domande indipendenti e a quelle basate su scenari, dovranno applicare i concetti e i principi spiegati durante il corso di formazione, analizzare problemi, identificare e valutare le alternative, unire diversi concetti o idee e così via.

Ogni domanda a scelta multipla ha tre opzioni, una delle quali è la risposta corretta (risposta a chiave) e due errate (distrattori).

Questo è un esame a libro aperto. Ai candidati è consentito l'uso dei seguenti materiali di riferimento:

- Una copia cartacea della Direttiva NIS 2
- Materiali del corso di formazione (accessibili tramite l'app PECB Exams e/o stampati)
- Eventuali appunti personali presi durante il corso di formazione (accessibili tramite l'app PECB Exams e/o stampati)
- Un dizionario cartaceo

Qui di seguito viene riportato un campione delle domande dell'esame.

Nota: PECB passerà progressivamente a esami a scelta multipla. Anche questi saranno a libro aperto e comprenderanno domande basate su scenari che consentiranno a PECB di valutare la conoscenza, la perizia e la capacità dei candidati di usare informazioni in situazioni nuove (applicazione), stabilire connessioni tra idee (analisi) e giustificare un punto di vista o una decisione (valutazione).

Per informazioni sui tipi di esame, sulle lingue disponibili e per altri dettagli, contattare examination.team@pecb.com o andare a List of PECB Exams.

Esempi di domande d'esame

TechLink, una multinazionale specializzata nell'erogazione di un'ampia gamma di servizi di cloud computing personalizzati per i settori della finanza e dell'assistenza sanitaria. I suoi servizi consentono alle organizzazioni di sfruttare l'intero potenziale della tecnologia cloud, guidando la trasformazione digitale e migliorando i servizi al pubblico a livello globale.

Lavorando con l'Unione europea, *TechLink* rientra nel quadro di riferimento della Direttiva NIS 2 Directive come entità essenziale. *TechLink* doveva ancora attuare le tutele necessarie a proteggere le proprie reti e i sistemi in modo adeguato e a garantire la conformità alla direttiva; ha quindi avviato un programma di cybersicurezza globale. L'azienda ha adottato un approccio che ha consentito di stabilire standard di produzione elevati senza fissare metodi specifici e trovare modalità efficienti e innovative per soddisfare gli standard.

Ai sensi dell'Articolo 21 della Direttiva NIS 2, l'azienda ha sviluppato una strategia di gestione della continuità operativa (BCM). Il suo approccio allo sviluppo della strategia BCM prevedeva una configurazione contrattuale di ripristino da parte di terzi per cercare un supporto esterno per ristabilire i processi fondamentali e un'opzione di modifica fondamentale per regolare i processi operativi in circostanze con risorse limitate. Questo approccio ha facilitato una risposta flessibile agli incidenti, equilibrando il supporto esterno con gli adeguamenti interni per rendere più veloce il processo di ripristino, risolvendo nel contempo problematiche di gestione chiave come portata della pianificazione, costi di attuazione, e accordi contrattuali con fornitori di terze parti.

Come parte del programma di cybersicurezza, *TechLink* si è concentrata per garantire la sicurezza delle reti e i sistemi informativi promuovendo la cultura della gestione del rischio che comprende le valutazioni del rischio e l'attuazione delle misure di cybersicurezza. Ai sensi della Direttiva NIS 2, queste misure sono state approvate dall'organo di gestione dell'azienda. L'organo di gestione è competente nelle pratiche generali di gestione del rischio, mentre l'azienda non ha ritenuto necessario fornire ulteriore formazione sulla gestione del rischio della cybersicurezza, dato che uno dei membri è esperto in cybersicurezza.

Recentemente, *TechLink* ha dovuto affrontare un grave incidente di cybersicurezza in cui un attacco informatico sofisticato ha colpito i suoi sistemi critici, provocando una violazione dei dati riservati dei clienti. Questo incidente ha dato la possibilità di dimostrare l'impegno per la conformità alla Direttiva NIS 2. L'azienda ha isolato i sistemi colpiti e ha contenuto l'intrusione per evitare ulteriori danni. Quindi, ha informato subito le autorità competenti, tra cui il governo nazionale entro 24 ore dal rilevamento dell'incidente. Si è inoltre messa in contatto con i clienti colpiti, fornendo informazioni sull'incidente e sui passi da intraprendere per proteggere i dati. L'azienda ha presentato un report comprendente una descrizione dettagliata, il tipo di minaccia, l'attenuazione applicata e in corso e l'impatto transfrontaliero.

