

ASIS INTERNATIONAL

MANUAL DE  
CERTIFICACIÓN

**CPP** Certified  
Protection  
Professional  
BOARD CERTIFIED IN SECURITY MANAGEMENT

**PCI**®  
Professional Certified Investigator  
Board Certified, ASIS International

**PSP**®  
Physical Security Professional  
Board Certified, ASIS International

**APP**  
Associate Protection Professional  
Board Certified in Security Management Fundamentals

# INFORMACIÓN DE CONTACTO DE ASIS INTERNATIONAL

¡ASIS está aquí para ayudar! Este manual cubre toda la información sobre los cuatro programas de certificación de ASIS. Si tiene preguntas después de revisar el manual, comuníquese con el Equipo de Certificación al:

**CORREO ELECTRÓNICO:** [certification@asisonline.org](mailto:certification@asisonline.org)

**TELÉFONO:** +1 703.519.6200

**SITIO WEB:** [asisonline.org](http://asisonline.org)

**DIRECCIÓN:**

ASIS International  
1625 Prince Street  
Alexandria, Virginia  
22314-2882, EE. UU.

**HORARIO DE OFICINA:** de lunes a viernes,  
de 9:00 am a 5:00 pm, hora estándar del este (excepto días festivos).

## CONTENTS

Certificaciones de ASIS International.....	6
Junta de Certificación Profesional de ASIS (PCB).....	6
Programas de certificación de ASIS International .....	6
Certificación versus programas certificados.....	7
¿Por qué escoger una certificación de ASIS?.....	7
¿Se requiere ser miembro de ASIS?.....	7
¿Cuál es el examen adecuado para usted?.....	7
Requisitos de elegibilidad para todos los solicitantes .....	8
Cambios en los requisitos de elegibilidad en 2021.....	8
APP: Certificación en Gestion Fundamentales de Seguridad .....	9
Requisitos de elegibilidad APP .....	9
Requisitos de Elegibilidad APP Con una Certificación ASIS .....	9
Áreas de conocimiento APP .....	10
CPP: Certificación en gestión de seguridad .....	15
Requisitos de elegibilidad CPP .....	15
Áreas de conocimiento CPP .....	16
PCI: Certificación en investigaciones .....	22
Requisitos de elegibilidad PCI .....	22
Área de conocimiento PCI.....	22
PSP: Certificación en seguridad física .....	25
Requisitos de elegibilidad PSP .....	25
Área de conocimiento PSP .....	25
¡Anunciando Exámenes Supervisados de Forma Remota!.....	29
Solicitud de exámenes .....	29
Documentos de solicitud que necesitará: .....	29
Recordatorios de fechas límite .....	29
Tarifas de solicitud .....	29

Reembolso .....	29
Retomar el examen.....	29
Notificación de aprobación de ASIS.....	30
Apelar una solicitud rechazada.....	30
Proceso de apelación relacionada para personas certificadas de la PCB.....	30
Programación de su examen .....	30
Hacer su cita para el examen.....	31
Adaptaciones de pruebas para candidatos con discapacidades y otras consideraciones especiales.....	31
Políticas de extensión – Solicitudes de examen .....	31
Política de cancelación.....	32
“No presentación” .....	32
El día del examen .....	32
Procedimientos de Registro en un Centro Prometric.....	32
Qué Llevar y qué No Llevar .....	33
Procedimiento de Registro para el Examen Supervisado Remoto.....	33
Documentos de Identificación Aceptables .....	33
Durante el examen.....	34
Resultados del examen.....	35
Emergencias por clima.....	35
¿Cómo están estructurados los exámenes?.....	35
Calificación del examen .....	35
Estudiar para el examen .....	36
Recursos de preparación para el examen.....	36
Aprobé el examen, ¿ahora qué?.....	37
Recertificación .....	37
Políticas de solicitud y de personas certificadas de ASIS.....	37
Declaración de Imparcialidad .....	37
Código de Responsabilidad Profesional de la Certificación de ASIS.....	38
Declaración de Elegibilidad Continua para Certificación.....	38

Revocación de certificación .....	39
Designación de por vida.....	39
Divulgación de información de candidatos y personas certificadas.....	40
Certificados de ASIS .....	40
Intervención De Terceros.....	40
Presentar una queja.....	40
Sobre nuestro socio del examen.....	40

## Sobre este manual

Este manual contiene todas las políticas y procedimientos de los cuatro programas de certificación de ASIS. Todas las personas que soliciten tomar un examen de certificación de ASIS deben aceptar cumplir con la información contenida en este manual. **Este manual se actualizó el 1º de junio 2021 y reemplaza todas las versiones anteriores.**

## CERTIFICACIONES DE ASIS INTERNATIONAL

ASIS International fue la primera organización en ofrecer una credencial específicamente para gerentes de seguridad, y nuestro programa sigue siendo el estándar global. Elaborado por profesionales para profesionales, las certificaciones de ASIS le proporcionan una ventaja competitiva.

Distinguido por su desarrollo y aplicación global, las certificaciones de ASIS son reconocidas a través de todos los sectores de la industria y fronteras geográficas. El papel y las tareas de los gerentes de seguridad se investigan y documentan para definir cada certificación. Asimismo, se realiza un análisis de trabajo de manera rutinaria para garantizar que los exámenes reflejen las prácticas actuales.

Nuestros requisitos son exigentes y, por consiguiente, solo un grupo distinguido de profesionales cuenta con nuestras certificaciones. Obtener su certificación como Profesional Certificado en Protección (CPP®), Investigador Profesional Certificado (PCI®), Profesional en Seguridad Física (PSP®) o Profesional de Protección Asociado (APP) transmite a sus compañeros, empleados y empleadores que usted posee experiencia relevante y sustancial, así como competencia demostrada y probada.



**UN PROGRAMA RECONOCIDO  
INTERNACIONALMENTE, ACREDITADO  
GLOBALMENTE**

Las certificaciones de ASIS se desarrollan y mantienen a través de un proceso intenso ejemplificado a través de la acreditación del programa de parte de American National Standards Institute (ANSI) frente a la Organización Internacional de Normalización International Organization for Standardization (ISO) 17024.



**DESIGNACIÓN DE LA LEY DE SEGURIDAD**

Los profesionales certificados de ASIS, sus empleadores y sus clientes están protegidos frente a demandas relacionadas con el proceso de certificación de ASIS que surja de un acto de terrorismo.



