

The logo for PECB, featuring the letters 'PECB' in a bold, white, sans-serif font. The letters are slightly spaced out, and the 'C' has a unique cutout design.

PECB

BEYOND RECOGNITION

A background image showing a modern office environment with large glass windows. In the foreground, a woman in a dark suit and a man in a light grey suit are walking and looking at a tablet together. The scene is dimly lit, suggesting an evening or indoor lighting.

ISO/IEC 27005 GERENTE DE RIESGOS

Manual del Candidato

Índice

SECCIÓN I: INTRODUCCIÓN	3
Acerca de PECB	3
El valor de la certificación de PECB	4
Código de ética de PECB	6
Introducción a ISO/IEC 27005 Gerente de Riesgos	8
SECTION II: PREPARACIÓN, REGLAS Y POLÍTICAS DE EXÁMENES	9
Preparar y programar el examen.....	9
Dominios de competencia.....	10
Presentar el examen	18
Política de seguridad del examen	22
Resultados del examen	23
Política de repetición del examen	23
SECCIÓN III: CERTIFICACIÓN PROCESO Y REQUISITOS	25
Credenciales de PECB ISO/IEC 27005.....	25
Solicitar la certificación	25
Experiencia profesional	26
Referencias profesionales.....	26
Experiencia en gestión del riesgo	26
Evaluación de las solicitudes de certificación	26
SECCIÓN IV: POLÍTICAS DE CERTIFICACIÓN.....	27
Denegación de certificación.....	27
Opciones de estado de certificación	27
Ascenso y degradación de credenciales	28
Renovación de la certificación	28
Cierre de un caso	28
Política de quejas y apelaciones.....	28
SECCIÓN V: POLÍTICAS GENERALES	30
Exámenes y certificaciones de otros organismos de certificación acreditados	30
No discriminación y adaptaciones especiales.....	30
Política de Comportamiento	30
Política de Reembolso	30

SECCIÓN I: INTRODUCCIÓN

Acerca de PECB

PECB, es un organismo de certificación que ofrece educación¹, 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

¹La 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 del Servicio Internacional de Acreditación (IAS, por sus siglas en inglés) (IAS-PCB-111), el Servicio de Acreditación del Reino Unido (UKAS, por sus siglas en inglés) (UKAS-No 21923) y el Consejo Coreano de Acreditación (KAB, por sus siglas en inglés) (KAB-PC-08) bajo la norma 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, por sus siglas en inglés) (ANAB-Accreditation ID 1003) bajo ANSI/ASTM E2659-18, Práctica Estándar para Programas de Certificación.

PECB es miembro asociado de la Asociación Independiente de Registradores Acreditados (The Independent Association of Accredited Registrars, IAAR, por sus siglas en inglés), miembro de pleno derecho de la Asociación Internacional de Certificación de Personal (International Personnel Certification Association, IPC, por sus siglas en inglés), 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

PECB

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 falsamente 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 ISO/IEC 27005 Gerente de Riesgos

ISO/IEC 27005 es una norma internacional que proporciona las directrices para la gestión del riesgo de seguridad de la información y apoya los conceptos generales de seguridad de la información especificados en la norma ISO/IEC 27001. Los procesos de la gestión del riesgo de seguridad de la información permiten a las organizaciones identificar, analizar, y tratar los riesgos asociados con el uso de la tecnología de la Información.

A medida que el ciberespacio se vuelve cada vez más peligroso, la protección contra las amenazas a la seguridad de la información se ha vuelto esencial para la mayoría de las organizaciones. Un componente esencial de la gestión del riesgo de seguridad de la información. Por lo tanto, una de las competencias más solicitadas en el mercado es la capacidad de establecer e implementar un enfoque sistemático de la gestión del riesgo de seguridad de la información.

La credencial de "Gerente de Riesgos de ISO/IEC 27005" es una certificación profesional para los profesionales en seguridad de la información cuyo objetivo es demostrar la competencia para gestionar eficazmente los riesgos de seguridad de la información. Una certificación reconocida internacionalmente añade un gran valor a su carrera y le ayudará a alcanzar sus objetivos profesionales.

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 Gerente de Riesgos en ISO/IEC 27005 de conformidad con la norma 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.