In base allo scenario indicato sopra, rispondere alle seguenti domande:

1. **Quali possibili sanzioni dovrò subire*TechLink* in caso di non conformità alla Direttiva NIS 2?**
   A. 7 milioni di euro o l'1,4% del fatturato mondiale annuo totale
   B. **10 milioni di euro o il 2% del fatturato mondiale annuo totale**
   C. 5 milioni di euro o l'1% del fatturato mondiale annuo totale

2. **Quale requisito della Direttiva NIS 2 è stato trascurato da *TechLink*?**
   A. **Formare i membri dell'organo di gestione sulle pratiche della gestione del rischio di cybersicurezza**
   B. Garantendo l'approvazione delle misure di cybersicurezza da parte dei Gruppi di resilienza delle infrastrutture critiche
   C. Creando un organo di gestione costituito da cinque membri che hanno una vasta esperienza nella cybersicurezza

3. **Quale approccio normativo ha adottato *TechLink* per essere conforme alla Direttiva NIS 2?**
   A. Comando e controllo
   B. **Basato sulla prestazione**
   C. Basato sulla gestione

4. **Considerate le azioni intraprese da *TechLink* in risposta all'attacco informatico ai suoi sistemi critici, quale aspetto dell'obbligo di segnalazione degli incidenti indicato nell'Articolo 23 della Direttiva NIS 2 non è stato rispettato da *TechLink*?**
   A. **Presentare un aggiornamento immediato dello stato su richiesta**
   B. Fornire a ENISA un report di riepilogo sull'incidente significativo
   C. Presentare una dichiarazione pubblica relativa all'incidente entro 48 ore dall'identificazione

5. **Che approccio è stato utilizzato da *TechLink* per lo sviluppo della strategia BCM?**
   A. Operazione multi-sito
   B. Modalità di backup
   C. **Modalità combinata**

Politica relativa alla sicurezzadell'esame

PECB si impegna a proteggere l'integrità degli esami e di tutto il processo di esame e si affida al comportamento etico dei richiedenti, dei possibili richiedenti, dei candidati e dei partner per mantenere la riservatezza degli esami PECB. Questa Politica intende risolvere le problematiche relative a un comportamento inaccettabile e garantire un trattamento equo a tutti i candidati.

Ogni divulgazione di informazioni relative al contenuto degli esami PECB è una violazione diretta di questa Politica e del Codice etico di PECB. I candidati che devono sostenere un esame PECB devono firmare un Accordo di non divulgazione e riservatezza sull'esame e devono attenersi a quanto segue:

1. le domande e le risposte del materiale di esame sono di proprietà esclusiva e riservata di PECB. Quando i candidati hanno presentato la richiesta di esame a PECB, non avranno più accesso all'esame originale o a una sua copia.
2. Ai candidati non è consentito divulgare informazioni relative alle domande e alle risposte dell'esame o parlarne con altre persone o candidati.
3. Ai candidati non è consentito portare materiali correlati all'esame fuori dall'aula di esame.
4. Ai candidati non è consentito copiare o cercare di fare copie (in forma scritta, di fotocopia o altro9 dei materiali di esame, tra cui, senza limitazione alcuna, domande, risposte o immagini dello schermo.
5. I candidati non devono partecipare o promuovere attività fraudolente per sostenere l'esame, come ad esempio:
    - Guardare il materiale di esame o il foglio delle risposte di un altro candidato
    - Dare o ricevere assistenza dal sorvegliante, da un candidato o da altri
    - Utilizzare senza autorizzazione guide, manuali, strumenti e così via, compresi l'uso di siti di "brain dump" che non sono autorizzati da PECB

Quando il candidato conosce o è già a conoscenza delle irregolarità o delle violazioni dei punti indicati sopra, deve attenersi, in caso contrario se si verificano queste irregolarità, i candidati saranno segnalati direttamente a PECB, o se osservano queste irregolarità devono segnalarle immediatamente a PECB.

I candidati sono gli unici responsabili della comprensione e della conformità ai Regolamenti e alle Politiche di esame, all'accordo di non divulgazione e riservatezza e al Codice etico di PECB. Quindi, nel caso in cui venga identificata una violazione di uno o più regolamenti, i candidati non riceveranno rimborsi. PECB può inoltre negare il diritto di sostenere un esame PECB o di invitare i candidati a sostenere un esame se vengono identificate irregolarità durante e dopo il processo di valutazione, in base alla gravità del caso.

