PECB

BEYOND RECOGNITION

Chief Information Security Officer (CISO)

Manual del Candidato

PECB

Índice

SECCIÓN I: INTRODUCCIÓN 3
Acerca de PECB 3
El Valor de la Certificación de PECB 4
Código de Ética de PECB 5
Introducción a Chief Information Security Officer (CISO) 7
SECTION II: PREPARACIÓN, REGLAS Y POLÍTICAS DE EXÁMENES 8
Preparar y programar el examen 8
Dominios de competencia 9
Presentar el examen 19
Política de Seguridad del Examen 23
Resultados del examen 24
Política de Repetición del Examen 24
SECCIÓN III: PROCESO Y REQUISITOS DE CERTIFICACIÓN 26
Credenciales CISO de PECB 26
Solicitar la certificación 26
Experiencia profesional 27
Referencias profesionales 27
Experiencia en proyectos 27
Evaluación de las solicitudes de certificación 27
SECCIÓN IV: POLÍTICAS DE CERTIFICACIÓN 28
Denegación de certificación 28
Opciones de estado de certificación 28
Ascenso y degradación de credenciales 29
Renovación de la certificación 29
Cierre de un caso 29
Política de Quejas y Apelaciones 30
SECCIÓN V: POLÍTICAS GENERALES 31
Exámenes y certificaciones de otros organismos de certificación acreditados 31
No discriminación y adaptaciones especiales 31
Política de Comportamiento 31
Política de Reembolso 31

SECCIÓN I: INTRODUCCIÓN

Acerca de PECB

PECB, es un organismo de certificación que ofrece educación[1], certificación y programas de certificado para personas en una amplia gama de disciplinas.

A través de nuestra presencia en más de 150 países, ayudamos a los profesionales a demostrar su competencia en diversas áreas de especialización al proporcionar valiosos programas de evaluación, certificación y programas de certificado bajo normas reconocidas internacionalmente.

Nuestros objetivos clave son:

1. Establecer los requisitos mínimos necesarios para certificar a los profesionales y para otorgar designaciones
2. Revisar y verificar las calificaciones de los candidatos para asegurar que son elegibles para la certificación
3. Mantener y mejorar continuamente el proceso de evaluación para certificar a las personas
4. Certificar a personas cualificadas, otorgar designaciones y mantener directorios respectivos
5. Establecer los requisitos para la renovación periódica de certificación y asegurar que las personas certificadas cumplen con tales requisitos
6. Comprobar que los profesionales de PECB cumplen con los estándares éticos en su práctica profesional
7. Representar a nuestras partes interesadas en asuntos de interés común
8. Promover los beneficios de los programas de certificación y programas de certificado a profesionales, negocios, gobiernos y el público en general

Nuestra misión

Proporcionar a nuestros clientes servicios integrales de examen, certificación y programa de certificado que inspiren confianza y beneficien a la sociedad en su conjunto.

Nuestra visión

Convertirse en el referente global en la prestación de servicios de certificación profesional y programas de certificado.

Nuestros valores

Integridad, Profesionalismo, Imparcialidad

[1]La educación se refiere a los cursos de capacitación desarrollados por PECB que son ofrecidos globalmente a través de nuestra red de socios.

El Valor de la Certificación de PECB

Reconocimiento mundial
Las credenciales de PECB son reconocidas internacionalmente y avaladas por muchos organismos de acreditación, por lo que los profesionales que buscan obtenerlas se beneficiarán de nuestro reconocimiento en los mercados nacionales e internacionales.

El valor de las certificaciones de PECB se valida mediante la acreditación de International Accreditation Service (IAS-PCB-111), United Kingdom Accreditation Service (UKAS-No 21923) y Korean Accreditation Board (KAB-PC-08) bajo ISO/IEC 17024 – Requisitos generales para los organismos que operan la certificación de personas. El valor de los programas de certificación de PECB es validado por la acreditación del Consejo Nacional de Acreditación del Instituto Estadounidense de Normas Nacionales (ANAB-Accreditation ID 1003) bajo ANSI/ASTM E2659-18, Práctica Estándar para Programas de Certificación.

PECB es miembro asociado de The Independent Association of Accredited Registrars (IAAR), miembro de pleno derecho de International Personnel Certification Association (IPC), miembro signatario de IPC MLA, y miembro del Club EBIOS, CPD Certification Service, CLUSIF, Credential Engine e ITCC. Además, PECB es un Socio Editor Autorizado (LPP, siglas en inglés) aprobado por el Organismo de Acreditación de Certificación de Modelo de Madurez de Ciberseguridad (CMMC-AB) para la norma de Certificación de Modelo de Madurez de Ciberseguridad (CMMC), está aprobado por el Club EBIOS para ofrecer la certificación de habilidades de Gerente de Riesgos EBIOS, y está aprobado por la CNIL (Commission Nationale de l'Informatique et des Libertés) para ofrecer la certificación DPO. Para obtener información más detallada, haga clic aquí.

Productos y servicios de alta calidad
Estamos orgullosos de ofrecer a nuestros clientes productos y servicios de alta calidad que se adaptan a sus necesidades y demandas. Todos nuestros productos son cuidadosamente preparados por un equipo de expertos y profesionales basados en las mejores prácticas y metodologías.

Cumplimiento con las normas
Nuestras certificaciones y programas de certificado son una demostración del cumplimiento de las normas ISO/IEC 17024 y ASTM E2659. Ellas aseguran que los requisitos de la norma se han cumplido y validado con la consistencia, profesionalismo e imparcialidad adecuados.

Servicio orientado al cliente
Somos una empresa centrada en el cliente y tratamos a cada uno de nuestros clientes con valor, importancia, profesionalidad y honestidad. PECB cuenta con un equipo de expertos que se encargan de atender las solicitudes, preguntas y necesidades. Hacemos todo lo posible para mantener un tiempo de respuesta máximo de 24 horas sin comprometer la calidad del servicio.

Flexibilidad y comodidad
Las oportunidades de aprendizaje en línea hacen que su desarrollo profesional sea más conveniente, ya que puede programar sus sesiones de aprendizaje de acuerdo con su estilo de vida. Dicha flexibilidad le brinda más tiempo libre, ofrece más oportunidades de avance profesional y reduce los costos.

Código de Ética de PECB

El Código de Ética representa los más altos valores y la ética que PECB está plenamente comprometido a seguir, ya que reconoce la importancia de ellos a la hora de prestar servicios y atraer clientes.

La División de Cumplimiento se asegura de que los empleados, instructores, evaluadores, supervisores de examen, socios y distribuidores de PECB, así como los miembros de diferentes consejos y comités asesores, las personas certificadas y los titulares de certificados (en adelante, "Profesionales de PECB") se adhieren a este Código de Ética. Además, la División de Cumplimiento enfatiza constantemente la necesidad de comportarse profesionalmente y con plena responsabilidad, competencia e imparcialidad en la prestación de servicios con partes interesadas internas y externas, tales como solicitantes, candidatos, personas certificadas, titulares de certificados, etc. autoridades de acreditación y autoridades gubernamentales.

PECB tiene la convicción de que para lograr el éxito organizacional, tiene que entender completamente las necesidades y expectativas de los clientes y las partes interesadas. Para ello, PECB fomenta una cultura basada en los más altos niveles de integridad, profesionalismo e imparcialidad, que son también sus valores. Estos valores son parte integral de la organización, y han caracterizado la presencia global y el crecimiento a lo largo de los años y han establecido la reputación que PECB goza hoy en día.