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, vaya a [Lista de distribuidores](#). El horario del curso de capacitación también está disponible en línea y se puede acceder en [Eventos de capacitación](#).
2. Realice un examen PECB de forma remota a través de la [aplicación de exámenes de PECB](#). Para programar un examen remoto, 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, por favor contacte a 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: \$1000²
- Examen de Gerente: \$700
- Examen de Fundamentos: \$500
- Examen de Transición: \$500

La cuota para la 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

El objetivo del examen de “Gerente de Riesgos en ISO 27005 de PECB” es asegurar que el candidato ha adquirido la competencia necesaria para establecer, implementar, y gestionar un programa de gestión del riesgo de seguridad de la información.

La certificación de Gerente de Riesgos de ISO/IEC 27005 está destinado a:

- Gerentes o consultores involucrados o responsables de la seguridad de la información en una organización
- Personas responsables de la gestión de riesgos de seguridad de la información
- Miembros de equipos de seguridad de la información, profesionales de TI y responsables de la privacidad
- Personas responsables de mantener la conformidad con los requisitos de seguridad de la información de ISO/IEC 27001 en una organización
- Gerentes de proyecto, consultores o asesores expertos que buscan dominar la gestión de los riesgos de seguridad de la información

El contenido del examen se divide de la siguiente manera:

- **Dominio 1:** Principios y conceptos fundamentales de una gestión del riesgo de seguridad de la información
- **Dominio 2:** Implementación de un programa de gestión del riesgo de seguridad de la información
- **Dominio 3:** Marco y procesos de gestión del riesgo de seguridad de la información basados en ISO/IEC 27005
- **Dominio 4:** Otros métodos de evaluación del riesgo de seguridad de la información

Dominio 1: Principios y conceptos fundamentales de una gestión del riesgo de seguridad de la información

Objetivo principal: Asegurar que el candidato entiende y es capaz de interpretar los principios y conceptos de gestión del riesgo de seguridad de la información.

Competencias	Declaración de conocimientos
<ol style="list-style-type: none"> 1. Capacidad para comprender y explicar la estructura de ISO/IEC 27005 2. Capacidad para comprender la relación entre la norma ISO/IEC 27005 y otros marcos regulatorios de gestión del riesgo 3. Capacidad para describir la finalidad de la gestión del riesgo y las ventajas de la norma ISO/IEC 27005 4. Capacidad para comprender y explicar los conceptos de seguridad de la información 5. Capacidad para comprender los principios de la seguridad de la información: confidencialidad, integridad y disponibilidad 6. Capacidad para comprender e interpretar la definición del riesgo 7. Capacidad para comprender los conceptos principales y los principios de la gestión del riesgo 8. Capacidad para comprender amenazas y vulnerabilidades de la seguridad de la información 9. Capacidad para explicar conceptos de evento, oportunidad, consecuencia y probabilidad 10. Capacidad para comprender la clasificación de los controles de seguridad por tipo y función 11. Capacidad para comprender el papel del propietario del riesgo 	<ol style="list-style-type: none"> 1. Conocimiento de los principales conceptos y la terminología de la norma ISO/IEC 27005 2. Conocimiento de las principales normas de la familia de ISO/IEC 27000 3. Conocimiento de las normas y marcos internacionales e industriales en materia de seguridad de la información y gestión del riesgo 4. Conocimiento de los riesgos de seguridad de la información, según la norma ISO/IEC 27005 5. Conocimiento de la definición de vulnerabilidad 6. Conocimiento de las diferencias entre los conceptos de riesgos y oportunidades 7. Conocimiento de la definición de amenaza 8. Conocimiento de la confidencialidad, integridad y disponibilidad de la información 9. Conocimiento del tipo y función de los controles de seguridad 10. Conocimiento de los principios de gestión del riesgo 11. Conocimiento de los roles y responsabilidades del propietario del riesgo 12. Conocimiento de las ventajas de la gestión del riesgo

Dominio 2: Implementación de un programa de gestión del riesgo de seguridad de la información

Objetivo principal: Garantizar que el candidato comprende y es capaz de iniciar la implementación de un programa de gestión del riesgo basado en la norma ISO/IEC 27005