Qualsiasi violazione dei punti indicati sopra provocherà un danno irreparabile a PECB che non potrà essere risarcito in denaro. PECB può quindi intraprendere le misure adeguate per porre rimedio o prevenire una divulgazione non autorizzata o l'uso improprio dei materiali di esame, tra cui l'ottenimento di un'ingiunzione immediata.
PECB si riserva il diritto di promuovere azioni contro ogni individuo che infranga queste regole e queste politiche, tra cui l’interdizione permanente relativa alla richiesta di credenziali PECB e la revoca di quelle esistenti. PECB si riserva inoltre il diritto di promuovere azioni legali nei confronti di individui o organizzazioni che violano i suoi diritti d’autore, diritti proprietari o diritti di proprietà intellettuale.

Risultati dell'esame

I risultati dell'esame saranno comunicati via email.

- Per la comunicazione dei risultati, dalla data dell'esame possono trascorrere da tre a otto settimane per l'esame basato su un modello e da due a quattro settimane per gli esami a scelta multipla in formato cartaceo.
- Per gli esami a scelta multipla online, i candidati hanno i risultati subito.

I candidati che superano l'esame con successo saranno in grado di presentare domanda per una delle credenziali del rispettivo schema di certificazione.

Per i candidati che non superano l'esame, all'e-mail sarà aggiunto un elenco delle aree in cui non hanno ottenuto risultati sufficienti per aiutarli a prepararsi meglio a ripetere l'esame.

I candidati che non sono d'accordo con i risultati possono presentare una richiesta di rivalutazione scrivendo a examination.team@pecb.com entro 30 giorni dalla ricezione dei risultati. Le richieste di rivalutazione ricevute dopo 30 giorni non saranno considerate. Se i candidati non sono d'accordo con i risultati della rivalutazione, hanno 30 giorni di tempo dalla data di ricezione per presentare un reclamo attraverso il PECB Ticketing System. I reclami ricevuti dopo 30 giorni non saranno considerate.

Politica di ripetizione dell'esame

Non sono stati stabiliti limiti per la ripetizione dell'esame da parte del candidato. Sono stati però stabiliti limiti relativi al periodo di tempo che deve trascorrere tra un esame e la sua ripetizione.

Se un candidato non supera l'esame al 1° tentativo, dovrà attendere 15 giorni dalla data iniziale dell'esame per il tentativo successivo (1a ripetizione).

Nota: I candidati che hanno completato il corso di formazione con uno dei partner e non hanno superato l'esame la prima volta, possono ritentare l'esame gratuitamente entro 12 mesi dalla data di ricezione del codice promozionale (la tassa pagata per il corso di formazione comprende il primo esame e la sua eventuale ripetizione). I tentativi successivi prevedono il pagamento di una tassa.

Ai candidati che non superano l'esame la seconda volta, PECB raccomanda di frequentare il corso di formazione per prepararsi meglio.

Per organizzare la ripetizione dell'esame, in base al suo formato, i candidati che hanno completato un corso di formazione devono procedere come segue:

1. Esame online: durante la programmazione della ripetizione dell'esame, usare il codice promozionale per non dover ripagare la tassa
2. Esami in formato cartaceo: i candidati devono contattare il Partner/Distributore di PECB che ha organizzato inizialmente la sessione di esame per concordarne la (data, luogo, costi).

I candidati che non hanno completato un corso di formazione con un partner, ma si sono presentati per l'esame online direttamente tramite PECB, non rientrano nella presente Politica. La procedura per programmare la ripetizione dell'esame è identica a quella dell'esame iniziale.

PECB

SEZIONE III: PROCESSO E REQUISITI PER LA CERTIFICAZIONE

Credenziali PECB Direttiva NIS 2

Tutte le certificazioni PECB hanno specifici requisiti relativi all'educazione e all'esperienza professionale. Per stabilire quale credenziale è adatta, è necessario prendere in considerazione le esigenze professionali e analizzare i criteri per le certificazioni.