El Consejo Estadounidense sobre la Educación ha revisado y recomendado la equivalencia de créditos universitarios para los programas de certificación como CPP, PCI y PSP de ASIS International\*.

\* El logotipo de ACE CREDIT es una marca registrada federalmente del Consejo Estadounidense sobre la Educación y no se puede usar ni reproducir sin el permiso expreso por escrito del Consejo Estadounidense sobre la Educación.

## JUNTA DE CERTIFICACIÓN PROFESIONAL DE ASIS (PCB)

La Junta de Certificación Profesional (Professional Certification Board, PCB) de ASIS rige los programas de certificación de ASIS. La PCB establece todas las políticas relacionadas con el programa, lo que incluye requisitos de elegibilidad, conjunto de conocimientos y desarrollo de exámenes. Todos los miembros de la PCB tienen certificación como CPP, PCI, PSP y/o APP.

Los miembros de la Junta de Certificación Profesional (PCB) gestionan los programas de certificación asegurándose de que se desarrollen y mantengan estándares y se implemente el control de calidad, así como asegurándose de que los exámenes reflejen de manera precisa los deberes y responsabilidades de profesionales de seguridad en las áreas de gestión de seguridad, investigaciones y seguridad física. La PCB es un comité de la Junta de directores de ASIS. Los miembros de la PCB se escogen a través de un proceso de nominación. La junta se reúne tres veces al año.

## PROGRAMAS DE CERTIFICACIÓN DE ASIS INTERNATIONAL

La certificación sirve como un reconocimiento visible de su dominio de principios y habilidades básicos de seguridad esenciales para la mejor práctica de la gestión de seguridad.

Sin embargo, no todas las certificaciones son iguales. Para diferenciarse realmente de los demás, usted

necesita una certificación que fomente el crecimiento profesional. Una que sea reconocida globalmente como el estándar de profesionalismo. Necesita una certificación de ASIS.

Al obtener una certificación como CPP, PCI, PSP o APP, su empleador, clientes y colegas lo reconocerán instantáneamente como "lo mejor de lo mejor". Obtener una certificación de ASIS es un logro importante que lo ayudará a lograr sus metas de carrera.

## Certificación versus programas certificados

A menudo, las personas no tienen clara la diferencia entre un programa de certificación y un programa certificado. La meta de ambos tipos de programa es el desarrollo profesional de expertos de la industria.

**Certificación profesional** (tal como CPP, PCI, PSP y APP) es el proceso voluntario mediante el cual una organización externa otorga un reconocimiento de duración limitada y el uso de una credencial a una persona después de verificar que han cubierto los criterios predeterminados y estandarizados, por lo general a través de requisitos de elegibilidad y un examen. La mayoría de los programas de certificación profesional requieren que las personas certificadas renueven la certificación después de un periodo establecido a fin de garantizar que se mantengan actualizados y con conocimientos en la industria.

Un **programa certificado** es un programa de capacitación en un tema especializado por el cual los participantes reciben un certificado después de completar el curso. Algunos programas certificados requieren que los asistentes aprueben una evaluación de algún tipo para comprobar que han aprendido lo que se les enseñó en clases. Muchos programas certificados entregarán un "certificado de culminación" al final del curso. ASIS ofrece una cantidad de programas certificados, muchos de los cuales se pueden usar para adquirir créditos de Educación Profesional Continua que se pueden usar para prepararse para programas de certificación de ASIS o para renovar la certificación.

## ¿Por qué escoger una certificación de ASIS?

- ◆ Eleva su nivel profesional y el reconocimiento de sus colegas.
- ◆ Obtiene una ventaja competitiva en su posición o ascenso laboral dentro de su organización.

- ◆ Logra satisfacción personal profunda y desarrollo profesional.
- ◆ Amplía sus conocimientos base.
- ◆ Lo mantiene al día con las mejores prácticas.
- ◆ Logra reconocimiento global como un experto altamente motivado en su campo.

Los profesionales certificados de ASIS son líderes, mentores voluntarios y socios estratégicos confiables que prestan servicio tanto a sus organizaciones como a la profesión.

Hoy, profesionales de seguridad de 91 países poseen con orgullo certificaciones de ASIS.

## ¿Se requiere ser miembro de ASIS?

No se requiere ser miembro de ASIS, sin embargo, los miembros disfrutan de muchas ventajas, incluyendo descuentos en todos los productos relacionados con la certificación y servicios incluyendo tarifa de examen, recursos de preparación, y más. Y, una vez certificado, miembros de ASIS continúan recibiendo descuentos en los programas de desarrollo profesional para obtener CPE créditos. Hágase miembro primero, antes de completar la solicitud de examen. ¡Enseguida vera los beneficios!

## ¿Cuál es el examen adecuado para usted?

ASIS ofrece cuatro certificaciones para los campos relacionados con la seguridad:

- ◆ Profesional Certificado en Protección (CPP)
- ◆ Investigador Profesional Certificado (PCI)
- ◆ Profesional en Seguridad Física (PSP)
- ◆ Profesional de Protección Asociado (APP)

Algunos profesionales cuentan con una certificación de ASIS, algunos con dos y otros cuentan con las tres certificaciones (El APP no puede mantenerse en conjunto con el CPP). A continuación, presentamos un resumen de los cuatro programas:

- ◆ El programa de **Profesional Certificado en Protección (CPP)** está diseñado para aquellos que han demostrado competencia en todas las áreas de gestión de seguridad.
- ◆ El programa de **Investigador Profesional Certificado (PCI)** está diseñado para aquellos cuyas responsabilidades incluyan gestión de casos, obtención de pruebas y preparación de

informes y testimonio para hallazgos fundamentados.

- ◆ El programa de **Profesional en Seguridad Física (PSP)** está diseñado para aquellos cuya responsabilidad principal sea realizar estudios de amenazas, diseñar sistemas integrados de seguridad que incluyan equipos, procedimientos y personas o instalar, operar y mantener esos sistemas.
- ◆ El programa de **Profesional de Protección Asociado (APP)** está diseñado para aquellos con 1-4 años de experiencia en los fundamentos de la gestión de la seguridad.

ASIS recomienda encarecidamente revisar el área de conocimiento para cada programa (descritos a continuación). Todas las preguntas de los exámenes se relacionan con uno de los campos indicados en las áreas de conocimiento de cada programa. Usando el temario de conocimientos, haga una evaluación honesta de sus propias experiencias en cada campo. Esto no solo lo va a ayudar a decidir cuál es el examen correcto para usted, sino que también lo ayudará a estructurar sus requisitos de estudio.