Competencias	Declaración de conocimientos
1. Capacidad para comprender la integración de un ciclo PHVA (PDCA, por sus siglas en inglés) en el programa de gestión del riesgo de seguridad de la información	1. Conocimiento del proceso de la gestión del riesgo
2. Capacidad para comprender y explicar los principales pasos necesarios para establecer e implementar un programa de gestión del riesgo de seguridad de la información	2. Conocimiento de cómo la alta dirección puede demostrar liderazgo y compromiso en relación con la gestión del riesgo
3. Capacidad para identificar las funciones y responsabilidades de las partes interesadas clave durante y después de la implementación y la operación de un programa de gestión del riesgo para la seguridad de la información	3. Conocimiento de las funciones y responsabilidades de un gerente de riesgos en relación con el programa de gestión del riesgo
4. Capacidad para comprender el concepto de evaluación del riesgo	4. Conocimiento de los roles y responsabilidades de las partes interesadas clave en la implementación de un programa de gestión del riesgo
5. Capacidad para comprender la importancia de una política de gestión del riesgo	5. Conocimiento de lo que suele constituir el contexto interno y externo de una organización
6. Capacidad para identificar los recursos necesarios para la implementación de un programa de gestión del riesgo	6. Conocimiento de la importancia de comprender los procesos y las actividades clave de una organización en la gestión del riesgo
7. Capacidad para analizar y comprender el contexto interno y externo de una organización	7. Conocimiento de los objetivos de la evaluación del riesgo y de cómo lograr resultados específicos
8. Capacidad para comprender los procesos clave y las actividades de una organización	8. Conocimiento de cómo se establecen los criterios de aceptación del riesgo y los criterios de evaluación del riesgo de la seguridad de la información
9. Capacidad para comprender y establecer objetivos para el programa de gestión del riesgo	9. Conocimiento de los ciclos de gestión del riesgo de seguridad de la información
10. Capacidad para establecer y mantener criterios de riesgo de seguridad de la información, incluidos criterios de aceptación del riesgo y criterios para realizar evaluaciones del riesgo seguridad de la información	10. Conocimiento de la aplicabilidad del análisis cuantitativo y cualitativo en la determinación de los criterios de aceptación del riesgo
11. Capacidad para definir y justificar el alcance del proceso de gestión del riesgo de seguridad de la información y adaptarlo a los objetivos de la organización	11. Conocimiento de los recursos necesarios para la gestión del riesgo de seguridad de la información
	12. Conocimiento del alcance y los límites de la gestión del riesgo de seguridad de la información

-
- | | |
|---|---|
| <p>12. Capacidad para definir un método adecuado de gestión del riesgo de seguridad de la información</p> | <p>13. Conocimiento de los enfoques y metodologías utilizados para la evaluación del riesgo de seguridad de la información</p> <p>14. Conocimiento de las principales etapas de planificación de las actividades de evaluación del riesgo</p> |
|---|---|

Dominio 3: Marco y procesos de gestión del riesgo de seguridad de la información basados en ISO/IEC 27005

Objetivo principal: Garantizar que el candidato es capaz de identificar, analizar, evaluar, tratar, comunicar, registrar, y hacer el seguimiento continuamente del riesgo de la seguridad de la información basándose en la norma ISO/IEC 27005.

