PECB

BEYOND RECOGNITION

ISO/IEC 27001
LEAD AUDITOR

Manual del Candidato

PECB

Índice

SECCIÓN I: INTRODUCCIÓN 3
Acerca de PECB 3
El Valor de la Certificación/Programa de Certificado de PECB 4
Código de Ética de PECB 5
Introducción a la Certificación PECB ISO/IEC 27001 Lead Auditor 6
SECCIÓN II: PREPARACIÓN, REGLAS Y POLÍTICAS DE EXÁMENES 7
Prepararse para, y programar el examen 7
Ámbitos de competencia 8
Rendir el examen 18
Resultados del examen 23
Política de Repetición del Examen 23
Política de Seguridaddel Examen 24
SECCIÓN III: PROCESO Y REQUISITOS DE CERTIFICACIÓN 25
Credenciales PECB ISO/IEC 27001 Lead Auditor 25
Solicitud de certificación 26
Experiencia profesional 26
Referencias profesionales 26
Experiencia en auditoría de SGSI 26
Evaluación de las solicitudes de certificación 26
SECCIÓN IV: POLÍTICAS DE CERTIFICACIÓN 28
Denegación de la Certificación/Programa de Certificado 28
Suspensión de la Certificación 28
Revocación de la Certificación 29
Otros Estatus 29
Ascenso y degradación de credenciales 30
Renovación de la certificación 31
Cierre de un caso 31
Política de Quejas y Apelaciones 31
SECCIÓN V: POLÍTICAS GENERALES 32
Exámenes y certificaciones de otros organismos de certificación acreditados 32
No discriminación y adaptaciones especiales 32
Política de Comportamiento 32
Política de Reembolso 32

SECCIÓN I: INTRODUCCIÓN

Acerca de PECB[1]

PECB es un organismo de certificación líder dedicado a fomentar la confianza digital a través de programas integrales de educación y certificación en diversas disciplinas. Empoderamos a los profesionales para que desarrollen y demuestren su competencia en seguridad digital y otras áreas de especialización, mediante la provisión de programas de certificación de clase mundial que cumplen con normas reconocidas internacionalmente.

Lema:
Más allá del Reconocimiento

Visión:
Como líder mundial en educación y certificación de confianza digital, nuestra visión es empoderar e inspirar a los profesionales mejorando sus habilidades y fomentando su éxito profesional.

Misión:
Nuestra misión es empoderar a los profesionales con el conocimiento y las habilidades para proteger sus activos digitales y garantizar la continuidad del negocio. A través de nuestros programas de capacitación integrales, nuestro objetivo es fomentar un ecosistema digital seguro donde la innovación prospere y los riesgos se gestionen de manera eficaz.

Valores
Crecimiento, Cambio, Armonía, Simplicidad, Fiabilidad y Calidad

[1] **Notas:**

- El nombre legal de PECB es “PECB Group Inc.”
- PECB es un acrónimo que significa Professional Evaluation and Certification Board.
- Educación (utilizado en la primera oración de esta página) se refiere a los cursos de capacitación desarrollados por PECB y ofrecidos a nivel mundial a través de su red de socios.
- Certificación se refiere a los servicios de certificación proporcionados conforme a ISO/IEC 17024.
- Programa de Certificado se refiere a los servicios de programas de certificado proporcionados conforme a ANSI/ASTM E2659.
- El término “certificado” solo debe utilizarse para certificaciones de personal, basadas en los requisitos de la norma ISO/IEC 17024. El término “titular de certificado” solo debe utilizarse para programas de certificado, basados en los requisitos de la norma ANSI/ASTM E2659. Los titulares de certificados no están certificados, licenciados, acreditados ni registrados para ejercer una ocupación o profesión específica.

El Valor de la Certificación/Programa de Certificado de PECB

Acreditación

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.

Nuestras certificaciones son distinguidas por acreditaciones globales prestigiosas, que afirman tanto su valor como su experiencia. Las certificaciones de PECB están validadas por organismos de primer nivel, incluyendo el International Accreditation Service (IAS-PCB-111), el United Kingdom Accreditation Service (UKAS-No. 21923), el Korean Accreditation Board (KAB-PC-08), y el Comité français d'accréditation (COFRAC N.º 4-0637) bajo la norma ISO/IEC 17024 – Requisitos generales para los organismos que realizan certificación de personas. Además, nuestros programas de certificado están validados por la acreditación de ANSI National Accreditation Board (ANAB-Accreditation ID 1003) conforme a la norma ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB también es un miembro asociado reconocido de The Independent Association of Accredited Registrars (IAAR), y miembro pleno de International Personnel Certification Association (IPC), firmante del IPC MLA, y miembro de Club EBIOS, CPD Certification Service y CLUSIF. Asimismo, poseemos la condición aprobada de Approved Publishing Partner (APP) por parte del Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) para la norma Cybersecurity Maturity Model Certification (CMMC), y estamos autorizados por Club EBIOS para ofrecer la certificación de competencias EBIOS Risk Manager Skills y por la CNIL (Commission Nationale de l'Informatique et des Libertés) para ofrecer la certificación de conocimientos y competencias de DPO (Delegado de Protección de Datos). Para obtener más información 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 certificación son una demostración del cumplimiento de las normas ISO/IEC 17024 y ASTM E2659. Esto garantiza que los requisitos de la norma se han cumplido y validado con la coherencia, 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. Nuestro equipo de Atención al Cliente está disponible las 24 horas del día, los 7 días de la semana para atender preguntas, solicitudes y necesidades.

Código de Ética de PECB

El Código de Ética representa los valores y principios éticos que PECB se compromete a seguir, y define las responsabilidades de los profesionales de PECB, incluidos empleados, instructores, examinadores, supervisores, miembros de diferentes comités, socios, distribuidores, personas certificadas y titulares de certificados.