## REQUISITOS DE ELEGIBILIDAD PARA TODOS LOS SOLICITANTES

Las siguientes páginas describen los requisitos de seguridad y el área de conocimiento para cada programa de certificación de ASIS. Además de los requisitos específicos de elegibilidad que están a continuación, **todos los solicitantes y personas certificadas deben:**

- ◆ Tener un empleo a tiempo completo en una función relacionada con la seguridad.
- ◆ Experiencia de trabajo adquirida mientras este inscrito en un programa académico, puede ser aplicable si es directamente relevante a la certificación, a tiempo completo, y compensado.
- ◆ No haber sido condenados por ningún delito que se reflejaría de manera negativa en la profesión de seguridad, ASIS o el programa de certificación.
- ◆ Firmar y aceptar adherirse al Código de Responsabilidad Profesional de la Certificación de ASIS (consulte la página 35).
- ◆ Aceptar adherirse a las políticas de los programas de certificación de ASIS.

## CAMBIOS EN LOS REQUISITOS DE ELEGIBILIDAD EN 2021

En 2020, el PCB votó a favor de reducir ligeramente los requisitos de elegibilidad para los cuatro programas de certificación. Estos cambios se realizaron después de una revisión total de cómo ha madurado la profesión de gestión de la seguridad en los últimos 40 años (cuando se lanzó el CPP), cómo se comparan nuestros programas con otras certificaciones relacionadas con la seguridad y una revisión de los antecedentes educativos y de experiencia de nuestros solicitantes.

2021 REQUISITOS DE ELEGIBILIDAD				
	APP	PSP	PCI	CPP
Sin Educación Superior	3 años	5 (4) años	5 (4) años	7 (6) años
Título de Licenciatura	2 años	4 (3) años	4 (3) años	6 (5) años
Maestría	1 año	3 (3) años	3 (3) años	5 (4) años
Cargo de Responsabilidad /Gestion de casos	0 años	0 años	2 años	3 años

**Nota:** Los números entre paréntesis indican los años para aquellos que tienen la certificación APP.



# Profesional de Protección Asociado

## APP: CERTIFICACIÓN EN GESTION FUNDAMENTALES DE SEGURIDAD

ASIS International lanzo Certificación para el Profesional de Protección Asociado (APP) en 2019, como parte de la estrategia continua para ofrecer desarrollo profesional y oportunidades educativas para profesionales en todos los niveles del campo de la gestión de la seguridad.

El **Profesional de Protección Asociado (APP)** destinada a aquellos con 1-3 años de experiencia\* en gestión de la seguridad. Este examen medirá el conocimiento profesional de fundamentos de la gestión de la seguridad, operaciones de negocios, gestión de riesgos y gestión de respuesta.

### Requisitos de elegibilidad APP

Experiencia* en Gestion de Seguridad	Educación
Un año	Maestría (o equivalente internacional)
Dos años	Licenciatura (o equivalente internacional) en Gestion de Seguridad
Tres años	Sin título de educación Superior

\*Experiencia se define como la persona que ha estado comprometido de manera personal en trabajos de seguridad o prevención de pérdidas a tiempo completo (no se permiten pasantías) o que lo tiene como un deber principal. Se incluye:

- Experiencia como profesional de seguridad en la protección de activos en el sector público o en el privado, el sistema de justicia penal, inteligencia gubernamental o agencias de investigación.
- Experiencia con compañías, asociaciones, gobierno u otras organizaciones que presten servicios o productos, lo que incluye firmas de

asesoría, siempre y cuando los deberes y responsabilidades se relacionen de manera sustancial con el diseño, la evaluación y la aplicación de sistemas, programas o equipos, o con el desarrollo y operación de servicios para la protección de activos en el sector público o en el privado.

- Experiencia como educador a tiempo completo en la facultad de una institución educativa acreditada, siempre que las responsabilidades de los cursos y otros deberes se relacionen principalmente con áreas de conocimiento pertinentes a la gestión y operación de programas de activos en el sector público o en el privado.

### Requisitos de Elegibilidad APP Con una Certificación ASIS

El cuadro a continuación muestra cómo se alterarían los requisitos de elegibilidad para quienes tienen la designación APP

CPP	Con Maestría	Con Licenciatura	Sin Título de Educación Superior
Experiencia Profesional	5 años	6 años	7 años
Si tiene APP	4 años	5 años	6 años
PCI	Con Maestría	Con Licenciatura	Sin Título de Educación Superior
Experiencia Profesional	3 años	4 años	5 años
Si tiene APP	3 años	3 años	4 años
PSP	Con Maestría	Con Licenciatura	Sin Título de Educación Superior
Experiencia Profesional	3 años	4 años	5 años
Si tiene APP	3 años	3 años	4 años

1. Requisitos de elegibilidad para el CPP, PCI o PSP se deben cumplir (por ejemplo, un cargo de responsabilidad o gestión de casos)
2. Si un candidato obtiene la designación CPP, la designación APP expirará (no puede tener ambas designaciones al mismo tiempo)
3. Los que tengan las designaciones PCI- y/o PSP-son elegibles para tomar el examen APP (siempre que cumplan con los requisitos del programa)
4. **CPPs no están permitidos a tomar el examen APP**

## Áreas de conocimiento APP

Para obtener una certificación como APP, un candidato debe aprobar un examen integral que consta de aproximadamente 125 preguntas de selección múltiple; 100 preguntas "en vivo" con calificación y hasta 25 preguntas previas a la prueba. Se prueba el conocimiento en cuatro áreas principales (campos).

La importancia de cada campo y las tareas, conocimientos y habilidades dentro de estos determinan las especificaciones del examen de APP. El orden relativo de importancia de los campos determina el porcentaje de las preguntas totales del examen.