PECB cree que los grandes valores éticos son esenciales para tener relaciones sanas y fuertes. Por lo tanto, es la responsabilidad principal de PECB asegurarse de que los profesionales de PECB muestren un comportamiento que cumpla plenamente con los principios y valores de PECB.

Los profesionales de PECB son responsables de:

1. Mostrar el comportamiento profesional en la prestación de servicios con honestidad, precisión, imparcialidad e independencia
2. Actuar en todo momento en la prestación de sus servicios únicamente en el mejor interés de su empleador, clientes, el público y la profesión de acuerdo con este Código de Ética y otras normas profesionales
3. Demostrar y desarrollar competencias en sus respectivos campos y esforzarse por mejorar continuamente sus habilidades y conocimientos
4. Proporcionar solo los servicios profesionales para los cuales son competentes y están calificados, así como informar adecuadamente a los clientes acerca de la naturaleza de los servicios propuestos incluyendo cualquier inquietud o riesgo
5. Informar a su empleador o cliente sobre cualquier interés o afiliaciones de negocio que pudieran influir o menoscabar su juicio
6. Preservar la confidencialidad de la información de cualquier empleador o cliente presente o anterior durante la prestación del servicio
7. Cumplir con todas las leyes y regulaciones aplicables de las jurisdicciones en el país donde se llevaron a cabo las disposiciones de servicio
8. Respetar la propiedad intelectual y las contribuciones de los demás
9. No comunicar, con intención, información falsa o falsificada que pueda poner en peligro la integridad del proceso de evaluación de un candidato a certificación o programa de certificado de PECB
10. No presentarse falsa o erróneamente como representantes de PECB sin una licencia adecuada o hacer mal uso del logotipo, certificaciones o certificados de PECB

11. No actuar de manera que pueda dañar la reputación, las certificaciones o los programas de certificado de PECB
12. Cooperar plenamente en la investigación tras una presunta infracción a este Código de Ética

Para leer la versión completa del Código de Ética de PECB, consulte el Código de Ética | PECB

Introducción a Chief Information Security Officer (CISO)

A medida que evoluciona el panorama digital, la seguridad de los activos organizacionales y la infraestructura de información se ha vuelto crucial. En consecuencia, la función del director de seguridad de la información o por su título en inglés, Chief Information Security Officer (CISO), nunca ha sido tan fundamental. Las organizaciones a nivel mundial se enfrentan a numerosas amenazas de seguridad de la información, y es responsabilidad del CISO navegar por los entornos complejos, garantizando tanto la seguridad como el cumplimiento. Este curso de capacitación proporcionará a los participantes una comprensión integral de las estrategias, tecnologías y habilidades de liderazgo esenciales para el papel del CISO.

Este curso de capacitación abarca las últimas metodologías de evaluación de riesgos, marcos de gobernanza, estrategias de respuesta a incidentes y el panorama de amenazas emergentes. Detalla el rol del CISO en la gestión de la seguridad, la adopción de medidas proactivas, la creación de estrategias dinámicas y el fomento de una cultura de concienciación sobre la seguridad en la organización. Después de completar con éxito este curso de capacitación, los participantes podrán implementar un programa holístico de seguridad de la información y asegurar el cumplimiento de los marcos y regulaciones de seguridad.

La certificación “Chief Information Security Officer” demuestra que una persona tiene competencia en establecer y dirigir un programa de seguridad de la información. Al adquirir esta certificación, las personas mejoran sus habilidades para abordar los desafíos contemporáneos de seguridad de la información y posicionarse como líderes en el campo.

Las certificaciones de PECB no son una licencia o simplemente una membresía. Avalan los conocimientos y habilidades de los candidatos que han adquirido a través de nuestros cursos de capacitación y se emiten a los candidatos que tienen la experiencia requerida y han aprobado el examen.

Este documento especifica el esquema de certificación de PECB para Chief Information Security Officer en conformidad con ISO/IEC 17024:2012. También describe los pasos que los candidatos deberían tomar para obtener y mantener sus credenciales. Como tal, es muy importante leer toda la información incluida en este documento antes de completar y enviar su solicitud. Si tiene alguna pregunta después de leerla, por favor contacte a la oficina internacional de PECB en certification.team@pecb.com.

.

PECB

SECTION II: PREPARACIÓN, REGLAS Y POLÍTICAS DE EXÁMENES

Preparar y programar el examen

Todos los candidatos son responsables de su propio aprendizaje y de preparación para los exámenes de certificación. Aunque los candidatos no están obligados a asistir al curso de capacitación para ser elegibles a tomar el examen, asistir a él puede aumentar significativamente sus posibilidades de aprobar con éxito el examen.

Para programar el examen, los candidatos tienen dos opciones:

1. Ponerse en contacto con uno de nuestros socios autorizados. Para encontrar un socio autorizado en su región, consulte la Lista de Distribuidores. El horario del curso de capacitación también está disponible en línea y se puede acceder en Eventos de Capacitación.
2. Realizar un examen PECB de forma remota a través de la aplicación PECB Exams. Para programar un examen remoto, por favor, vaya al siguiente enlace: Eventos de Examen.

Para obtener más información sobre exámenes, dominios de competencia y áreas de conocimientos, por favor consulte la *Sección III* de este documento.

Reprogramar el examen

Para cualquier cambio en la fecha, hora, lugar y otros detalles del examen, póngase en contacto con online.exams@pecb.com.

Cuotas para solicitud del examen y la certificación

Los candidatos pueden realizar el examen sin asistir al curso de capacitación. Los precios aplicables son los siguientes:

- Examen de Líder: $1000[2]
- Examen de Gerente: $700
- Examen de Fundamentos: $500
- Examen de Transición: $500

La cuota para solicitud de certificación es de $500.

Para todos los candidatos que hayan tomado el curso de capacitación con uno de los socios de PECB, la cuota de solicitud incluye los costos del examen (primer intento y primera repetición) la solicitud de certificación y el primer año de la Cuota de Mantenimiento Anual (CMA).

[2] Todos los precios listados en este documento están en dólares estadounidenses.

Dominios de competencia

La credencial CISO es una certificación profesional para personas que buscan mostrar su experiencia en la implementación y el liderazgo de un programa integral de seguridad de la información.

El rol del CISO abarca una amplia gama de responsabilidades, y por lo tanto, requiere un conjunto de habilidades diversas. Si bien el conocimiento técnico y la experiencia son críticos, podría decirse que la habilidad más importante para que un CISO dirija un programa de seguridad de la información de manera efectiva es el liderazgo estratégico.