Para leer la versión completa del Código de Ética de PECB, visite Code of Ethics | PECB.

Introducción a la Certificación PECB ISO/IEC 27001 Lead Auditor

Este documento especifica el esquema de certificación PECB ISO/IEC 27001 Lead Auditor conforme a la norma ISO/IEC 17024:2012. También describe los pasos que los candidatos deberían seguir para obtener y mantener sus credenciales. Como tal, es muy importante que usted lea toda la información incluida en este manual del candidato antes de completar y enviar su solicitud. Si tiene preguntas o necesita más información después de leerlo, por favor contacte a certification.team@pecb.com.

SECCIÓN II: PREPARACIÓN, REGLAS Y POLÍTICAS DE EXÁMENES

Prepararse para, y programar el examen

Los candidatos son responsables de su propio estudio y preparación para los exámenes de certificación. No se requiere ningún conjunto específico de cursos de capacitación ni plan de estudios como parte del proceso de certificación.

Para programar el examen, los candidatos tienen dos opciones:

1. **En línea:** A través dePECB Exams application. Para programar un examen remoto, por favor visite el siguiente enlace: Exam Events.
2. **En papel:** Comunicándose con el socio autorizado de PECB que proporcionó el curso de capacitación. El socio organiza la fecha, la hora y el lugar donde el candidato presentará el 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 relacionado con la fecha, hora, lugar u otros detalles del examen, por favor contacte a online.exams@pecb.com.

Tarifas para la 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 tarifa de solicitud para la certificación es la siguiente:

- Certificación Máster: $100
- Certificación Fundamentos: $200
- Certificación Transición: $200
- Todas las demás certificaciones: $500

Para los candidatos que hayan tomado el curso de capacitación y hayan realizado el examen con uno de los socios de PECB, la tarifa de solicitud incluye los costos asociados al 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.

Ámbitos de competencia

La certificación ISO/IEC 27001 Lead Auditor está destinada a:

- Auditores que deseen realizar y liderar auditorías del sistema de gestión de seguridad de la información (SGSI)
- Gerentes o consultores que deseen dominar el proceso de auditoría del sistema de gestión de seguridad de la información
- Personas responsables de mantener la conformidad con los requisitos del SGSI en una organización
- Expertos técnicos que deseen prepararse para una auditoría del sistema de gestión de seguridad de la información
- Asesores expertos en la gestión de la seguridad de la información

El contenido del examen se divide de la siguiente manera:

- **Dominio 1:** Principios y conceptos fundamentales de un sistema de gestión de seguridad de la información (SGSI)
- **Dominio 2:** Sistema de gestión de seguridad de la información (SGSI)
- **Dominio 3:** Conceptos y principios fundamentales de auditoría
- **Dominio 4:** Preparación para una auditoría ISO/IEC 27001
- **Dominio 5:** Realización de una auditoría ISO/IEC 27001
- **Dominio 6:** Cierre de una auditoría ISO/IEC 27001
- **Dominio 7:** Gestión de un programa de auditoría ISO/IEC 27001

Dominio 1: Principios y conceptos fundamentales de un sistema de gestión de seguridad de la información (SGSI)

Objetivo principal: Asegurar que el candidato sea capaz de explicar y aplicar los principios y conceptos de la norma ISO/IEC 27001.

Competencias	Declaración de conocimientos
1. Capacidad para comprender y explicar los conceptos principales del sistema de gestión de seguridad de la información 2. Capacidad para comprender y explicar las operaciones de la organización y el desarrollo de normas de seguridad de la información 3. Capacidad para identificar, analizar y evaluar los requisitos de conformidad en materia de seguridad de la información para una organización 4. Capacidad para explicar e ilustrar los conceptos principales en seguridad de la información y gestión de riesgos de seguridad de la información 5. Capacidad para distinguir y explicar la diferencia entre activo de información, dato y registro 6. Capacidad para comprender, interpretar e ilustrar la relación entre los aspectos de la seguridad de la información, tales como controles, vulnerabilidades, amenazas, riesgos y activos 7. Capacidad para identificar e ilustrar big data, inteligencia artificial, aprendizaje automático, computación en la nube y operaciones externalizadas	1. Conocimiento de las leyes, regulaciones, normas internacionales e industriales, contratos, prácticas del mercado, políticas internas, etc., con las que una organización debe cumplir 2. Conocimiento de las principales normas relacionadas con la seguridad de la información 3. Conocimiento de los conceptos y la terminología principales de la norma ISO/IEC 27001 4. Conocimiento del concepto de riesgo y su aplicación en la seguridad de la información 5. Conocimiento de la relación entre los aspectos de la seguridad de la información 6. Conocimiento de la diferencia y características de los objetivos de seguridad y los controles 7. Conocimiento del uso de los atributos de control y de la diferencia entre controles preventivos, de detección y correctivos 8. Conocimiento de las características principales de big data, inteligencia artificial, aprendizaje automático, computación en la nube y operaciones externalizadas

Dominio 2: Sistema de gestión de seguridad de la información (SGSI) y requisitos de la norma ISO/IEC 27001

Objetivo principal: Asegurar que el candidato sea capaz de identificar y explicar los requisitos de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001**.**