Le credenziali nello schema PECB per la Direttiva NIS 2 comprendono i requisiti riportati qui di seguito:

Credenziale	Educazione	Esame	Esperienza professionale	Esperienza in progetti MS	Altri requisiti
PECB Certified NIS 2 Directive Provisional Implementer	Almeno istruzione di livello secondario	Esame PECB Certified NIS 2 Directive Lead Implementer or equivalente	Nessuno	Nessuno	Signing the PECB Code of Ethics
PECB Certified NIS 2 Directive Implementer			Due anni: Un anno di esperienza lavorativa nella gestione della cybersicurezza	Attività di progetto: 200 ore totali	
PECB Certified NIS 2 Directive Lead Implementer			Cinque anni: Due anni di esperienza lavorativa nella gestione della cybersicurezza	Attività di progetto: 300 ore totali	
PECB Certified NIS 2 Directive Senior Lead Implementer			Dieci anni: Sette anni di esperienza lavorativa nella gestione della cybersicurezza	Attività di progetto: 1.000 ore totali	

Per essere valide, le attività di attuazione devono seguire le buone pratiche di attuazione e gestione e comprendere quanto segue:

1. Esecuzione completa della valutazione del rischio specifica per i sistemi di infrastrutture critiche
2. Gestione dei piani di risposta agli incidenti adeguati ai requisiti della Direttiva NIS 2
3. Attuazione di misure e controlli adeguati sulla sicurezza
4. Attuazione dei parametri e degli indicatori di prestazione
5. Gestione e risposta agli incidenti di cybersicurezza
6. Esecuzione di una revisione della gestione
7. Gestione di un team di cybersicurezza

Domanda di certificazione

Tutti i candidati che superano l'esame (o un equivalente accettato da PECB) possono richiedere le credenziali PECB per i quali sono stati valutati. Per poter ottenere una certificazione PECB è necessario soddisfare specifici requisiti educativi e professionali. I candidati devono compilare il modulo di domanda di certificazione online (accessibile attraverso il proprio account PECB), compresi i dati delle persone che

saranno contattate per convalidare l'esperienza professionale del candidato. I candidati possono presentare la domanda in inglese, francese, tedesco, spagnolo o coreano. Possono scegliere di saldare l'importo online o ricevere la fattura. Per ulteriori informazioni, contattare certification.team@pecb.com.

La procedura per la richiesta della certificazione online è semplicissima e breve:

- Registrare il proprio account
- Controllare il link di conferma ricevuto via email
- Effettuare il log in per presentare domanda di certificazione

Per ulteriori informazioni sulla domanda di certificazione, fare clic qui.

Il Dipartimento di certificazione conferma che il candidato soddisfa tutti i requisiti di certificazione relativi alla rispettiva credenziale. Il candidato riceverà un'e-mail sullo stato della sua richiesta che comprende la decisione relativa alla certificazione.

A seguito dell'approvazione della richiesta da parte del Dipartimento di certificazione, il candidato potrà scaricare il certificato e richiedere il corrispondente Badge digitale. Per sapere come scaricare il certificato, fare clic qui e per ulteriori informazioni sulla richiesta del Badge digitale, fare clic qui.

PECB fornisce supporto in inglese e in francese.

Esperienza professionale

I candidati devono fornire informazioni complete e corrette sulla loro esperienza professionale, tra cui la/e posizione/i lavorativa/e, la/e data/e di inizio e fine, la/e descrizione/i delle mansioni e altro. Si consiglia ai candidati di riepilogare i propri incarichi precedenti o attuali fornendo dettagli sufficienti a descrivere la natura delle responsabilità per ogni posizione lavorativa. Nel curriculum si possono includere informazioni più dettagliate.

Referenze professionali

Per ogni domanda di certificazione sono obbligatorie due referenze professionali, che devono provenire da individui che abbiano lavorato con il candidato in ambito professionale e possano convalidare la sua esperienza nella gestione della cybersicurezza, oltre alla sua carriera lavorativa presente e passata. Non si considerano valide le referenze professionali di persone che sono sotto la supervisione del candidato o sono suoi parenti.

Esperienza in progetti relativi alla cybersicurezza

Sarà controllato il registro dei progetti relativi alla cybersicurezza per accertarsi che il candidato abbia il numero richiesto di ore.

Valutazione delle domande di certificazione

Il Dipartimento di certificazione valuterà ogni domanda per confermare l'idoneità del candidato per la certificazione o per il programma di certificazione. Se la domanda di un candidato è in fase di revisione, sarà inviata una comunicazione scritta e se necessario, concesso un ulteriore periodo di tempo per fornire la documentazione aggiuntiva. Se il candidato non risponde entro la scadenza o non fornisce la

documentazione richiesta entro i tempi stabiliti, il Dipartimento di certificazione convaliderà la domanda in base alle informazioni fornite inizialmente, ma in questo modo potrebbe essere necessario un declassamento delle credenziali dei candidati.