## CAMPO UNO

### Principios de la seguridad (35 %)

**Tarea 1: Implementar y coordinar el(los) programa(s) de seguridad de la organización para proteger los activos de la organización**

#### Conocimiento de

1. Teoría y terminología de la seguridad
2. Técnicas de gestión de proyectos
3. Estándares del sector de la seguridad
4. Técnicas y métodos de protección
5. Evaluación del programa y los procedimientos de seguridad
6. Principios de seguridad de planificación, organización y control

**Tarea 2: Implementar métodos para mejorar el programa de seguridad en una base continua a través del uso de auditorías, revisiones y evaluaciones**

#### Conocimiento de

1. Técnicas para recopilación de datos y análisis de inteligencia
2. Procesos continuos de evaluación y mejora
3. Técnicas de auditoría y pruebas

**Tarea 3: Desarrollar y coordinar programas de relaciones externas con las organizaciones de aplicación de la ley del sector público u otras organizaciones para lograr los objetivos de seguridad**

#### Conocimiento de:

1. Funciones y responsabilidades de organizaciones y agencias externas
2. Asociaciones públicas/privadas a nivel local, nacional e internacional
3. Métodos para crear relaciones laborales eficaces

**Tarea 4. Desarrollar, implementar y coordinar programas de sensibilización en seguridad para empleados**

#### Conocimiento de

1. El carácter de la comunicación verbal y no verbal y consideraciones culturales
2. Estándares del sector de la seguridad
3. Metodologías de capacitación
4. Estrategias, técnicas y métodos de comunicación
5. Objetivos y métricas del programa de sensibilización en seguridad

**Tarea 5: Implementar y/o coordinar un programa de investigación**

#### Conocimiento de

1. Preparación de informes para fines internos y procedimientos legales
2. Componentes de los procesos de investigación
3. Tipos de investigaciones (p.ej., incidentes, mala conducta, cumplimiento, etc.)
4. Recursos internos y externos para respaldar funciones de investigación

**Tarea 6: Ofrecer coordinación, asistencia y evidencia como documentación y testimonios para apoyar procedimientos legales**

#### Conocimiento de

1. Componentes requeridos de documentación eficaz (p.ej., legal, empleado, procedimientos, políticas, cumplimiento, etc.)
2. Recopilación de evidencias y técnicas de protección
3. Leyes y reglamentos relevantes concernientes a las prácticas de gestión, retención, conservaciones por razones legales y destrucción de registros

**Tarea 7: Realizar investigaciones de antecedentes para contratación, promoción y/o retención de personas**

Conocimiento de

1. Investigaciones de antecedentes y técnicas de selección de personal
2. Calidad y tipos de fuentes de información y datos
3. Leyes y procedimientos penales, civiles y laborales

**Tarea 8: Desarrollar, implementar, coordinar y evaluar políticas, procedimientos, programas y métodos para protección de personas de amenazas humanas en el lugar de trabajo**

(por ejemplo, acoso, violencia, etc.)

Conocimiento de

1. Principios y técnicas de desarrollo de políticas y procedimientos
2. Personal, tecnología y procesos de protección
3. Reglamentos y estándares que rigen o afectan al sector de la seguridad y la protección de personas, propiedades e información
4. Diseño e implementación de programas educativos y de sensibilización

**Tarea 9: Realizar y/o coordinar un programa de protección ejecutivo/de personal**

Conocimiento de

1. Componentes del programa de seguridad de viajes
2. Componentes del programa de protección ejecutivo/de personal
3. Personal, tecnología y procesos de protección

**Tarea 10: Desarrollar y/o mantener un programa de seguridad física para un activo organizacional**

Conocimiento de

1. Técnicas de gestión de recursos
2. Mantenimiento preventivo y correctivo de sistemas
3. Equipo, tecnología y personal para protección de seguridad física
4. Teoría, técnicas y procesos de seguridad
5. Principios de diseño de sistemas de seguridad

**Tarea 11: Recomendar, implementar y coordinar controles de seguridad física para mitigar riesgos de seguridad**

Conocimiento de

1. Técnicas de mitigación de riesgos (p.ej., tecnología, personal, proceso, diseño de instalaciones, infraestructura, etc.)
2. Equipo, tecnología y personal para protección de seguridad física
3. Técnicas de inspección de seguridad

**Tarea 12: Evaluar e integrar tecnología en un programa de seguridad para cumplir objetivos organizacionales**

Conocimiento de

1. Técnicas y tecnología de vigilancia
2. Integración de tecnología y personal
3. Planos, diagramas y esquemas
4. Metodología de la teoría y sistemas de seguridad de la información

**Tarea 13: Coordinar e implementar políticas de seguridad que contribuyan a un programa de seguridad de la información**

Conocimiento de

1. Prácticas para proteger información patentada y propiedad intelectual
2. Tecnología, investigaciones y procedimientos para proteger la información
3. Componentes del programa de seguridad de la información (p.ej., protección de activos, seguridad física, seguridad de procedimientos, seguridad de los sistemas de información, sensibilización del empleado y capacidades de destrucción y recuperación de información)
4. Amenazas a la seguridad de la información

## CAMPO DOS

### Operaciones comerciales (22 %)

**Tarea 1: Proponer presupuestos e implementar controles financieros para garantizar la responsabilidad fiscal**

Conocimiento de

1. Técnicas de análisis de datos y análisis de costo-beneficio
2. Principios de gestión comercial contable, control y auditorías
3. Análisis de retorno de la inversión (ROI)
4. Principios de finanzas comerciales e informes financieros
5. Proceso de planificación del presupuesto

- Componentes necesarios de la documentación eficaz (p.ej., presupuesto, hoja de balance, orden de trabajo de proveedores, contratos, etc.)

**Tarea 2: Implementar políticas, procedimientos, planes y directivas de seguridad para alcanzar los objetivos organizacionales**

Conocimiento de

- Principios y técnicas de desarrollo de políticas/procedimientos
- Normas para el comportamiento individual y corporativo
- Técnicas de mejora (por ejemplo, programas piloto, educación y capacitación)

**Tarea 3: Desarrollar procedimientos/técnicas para medir y mejorar la productividad departamental**

Conocimiento de

- Estrategias, métodos y técnicas de comunicación
- Técnicas para cuantificación de productividad/métricas/indicadores de desempeño clave (KPI, por sus siglas en inglés)
- Principios, herramientas y técnicas de gestión de proyectos
- Principios de evaluación del desempeño, revisiones 360 y coaching

**Tarea 4: Desarrollar, implementar y coordinar procesos de dotación de personal de seguridad y programas de desarrollo del personal para lograr los objetivos organizacionales**

Conocimiento de

- Estrategias y metodologías de retención
- Procesos de análisis de empleo
- Colaboración multifuncional
- Estrategias, métodos y técnicas de capacitación
- Gestión de talentos y planificación de sucesiones
- Técnicas de selección, evaluación y entrevistas para dotación de personal

**Tarea 5: Supervisar y asegurar una cultura ética sólida de acuerdo con los requisitos reglamentarios y los objetivos organizacionales**