Competencias	Declaración de conocimientos
1. Capacidad para comprender la estructura de la norma ISO/IEC 27001:2022	1. Conocimiento de la norma ISO/IEC 27001:2022 y sus normas complementarias
2. Capacidad para comprender los componentes de un sistema de gestión de seguridad de la información basado en ISO/IEC 27001 y sus procesos principales	2. Conocimiento de los conceptos, principios y terminología relacionados con los sistemas de gestión
3. Capacidad para comprender, interpretar y analizar los requisitos de la norma ISO/IEC 27001	3. Conocimiento de las características principales de un sistema de gestión integrado
4. Capacidad para comprender, explicar e ilustrar los pasos principales para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización	4. Conocimiento de los requisitos de la norma ISO/IEC 27001 presentados en las cláusulas 4 a 10
5. Capacidad para establecer los factores externos e internos relacionados con el SGSI y determinar las partes interesadas y sus necesidades	5. Conocimiento de los 93 controles enumerados en el Anexo A de la norma ISO/IEC 27001
6. Capacidad para determinar el alcance del SGSI	6. Conocimiento de los factores internos y externos del SGSI y de las partes interesadas
7. Capacidad para asegurar el compromiso de la dirección, establecer una política de seguridad de la información y asignar los roles y responsabilidades del SGSI	7. Conocimiento de los pasos principales para establecer el alcance del SGSI y la política de seguridad de la información
8. Capacidad para planificar los cambios y las acciones para abordar los riesgos	8. Conocimiento del liderazgo y compromiso de la alta dirección y de los roles y responsabilidades organizacionales relacionados con el SGSI
9. Capacidad para comprender los procesos de evaluación de riesgos y tratamiento de riesgos	9. Conocimiento de los objetivos de seguridad, procesos y procedimientos relevantes para la gestión de riesgos y la mejora de la seguridad de la información para obtener resultados conforme a las políticas y objetivos generales de una organización
10. Capacidad para comprender la selección de controles apropiados basándose en el Anexo A de la norma ISO/IEC 27001 y otras fuentes	10. Conocimiento de los enfoques y metodologías de evaluación y tratamiento de riesgos
11. Capacidad para asegurar que los empleados estén conscientes y sean competentes para desempeñar sus tareas relacionadas con el SGSI	11. Conocimiento de la selección de controles del Anexo A y controles adicionales basados en otras fuentes, así como su inclusión en la Declaración de Aplicabilidad
12. Capacidad para monitorear y evaluar el desempeño del SGSI y realizar auditorías internas y revisiones por la dirección	12. Conocimiento del proceso de evaluación del desempeño, incluyendo el seguimiento, la medición, el análisis y la evaluación, la auditoría interna y la revisión por la dirección
	13. Conocimiento del concepto de mejora continua y su aplicación a un SGSI

13. Capacidad para asegurar la mejora continua e implementar acciones apropiadas para tratar las no conformidades	

Dominio 3: Conceptos y principios fundamentales de auditoría

Objetivo principal: Asegurar que el candidato sea capaz de interpretar y aplicar los conceptos y principios principales relacionados con una auditoría de un SGSI.

Competencias	Declaración de conocimientos
1. Capacidad para comprender, explicar e ilustrar la aplicación de los principios de auditoría en una auditoría de un SGSI	1. Conocimiento de los principales conceptos y la terminología de auditoría según lo descrito en la norma ISO 19011
2. Capacidad para diferenciar auditorías de primera, segunda y tercera parte	2. Conocimiento de las diferencias entre auditorías de primera, segunda y tercera parte
3. Capacidad para identificar y juzgar situaciones que desacreditarían la profesionalidad del auditor y violen el código de ética de PECB	3. Conocimiento de los principios de auditoría, tales como integridad, presentación imparcial, diligencia profesional, confidencialidad, independencia, enfoque basado en evidencia y enfoque basado en riesgos
4. Capacidad para identificar y juzgar cuestiones éticas considerando las obligaciones relacionadas con el cliente de la auditoría, el auditado, las autoridades legales y los organismos reguladores	4. Conocimiento de la responsabilidad profesional del auditor y del Código de Ética de PECB
5. Capacidad para comprender las acciones que el auditor debería realizar con respecto a las implicaciones legales relacionadas con cualquier irregularidad cometida por el auditado	5. Conocimiento del enfoque basado en evidencia en una auditoría
6. Capacidad para explicar, ilustrar y aplicar el enfoque basado en evidencia de auditoría en el contexto de una auditoría de un SGSI	6. Conocimiento de los diferentes tipos de evidencia de auditoría, tales como física, matemática, confirmativa, técnica, analítica, documental y verbal
7. Capacidad para explicar y comparar los tipos de evidencia y sus características	7. Conocimiento de las leyes y regulaciones aplicables al auditado y al país en el que opera
8. Capacidad para determinar y justificar el tipo y la cantidad de evidencia requerida en una auditoría de un SGSI	8. Conocimiento del uso de big data en auditorías
9. Capacidad para comprender el impacto de las tendencias y la tecnología en la auditoría	9. Conocimiento de la auditoría de operaciones externalizadas

Dominio 4: Preparación para una auditoría ISO/IEC 27001

Objetivo principal: Asegurar que el candidato sea capaz de preparar una auditoría de un sistema de gestión de seguridad de la información.

Competencias	Declaración de conocimientos
1. Capacidad para comprender e ilustrar los pasos y actividades para preparar una auditoría de un SGSI considerando el contexto específico de la auditoría 2. Capacidad para determinar y evaluar el nivel de materialidad y aplicar el enfoque basado en riesgos durante las diferentes etapas de una auditoría de un SGSI 3. Capacidad para juzgar el nivel apropiado de seguridad razonable necesario para una auditoría de un SGSI 4. Capacidad para comprender y explicar los roles y responsabilidades del líder del equipo auditor, los miembros del equipo auditor y los expertos técnicos 5. Capacidad para determinar la viabilidad de la auditoría 6. Capacidad para determinar, evaluar y confirmar los objetivos de la auditoría, los criterios de auditoría y el alcance de la auditoría para una auditoría de un SGSI 7. Capacidad para explicar, ilustrar y definir las características de los términos del compromiso de auditoría y aplicar las mejores prácticas para establecer el contacto inicial con el auditado	1. Conocimiento del procedimiento de preparación del plan de auditoría 2. Conocimiento del enfoque basado en riesgos en una auditoría y de los diferentes tipos de riesgos relacionados con las actividades de auditoría, tales como riesgo inherente, riesgo de control y riesgo de detección 3. Conocimiento del concepto de materialidad y su aplicación en una auditoría 4. Conocimiento del concepto de seguridad razonable y su aplicación en una auditoría 5. Conocimiento de las principales responsabilidades del líder del equipo auditor, los miembros del equipo auditor y los expertos técnicos 6. Conocimiento de los objetivos de la auditoría, el alcance de la auditoría y los criterios de auditoría 7. Conocimiento de la diferencia entre el alcance del SGSI y el alcance de la auditoría 8. Conocimiento de los factores que deben tenerse en cuenta durante la evaluación de la viabilidad de la auditoría 9. Conocimiento de los aspectos culturales que deben considerarse en una auditoría 10. Conocimiento de las características de los términos del compromiso de auditoría y de las mejores prácticas para establecer el contacto inicial con el auditado