La certificación de CISO está destinada a:

- Profesionales que participan activamente en la gestión de la seguridad de la información
- Los CISO experimentados que buscan mejorar sus conocimientos, mantenerse al día con las últimas tendencias y refinar sus habilidades de liderazgo
- Gerentes de TI responsables de supervisar los programas y activos de seguridad de la información
- Profesionales de la seguridad que aspiran a avanzar en roles de liderazgo, tales como arquitectos de seguridad o analistas de seguridad
- Profesionales responsables de la gestión del riesgo de seguridad de la información y el cumplimiento dentro de las organizaciones
- Ejecutivos, incluidos directores generales, de informática y operativos, que desempeñan un papel crucial en los procesos de toma de decisiones relacionados con la seguridad de la información
- Profesionales que buscan roles de seguridad de la información a nivel ejecutivo

El contenido del examen se divide de la siguiente manera:

- **Dominio 1:** Conceptos fundamentales de la seguridad de la información
- **Dominio 2:** El rol del CISO en un programa de seguridad de la información
- **Dominio 3:** Selección de un programa de cumplimiento de seguridad, gestión de riesgos y arquitectura y diseño de la seguridad
- **Dominio 4:** Aspectos operacionales de los controles de seguridad de la información, gestión de incidentes y gestión de cambios
- **Dominio 5:** Fomentar una cultura de seguridad de la información, medición, seguimiento y mejora de un programa de seguridad de la información

Dominio 1: Conceptos fundamentales de la seguridad de la información

Objetivo principal: Asegurar que el candidato sea capaz de interpretar los conceptos y principios fundamentales de la seguridad de la información.

Competencias	Declaraciones de conocimientos
1. Capacidad para explicar los principales conceptos de seguridad de la información 2. Capacidad para explicar la confidencialidad, integridad y disponibilidad (la tríada CIA) 3. Capacidad para explicar la divulgación, alteración y negación (la tríada DAD) 4. Capacidad para explicar el marco de seguridad de identificación, autenticación, autorización y rendición de cuentas (IAAA) 5. Capacidad para identificar y categorizar diferentes tipos de amenazas y vulnerabilidades 6. Capacidad para reconocer y mitigar los proveedores de ataques comunes 7. Capacidad para explicar las políticas y procedimientos de seguridad de la información 8. Capacidad para clasificar los controles de seguridad 9. Capacidad para identificar tipos de software malicioso y ataques de ingeniería social 10. Capacidad de reconocer la importancia de la seguridad física, la seguridad de la red, la seguridad de las aplicaciones, la seguridad en la nube, la inteligencia contra amenazas, y la criptografía en la protección de los activos de información	1. Conocimiento de los principales conceptos y principios de seguridad de la información 2. Conocimiento de la tríada CIA 3. Conocimiento de la tríada DAD 4. Conocimiento del marco de seguridad de identificación, autenticación, autorización y rendición de cuentas (IAAA) 5. Conocimiento de los diversos tipos de amenazas y vulnerabilidades 6. Conocimiento de las políticas y procedimientos de seguridad 7. Conocimiento de los riesgos de seguridad de la información 8. Conocimiento del tipo y función de los controles de seguridad 9. Conocimiento de diversas normas y marcos de seguridad 10. Conocimiento de software malicioso y ataques de ingeniería social 11. Conocimiento de seguridad física, seguridad de red, seguridad de aplicaciones, inteligencia contra amenazas y criptografía

Dominio 2: El rol del CISO en un programa de seguridad de la información

Objetivo principal: Asegurar que el candidato sea capaz de definir, establecer, gestionar y mejorar un programa de seguridad de la información, al tiempo que personifica con éxito el rol de un CISO en la alineación de los imperativos de seguridad con los objetivos de la organización.

Competencias	Declaraciones de conocimientos
1. Capacidad para definir los roles y responsabilidades de un CISO dentro de una organización	1. Conocimiento de las responsabilidades básicas de un CISO dentro de una organización
2. Capacidad para involucrarse y cooperar con otros ejecutivos	2. Conocimiento de las responsabilidades del CISO, CIO, CTO y CPO
3. Capacidad para comprender y comparar las responsabilidades del CISO, CIO, CTO y CPO	3. Conocimiento de los rasgos clave de liderazgo necesarios para el papel de CISO
4. Capacidad para abordar y superar los desafíos comunes encontrados por un CISO	4. Conocimiento de estrategias de comunicación efectivas
5. Capacidad para obtener las cualidades de liderazgo necesarias para el rol del CISO	5. Conocimiento de los desafíos potenciales que un CISO podría enfrentar
6. Capacidad de adherirse a los estándares éticos	6. Conocimiento de las consideraciones éticas y normas relativas al papel de CISO
7. Capacidad para definir objetivos de seguridad de la información claros y relevantes alineados con los objetivos de la organización	7. Conocimiento del programa de seguridad de la información
8. Capacidad para establecer un programa integral de seguridad de la información	8. Conocimiento de objetivos de seguridad de la información
9. Capacidad para diseñar e implementar una estructura organizativa eficaz para el programa de seguridad de la información	9. Conocimiento de las estructuras organizativas que apoyan la seguridad de la información
10. Capacidad para definir el alcance de un programa de seguridad de la información	10. Conocimiento del alcance de un programa de información
11. Capacidad para asignar y gestionar recursos de manera efectiva para el programa de seguridad de la información	11. Conocimiento de los recursos, herramientas y personal esenciales para un programa de seguridad de la información robusto
12. Capacidad para desarrollar e implementar estrategias proactivas de seguridad de la información	12. Conocimiento de planificación e implementación estratégicos en el contexto de la seguridad de la información

Dominio 3: Selección de un programa de cumplimiento de seguridad, gestión de riesgos y arquitectura y diseño de la seguridad

Objetivo principal: Asegurar que el candidato sea capaz de interpretar, desarrollar y mantener el programa de cumplimiento de una organización, gestionar los riesgos de manera efectiva, analizar los controles de seguridad existentes y diseñar arquitecturas de seguridad robustas mediante la selección de una arquitectura de seguridad y un marco de diseño adecuados.

Competencias	Declaraciones de conocimientos
1. Capacidad para desarrollar, implementar y monitorear un programa de cumplimiento basado en las necesidades específicas de la organización 2. Capacidad para asegurar el cumplimiento de las regulaciones y estándares específicos de la industria 3. Capacidad para revisar y actualizar regularmente el programa de cumplimiento 4. Capacidad para educar y capacitar a los empleados sobre los requisitos de cumplimiento y las mejores prácticas 5. Capacidad para coordinarse con los departamentos legales y de otro tipo para asegurar un cumplimiento integral 6. Capacidad para identificar, evaluar y priorizar los riesgos dentro del contexto organizacional 7. Capacidad para evaluar la eficacia de controles de seguridad 8. Capacidad para identificar brechas en los controles de seguridad existentes 9. Aptitud para examinar las capacidades de seguridad de la información en áreas clave como el riesgo y la resiliencia, la inteligencia y la conciencia de la seguridad operativa, la seguridad física y la gestión de la cadena de suministro 10. Capacidad para utilizar el análisis de brechas en la identificación y evaluación de las capacidades de seguridad de la información existentes 11. Capacidad para desarrollar e implementar estrategias de mitigación de riesgos 12. Capacidad para identificar, analizar y evaluar riesgos	1. Conocimiento de los principales marcos regulatorios y normas aplicables a la industria 2. Conocimiento de los distintos organismos y su función específica en materia de seguridad de la información 3. Conocimiento de las funciones básicas, categorías y subcategorías descritas en el marco de ciberseguridad de NIST 4. Conocimiento de los niveles de implementación y cómo apoyan el proceso de gestión de riesgos 5. Conocimiento de los objetivos y requisitos de la Directiva NIS 2 6. Conocimiento de los métodos para implementar y supervisar la efectividad de los controles CIS 7. Conocimiento de la estructura marco de COBIT, incluyendo sus componentes de gobernanza y prácticas de gestión 8. Conocimiento de los requisitos de ISO/IEC 27001 para un sistema de gestión de la seguridad de la información (SGSI) 9. Conocimiento de las cinco etapas de ITIL, PCI DSS, CSA STAR Program, RGPD y requisitos de HIPPA 10. Conocimiento de una política de seguridad de la información y su papel en la orientación del comportamiento organizacional y en el aseguramiento del cumplimiento de la seguridad 11. Conocimiento de las capacidades de seguridad de la información 12. Conocimiento de las capacidades de gestión de la cadena de suministro