Conocimiento de

- Técnicas de comunicación y Retroalimentación interpersonales
- Leyes y reglamentos pertinentes

- Normas de gobierno y cumplimiento
- Principios éticos generalmente aceptados
- Normas para el comportamiento individual y corporativo

**Tarea 6: Ofrecer consejo y asistencia para desarrollar indicadores de desempeño clave y negociar términos contractuales para vendedores/proveedores de seguridad**

Conocimiento de

- Técnicas y métodos de protección de información confidencial
- Leyes y reglamentos pertinentes
- Conceptos clave en la preparación de solicitudes de propuestas y revisiones/evaluaciones de ofertas
- Definición, medición e informes de Acuerdos de Nivel de Servicio (SLA)
- Principios de la ley contractual, indemnización y seguro de responsabilidad
- Procesos de supervisión para garantizar el cumplimiento de las necesidades organizacionales y los requisitos contractuales
- Calificación y proceso de selección de proveedores

## CAMPO TRES

### Gestión de riesgo (25 %)

**Tarea 1: Llevar a cabo procesos de evaluación de riesgos iniciales y continuos**

Conocimiento de

- Estrategias de gestión de riesgos (por ejemplo, evitar, asumir/aceptar, transferir, mitigar, etc.)
- Metodología de gestión de riesgos y análisis de impacto comercial
- Teoría y terminología de gestión de riesgos (por ejemplo, amenazas, probabilidad, vulnerabilidad, impacto, etc.)

**Tarea 2: Evaluar y priorizar amenazas para abordar las consecuencias potenciales de incidentes**

Conocimiento de

- Amenazas potenciales a una organización
- Enfoque holístico para evaluar amenazas de todos los peligros
- Técnicas, herramientas y recursos relacionados con amenazas internas y externas

**Tarea 3: Preparar, planificar y comunicar la forma en que la organización identificará, clasificará y abordará los riesgos**

Conocimiento de

1. Prueba de cumplimiento de la gestión de riesgos (por ejemplo, auditoría de programas, controles internos, autoevaluación, etc.)
2. Evaluaciones cuantitativas y cualitativas de riesgos
3. Estándares de gestión de riesgos
4. Evaluaciones de vulnerabilidad, amenaza e impacto

**Tarea 4: Implementar y/o coordinar contramedidas recomendadas para nuevas estrategias de tratamiento de riesgos**

Conocimiento de

1. Contramedidas
2. Técnicas de mitigación
3. Métodos de análisis de costo-beneficio para estrategias de tratamiento de riesgos

**Tarea 5: Establecer un plan de continuidad comercial o un plan de continuidad de operaciones (COOP)**

Conocimiento de

1. Estándares de continuidad comercial
2. Técnicas de planificación de emergencias
3. Análisis de riesgos
4. Análisis de brechas

**Tarea 6: Garantizar la planificación de recursos previa a incidentes (por ejemplo, acuerdos de ayuda mutua, ejercicios de simulación, etc.)**

Conocimiento de

1. Técnicas para recopilación de datos y análisis de tendencias
2. Técnicas, herramientas y recursos relacionados con amenazas internas y externas
3. Calidad y tipos de fuentes de información y datos
4. Enfoque holístico para evaluar amenazas de todos los peligros

## CAMPO CUATRO

### Gestión de respuestas (18 %)

**Tarea 1: Responder ante un incidente y gestionarlo usando las mejores prácticas**

Conocimiento de

1. Funciones y deberes principales en una estructura de comando de incidente
2. Principios de gestión y prácticas de un centro de operaciones de emergencias (EOC)

**Tarea 2: Coordinar la recuperación y la reanudación de operaciones después de un incidente**

Conocimiento de

1. Recursos de asistencia para recuperación
2. Oportunidades de mitigación durante procesos de respuesta y recuperación

**Tarea 3: Llevar a cabo una revisión posterior al incidente**

Conocimiento de

1. Oportunidades de mitigación durante procesos de respuesta y recuperación
2. Técnicas de revisión posterior al incidente

**Tarea 4: Implementar planes de contingencia para tipos comunes de incidentes (por ejemplo, amenaza de bomba, tirador activo, desastres naturales, etc.)**

Conocimiento de

1. Estrategias de recuperación a corto y largo plazo
2. Sistemas y protocolos para gestión de incidentes

**Tarea 5: Identificar vulnerabilidades y coordinar contramedidas adicionales para un activo en condiciones de degradación después de un incidente**

Conocimiento de

1. Técnicas de clasificación/priorización y evaluación de daños
2. Tácticas de prevención, intervención y respuesta

**Tarea 6: Evaluar y priorizar amenazas para mitigar consecuencias de incidentes**

Conocimiento de

1. Técnicas de clasificación/priorización y evaluación de daños
2. Técnicas de gestión de recursos

**Tarea 7: Coordinar y asistir en la recopilación de evidencias para la revisión posterior a incidentes (por ejemplo, documentación, testimonios)**

Conocimiento de

1. Técnicas de comunicación y protocolos de notificación

2. Técnicas de comunicación y protocolos de enlace

**Tarea 8: Coordinar con los servicios de emergencias durante la respuesta a incidentes**

Conocimiento de

1. Conceptos y diseño del centro de operaciones de emergencias (EOC)
2. Principios de gestión y prácticas de un centro de operaciones de emergencias (EOC)
3. Técnicas de comunicación y protocolos de enlace

**Tarea 9: Supervisar la eficacia de la respuesta a incidentes**

Conocimiento de

1. Técnicas de revisión posterior a incidentes
2. Sistemas y protocolos para gestión de incidentes

**Tarea 10: Comunicar actualizaciones regulares de las condiciones a la dirección y otros grupos de interés claves a lo largo del incidente**

Conocimiento de

1. Técnicas de comunicación y protocolos de enlace
2. Técnicas de comunicación y protocolos de notificación

**Tarea 11: Supervisar y auditar el plan de cómo responderá la organización ante incidentes**

Conocimiento de

1. Técnicas de capacitación y ejercicios
2. Técnicas de revisión posterior al incidente

---

# Profesional Certificado en Protección

---

## CPP: CERTIFICACIÓN EN GESTIÓN DE SEGURIDAD

El estándar dorado por más de 40 años, la credencial de Profesional Certificado en Protección (CPP®) es una prueba de conocimientos y habilidades de gestión en siete campos clave de seguridad.