Dominio 5: Realización de una auditoría ISO/IEC 27001

Objetivo principal: Asegurar que el candidato sea capaz de llevar a cabo una auditoría de un SGSI.

Competencias	Declaración de conocimientos
1. Capacidad para llevar a cabo la etapa 1 de la auditoría , teniendo en cuenta los criterios de evaluación de la información documentada	1. Conocimiento de los objetivos y el contenido de la reunión de apertura en una auditoría
2. Capacidad para organizar y conducir una reunión de apertura	2. Conocimiento de la diferencia entre la etapa 1 de la auditoríay la etapa 2 de la auditoría
3. Capacidad para llevar a cabo la etapa 2 de la auditoría siguiendo adecuadamente los procedimientos que esta etapa implica	3. Conocimiento de los requisitos, pasos y actividades de la etapa 1 de la auditoría
4. Capacidad para aplicar las mejores prácticas de comunicación para recopilar la evidencia de auditoría apropiada	4. Conocimiento de los criterios de evaluación de la información documentada y de los requisitos de la norma ISO/IEC 27001
5. Capacidad para considerar los roles y responsabilidades de todas las partes interesadas involucradas	5. Conocimiento de los requisitos, pasos y actividades de la etapa 2 de la auditoría
6. Capacidad para explicar, ilustrar y aplicar los procedimientos y herramientas de recopilación de evidencia	6. Conocimiento de las mejores prácticas de comunicación durante una auditoría
7. Capacidad para explicar, ilustrar y aplicar los principales métodos de muestreo en una auditoría	7. Conocimiento de los roles y responsabilidades de los guías y observadores durante una auditoría
8. Capacidad para recopilar evidencia apropiada a partir de la información disponible durante una auditoría y evaluarla objetivamente	8. Conocimiento de las diferentes técnicas de resolución de conflictos
9. Capacidad para elaborar papeles de trabajo de auditoría y desarrollar planes de prueba de auditoría adecuados en una auditoría de un SGSI	9. Conocimiento de los procedimientos y herramientas de recopilación de evidencia, tales como entrevistas, revisión de información documentada, observación, análisis, muestreo y verificación técnica
10. Capacidad para explicar y aplicar el proceso de evaluación de la evidencia para redactar los hallazgos de auditoría	10. Conocimiento de las técnicas de análisis de evidencia mediante corroboración y evaluación
11. Capacidad para comprender, explicar e ilustrar el concepto del beneficio de la duda	11. Conocimiento de los principales conceptos, principios y procedimientos de recopilación de evidencia utilizados en una auditoría
12. Capacidad para reportar observaciones de auditoría apropiadas conforme a las reglas y principios de auditoría	12. Conocimiento de las ventajas y desventajas del uso de listas de verificación de auditoría
13. Capacidad para realizar revisiones de la calidad a la documentación de auditoría	13. Conocimiento de los principales métodos de muestreo en auditoría y sus características
14. Capacidad para completar los documentos de trabajo de auditoría	14. Conocimiento del procedimiento de preparación del plan de auditoría
	15. Conocimiento de la preparación y elaboración de los documentos de trabajo de auditoría
	16. Conocimiento de las mejores prácticas para la creación de planes de prueba de auditoría
	17. Conocimiento del proceso de evaluación de la evidencia para redactar los hallazgos de auditoría

Dominio 6: Cierre de una auditoría ISO/IEC 27001

Objetivo principal: Asegurar que el candidato sea capaz de concluir una auditoría de un SGSI y llevar a cabo actividades de seguimiento de auditoría.

Competencias	Declaración de conocimientos
1. Capacidad para explicar y aplicar el proceso de evaluación de evidencia para preparar las conclusiones de auditoría	1. Conocimiento del proceso de evaluación de evidencia para preparar las conclusiones de auditoría
2. Capacidad para justificar la recomendación para la certificación	2. Conocimiento de la presentación de conclusiones de auditoría
3. Capacidad para redactar y presentar las conclusiones de auditoría	3. Conocimiento de las directrices y mejores prácticas para presentar las conclusiones de auditoría a la dirección de una organización auditada
4. Capacidad para organizar y llevar a cabo una reunión de cierre	4. Conocimiento de las posibles recomendaciones que un auditor puede emitir durante la auditoría de certificación
5. Capacidad para redactar y distribuir un informe de auditoría ISO/IEC 27001	5. Conocimiento de la agenda de la reunión de cierre
6. Capacidad para evaluar planes de acción	6. Conocimiento de las directrices y mejores prácticas para evaluar planes de acción

Dominio 7: Gestión de un programa de auditoría ISO/IEC 27001

Objetivo principal: Asegurar que el candidato sea capaz de establecer y gestionar un programa de auditoría de un SGSI.