13. Capacidad para seleccionar opciones de tratamiento de riesgos de la información 14. Capacidad para crear un plan de tratamiento de riesgos 15. Capacidad para identificar herramientas de gestión de riesgos y software que se puede utilizar para automatizar procesos 16. Capacidad para conectar la comunicación de riesgos con los objetivos de negocio 17. Capacidad para establecer un plan de comunicación de riesgos con partes internas y externas 18. Capacidad para registrar, reportar, supervisar y revisar riesgos 19. Capacidad para explicar la arquitectura y el diseño de seguridad 20. Capacidad para seleccionar un marco de arquitectura de seguridad y alinearlo con los recursos de negocio 21. Capacidad para explicar la arquitectura de principio de confianza cero 22. Capacidad para seleccionar el componente de diseño de arquitectura de seguridad 23. Capacidad para explicar la diferencia entre los sistemas de seguridad de la información y la seguridad de la infraestructura	13. Conocimiento de las metodologías de evaluación de riesgos 14. Conocimiento de técnicas y herramientas de mitigación de riesgos 15. Conocimiento de los principios de seguimiento continuo de la gestión de riesgos 16. Conocimiento de técnicas de identificación de riesgos, métodos de análisis de riesgos y criterios de valoración de riesgos 17. Conocimiento del proceso de tratamiento de riesgos sobre cómo abordar, mitigar, transferir o aceptar riesgos 18. Conocimiento de estrategias efectivas de comunicación de riesgos 19. Conocimiento de los mecanismos de seguimiento y revisión para mejorar el proceso de gestión de riesgos 20. Conocimiento de los marcos y metodologías que guían la gestión eficaz del riesgo 21. Conocimiento de los principios y estructuras de las arquitecturas de seguridad organizacional y su aplicación 22. Conocimiento del marco de arquitectura de seguridad de Zachman, SABSA, TOGAF y OSA 23. Conocimiento de principio de confianza cero 24. Conocimiento de componentes de arquitectura de seguridad como NFV, SASE, SSE, servicios de red superpuestos y arquitectura multinube

Dominio 4: Aspectos operacionales de los controles de seguridad de la información, gestión de incidentes y gestión de cambios

Objetivo principal: Asegurar que el candidato sea capaz de seleccionar, diseñar, implementar y evaluar los controles de seguridad de la información, gestionar incidentes de seguridad y supervisar el proceso de gestión de cambios de TI.

Competencias	Declaraciones de conocimientos
1. Capacidad para clasificar, seleccionar e implementar controles efectivos de seguridad de la información	1. Conocimiento de diversas clasificaciones de controles de seguridad de la información
2. Capacidad para documentar los controles de seguridad de la información establecidos de manera integral	2. Conocimiento de los procesos y mejores prácticas para la selección y diseño de controles
3. Capacidad para implementar controles específicos para inteligencia contra amenazas y seguridad operativa	3. Conocimiento de normas de documentación para controles de seguridad de la información
4. Capacidad para incorporar la seguridad física en el marco más amplio de los controles de seguridad de la información	4. Conocimiento de los controles específicos de la inteligencia contra amenazas y sus aplicaciones
5. Capacidad para diseñar e implementar controles para la gestión de la seguridad	5. Conocimiento de los componentes clave de los controles de seguridad operacional y física
6. Capacidad para identificar tecnologías emergentes relevantes para los CISO	6. Conocimiento de los controles de gestión de la cadena de suministro y su importancia para asegurar el cifrado de extremo a extremo
7. Capacidad para probar y evaluar la eficacia de los controles de seguridad establecidos	7. Conocimiento de las tecnologías emergentes y sus implicaciones para los CISO
8. Capacidad para gestionar eficazmente los incidentes de seguridad de la información	8. Conocimiento de protocolos de prueba y métricas de evaluación para controles de seguridad
9. Capacidad para monitorear, documentar e informar incidentes de seguridad	9. Conocimiento del ciclo de vida de la gestión de incidentes de seguridad de la información
10. Capacidad para diseñar e implementar programas de capacitación en respuesta a incidentes y concienciación sobre la seguridad	10. Conocimiento de técnicas de seguimiento y normas de documentación para incidentes de seguridad
11. Capacidad para desarrollar planes de continuidad del negocio	11. Conocimiento sobre el diseño de módulos de capacitación en respuesta a incidentes y la importancia de los programas de concienciación sobre seguridad
12. Capacidad para redactar y ejecutar un plan de recuperación de desastres	12. Conocimiento de la planificación de la continuidad del negocio
13. Capacidad para explicar e implementar procesos de gestión de cambios de TI	13. Conocimiento de la planificación de recuperación ante desastres
14. Capacidad para categorizar y priorizar los cambios de TI en función de su impacto y relevancia	14. Conocimiento de la gestión de cambios de TI y su importancia

15. Capacidad para establecer controles de gestión de cambios para supervisar y asegurar transiciones exitosas 16. Capacidad para reconocer y llevar a cabo roles y responsabilidades en la gestión de cambios de TI, incluido el rol de CISO	15. Conocimiento de tres categorías de cambios de TI 16. Conocimiento de los mecanismos de control de gestión de cambios 17. Conocimiento del procedimiento paso a paso para una gestión eficiente de cambios de TI 18. Conocimiento de los diversos roles y responsabilidades dentro de la gestión de cambios de TI 19. Conocimiento del rol del CISO en supervisar y guiar la gestión de cambios de TI

Dominio 5: Fomentar una cultura de seguridad de la información, medición, seguimiento y mejora de un programa de seguridad de la información

Objetivo principal: Asegurar que el candidato sea capaz de desarrollar y evaluar programas eficaces de capacitación y concienciación, establecer un proceso de seguimiento robusto y comprender la importancia de los programas de aseguramiento.

Competencias	Declaraciones de conocimientos
1. Capacidad para establecer y mejorar un programa de capacitación y concienciación	1. Conocimiento de los componentes clave de los programas de concienciación y capacitación
2. Capacidad para llevar a cabo las responsabilidades del CISO en el programa de concienciación y capacitación	2. Conocimiento del rol del CISO en la orientación y dirección de las actividades de capacitación y concienciación
3. Capacidad para asignar fondos de manera efectiva para el programa de capacitación y concienciación	3. Conocimiento de las necesidades de financiación y estrategias de asignación para los programas de capacitación
4. Capacidad para diseñar estructuras de programas de desarrollo de competencias	4. Conocimiento de diferentes estructuras y tipos de programas de desarrollo de competencias
5. Capacidad para seleccionar e implementar métodos de capacitación efectivos	5. Conocimiento de los diferentes métodos de capacitación y su eficacia
6. Capacidad para adaptarse y explicar el cambio cultural dentro de la organización	6. Conocimiento de los mecanismos de cambio cultural dentro de las organizaciones
7. Capacidad para evaluar los resultados de las sesiones de capacitación	7. Conocimiento de las técnicas de evaluación para los resultados de la capacitación
8. Capacidad para implementar prácticas de seguimiento continuo para la seguridad de la información	8. Conocimiento del monitoreo continuo de seguridad de la información (ISCM) y su importancia
9. Capacidad para evaluar la eficacia global del programa de seguridad de la información	9. Conocimiento de técnicas de evaluación para la evaluación del programa de seguridad
10. Capacidad para definir y utilizar métricas de seguridad relevantes e indicadores clave de desempeño (KPI)	10. Conocimiento en el diseño de métricas y los KPI relevantes para la seguridad de la información
11. Capacidad para evaluar el desempeño y revisar los KPI	11. Conocimiento de la evaluación del desempeño y revisiones de los KPI
12. Capacidad para informar efectivamente los resultados de la medición	12. Conocimiento de mecanismos eficaces de notificación de resultados de medición
13. Capacidad para explicar e implementar un programa de aseguramiento	13. Conocimiento de los fundamentos y la importancia de un programa de aseguramiento
14. Capacidad para probar, revisar e informar sobre los procedimientos de seguridad de la información	14. Conocimiento de técnicas para probar y revisar procedimientos de seguridad de la información y reportar resultados
15. Capacidad para llevar a cabo auditorías de seguridad comprehensivas	15. Conocimiento de los procedimientos de auditoría de seguridad