Obtener una certificación como CPP proporciona confirmación independiente de su capacidad para asumir responsabilidades de liderazgo y gestionar de manera efectiva asuntos amplios de seguridad.

### Requisitos de elegibilidad CPP

Los candidatos que deseen tomar el examen de CPP deben cubrir los siguientes requisitos de elegibilidad:

#### EXPERIENCIA LABORAL

##### Sin educación superior:

**Siete (7) años de experiencia\* en seguridad**, (o si tiene el APP seis años), al menos tres (3) años de los cuales deben haber estado en un cargo de responsabilidad\*\* de una función de seguridad.

##### Con educación superior:

**Maestría o equivalente internacional** de una institución acreditada de educación superior y tener **cinco (5) años de experiencia\* en seguridad** (o si tiene el APP cuatro años), al menos tres (3) años de los cuales deben haber estado en un cargo de responsabilidad\*\* de una función de seguridad.

#### O BIEN

**Título de licenciatura o equivalente internacional** de una institución acreditada de educación superior y **tener seis (6) años de experiencia\* en seguridad**, (o si tiene el APP cinco años), al menos tres (3) años de los cuales deben haber estado en un cargo de responsabilidad\*\* de una función de seguridad.

\*Experiencia se define como la persona que ha estado comprometido de manera personal en trabajos de

seguridad o prevención de pérdidas a tiempo completo (no se permiten pasantías) o que lo tiene como un deber principal. Se incluye:

- a.) Experiencia como profesional de seguridad en la protección de activos en el sector público o en el privado, el sistema de justicia penal, inteligencia gubernamental o agencias de investigación.
- b.) Experiencia con compañías, asociaciones, gobierno u otras organizaciones que presten servicios o productos, lo que incluye firmas de asesoría, siempre y cuando los deberes y responsabilidades se relacionen de manera sustancial con el diseño, la evaluación y la aplicación de sistemas, programas o equipos, o con el desarrollo y operación de servicios para la protección de activos en el sector público o en el privado.
- c.) Experiencia como educador a tiempo completo en la facultad de una institución educativa acreditada, siempre que las responsabilidades de los cursos y otros deberes se relacionen principalmente con áreas de conocimiento pertinentes a la gestión y operación de programas de activos en el sector público o en el privado.

\*\* Cargo de responsabilidad significa que el solicitante tiene la autoridad para tomar decisiones independientes y tomar acciones independientes para determinar la metodología operativa y gestionar la ejecución de un proyecto o proceso relacionado con la seguridad. Esta definición no requiere que el individuo supervise a otros y generalmente excluye puestos tales como oficial de patrulla o equivalente.



## Áreas de conocimiento CPP

Para obtener una certificación como CPP, un candidato debe aprobar un examen integral que consta de aproximadamente 225 preguntas de selección múltiple; 200 preguntas "en vivo" con calificación y hasta 25 preguntas previas a la prueba. Se prueba el conocimiento en siete áreas principales (campos).

La importancia de cada campo y las tareas, conocimientos y habilidades dentro de estos determinan las especificaciones del examen de CPP. El orden relativo de importancia de los campos determina el porcentaje de las preguntas totales del examen.

En 2019/2020, ASIS realizó un estudio de análisis de trabajo para garantizar que las áreas de conocimientos de la certificación CPP aún represente el conocimiento y las habilidades necesarias para ser un administrador de seguridad exitoso. Se han efectuado ligeros cambios los cuales están señaladas a continuación en **rojo** (estos son cambios menores que no cambiaron el significado y se hicieron para mayor claridad). La información completamente nueva está marcada en **verde (Dominio Uno, Tarea Uno y Dominio Tres, Tarea 4)**. Las preguntas del examen sobre la nueva información comenzarán a aparecer en el examen a principios de 2021.

## CAMPO UNO

**Principios y prácticas de seguridad (22% -- fue 21%)**

**Tarea 1: Planificar, desarrollar, implementar y gestionar el programa de seguridad de la organización para proteger sus activos.**

### Conocimientos de

1. Principios de planificación, organización y control
2. Teoría, técnicas y procesos de seguridad (p.ej., **inteligencia artificial, IoT**)
3. Estándares del sector de seguridad (p. ej., **ASIS/ISO**)
4. Procesos continuos de evaluación y mejora
5. Colaboración interfuncional dentro de la organización
6. **Gestión de Riesgos de Seguridad Empresarial (ESRM)**

**Tarea 2: Desarrollar, gestionar o llevar a cabo el proceso de evaluación de riesgo de seguridad.**

### Conocimientos de

1. Evaluaciones cuantitativas y cualitativas de riesgo
2. Evaluaciones de vulnerabilidad, amenaza e impacto
3. Posibles amenazas de seguridad (p. ej., todos los peligros, actividad criminal, etc.)

**Tarea 3: Evaluar métodos para mejorar el programa de seguridad de manera continua a través del uso de auditoría, revisión y evaluación.**

### Conocimientos de

1. Métodos de análisis costo-beneficio
2. Estrategias de gestión de riesgos (p. ej., evitar, asumir/aceptar, transferir, distribuir, etc.)
3. Técnicas de mitigación de riesgos (p. ej., tecnología, personal, proceso, diseño de instalaciones, etc.)
4. Técnicas de recopilación de datos y de análisis de tendencias

**Tarea 4: Desarrollar y gestionar programas de relaciones profesionales con organizaciones externas para lograr objetivos de seguridad.**

### Conocimientos de

1. Funciones y responsabilidades de organizaciones y agencias externas
2. Métodos para crear relaciones efectivas de trabajo
3. Técnicas y protocolos de enlace
4. Asociaciones públicas/privadas a nivel local y nacional

**Tarea 5: Desarrollar, implementar y gestionar programas de sensibilización de seguridad laboral para lograr metas y objetivos organizacionales.**

### Conocimientos de

1. Metodologías de capacitación
2. Estrategias, técnicas y métodos de comunicación
3. Objetivos y medidas del programa de sensibilización
4. Elementos de un programa de sensibilización de seguridad (p. ej., funciones y responsabilidades,



riesgo físico, riesgo de comunicación, privacidad, etc.)