Competencias	Declaración de conocimientos
1. Capacidad para llevar a cabo las actividades posteriores a una auditoría inicial, incluyendo seguimientos de auditoría y actividades de vigilancia	1. Conocimiento de los seguimientos de auditoría, auditorías de vigilancia y requisitos, pasos y actividades de auditoría de recertificación
2. Capacidad para comprender y explicar el establecimiento de un programa de auditoría y la aplicación del ciclo PHVA (Planificar-Hacer-Verificar-Actuar) en un programa de auditoría	2. Conocimiento de las condiciones para la modificación, ampliación, suspensión o retiro de la certificación de una organización
3. Capacidad para comprender y explicar la importancia de proteger la integridad, disponibilidad y confidencialidad de los registros de auditoría, así como las responsabilidades de los auditores al respecto	3. Conocimiento de la aplicación del ciclo PHVA en la gestión de un programa de auditoría
4. Capacidad para comprender y explicar las responsabilidades para la protección de la integridad, disponibilidad y confidencialidad de los registros de auditoría	4. Conocimiento de los requisitos, directrices y mejores prácticas relacionadas con los recursos, procedimientos y políticas de auditoría
5. 5. Capacidad para comprender los requisitos relacionados con los componentes del sistema de gestión de un programa de auditoría, como la gestión de la calidad, la gestión de los registros y la gestión de quejas	5. Conocimiento de los tipos de herramientas utilizadas por auditores profesionales
6. 6. Capacidad para comprender y explicar la forma en que se gestionan las auditorías combinadas dentro de un programa de auditoría	6. Conocimiento de los requisitos, directrices y mejores prácticas relacionadas con la gestión de los registros de auditoría
7. Capacidad para comprender el proceso de gestión de la información documentada	7. Conocimiento de la aplicación del concepto de mejora continua en la gestión de un programa de auditoría
8. Capacidad para comprender el proceso de evaluación de la eficacia del programa de auditoría mediante el monitoreo del desempeño de cada auditor y miembro del equipo auditor	8. Conocimiento de las particularidades para implementar y gestionar un programa de auditoría de primera, segunda o tercera parte Conocimiento del concepto de competencia y su aplicación a los auditores
9. Capacidad para demostrar la aplicación de los atributos personales y comportamientos asociados con auditores profesionales	9. Conocimiento de la gestión de auditorías combinadas
	10. Conocimiento de los atributos personales y comportamientos de un auditor profesional

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

				Nivel de comprensión (Cognitivo/Taxonomía) requerido	
		Número de preguntas/puntos por dominio de competencia	% del examen dedicado/puntos a/para cada dominio de competencia	Preguntas que miden la comprensión, la aplicación y el análisis	Preguntas que miden la evaluación
Ámbitos de competencia	Principios y conceptos fundamentales de un sistema de gestión de seguridad de la información (SGSI)	13	16.25	X	
	Sistema de gestión de seguridad de la información (SGSI) y requisitos de la norma ISO/IEC 27001	8	10	X	
	Conceptos y principios fundamentales de auditoría	14	17.5		X
	Preparación de una auditoría ISO/IEC 27001	12	15	X	
	Realización de una auditoría ISO/IEC 27001	18	22.5		X
	Cierre de una auditoría ISO/IEC 27001	7	8.75	X	
	Gestión de un programa de auditoría ISO/IEC 27001	8	10		X
	Total	**80**	**100%**		
	Número de preguntas por nivel de comprensión			**40**	**40**
	% del examen dedicado a cada nivel de comprensión (cognitivo/taxonomía)			**50%**	**50%**

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

Rendir el examen

Información general sobre el examen
Los candidatos deben llegar/presentarse por lo menos 30 minutos antes del comienzo del examen.

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 rinden el examen en un idioma distinto al materno, tal como se indica a continuación:

- 10 minutos adicionales para los exámenes de Fundamentos
- 20 minutos adicionales para los exámenes de Gerente
- 30 minutos adicionales para los exámenes de Líder

Formato y tipo de examen de PECB

1) Examen en línea: Los exámenes se realizan electrónicamente a través de la aplicación de Exámenes PECB. No se permite el uso de dispositivos electrónicos secundarios, tales como tabletas y teléfonos, durante el examen. 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.

Tipos de Exámenes de PECB:

a. De opción múltiple, a libro cerrado, en los que no se permite a los candidatos utilizar ningún material de referencia. Generalmente, los exámenes de Fundamentos y Transición son de este tipo.

b. Tipo ensayo, a libro abierto, en los que se permite a los candidatos utilizar los siguientes materiales de referencia:

    - Una copia impresa de la norma principal
    - Materiales del curso de capacitación (a través de KATE y/o impresos)
    - Cualquier nota personal tomada durante el curso de capacitación (a través de KATE y/o impresas)
    - Un diccionario en formato impreso

c. De opción múltiple, a libro abierto, en los que se permite a los candidatos utilizar los siguientes materiales de referencia:

    - Una copia impresa de la norma principal
    - Materiales del curso de capacitación (a través de KATE y/o impresos)
    - Cualquier nota personal tomada durante el curso de capacitación (a través de KATE y/o impresas)
    - Un diccionario en formato impreso

2) Basado en papel: Los exámenes también están disponibles en formato papel. 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.

Tipos de exámenes de PECB:

a. De opción múltiple, a libro cerrado, en los que no se permite a los candidatos utilizar ningún material de referencia. Generalmente, los exámenes de Fundamentos y Transición son de este tipo.

b. Tipo ensayo, a libro abierto, en los que se permite a los candidatos utilizar los siguientes materiales de referencia:

- Una copia impresa de la norma principal
- Materiales del curso de capacitación (impresos)
- Cualquier nota personal tomada durante el curso de capacitación (impresas)
- Un diccionario en formato impreso

c. De opción múltiple, a libro abierto, en los que se permite a los candidatos utilizar los siguientes materiales de referencia:

- Una copia impresa de la norma principal
- Materiales del curso de capacitación (impresos)
- Cualquier nota personal tomada durante el curso de capacitación (impresas)
- Un diccionario en formato impreso

Para información específica sobre los tipos de examen, idiomas disponibles y otros detalles, por favor contacte support@pecb.com o visite la Lista de Exámenes de PECB.