16. Capacidad para explicar la importancia de las pruebas de penetración y analizar sus resultados 17. Capacidad para incorporar actividades de escaneo de vulnerabilidades en el programa de aseguramiento de la organización 18. Capacidad para evaluar la postura general de seguridad de la organización 19. Capacidad para guiar y supervisar auditorías internas y externas	16. Conocimiento de las metodologías de evaluación de riesgos y su impacto en la seguridad 17. Conocimiento de los principios y prácticas de las pruebas de penetración 18. Conocimiento de herramientas y metodologías de escaneo de vulnerabilidades 19. Conocimiento de las evaluaciones de postura de seguridad 20. Conocimiento de procesos de auditoría interna y externa

Con base en los dominios antes mencionados y su relevancia, el examen contiene 80 preguntas de opción múltiple, como se resumen en la siguiente tabla:

				Nivel de comprensión (Cognitivo/Taxonomía) requerido	
		Número de preguntas/puntos por dominio de competencia	% del examen dedicado/apunta a/para cada dominio de competencia	Preguntas que miden la comprensión, la aplicación y el análisis	Preguntas que miden la evaluación
Dominios de competencia	Conceptos fundamentales de la seguridad de la información	9	11.25	X	
	El rol del CISO en un programa de seguridad de la información	20	25	X	
	Selección de un programa de cumplimiento de seguridad, gestión de riesgos y arquitectura y diseño de la seguridad	20	25	X	
	Aspectos operacionales de los controles de seguridad de la información, gestión de incidentes y gestión de cambios	21	26.25		X
	Fomentar una cultura de seguridad de la información, medición, seguimiento y mejora de un programa de seguridad de la información	10	12.5		X
	Total	**80**	**100%**		
	Número de preguntas por nivel de comprensión			**49**	**31**
	% del examen dedicado a cada nivel de comprensión (cognitivo/taxonomía)			**61.25%**	**38.75%**

La puntuación mínima para aprobar el examen es de **70%.**

Después de aprobar el examen, los candidatos podrán solicitar la credencial "PECB Chief Information Security Officer".

Presentar el examen

Información general sobre el examen
Se les pide a los candidatos llegar/estar presentes por lo menos 30 minutos antes de que el examen comience.

A los candidatos que lleguen tarde no se les dará tiempo compensatorio por su llegada tardía y se les podría denegar la entrada al examen.

Los candidatos deberán presentar un documento de identidad válido (credencial de identidad nacional, permiso de conducir o pasaporte) ante el supervisor de examen.

Si se solicita el día del examen (en el caso de examen en papel), es posible otorgar tiempo adicional a los candidatos que presentan el examen en un idioma distinto al materno, como se indica a continuación:
- 10 minutos adicionales para los exámenes de Fundamentos
- 20 minutos adicionales para examen de Gerente
- 30 minutos adicionales para examen de Líder

Formato y tipo de examen de PECB
1. **En papel:** Los exámenes se proporcionan en papel, y a los candidatos no se les permite que usen más que la hoja de examen y un bolígrafo. No se permite el uso de dispositivos electrónicos tales como computadoras portátiles, tabletas o teléfonos. La sesión de examen es vigilada por un Supervisor de Examen aprobado por PECB en la ubicación donde el Socio ha organizado el curso de capacitación.
2. **En línea:** Los exámenes son proporcionados electrónicamente a través de la aplicación de Exámenes PECB. No se permite el uso de dispositivos electrónicos tales como tabletas y teléfonos celulares. La sesión de examen es vigilada de forma remota por un Supervisor de Examen de PECB a través de la aplicación de Exámenes PECB y una cámara integrada/externa.

Para obtener más información sobre los exámenes en línea, consulte la Guía del Examen en Línea de PECB.

Los exámenes de PECB están disponibles en dos tipos:
1. Examen de preguntas de tipo ensayo
2. Examen de preguntas de opción múltiple

Este examen contiene preguntas de opción múltiple: El examen de opción múltiple se puede utilizar para evaluar la comprensión de un candidato tanto en conceptos simples como en complejos. Incluye preguntas independientes y basadas en escenarios. Las preguntas independientes se mantienen de forma separada dentro del examen y no dependen del contexto, mientras que las preguntas basadas en escenarios dependen del contexto, es decir, se desarrollan en función de un escenario que se pide a un candidato que lea y se espera que proporcione respuestas a cinco preguntas relacionadas con ese escenario. Al responder preguntas independientes y basadas en escenarios, los candidatos deberán aplicar varios conceptos y principios explicados durante el curso de capacitación, analizar problemas, identificar y evaluar alternativas, combinar varios conceptos o ideas, etc.

Cada pregunta de opción múltiple tiene tres opciones, de las cuales una es la opción de respuesta correcta (respuesta clave) y dos opciones de respuesta incorrecta (distractores).

Este es un examen a libro abierto. El candidato puede utilizar los siguientes materiales de referencia:

- Materiales del curso de capacitación (a los que se accede a través de la aplicación de PECB Exams y/o en copia impresa)
- Cualquier nota personal tomada durante el curso de capacitación (a la que se accede a través de la aplicación de PECB Exams y/o en copia impresa)
- Un diccionario impreso

A continuación se proporciona una muestra de las preguntas del examen.

Nota: PECB cambiará progresivamente a exámenes de opción múltiple. También serán a libro abierto e incluirán preguntas basadas en escenarios que permitirán a PECB evaluar los conocimientos, habilidades y capacidades de los candidatos para usar la información en nuevas situaciones (aplicar), establecer conexiones entre ideas (analizar) y justificar una posición o decisión (evaluar).

Para obtener información específica acerca de los tipos de examen, los idiomas disponibles, y otros detalles, por favor contacte a examination.team@pecb.com o consulte la Lista de Exámenes de PECB.

Muestra de preguntas de examen

Zootron, una empresa líder en tecnología alemana, recientemente sufrió una transformación estructural en su departamento de TI. Reconociendo el aumento de las amenazas cibernéticas, establecieron un puesto dedicado para un director de seguridad de la información (CISO). Jenah, con experiencia en tecnología y gestión, fue designada.

En el primer mes, Jenah revisó los fundamentos de la seguridad de la información. Reconoció las brechas en la gestión de los riesgos de ciberseguridad y el incumplimiento de las normas de privacidad y seguridad e identificó los riesgos a través de una evaluación detallada.