## CAMPO DOS

### Principios y prácticas comerciales (15% fue 13%)

**Tarea 1: Desarrollar y administrar presupuestos y controles financieros para lograr la responsabilidad fiscal.**

#### Conocimientos de

1. Principios de contabilidad de gestión, control, auditorías y responsabilidad fiduciaria.
2. Principios de finanzas comerciales e informes financieros
3. Análisis de rentabilidad (Return on Investment, ROI)
4. El ciclo de vida para fines de planificación de presupuestos

**Tarea 2: Desarrollar, implementar y gestionar políticas, procedimientos, planes y directivas para lograr objetivos organizacionales.**

#### Conocimientos de

1. Principios y técnicas de desarrollo de políticas/procedimientos
2. Estrategias, métodos y técnicas de comunicación
3. Estrategias, métodos y técnicas de capacitación
4. Colaboración interfuncional
5. Leyes y reglamentos pertinentes

**Tarea 3: Desarrollar procedimientos/técnicas para medir y mejorar productividad organizacional.**

#### Conocimientos de

1. Técnicas para cuantificar productividad/mediciones/indicadores clave de desempeño (key performance indicators, KPI)
2. Técnicas de análisis de datos y análisis de costo-beneficio
3. Técnicas de mejora (p. ej., programas piloto/beta, educación y capacitación)

**Tarea 4: Desarrollar, implementar y gestionar procesos de dotación de personal de seguridad y programas de desarrollo de personal a fin de lograr objetivos organizacionales.**

#### Conocimientos de

1. Técnicas de entrevistas para dotación de personal
2. Técnicas de selección y evaluación de candidatos
3. Procesos de análisis de trabajo
4. Verificación de antecedentes laborales antes de la contratación
5. Principios de evaluaciones de desempeño, revisiones 360 y coaching/tutoría
6. Técnicas interpersonales y de feedback
7. Estrategias, metodologías y recursos de capacitación
8. Estrategias y metodologías de retención
9. Gestión de talentos y planificación de sucesión

**Tarea 5: Monitorear y garantizar un clima ético aceptable conformidad con requisitos reglamentarios y cultura organizacional.**

#### Conocimientos de

1. Estándares de gobernanza
2. Normas para el comportamiento individual y corporativo
3. Principios éticos generalmente aceptados
4. Técnicas y métodos de protección de información confidencial
5. Cumplimiento legal y regulatorio

**Tarea 6: Desarrollar requisitos de desempeño y términos contractuales para vendedores/proveedores de seguridad.**

#### Conocimientos de

1. Conceptos clave en la preparación de solicitudes de propuestas y revisiones/evaluaciones de ofertas
2. Términos, medición e informes de Acuerdos de Nivel de Servicio (Service Level Agreements, SLA)
3. Principios de ley contractual, indemnización y seguro de responsabilidad
4. Procesos de supervisión para garantizar que se estén cubriendo necesidades de la organización y requisitos contractuales

## CAMPO TRES

### Investigaciones (9% -- fue 10%)

**Tarea 1: Identificar, desarrollar, implementar y gestionar funciones de investigación.**

#### Conocimientos de

1. Principios y técnicas de desarrollo de políticas y procedimientos
2. Objetivos organizacionales y colaboración interfuncional
3. Tipos de investigaciones (p. ej., incidente, mala conducta, cumplimiento, debida diligencia)
4. Recursos internos y externos para respaldar funciones de investigación
5. Preparación de informes para fines internos/externos y procedimientos legales
6. Leyes concernientes al desarrollo y gestión de programas de investigación

**Tarea 2: Gestionar o llevar a cabo la recopilación, preservación y disposición de evidencias para respaldar acciones de investigación.**

#### Conocimientos de

1. Técnicas de recopilación de pruebas
2. Protección/preservación de escenas de crímenes
3. Requisitos de cadena de custodia
4. Métodos para preservación/disposición de evidencia
5. Leyes concernientes a la recopilación, preservación y disposición de evidencia

**Tarea 3: Gestionar o llevar a cabo procesos de vigilancia.**

#### Conocimientos de

1. Técnicas de vigilancia y contra vigilancia
2. Tecnología/equipos y personal para tareas de vigilancia (p.ej. Sistemas de aeronaves no tripuladas (UAS), robóticos)
3. Leyes concernientes a la gestión de procesos de vigilancia

**Tarea 4: Gestionar y llevar a cabo investigaciones que requieran herramientas, técnicas y recursos especializados.**

#### Conocimientos de

1. Delitos financieros y relacionados con fraudes
2. Delitos de propiedad intelectual y espionaje industrial
3. Delitos contra propiedades (p.ej., incendio provocado, vandalismo, robo, sabotaje)

4. Delitos cibernéticos (p.ej., denegación de servicio distribuida (DDoS), phishing, ransomware)
5. Delitos contra personas (p.ej., violencia en el trabajo, el tráfico de personas, el acoso)

**Tarea 5: Gestionar o llevar a cabo entrevistas de investigación.**

#### Conocimientos de

1. Entrevistas y técnicas de interrogación
2. Técnicas para detectar engaños
3. Comunicación no verbal y consideraciones culturales
4. Derechos de los entrevistados
5. Componentes requeridos de declaraciones escritas
6. Consideraciones legales relacionadas con la gestión de entrevistas de investigación.

**Tarea 6: Proporcionar apoyo al consejo legal en crímenes o procedimientos civiles reales o posibles.**

#### Conocimientos de

1. Estatutos, reglamentos y jurisprudencia que rigen o afectan la industria de la seguridad y la protección de personas, propiedades e información
2. Derecho penal y procedimientos
3. Derecho civil y procedimiento
4. Derecho laboral (p. ej., información confidencial, despido indebido, discriminación, acoso)

## **CAMPO CUATRO**

### **Seguridad personal (11% -- fue 12%)**

**Tarea 1: Desarrollar, implementar y gestionar investigaciones de antecedentes para contratar, ascender y retener personas.**

#### Conocimientos de

1. Investigaciones de antecedentes y técnicas de selección de personal
2. Calidad y tipos de fuentes de información (p. ej., código abierto, redes sociales, bases de datos gubernamentales, informes de crédito)
3. Políticas y normas de selección
4. Leyes y reglamentos concernientes a selección de personal

**Tarea 2: Desarrollar, implementar, gestionar y evaluar políticas y procedimientos para proteger personas en el lugar de trabajo contra amenazas humanas (p. ej., acoso, violencia, asaltante).**

Conocimientos de

1. Técnicas y métodos de protección
2. Evaluación de amenazas
3. Técnicas de prevención, intervención y respuesta
4. Diseño e implementación de programa educativo y de sensibilización
5. Seguridad de viajes (p. ej., planificación de vuelos, amenazas globales, servicios consulados, selección de rutas, planificación de contingencias)
6. Industria/regulaciones laborales y leyes aplicables
7. Esfuerzos organizacionales para reducir el abuso de sustancias en empleados