Competencias	Declaración de conocimientos
1. Capacidad para comprender los procesos de identificación, análisis, y valoración del riesgo de la seguridad de la información	1. Conocimiento de los procesos de evaluación del riesgo de seguridad de la información, incluyendo la identificación, el análisis y la valoración del riesgo
2. Capacidad para determinar el enfoque de la identificación del riesgo y comprender e interpretar las técnicas de recopilación de información	2. Conocimiento de los enfoques para realizar la identificación del riesgo de seguridad de la información
3. Capacidad para identificar los activos, amenazas, controles existentes, las vulnerabilidades, las consecuencias (impactos) potenciales y propietarios del riesgo	3. Conocimiento de las técnicas de recopilación de información
4. Capacidad para comprender e interpretar las metodologías de análisis del riesgo	4. Conocimiento de la definición de un activo y la identificación de los activos primarios y secundarios
5. Capacidad para comprender y llevar a cabo la evaluación de las consecuencias	5. Conocimiento de la identificación y clasificación de vulnerabilidades, amenazas y controles existentes
6. Capacidad para determinar los niveles del riesgo basándose en los criterios de valoración del riesgo	6. Conocimiento de la identificación de consecuencias potenciales que pueden afectar la disponibilidad, confidencialidad e integridad
7. Capacidad para comprender la priorización del riesgo	7. Conocimiento de las técnicas de análisis del riesgo
8. Capacidad para comprender el proceso de tratamiento del riesgo y las opciones de tratamiento del riesgo basándose en la norma ISO/IEC 27005	8. Conocimiento de cómo deberían evaluarse las consecuencias y la probabilidad y cómo debería determinarse el nivel del riesgo
9. Capacidad para seleccionar los controles apropiados para reducir, retener, evitar o compartir los riesgos	9. Conocimiento de la valoración de los niveles del riesgo basándose en los criterios de valoración del riesgo
10. Capacidad para comprender y explicar los criterios de aceptación del riesgo de seguridad de la información	10. Conocimiento de la priorización del riesgo
11. Capacidad para comprender la gestión del riesgo residual	11. Conocimiento del proceso y las opciones de tratamiento del riesgo, incluidas la modificación del riesgo, la retención del riesgo, la elusión del riesgo y el riesgo compartido
12. Capacidad para comprender e interpretar el concepto del riesgo de comunicación y consulta	12. Conocimiento de los principales componentes y aprobación de un plan de tratamiento del riesgo

-
- | | |
|---|---|
| 13. Capacidad para comprender e interpretar los principios de una comunicación efectiva | 13. Conocimiento de cómo es valorado y aceptado el riesgo residual |
| 14. Capacidad para comprender y establecer una comunicación interna y externa | 14. Conocimiento del proceso de comunicación del riesgo de seguridad de la información |
| 15. Capacidad para comprender los los objetivos y las actividades de comunicación | 15. Conocimiento de los principios de una estrategia de comunicación eficaz |
| 16. Capacidad para comprender los enfoques y herramientas de comunicación | 16. Conocimiento de cómo debería ser establecida la comunicación interna y externa |
| 17. Capacidad para documentar los procesos de la gestión del riesgo de seguridad de la información | 17. Conocimiento de los enfoques y herramientas de comunicación |
| 18. Capacidad para registrar y comunicar los resultados de la evaluación y el tratamiento del riesgo | 18. Conocimiento de la información documentada y de la importancia de registrar el riesgo |
| 19. Capacidad para dar seguimiento y revisión a la eficacia de un programa de gestión del riesgo de seguridad de la información | 19. Conocimiento de la documentación de los resultados de la gestión del riesgo |
| 20. Capacidad para comprender el concepto de mejora continua y sus ventajas en relación con la gestión del riesgo | 20. Conocimiento de los principales conceptos relacionados con la mejora continua |
| 21. Capacidad para asesorar a una organización sobre cómo mejorar continuamente la eficacia y la eficiencia de un programa de gestión del riesgo de seguridad de la información | 21. Conocimiento de los procesos que necesitan seguimiento y revisión continuamente |

Dominio 4: Otros métodos de evaluación del riesgo de seguridad de la información

Objetivo principal: Garantizar que el candidato pueda utilizar metodologías y marcos de evaluación del riesgo, como OCTAVE, MEHARI, EBIOS, NIST, TRA Armonizado y CRAMM.