Este examen contiene preguntas de opción múltiple: El examen de opción múltiple se puede utilizar para evaluar la comprensión de un candidato en conceptos tanto simples como 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 una o más preguntas relacionadas con ese escenario. Al responder preguntas independientes y basadas en escenarios, los candidatos deberán aplicar diversos 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. Los candidatos están autorizados a hacer uso únicamente de los siguientes materiales de referencia:

- Una copia impresa de la norma ISO/IEC 27001
- Materiales del curso de capacitación (a los que se accede a través de la aplicación Exámenes PECB y/o impresos)

- Cualquier nota personal tomada durante el curso de capacitación (a la que se accede a través de la aplicación Exámenes PECB y/o impresa)
- Un diccionario impreso

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

Muestra de preguntas de examen

La *Empresa A* es una compañía de seguros con sede central en Chicago. Ofrece una variedad de servicios y productos relacionados con seguros médicos y de automóviles. Recientemente, la empresa se ha convertido en una de las compañías de seguros más exitosas y grandes, con más de 70 oficinas en todo el país.

Los objetivos de la empresa son mantener adecuadamente sus activos y proteger la confidencialidad de la información de sus clientes. La empresa decidió certificarse conforme a la norma ISO/IEC 27001, ya que esto le ayudaría no solo a alcanzar sus objetivos organizacionales y cumplir con leyes y regulaciones internacionales, sino también a aumentar su reputación. La empresa inició la implementación del SGSI definiendo una estrategia de implementación basada en un análisis detallado de sus procesos existentes y de los requisitos del SGSI. Prestó especial atención a la evaluación de riesgos de seguridad de la información, lo cual fue crucial para comprender las amenazas y vulnerabilidades a las que se enfrenta También definió los criterios de riesgo con el objetivo de evaluar los riesgos identificados.

La *Empresa A* experimentó un crecimiento rápido que resultó en un procesamiento de datos complejo e intensivo, y con base en los resultados de la evaluación de riesgos decidieron actualizar inicialmente su esquema de clasificación de la información existente y luego implementar los controles de seguridad necesarios según el nivel de protección requerido por cada clasificación de la información.

Las reclamaciones médicas de sus clientes, clasificadas como información sensible, fueron cifradas utilizando el cifrado AES y luego trasladadas a la nube privada. La *Empresa A* utilizó almacenamiento en la nube por su facilidad de acceso. Debido al acceso frecuente de sus empleados a este servicio, la empresa también decidió utilizar el proceso de registro de eventos . El servicio fue configurado para conceder automáticamente el acceso al almacenamiento en la nube a todos los empleados responsables de gestionar las reclamaciones médicas.

Dado que los servicios de almacenamiento en la nube experimentaron brechas de seguridad, ya sea por errores humanos o ataques deliberados, el departamento de TI de la empresa decidió restringir el acceso a la información sensible almacenada en la nube si no se utilizaban correos electrónicos profesionales de la empresa. Además, utilizaron un software de gestión de contraseñas para administrar las contraseñas de estas direcciones de correo electrónico y generar contraseñas más robustas

De acuerdo con este escenario, responda las siguientes preguntas:

1. **El Departamento de TI no restringió el acceso al almacenamiento en la nube. ¿Cuál de las amenazas a continuación puede explotar dicha vulnerabilidad?**
   A. Manipulación del hardware
   B. **Uso no autorizado de información sensible**
   C. Capacitación insuficiente sobre almacenamiento en la nube

2. **La *Empresa A* cifra la información sensible antes de trasladarla a la nube. ¿Qué principio de seguridad de la información se sigue en este caso?**
   A. **Confidencialidad, porque el cifrado garantiza que solo los usuarios autorizados puedan acceder a la información cifrada**
   B. Disponibilidad, porque el cifrado garantiza que la información esté protegida tanto en reposo como en tránsito, y por lo tanto accesible cuando se necesite
   C. Integridad, porque el cifrado garantiza que solo se realicen modificaciones autorizadas a la información cifrada

3. **La *Empresa A* decidió restringir el acceso a la información sensible almacenada en la nube si no se utilizaban correos electrónicos profesionales de la empresa. ¿Qué control de seguridad se implementó en este caso?**
   A. Control de detección
   B. **Control preventivo**
   C. Control correctivo

4. **La *Empresa A* definió los criterios de riesgo al evaluar sus riesgos ¿Es esto necesario?**
   A. **Sí, porque la empresa debe establecer y mantener los criterios de riesgo al evaluar los riesgos de seguridad de la información.**
   B. No, porque los criterios de riesgo deben establecerse únicamente cuando se definen las opciones de tratamiento de riesgos
   C. No, porque los criterios de riesgo se establecen cuando se aceptan los riesgos residuales de seguridad de la información

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 agregará al correo electrónico una lista de los dominios en los que han fallado, para ayudarlos a prepararse mejor para una repetición.

Si los candidatos no están de acuerdo con los resultados, disponen de 30 días a partir de la fecha de recepción de los resultados para presentar una queja a través del Sistema de Tickets de PECB. Las quejas recibidas después de los 30 días no serán procesadas.

Política de Repetición del Examen

No existe un límite en el número de veces que un candidato puede volver a rendir 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 (1ra repetición).

Nota: Los candidatos que hayan tomado el curso de capacitación con uno de nuestros socios y desaprueban en el primer intento de examen, pueden volver a realizar el examen de forma gratuita dentro de 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 fallen el examen en la repetición, PECB recomienda asistir al 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 eximir la tarifa.
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.