PECB

SEZIONE IV: POLITICHE DI CERTIFICAZIONE

Rifiuto di certificazione

PECB può rifiutare la certificazione/il programma di certificazione se i candidati:

- Falsificano la domanda
- Violano le procedure dell'esame
- Violano il Codice etico PECB

I candidati a cui è stata negata la certificazione/il programma di certificazione possono presentare un reclamo tramite le procedure di reclamo e appello. Per ulteriori informazioni, consultare la sezione **Complaint and Appeal Policy** .

Il pagamento effettuato per la domanda di certificazione/programma di certificazione non è rimborsabile.

Opzioni dello stato di certificazione

Attivo

Significa che la certificazione è a posto e valida e viene mantenuta attraverso la conformità ai requisiti di PECB relativi al CPD (Continual Professional Development, Sviluppo professionale continuo) e all'AMF.

Sospeso

PECB può sospendere temporaneamente la certificazione se i candidati non sono conformi ai requisiti. Tra le altre ragioni per la sospensione della certificazione figurano:

- Reclami eccessivi o gravi a PECB dalle parti interessate (la sospensione si applicherà fino al completamento dell'inchiesta)
- Uso improprio dei logo di PECB o degli organismi di accreditamento
- Mancato rimedio all'uso improprio di un marchio di certificazione entro i tempi stabiliti da PECB
- Richiesta volontaria di sospensione da parte dell'individuo certificato
- Altre condizioni che PECB ritenga appropriate per sospendere la certificazione

Revocato

PECB può revocare (vale a dire cancellare) la certificazione se il candidato non è conforme ai requisiti. In questi casi, i candidati non saranno più autorizzati a presentarsi come Professionisti certificati da PECB. La certificazione può inoltre essere revocata quando i candidati:

- Violano il Codice etico PECB
- Presentano in modo errato e forniscono informazioni false sul campo di applicazione della certificazione
- Non rispettano qualsiasi altra regola di PECB
- Qualsiasi altra ragione ritenuta valida da PECB

I candidati a cui è stata revocata la certificazione possono presentare un reclamo tramite le procedure di reclamo e appello. Per ulteriori informazioni, consultare la sezione **Complaint and Appeal Policy** .

Altri stati
Oltre a essere attiva, sospesa o revocata, una certificazione può essere volontariamente ritirata o indicata come Emeritus. Per saperne di più sugli stati e sullo stato di cessazione permanente, consultare Certification Status Options.

Passaggio a una categoria superiore e declassamento delle credenziali

Passaggio delle credenziali a una categoria superiore
I professionisti possono richiede un passaggio delle credenziali a una categoria superiore (upgrade) non appena sono in grado di dimostrare la conformità ai requisiti.

Per richiedere un passaggio delle credenziali a una categoria superiore, i candidati devono accedere all'account PECB, aprire la scheda "My Certifications" e selezionare il link "Upgrade". La tassa per la domanda di passaggio delle credenziali a una categoria superiore è di 100 dollari.

Declassamento delle credenziali
Una Certificazione PECB può essere declassata a una credenziale inferiore per le ragioni indicate qui di seguito:

- Tassa AMF non versata
- Non sono state presentate le ore relative al CPD
- Le ore relative al CPS non sono sufficienti
- La prova delle ore relative al CPD non è stata presentata quando richiesto.

Nota: *La certificazione PECB di livello Lead dei professionisti che non hanno fornito le prove relative ai requisiti di mantenimento della certificazione, sarà declassata a una credenziale inferiore. Ai titolari di certificazione di livello Master che non presentano i CPD o non versano le AMF saranno revocate le certificazioni.*

Rinnovo della certificazione

Le certificazioni PECB sono valide per tre anni. Per mantenerle attive, i professionisti certificati PECB devono essere conformi ai requisiti relativi alla credenziale indicata, vale a dire devono essere conformi al numero di ore di sviluppo professionale continuo (CPD). Devono inoltre pagare la tassa annuale di mantenimento (120 dollari). Per ulteriori informazioni, andare alla pagina Certification Maintenance sul sito Web di PECB.

Chiusura di un caso

Se un candidato non presenta la domanda di certificazione entro un anno, il suo caso verrà chiuso. Dopo la scadenza del periodo di certificazione i candidati hanno comunque il diritto di riaprire il loro caso. PECB non si ritiene comunque responsabile per eventuali variazioni relative a condizioni, norme, politiche e guida del candidato che erano in vigore prima della chiusura del caso. Un candidato che vuole chiedere la riapertura del suo caso deve presentare una richiesta scritta a certification.team@pecb.com e versare la tassa richiesta.