Competencias	Declaración de conocimientos
1. Capacidad para comprender e interpretar las metodologías OCTAVE: Método OCTAVE, OCTAVE-S, OCTAVE-Allegro, y OCTAVE FORTE	1. Conocimiento de las tres etapas del método OCTAVE
2. Capacidad para realizar una evaluación del riesgo de seguridad de la información basándose en la metodología OCTAVE Allegro	2. Conocimiento de las fases de OCTAVE-S para llevar a cabo la evaluación del riesgo
3. Capacidad para analizar y gestionar los riesgos basados en el método MEHARI	3. Conocimiento de cómo las etapas de OCTAVE-Allegro pueden ser utilizadas para realizar una evaluación del riesgo de seguridad de la información
4. Capacidad para comprender y utilizar el método EBIOS para realizar evaluaciones del riesgo	4. Conocimiento de las etapas del OCTAVE FORTE para la gestión del riesgo
5. Capacidad para identificar las publicaciones del NIST para la gestión del riesgo	5. Conocimiento de las tres fases principales de MEHARI para la gestión del riesgo
6. Capacidad para comprender e interpretar el marco de gestión del riesgo del NIST y utilizarlo en la gestión del riesgo de seguridad de la información	6. Conocimiento de cómo los riesgos de seguridad de la información pueden ser identificados, estimados, valorados, y tratados utilizando MEHARI
7. Capacidad para comprender e interpretar la metodología CRAMM para la gestión del riesgo	7. Conocimiento de la metodología de evaluación del riesgo EBIOS y de sus cinco talleres y módulos
8. Capacidad para comprender y explicar cómo puede utilizarse el método de evaluación armonizada de amenazas del riesgo (Harmonized Threat and Risk Assessment, TRA, por sus siglas en inglés) para llevar a cabo la evaluación del riesgo	8. Conocimiento de las publicaciones del NIST para la gestión del riesgo
	9. Conocimiento de las siete etapas del marco de gestión del riesgo del NIST
	10. Conocimiento de la metodología y la herramienta de análisis y gestión del riesgo CRAMM
	11. Conocimiento de las cinco etapas de la metodología de evaluación armonizada de amenazas del riesgo (Harmonized Threat and Risk Assessment, TRA, por sus siglas en inglés)

Con base en los dominios antes mencionados y su relevancia, el examen contiene 60 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/puntos a/para cada dominio de competencia	Preguntas que miden la comprensión, la aplicación y el análisis	Preguntas que miden la evaluación
Dominios de competencia	Principios y conceptos fundamentales de una gestión del riesgo de seguridad de la información	13	21.67	X	
	Implementación de un programa de gestión del riesgo de seguridad de la información	7	11.67	X	
	Marco y procesos de gestión del riesgo de seguridad de la información basados en ISO/IEC 27005	31	51.67		X
	Otros métodos de evaluación del riesgo de seguridad de la información	9	15	X	
Total		60	100%		
Número de preguntas por nivel de comprensión				29	31
% del examen dedicado a cada nivel de comprensión (cognitivo/taxonomía)				48.3%	51.7%

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

Después de aprobar con éxito el examen, los candidatos podrán solicitar la credencial de “Gerente de Riesgos en ISO/IEC 27005 Certificado por PECB”.

Presentar 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 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 los candidatos sólo pueden utilizar 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 se realizan electrónicamente a través de la aplicación de Exámenes PECB. No está permitido el uso de dispositivos electrónicos, 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 de PECB en línea](#).

Los exámenes de PECB están disponibles en dos tipos:

1. Examen con preguntas 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:

- Una copia impresa de la norma ISO/IEC 27005
- Materiales del curso de capacitación (acceso a través de la aplicación de Exámenes PECB y/o en copia impresa)
- Cualquier nota personal tomada durante el curso de capacitación (acceso a través de la aplicación de Exámenes PECB 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

Techonics es una empresa de tecnología especializada en programas informáticos (software) y electrónicos de consumo. Realizan periódicamente evaluaciones del riesgo para garantizar la seguridad de la información. A través de su bien establecido proceso de gestión del riesgo de seguridad de la información, *Techonics* es capaz de identificar los riesgos potenciales asociados a los activos de información y encontrar soluciones. Su marco de gestión del riesgo está basado en las directrices de ISO/IEC 27005.

El último proceso de evaluación del riesgo de seguridad de la información en *Techonics* tuvo lugar el mes pasado. Lo llevó a cabo la gerente de riesgos de *Techonics*, Lana, y sus resultados pusieron de manifiesto algunos riesgos nuevos relacionados con la política de contraseñas. Siguiendo el marco de gestión del riesgo de *Techonics*, el proceso de evaluación del riesgo se inició con un análisis exhaustivo de la empresa y sus objetivos. A continuación, se definieron los criterios básicos en materia de gestión del riesgo.

Lana, realizó entrevistas con el personal clave. Descubrió que la mayoría de los empleados de *Techonics* eran conscientes de que la política de contraseñas les obliga a cambiarlos una vez cada tres meses. Sin embargo, la mayoría de ellos no cumplía esta regla, ya que el sistema no la hacía cumplir.

Además, descubrió que los empleados tendían a utilizar contraseñas débiles, como su nombre y apellido. Teniendo en cuenta que las contraseñas débiles son fáciles de adivinar, esto podría convertirse en un grave problema para la seguridad de *Techonics*. Lana identificó varios escenarios de riesgo en relación con la situación identificada, de los cuales dos tenían un nivel de ocurrencia "alto".