Política de Seguridaddel Examen

Un componente significativo de una credencial de certificación profesional es mantener la seguridad y la confidencialidad del examen. PECB confía en el comportamiento ético de los titulares de certificaciones y solicitantes para mantener la seguridad y confidencialidad de los exámenes de PECB. Cualquier divulgación de información sobre el contenido de los exámenes de PECB constituye una violación directa del Código de Ética de PECB. PECB tomará medidas contra cualquier persona que infrinja dichas reglas y políticas, incluyendo la prohibición permanente de obtener credenciales de PECB y la revocación de cualquier credencial previa. 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.

SECCIÓN III: PROCESO Y REQUISITOS DE CERTIFICACIÓN

Credenciales PECB ISO/IEC 27001 Lead Auditor

Todas las certificaciones de PECB tienen requisitos específicos con respecto a la 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 PECB ISO/IEC 27001 Lead Auditor tienen los siguientes requisitos:

Credencial	Examen	Experiencia profesional	Experiencia en auditoría/evaluación de sistemas de gestión (SG)	Otros requisitos
Auditor Provisional Certificado por PECB en ISO/IEC 27001	Examen PECB Certified ISO/IEC 27001 Lead Auditor o equivalente	Ninguna	Ninguna	Firma del Código de Ética de PECB
Auditor Certificado por PECBenISO/IEC 27001		Dos años: Un año de experiencia laboral en la gestión de la seguridad de la información	Actividades de auditoría: un total de 200 horas	
Auditor Líder Certificado por PECBenISO/IEC 27001		Cinco años: Dos años de experiencia laboral en la gestión de la seguridad de la información	Actividades de auditoría: un total de 300 horas	
Auditor Líder Senior Certificado por PECBen ISO/IEC 27001		Diez años: Siete años de experiencia laboral en la gestión de la seguridad de la información	Actividades de auditoría: un total de 1.000 horas	

Para ser consideradas válidas, las actividades de auditoría deberían seguir las mejores prácticas de auditoría e incluir lo siguiente:

1. Planificación de una auditoría
2. Gestión de un programa de auditoría
3. Redacción de informes de auditoría
4. Redacción de informes de no conformidad
5. Redacción de documentos de trabajo de auditoría
6. Revisión y gestión de la información documentada relacionada con la auditoría
7. Realización de auditorías in situ
8. Seguimiento de las no conformidades
9. Encabezar un equipo auditor

Solicitud de 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 deben cumplir requisitos específicos de experiencia profesional para obtener una 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 de contacto de las personas a quienes se contactará con el fin de validar la experiencia profesional de los candidatos. Ellos pueden elegir pagar en línea o ser facturados. Para información adicional, por favor contacte acertification.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 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 credencial respectiva. 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 reclamar la Insignia Digital correspondiente. Para más información sobre cómo descargar el certificado, haga clic aquí, y para más información sobre cómo reclamar la Insignia Digital, haga clic aquí.

Experiencia profesional

Los candidatos deben proporcionar información completa y correcta con respecto a su experiencia profesional, incluidos cargo(s), fecha(s) de comienzo y finalización, descripción(es) de puesto(s) 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 más detallada puede incluirse en el CV.

Referencias profesionales

Para cada solicitud, se requieren dos referencias profesionales. Las referencias profesionales deben ser personas que hayan trabajado con usted en un entorno profesional y puedan validar su experiencia en el campo correspondiente, así como su historial laboral actual y anterior. No puede utilizar como referencia a personas que estén bajo su supervisión o que sean parientes suyos.

Experiencia en auditoría de SGSI

El registro de auditorías del candidato será verificado para asegurar que haya completado el número requerido de horas de auditoría. Los siguientes tipos de auditoría constituyen experiencia válida en auditoría: pre-auditorías, auditorías internas, auditorías de segunda parte o auditorías de tercera parte.

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 certificación. 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 la Certificación/Programa de Certificado

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
- Reprueban el examen

Cualquier inquietud relacionada con la denegación de la certificación/programa de certificado puede ser presentada mediante una queja o apelación siguiendo el proceso correspondiente de quejas y apelaciones. (https://pecb.com/es/complaint-and-appeal-policy).

El pago por la solicitud del certificado/programa de certificado no es reembolsable. Esto se debe al proceso de verificación de la solicitud, a la evidencia presentada por los candidatos y a la participación de los departamentos correspondientes en este proceso.

Suspensión de la Certificación

PECB puede suspender temporalmente la certificación si el candidato no cumple con los requisitos de PECB. Motivos adicionales de suspensión pueden ser:

- PECB recibe quejas excesivas o graves por parte de las partes interesadas (la suspensión se aplicará hasta que se haya completado la investigación).
- 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 pedido voluntariamente una suspensión.
- PECB considera apropiadas otras condiciones para la suspensión de la certificación/programa de certificado.

Las personas cuya certificación ha sido suspendida no están autorizadas a seguir promocionando su certificación mientras esta se encuentre suspendida.

Una certificación suspendida puede:

- Ser restablecida ─ si las razones de la suspensión se corrigen dentro del plazo establecido por PECB
- Ser revocada ─ si las razones de la suspensión no se corrigen dentro del plazo establecido por PECB

Los miembros suspendidos deben remediar su suspensión en un período máximo de 6 meses.

NOTA 1: *Para ISO/IEC 27005:2022 Risk Manager/Lead Risk Manager, el no presentar el DPC ni efectuar el pago de la CMA durante el ciclo resultará en un período de suspensión de 12 meses, durante el cual podrá abordar cualquier CMA y DPC pendiente. Si no se toma ninguna medida durante el período de suspensión, la certificación será revocada.*

NOTA 2: *Para CNIL– DPO, el incumplimiento de los requisitos de recertificación (experiencia laboral en protección de datos y aprobación del examen de recertificación CNIL– DPO) resultará en un período de suspensión de 12 meses. Si no se toma ninguna medida durante el período de suspensión, la certificación será revocada.*

Revocación de la Certificación

PECB puede revocar (es decir, retirar) la certificación si el candidato no cumple con los requisitos de PECB. Los candidatos ya no podrán representarse como profesionales certificados por PECB. Razones adicionales pueden ser si los candidatos:

- Violan el Código de Ética de PECB
- Falsifican o proporcionan información incorrecta sobre el alcance de la certificación/programa de certificado
- Rompen cualquier otra regla de PECB
- Cualquier otro motivo que PECB considere apropiado

Las personas cuya certificación ha sido revocada no están autorizadas a utilizar ninguna referencia a un estatus de certificado.