Politica di reclamo e appello

Qualsiasi reclamo dovrà essere presentato entro 30 giorni dal ricevimento della decisione relativa alla certificazione. PECB invierà una risposta scritta al candidato entro 30 giorni lavorativi dalla ricezione del reclamo. Se i candidati ritengono che la risposta non sia soddisfacente, hanno il diritto di presentare appello.

Per ulteriori informazioni relative alla Politica di reclamo e appello, fare clic qui.

SEZIONE V: POLITICHE GENERALI

Esami e certificazioni da parte di altri organismi di certificazione accreditati

PECB accetta certificazioni ed esami da parte di altri organismi di certificazione accreditati e riconosciuti. PECB valuterà le richieste attraverso il suo processo di equivalenza per decidere se la/e certificazione/e o l'esame/gli esami possono essere accettati come equivalenti alla rispettiva certificazione PECB (ad es. la certificazione ISO/IEC 27001 Lead Implementer).

Non discriminazione e facilitazioni speciali

Le domande di tutti i candidati saranno valutate obiettivamente indipendentemente da età, genere, etnia, religione, nazionalità o stato civile dei candidati.

Per garantire pari opportunità a tutte le persone qualificate, se necessario PECB metterà a disposizione alcune facilitazioni[3]. Se i candidati hanno necessità di facilitazioni speciali a causa di disabilità o di specifiche condizioni fisiche, devono informare il partner/distributore in modo che si possa organizzare in tal senso[4]. Ogni informazione che i candidati forniscono in merito alla loro disabilità/esigenza speciale sarà trattata con la massima riservatezza. Per scaricare l'apposito modulo Candidati con disabilità, fare clic qui.

Politica sul comportamento

PECB intende fornire servizi di alto-livello, coerenti e accessibili a vantaggio delle parti interessate esterne: distributori, partner, formatori, sorveglianti, esaminatori, membri di comitati e comitati consultivi e clienti (tirocinanti, esaminandi individui certificati e titolari di certificati), oltre a creare e mantenere un ambiente di lavoro favorevole che garantisca la sicurezza e il benessere del personale, basandosi su dignità, rispetto e diritti umani.

Questa Politica si propone di garantire che PECB gestisca i comportamenti inaccettabili delle parti interessate esterne nei confronti del personale PECB in modo imparziale, riservato, equo e tempestivo. Per consultare la Politica sul comportamento, fare clic qui.

Politica di rimborso

PECB rimborserà i pagamenti se vengono rispettati i requisiti della Politica di rimborso. Per consultare la Politica di rimborso, fare clic qui.

[3] In base all'ADA (Americans with Disabilities Act, Legge sulla Disabilità degli Stati Uniti), il termine "facilitazione ragionevole" può comprendere: (A) strutture esistenti usate dai dipendenti rese accessibili e utilizzabili a individui portatori di disabilità e (B) riassegnazione delle mansioni, part-time o modifica degli orari di lavoro, riassegnazione a un posto vacante, acquisizione o modifica di attrezzature o dispositivi, adeguamento o modifiche appropriate di esami, materiali di formazione o politiche, uso di lettori o interpreti qualificati e altre facilitazioni simili per individui con disabilità.

[4] Direttiva ADA sugli emendamenti del 2008 (P.L. 110-325), Sez. 12189. Esami e corsi. [Sezione 309]: Ogni persona che offra esami o corsi legati a domande, licenze, certificazioni o credenziali per educazione secondaria o post-secondaria, professionale o commerciale, dovrà offrire tali esami o corsi in un luogo e in una modalità che siano accessibile a persone portatrici di disabilità, o offrire sistemazioni alternative accessibili a tali individui.

Indirizzo:

Sede generale
6683 Jean Talon E,
Suite 336 Montréal,
H1S 0A5, QC,
CANADA

Tel./Fax:

T: +1-844-426-7322
F: +1-844-329-7322

Indirizzi email:

Procedura d'esame:
examination.team@pecb.com

Certificazione:
certification.team@pecb.com

Assistenza clienti:
support@pecb.com

PECB Help Center

Nel nostro Help Center è possibile consultare la sessione domande e risposte (FAQ), analizzare i manuali per l'uso del sito Web e delle applicazioni PECB, leggere i documenti relativi alle procedure PECB, o contattarci attraverso il sistema di monitoraggio online del nostro Support Center.

www.pecb.com