Para el tercer mes, Jenah inició un programa de concienciación y capacitación. Abogó por fomentar una cultura de trabajo positiva, aumentar la productividad y asegurar fondos para la capacitación, asegurando una combinación de métodos para acomodar a todos los estudiantes. También señaló la necesidad de un seguimiento continuo e implementó prácticas para gestionar los riesgos, monitorear las anomalías, evaluar las vulnerabilidades y reconocer las amenazas. Utilizó herramientas que proporcionaron información sobre varias medidas de seguridad para evaluar la efectividad del programa de seguridad de la información de *Zootron*.

Después de seis meses, Jenah propuso el inicio de un programa de aseguramiento. Esto incluyó una auditoría de seguridad exhaustiva que tuvo como objetivo evaluar la red de la empresa, identificar debilidades y asegurar el cumplimiento de las normas y regulaciones aplicables. Las auditorías fueron llevadas a cabo por profesionales de *Zootron*que también se encargaron de asesorar a la organización sobre las medidas de mejora. Además, Jenah propuso el uso de herramientas para detectar posibles exposiciones a riesgos de seguridad en el sistema de *Zootron*, así como ataques simulados de hacking para identificar las causas raíz de los ataques de ciberseguridad. Esta iniciativa ayudaría a *Zootron* a identificar puntos débiles en las capacidades existentes de la organización para proteger los componentes de tecnología de seguridad de la información, los servicios y las aplicaciones de software, así como los sistemas basados en la nube.

De acuerdo con el escenario anterior, responda las siguientes preguntas:

1. **En base a la información que Jenah recopiló durante el primer mes, ¿qué marcos de cumplimiento debería implementar la empresa?**
   A. COBIT e HIPAA
   B. **NIST, CSF y RGPD**
   C. Controles CIS y el programa CSA STAR

2. **Cuando Jenah inició un programa de concienciación y capacitación, ¿qué enfatizó?**
   A. Adhesión a protocolos de seguridad estrictos
   B. La colaboración entre departamentos
   C. **La transformación cultural**

3. **¿Cómo aseguró Jenah la efectividad del programa de seguridad de la información de *Zootron*?**
   A. **Mediante la implementación de prácticas ISCM y métricas de KPI**
   B. Centrándose únicamente en programas de capacitación en concienciación
   C. Mediante la realización de una auditoría externa

4. **Basado en el escenario anterior, Jenah propuso ataques simulados de hacking dentro de *Zootron* para identificar la causa raíz de los ataques potenciales. ¿Es esto aceptable?**
   A. **Sí, las simulaciones de ataque pueden ser realizadas por usuarios autorizados dentro de la organización**
   B. No, las simulaciones de ataque son poco éticas y no pueden ser realizadas por individuos dentro de la organización
   C. No, Jenah debería haber esperado a que se produjeran ataques reales para identificar su causa raíz

5. **¿Qué capacidad de seguridad de la información de *Zootron* pretendía mejorar la iniciativa del programa de aseguramiento de Jenah?**
   A. Gestión de la cadena de suministro
   B. **Seguridad operacional**
   C. Inteligencia contra amenazas

Política de Seguridad del Examen

PECB se compromete a proteger la integridad de sus exámenes y el proceso general de examen, y se basa en el comportamiento ético de los solicitantes, solicitantes potenciales, candidatos y socios para mantener la confidencialidad de los exámenes de PECB. Esta política tiene como objetivo abordar el comportamiento inaceptable y asegurar un trato justo de todos los candidatos.

Cualquier divulgación de información sobre el contenido de los exámenes de PECB es una violación directa a esta Política y al Código de Ética de PECB. Por lo tanto, los candidatos que tomen un examen PECB deben firmar un Acuerdo de confidencialidad y no divulgación del examen y deben cumplir con lo siguiente:

1. Las preguntas y respuestas de los materiales del examen son propiedad exclusiva y confidencial de PECB. Una vez que los candidatos entreguen el examen a PECB, ya no tendrán acceso al examen original ni a una copia del mismo.
2. Los candidatos tienen prohibido revelar cualquier información sobre las preguntas y respuestas del examen o discutir dichos detalles con cualquier otro candidato o persona.
3. Los candidatos no pueden llevar consigo ningún material relacionado con el examen, fuera de la sala de examen.
4. No se permite a los candidatos copiar o intentar hacer copias (ya sean escritas, fotocopiadas o de otro modo) de cualquier material del examen, incluyendo, sin limitación, cualquier pregunta, respuesta o imágenes de pantalla.
5. Los candidatos no deben participar ni promover actividades fraudulentas de realización de exámenes, tales como:
    - Mirar el material de examen o la hoja de respuestas de otro candidato
    - Dar o recibir ayuda del supervisor de examen, candidato o cualquier otra persona
    - El uso de guías de referencia no autorizadas, manuales, herramientas, etc., incluyendo el uso de sitios de “almacén de conocimientos”, ya que no están autorizados por PECB

Una vez que un candidato descubra o ya tenga conocimiento de las irregularidades o infracciones a los puntos mencionados anteriormente, es responsable de cumplirlos, de lo contrario, si tales irregularidades se presentasen, los candidatos serán reportados directamente a PECB, o si observan dichas irregularidades deben informar inmediatamente a PECB.

Los candidatos son los únicos responsables de comprender y cumplir con las Reglas y Políticas del Examen, el Acuerdo de Confidencialidad y No Divulgación y el Código de Ética de PECB. Por lo tanto, si se identifica un incumplimiento de una o más reglas, los candidatos no recibirán ningún reembolso. Además, PECB tiene el derecho de negar el derecho de ingresar a un examen PECB o de invitar a los candidatos a una repetición del examen si se identifican irregularidades durante y después del proceso de calificación, dependiendo de la gravedad del caso.

Cualquier violación de los puntos mencionados anteriormente causará a PECB daños irreparables que ningún remedio monetario puede compensar. Por lo tanto, PECB puede tomar las medidas apropiadas para remediar o prevenir cualquier divulgación no autorizada o uso indebido de los materiales del examen, incluida la obtención de una orden judicial inmediata.

PECB tomará medidas contra las personas que violen las reglas y políticas, incluyendo su prohibición permanente para obtener credenciales de PECB y la revocación de las obtenidas anteriormente. PECB

emprenderá igualmente acciones legales en contra de las personas u organizaciones que infrinjan los derechos de autor, derechos de patente y los derechos de propiedad intelectual.

Resultados del examen

Los resultados del examen se comunicarán por correo electrónico.

- El tiempo de comunicación comienza a contar a partir de la fecha del examen y tarda de tres a ocho semanas para los exámenes de tipo ensayo y dos a cuatro semanas para los de opción múltiple en papel.
- Para los exámenes de opción múltiple en línea, los candidatos reciben sus resultados al instante.

Los candidatos que aprueben el examen estarán en condición de solicitar una de las credenciales del esquema de certificación correspondiente.

Para los candidatos que no aprueben el examen, se incluirá en el correo electrónico una lista de los dominios en los que hayan tenido dificultad para ayudarles a prepararse mejor para la repetición del examen.