Sam, el gerente de seguridad de la información, propuso la implementación de un gerente de contraseñas multiplataforma en la nube. La plataforma podría ser utilizada por todos los empleados para generar contraseñas complejas y almacenarlas en una base de datos segura. *Techonics* aceptó su recomendación y empezó a utilizar la plataforma para minimizar el riesgo relacionado con las contraseñas débiles. Además, se decidió que Sam organizaría una capacitación sobre seguridad de la información para sensibilizar a al personal sobre la importancia de proteger las contraseñas.

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

- 1. *Techonics* utilizó la norma ISO/IEC 27005 como guía para establecer su marco de gestión del riesgo de seguridad de la información. ¿Es esto aceptable?**
 - A. No, ISO/IEC 27005 especifica los requisitos para lograr la seguridad de la información mediante la implementación de un SGSI
 - B. Sí, ISO/IEC 27005 se puede aplicar a cualquier tipo de riesgo, cualquiera que sea su naturaleza o sus consecuencias
 - C. **Sí, la norma ISO/IEC 27005 proporciona una guía para orientar a las organizaciones a realizar actividades de gestión del riesgo de seguridad de la información.**
- 2. Lana, la gerente de riesgos, ha descubierto que los empleados de *Techonics* no cambian sus contraseñas como requiere la política de contraseñas. ¿Qué ha descubierto Lana?**
 - A. **Una vulnerabilidad**
 - B. Una amenaza
 - C. Un riesgo

3. ¿Qué opción de tratamiento del riesgo se propuso para tratar los riesgos identificados en relación con el uso de contraseñas?
- A. Evitar el riesgo
 - B. **Modificación del riesgo**
 - C. Retención del riesgo

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 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 reevaluación escribiendo a examination.team@pecb.com dentro de los 30 días posteriores a la recepción de los resultados. Las solicitudes de reevaluación recibidas después de 30 días no serán procesadas. Si los candidatos no están de acuerdo con los resultados de la reevaluación, tienen 30 días adicionales a partir de la fecha en que recibieron los resultados de la reevaluación para presentar una queja a través del [Sistema de tickets de 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 (1ra repetición).

Nota: Los candidatos que hayan tomado el curso de capacitación con uno de nuestros socios y reprobaban 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 fallen 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.

SECCIÓN III: CERTIFICACIÓN PROCESO Y REQUISITOS

Credenciales de PECB ISO/IEC 27005

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 ISO/IEC 27005 de PECB tienen los siguientes requisitos:

Credencial	Educación	Examen	Experiencia profesional	Experiencia en gestión del riesgo	Otros requisitos
Gerente Provisional de Riesgos Certificado en ISO/IEC 27005 de PECB	Educación secundaria como mínimo	Examen de Gerente de Riesgos Certificado en ISO/IEC 27005 de PECB o equivalente	Ninguna	Ninguna	Firmar el código de ética de PECB
Gerente de Riesgos en ISO/IEC 27005 Certificado por PECB			Dos años: Un año de experiencia laboral en gestión del riesgo de seguridad de la información	Actividades de gestión del riesgo de seguridad de la información, un total de 200 horas	

Para ser consideradas como válidas, las actividades deberían seguir las mejores prácticas e incluir las siguientes:

1. Definición de un enfoque de gestión del riesgo
2. Determinar los objetivos y el alcance de la gestión del riesgo
3. Llevar a cabo la evaluación del riesgo
4. Desarrollar un programa de gestión del riesgo
5. Definición de los criterios de valoración del riesgo y aceptación del riesgo
6. Evaluar las opciones de tratamiento del riesgo
7. Seguimiento y revisión del programa de gestión del riesgo

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 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 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 del riesgo 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 gestión del riesgo

El historial de proyectos de gestión del riesgo del candidato se verificará para asegurar que el candidato cuenta con el número de horas 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

PECB

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 la(s) certificación(es) o examen(es) respectivo puede ser aceptado como equivalente a la certificación de PECB respectiva (por ejemplo, la certificación de Gerente de Riesgos en ISO/IEC 27005).

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 adaptaciones³ 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 pertinentes⁴. 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.

⁴Ley 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