Las personas cuya certificación ha sido revocada pueden presentar una queja o apelación siguiendo el proceso correspondiente de quejas y apelaciones.(https://pecb.com/es/complaint-and-appeal-policy).

NOTA 1: *Para ISO/IEC 27005:2022 Risk Manager/Lead Risk Manager, el no presentar el DPC ni efectuar el pago de la CMA durante el ciclo resultará en un período de suspensión de 12 meses, durante el cual podrá abordar cualquier CMA y DPC pendiente. Si no se toma ninguna medida durante el período de suspensión, la certificación será revocada.*

NOTA 2: *Para CNIL– DPO, el incumplimiento de los requisitos de recertificación (experiencia laboral en protección de datos y aprobación del examen de recertificación CNIL– DPO) resultará en un período de suspensión de 12 meses. Si no se toma ninguna medida durante el período de suspensión, la certificación será revocada.*

Otros Estatus

Además de estar activa, suspendida o revocada, una certificación puede ser retirada voluntariamente o designada como Emeritus.

Estatus Emeritus

Significa que su certificación está en regla, pero no necesita mantenerse cumpliendo con los requisitos de DPC ni de CMA.

Para calificar y ser elegible para solicitar el estatus Emeritus, debe tener más de 60 años, haber mantenido una certificación de PECB durante al menos cinco años, y ya no debe ejercer funciones laborales específicas para la certificación.

Opcionalmente, los Emeritus que deseen continuar ejerciendo funciones laborales, tales como auditorías y/o proyectos de implementación, deben reportar sus DPC anualmente y cumplir con un requisito mínimo anual de 20 horas de experiencia laboral, experiencia relacionada con implementación/auditoría o consultoría, capacitación, estudio privado, tutoría, asistencia a seminarios y conferencias, u otras actividades relevantes. No se requiere la CMA.

Para solicitar este estatus, por favor complete el formulario y envíelo acertification@pecb.com.

Nota importante: *Para regresar al estatus de certificación activa, se requiere volver a presentar el examen y solicitar la certificación.*

Consulte el folleto para obtener más información sobre los beneficios del Estatus de Certificación Emeritus.

Estatus de Retiro Voluntario

Significa que su certificación está en regla, pero usted decide que ya no desea mantener su(s) certificación(es).

Para solicitar este estatus, por favor complete el formulario y envíelo acertification@pecb.com.
Las personas cuya certificación ha sido retirada voluntariamente ya no podrán presentarse como Profesionales Certificados por PECB.

Nota importante: *Para regresar al estatus de certificación activa, se requiere volver a presentar el examen y solicitar la certificación.*

Estatus de Cese Permanente

En caso de que la persona certificada fallezca o quede incapacitada (por ejemplo, debido a un accidente), el representante legal es responsable de enviar la información requerida a PECB (es decir, el certificado de defunción o certificado médico). En consecuencia, el nombre de la persona será eliminado de la lista de contactos y la cuenta de PECB será eliminada.

Ascenso y degradación de credenciales

Ascenso de credenciales
Los Profesionales PECB pueden solicitar una credencial superior una vez que proporcionen evidencia que demuestre que cumplen con los requisitos de dicha credencial.

Las Certificaciones de PECB pueden ser subidas a un nivel más alto en línea a través de su panel de control iniciando sesión [aquí], haciendo clic en **Mis Certificaciones** y luego en el botón **Subir de nivel** (Upgrade).

Para más información sobre la tarifa de Subida de nivel, visite la página de Mantenimiento de la Certificación en el sitio web de PECB.

Nota: *Para las certificaciones degradadas que necesitan ser actualizadas, se realizará una evaluación para determinar si se requiere un examen antes de obtener la certificación mejorada.*

Degradación de credenciales

Una Certificación PECB puede ser degradada a una credencial inferior por alguna de las siguientes razones:

- No se ha pagado la CMA.
- No se han presentado las horas de DPC.
- La cantidad de horas de DPC es insuficiente.
- La evidencia sobre las horas DPC no se ha enviado bajo petición.

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 tarifa anual de mantenimiento (CMA). Para 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 la reapertura de su caso debe hacerlo por escrito a certification.team@pecb.com y pagar la tarifa correspondiente.

Política de Quejas y Apelaciones

Cualquier queja que tenga un candidato debe presentarse por escrito a más tardar 30 días después de la decisión inicial de PECB. En un plazo de 30 días laborables a partir de la recepción de la queja, PECB proporcionará una respuesta por escrito al candidato, detallando los resultados de la revisión y cualquier acción tomada.

Los candidatos pueden solicitar una re evaluación de los resultados del examen o de la decisión de certificación dentro de los 30 días. Si no están satisfechos, pueden presentar una apelación a través del Sistema de Tickets de PECB. Para información más detallada, por favor consulte la Complaint and Appeal Policy | PECB

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 la(s) certificación(es) o examen(es) respectivos pueden ser aceptados como equivalentes a la certificación correspondiente de PECB (por ejemplo, la certificación ISO/IEC 27001 Lead Auditor).

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. Para descargar el Formulario para Candidatos con Discapacidad, haga clic aquí.

Política de Comportamiento

PECB tiene como objetivo proporcionar servicios de alta calidad, coherentes 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 Conducta, 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) re estructuración 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) Sección. 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 pos secundaria, 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,
CANADÁ

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