Los candidatos que no estén de acuerdo con los resultados pueden solicitar una revaluación escribiendo a examination.team@pecb.com dentro de los 30 días posteriores a la recepción de los resultados. Las solicitudes de revaluación recibidas después de 30 días no serán procesadas. Si los candidatos no están de acuerdo con los resultados de la revaluación, tienen 30 días adicionales a partir de la fecha en que recibieron los resultados de la revaluación para presentar una queja a través del Sistema de Tickets PECB. Cualquier queja recibida después de 30 días no será procesada.

Política de Repetición del Examen

No existe un límite en el número de veces que un candidato puede volver a tomar un examen. Sin embargo, existen algunas limitaciones en cuanto al margen de tiempo permitido entre repeticiones de exámenes.

Si un candidato no aprueba el examen en el primer intento, debe esperar 15 días a partir de la fecha inicial del examen para realizar el siguiente intento (1a repetición).

Nota: Los candidatos que hayan tomado el curso de capacitación con uno de nuestros socios y reprueban en el primer intento de examen, pueden volver a realizar el examen de forma gratuita en un periodo de 12 meses a partir de la fecha de recepción del código de cupón (el costo del curso de capacitación incluye un primer intento de examen y una repetición). De lo contrario, la repetición del examen tiene un costo.

Para los candidatos que reprueben el examen en la repetición, PECB recomienda asistir a un curso de capacitación a fin de estar mejor preparados para el examen.

Para organizar las repeticiones del examen, dependiendo del formato del examen, los candidatos que hayan completado un curso de capacitación deben seguir los pasos que se indican a continuación:

1. Examen en línea: Al programar la repetición del examen, utilice el código de cupón inicial para exentar el costo

2. Examen en papel: Los candidatos deben ponerse en contacto con el Socio/Distribuidor de PECB que organizó inicialmente la sesión para acordar la repetición del examen (fecha, hora, lugar, costos).

Los candidatos que no han tomado un curso de capacitación con uno de nuestros socios, sino que han presentado el examen en línea directamente con PECB, no entran en esta Política. El proceso para programar la repetición del examen es el mismo que para el examen inicial.

PECB

SECCIÓN III: PROCESO Y REQUISITOS DE CERTIFICACIÓN

Credenciales CISO de PECB

Todas las certificaciones de PECB tienen requisitos específicos de formación y experiencia profesional. Para determinar qué credencial es la adecuada para usted, tenga en cuenta sus necesidades profesionales y analice los criterios para las certificaciones.

Las credenciales del esquema CISO de PECB tienen los siguientes requisitos:

Credencial	Examen	Experiencia profesional	Experiencia en proyectos de seguridad de la información	Otros requisitos
Information Security Officer de PECB	Examen de Chief Information Security Officer de PECB	Ninguna	Ninguna	Firmar el Código de Ética de PECB
Chief Information Security Officer de PECB		Cinco años: Dos años de experiencia laboral en seguridad de la información	Actividades de proyecto: un total de 300 horas	

Las prácticas eficaces de seguridad de la información para un CISO deberían adherirse a las mejores estrategias de implementación, abarcando los siguientes aspectos clave:

1. Desarrollo de negocios de seguridad y prácticas de comunicación
2. Identificación de objetivos y métricas de seguridad
3. Asegurar que la empresa cumpla con las normas de los organismos pertinentes
4. Hacer cumplir la aplicación de las mejores prácticas de seguridad de la información
5. Gestionar el equipo de respuesta a incidentes
6. Realización de descubrimientos electrónicos e investigaciones forenses digitales
7. Llevar a cabo capacitación de empleados sobre concienciación en la seguridad

Solicitar la certificación

Todos los candidatos que aprueben el examen (o un equivalente aceptado por PECB) están facultados para solicitar la credencial de PECB para la cual fueron evaluados. Se necesita cumplir con ciertos requisitos profesionales y académicos para poder obtener la certificación de PECB. Los candidatos deben llenar el formulario de solicitud de certificación en línea (accesible desde su cuenta en línea de PECB), incluyendo la información para contactar a las personas con el fin de validar la experiencia profesional de los candidatos. Los candidatos pueden presentar su solicitud en idioma inglés, francés, alemán, español o coreano. Ellos pueden elegir pagar en línea o ser facturados. Para más información, póngase en contacto con nosotros a la dirección certification.team@pecb.com.

El proceso de solicitud de certificación en línea es muy simple y toma solo unos minutos:

- Registre su cuenta
- Compruebe su correo electrónico para el enlace de confirmación
- Inicie Sesión para solicitar la certificación

Para obtener más información sobre cómo solicitar la certificación, haga clic aquí.

El Departamento de Certificación valida que el candidato cumple con todos los requisitos de certificación relativos a la respectiva credencial. El candidato recibirá un correo electrónico sobre el estado de la solicitud, incluida la decisión de certificación.

Tras la aprobación de la solicitud por parte del Departamento de Certificación, el candidato podrá descargar el certificado y obtener la insignia digital correspondiente. Para obtener más información sobre la descarga del certificado, haga clic aquí, y para obtener más información sobre cómo solicitar la insignia digital, haga clic aquí.

PECB ofrece soporte tanto en inglés como en francés.

Experiencia profesional

Los candidatos deberán proporcionar información completa y correcta con respecto a su experiencia profesional, incluidos los cargos, las fechas de comienzo y finalización, las descripciones de los puestos y más. Se recomienda a los candidatos sintetizar sus cargos anteriores y actuales, brindando información suficientemente detallada para describir la naturaleza de las responsabilidades que han desempeñado en cada cargo. Información adicional puede ser detallada en su hoja de vida.

Referencias profesionales

Para cada solicitud, se requieren dos referencias profesionales. Deben ser de personas que hayan trabajado con el candidato en un entorno profesional y puedan validar su experiencia en gestión de seguridad de la información, así como su historial laboral actual y anterior. Las referencias profesionales de personas subordinadas al candidato o son sus familiares no son válidas.

Experiencia en proyectos

El historial de proyectos de seguridad de la información del candidato se verificará para asegurar que el candidato cuenta con el número de horas de actividad del proyecto requeridas.

Evaluación de las solicitudes de certificación

El Departamento de Certificación evaluará cada solicitud para verificar la elegibilidad del candidato para la certificación o programa de certificado. Un candidato cuya solicitud está en revisión será notificado por escrito y, si es necesario, se le dará un plazo razonable para proporcionar cualquier documentación adicional. Si un candidato no responde dentro del plazo o no proporciona la documentación requerida dentro del plazo establecido, el Departamento de Certificación validará la solicitud basándose en la información inicial proporcionada, lo que puede resultar en la degradación de la credencial del candidato.

SECCIÓN IV: POLÍTICAS DE CERTIFICACIÓN

Denegación de certificación

PECB puede denegar la certificación o programa de certificado si los candidatos:

- Falsifican la solicitud
- Infringen los procedimientos de examen
- Infringen el Código de Ética de PECB

Los candidatos cuya certificación/programa de certificado haya sido denegado pueden presentar una queja a través del procedimiento de quejas y apelaciones. Para obtener información más detallada, consulte la sección de la **Política de Quejas y Apelaciones**.

El pago por la solicitud del certificado/programa de certificado no es reembolsable.

Opciones de estado de certificación

Activa

Significa que su certificación está en buen estado y es válida, y se mantiene cumpliendo con los requisitos de PECB con respecto a DPC y CMA.

Suspendida

PECB puede suspender temporalmente la certificación del candidato si no cumple los requisitos. Otras razones para suspender la certificación incluyen:

- PECB recibe quejas graves o excesivas por las partes interesadas (la suspensión se aplicará hasta que la investigación haya finalizado).
- Los logotipos de PECB o de los organismos de acreditación se utilizan de forma indebida deliberadamente.
- El candidato no corrige el uso indebido de una marca de certificación en el plazo determinado por PECB.
- La persona certificada ha solicitado voluntariamente una suspensión.
- PECB considera pertinentes otras condiciones para la suspensión de la certificación.

Revocada

PECB puede revocar (esto es, retirar) la certificación si el candidato no cumple los requisitos. En tales casos, ya no se permite a los candidatos presentarse a sí mismos como Profesionales Certificados por PECB.
Otras razones para revocar la certificación pueden ser si los candidatos:

- Infringen el Código de Ética de PECB
- Tergiversan y proporcionan información falsa del alcance de la certificación
- Rompen cualquier otra regla de PECB
- Cualquier otro motivo que PECB considere apropiado

Los candidatos cuya certificación haya sido revocada pueden presentar una queja a través del procedimiento de quejas y apelaciones. Para obtener información más detallada, consulte la sección de la **Política de Quejas y Apelaciones**.

Otros estados
Además de estar activa, suspendida o revocada, una certificación puede ser retirada voluntariamente o designada como emérita. Para obtener más información sobre estos estados y el estado de cese permanente, vaya a Opciones de Estado de Certificación.

Ascenso y degradación de credenciales

Actualización de credenciales
Los profesionales pueden ascender sus credenciales tan pronto como puedan demostrar que cumplen con los requisitos.

Para solicitar un ascenso, los candidatos deben iniciar sesión en su cuenta de PECB, ir a la pestaña de "Mis Certificaciones" y hacer clic en el enlace "Ascenso". La cuota de solicitud de actualización es de $100.

Degradación de credenciales
Un certificado de PECB puede ser degradado a una credencial inferior por alguna de las siguientes razones:
- No se pagó la CMA.
- No se presentó el número de horas de DPC.
- La cantidad de horas de DPC es insuficiente.
- La evidencia sobre las horas DPC no se ha enviado bajo petición.

Nota: *Los profesionales certificados que posean certificaciones de Líder y no presenten evidencia del cumplimiento de los requisitos para mantenimiento de la certificación se les degradarán las certificaciones. Los titulares de Certificaciones Máster que no envíen sus DPC ni paguen las CMA, les serán revocados sus certificados.*

Renovación de la certificación
Las certificaciones de PECB tienen una validez de tres años. Para mantenerlas, los profesionales certificados por PECB deben cumplir con los requisitos relacionados con la credencial designada, por ejemplo, deben cumplir con el número requerido de horas de desarrollo profesional continuo (DPC). Además, deben pagar la cuota anual de mantenimiento ($120). Para obtener más información, visite la página de Mantenimiento de la Certificación en el sitio web de PECB.

Cierre de un caso
Si los candidatos no solicitan la certificación dentro de un año, su caso será cerrado. Aunque el período de certificación expira, los candidatos tienen el derecho de reabrir su caso. Sin embargo, PECB ya no será responsable de los cambios en las condiciones, normas, políticas y manual del candidato que eran aplicables antes de que el caso fuera cerrado. Un candidato que solicite reabrir su caso debe hacerlo por escrito a certification.team@pecb.com y pagar la cuota requerida.

Política de Quejas y Apelaciones

Cualquier queja debe presentarse a más tardar 30 días después de recibir la decisión de certificación. PECB proporcionará una respuesta por escrito al candidato dentro de los 30 días hábiles posteriores a la recepción de la queja. Si el candidato no encuentra satisfactoria la respuesta, tiene derecho a presentar una apelación.

Para obtener más información sobre la Política de Quejas y Apelaciones, haga clic aquí.

SECCIÓN V: POLÍTICAS GENERALES

Exámenes y certificaciones de otros organismos de certificación acreditados

PECB acepta certificaciones y exámenes de otros organismos de certificación acreditados reconocidos. PECB evaluará las solicitudes a través de su proceso de equivalencia para decidir si las certificaciones o exámenes respectivos pueden ser aceptados como equivalentes a la certificación PECB correspondiente.

No discriminación y adaptaciones especiales

Todas las solicitudes de los candidatos serán evaluadas de manera objetiva, sin distinción de edad, género, raza, religión, nacionalidad o estado civil.

Con el fin de asegurar la igualdad de oportunidades para todas las personas calificadas, PECB hará adaptaciones[3] razonables para los candidatos cuando proceda. Si los candidatos necesitan adaptaciones especiales debido a una discapacidad o una condición física específica, deberían informar al socio/distribuidor para que ellos puedan hacer los arreglos pertinentes[4]. Cualquier información que los candidatos proporcionen sobre su discapacidad/necesidad especial se tratará con confidencialidad. Haga clic aquí para descargar el Formulario para Candidatos con Discapacidades.

Política de Comportamiento

PECB tiene como objetivo proporcionar servicios de alta calidad, consistentes y accesibles para el beneficio de sus partes interesadas externas: distribuidores, socios, instructores, supervisores de examen, evaluadores, miembros de diferentes comités y consejos asesores, así como clientes (candidatos, examinados, personas certificadas y titulares de certificados), como también crear y mantener un ambiente de trabajo positivo que garantice la seguridad y el bienestar de su personal, y que tenga en alta estima la dignidad, el respeto y los derechos humanos de su personal.

El propósito de esta Política es asegurar que PECB está gestionando el comportamiento inaceptable de las partes interesadas externas hacia el personal de PECB de una manera imparcial, confidencial, justa y oportuna. Para leer la Política de Comportamiento, haga clic aquí.

Política de Reembolso

PECB reembolsará su pago, si se cumplen los requisitos de la Política de Reembolso. Para leer la Política de Reembolso, haga clic aquí.

[3] De acuerdo con la ADA, el término "acomodo razonable" puede incluir: (A) hacer que las instalaciones existentes utilizadas por los empleados sean fácilmente accesibles y utilizables por las personas con discapacidades; y (B) reestructuración del trabajo, horarios de trabajo a tiempo parcial o modificados, reasignación a un puesto vacante, adquisición o modificación de equipos o dispositivos, ajuste o modificaciones apropiadas de exámenes, materiales o políticas de capacitación, provisión de lectores o intérpretes calificados, y otras adaptaciones similares para personas con discapacidades.

[4] Ley de Enmiendas de la ADA de 2008 (P.L. 110– 325) Secc. 12189. Exámenes y cursos. [Sección 309]: Cualquier persona que ofrezca exámenes o cursos relacionados con solicitudes, licencias, certificaciones o acreditaciones para fines de educación secundaria o postsecundaria, profesional o comercial, ofrecerá dichos exámenes o cursos en un lugar y manera accesible para personas con discapacidades u ofrecerá arreglos alternativos accesibles para dichas personas.

Dirección:

Sede central
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax:

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

Correos electrónicos:

Examen:
examination.team@pecb.com

Certificación:
certification.team@pecb.com

Servicio al Cliente:
support@pecb.com

Centro de Ayuda de PECB

Visite nuestro Centro de Ayuda para consultar las Preguntas más frecuentes (FAQ), ver manuales para usar el sitio web y las aplicaciones de PECB, leer documentos relacionados con los procesos de PECB o ponerse en contacto con nosotros a través del sistema de seguimiento en línea del Centro de Soporte.

www.pecb.com