**Tarea 3: Desarrollar, implementar y gestionar programas de protección ejecutiva.**

Conocimientos de

1. Técnicas y métodos de protección ejecutiva
2. Análisis de amenazas
3. Técnicas de gestión de enlaces y recursos
4. Selección, costos y efectividad de propiedades y contrato de personal de protección ejecutiva

## CAMPO CINCO

### Seguridad física (16% -- fue 25%)

**Tarea 1: Llevar a cabo estudios de instalaciones para determinar el estado actual de seguridad física.**

Conocimientos de

1. Equipo y personal de protección de seguridad (p.ej. Sistemas de aeronaves no tripuladas (UAS), robóticos)
2. Técnicas de realización de estudios (p.ej., revisión de documentos, lista de verificación, visita in situ, entrevistas con partes interesadas)
3. Desarrollo de planos, dibujos y esquemas
4. Técnicas de evaluación de riesgos
5. Análisis de brechas

**Tarea 2: Seleccionar, implementar y gestionar estrategias de seguridad física para mitigar riesgos de seguridad.**

Conocimientos de

1. Principios de diseño de sistema de seguridad
2. Medidas compensatorias (p. ej., políticas, tecnología, procedimientos)
3. Proceso de desarrollo de proyección presupuestaria (p. ej., tecnología, hardware, mano de obra)
4. Proceso de desarrollo y evaluación de paquete de oferta
5. Proceso de cualificación y selección de proveedor
6. Procedimientos de pruebas y aceptación final (p. ej., Procedimientos de prueba y aceptación final (por ejemplo, puesta en marcha, prueba de aceptación de fábrica)
7. Técnicas de gestión de proyectos
8. Técnicas de análisis costo-beneficio
9. Relación trabajo-tecnología

**Tarea 3: Evaluar la efectividad de medidas de seguridad física mediante pruebas y supervisión.**

Conocimientos de

1. Protección del personal, hardware, tecnología y procesos
2. Técnicas de auditoría y pruebas (p. ej., pruebas de operación)
3. Mantenimiento predictivo, preventivo y correctivo.

## CAMPO SEIS

### Seguridad de la información (14% -- fue 9%)

**Tarea 1: Realizar estudios para evaluar el estado actual de programas de seguridad de la información.**

Conocimientos de

1. Elementos de un programa de seguridad de la información, que incluye seguridad física; seguridad de procedimientos; seguridad de sistemas de información; sensibilización de empleados; y capacidades destrucción de información y recuperación
2. Técnicas de realización de estudios
3. Evaluaciones cuantitativas y cualitativas de riesgo

4. Estrategias de mitigación de riesgos (p. ej., tecnología, personal, proceso, diseño de instalaciones, etc.)
5. Métodos de análisis costo-beneficio
6. Tecnología, equipos y procedimientos de protección (p. ej., interoperabilidad)
7. Amenazas de seguridad de la información
8. Integración de instalaciones, planes del sistema, dibujos y esquemas

**Tarea 2: Desarrollar políticas y procedimientos para garantizar que se evalúe la información y se proteja contra vulnerabilidades y amenazas.**

Conocimientos de

1. Principios de gestión de seguridad de la información
2. Teoría y terminología de seguridad de la información
3. Estándares del sector de seguridad de la información (p. ej., ISO, Información Personalmente Identificable (Personally Identifiable Information, PII), Control de Protocolos de Información (Protocol Control Information, PCI, etc.)
4. Leyes y reglamentos relacionados con la gestión de registros incluyendo, retención, conservaciones por razones legales y practica de disposición (p. ej., Reglamento general de protección de datos (GDPR), información biométrica)
5. Prácticas para proteger información patentada y propiedad intelectual
6. Medidas de protección de la información que incluye procesos de seguridad, sistemas para acceso físico, y gestión de datos

**Tarea 3: Implementar y gestionar un programa integrado de seguridad de la información.**

Conocimientos de

1. Seguridad de la información que incluye confidencialidad, integridad y disponibilidad
2. Metodología de sistemas de seguridad de la información
3. Técnicas de autenticación (p. ej., multifactorial, biometría)
4. Programas de evaluación y mejora continua

5. Técnicas y prácticas de pruebas éticas de piratería y ataques
6. Técnicas de codificación y ocultación de datos (p. ej., criptografía)
7. Técnicas de integración de sistemas (p. ej., interoperabilidad, licencias, redes)
8. Metodología de análisis costo-beneficio
9. Técnicas de gestión de proyectos
10. Proceso de revisión del presupuesto (p. ej., ciclo de vida de desarrollo del sistema)
11. Proceso de evaluación y selección de proveedor
12. Aceptación final y procedimientos de pruebas
13. Tecnología de protección e investigaciones forenses
14. Programas de capacitación y sensibilización para mitigar amenazas y vulnerabilidades (p. ej., phishing, ingeniería social, ransomware, amenazas internas)

## CAMPO SIETE

### Gestión de crisis (13% -- fue 10%)

**Tarea 1: Evaluar y priorizar amenazas para mitigar posibles consecuencias de incidentes.**

Conocimientos de

1. Amenazas por tipo, probabilidad de ocurrencia y consecuencias
2. Enfoque de "todos los peligros" para evaluar amenazas (p. ej., desastres naturales, químicos, biológicos, radiológicos, nucleares, explosivos (CBRNE))
3. Análisis costo-beneficio
4. Estrategias de mitigación
5. Metodología de gestión de riesgos y análisis de impacto comercial
6. Estándares de continuidad comercial (p. ej., ASIS ORM.1, ISO 22301)

**Tarea 2: Preparar y planificar cómo la organización responderá a incidentes.**

Conocimientos de

1. Técnicas de gestión de recursos (p. ej., acuerdos de ayuda mutua, MOUs)
2. Técnicas de planificación de emergencia
3. Técnicas de evaluación de priorización y daños

4. Técnicas de comunicación y protocolos de notificación (p. ej., interoperabilidad, términos operativos comunes, sistema de notificación de emergencia)
5. Técnicas de capacitación y ejercicios (p. ej., ejercicios de mesa y de gran escala)
6. Conceptos y diseño de centros de operaciones de emergencia (emergency operations center, EOC)
7. Funciones y deberes principales en una estructura de comando de incidente (p. ej., difusión de información, enlace, oficial de información pública (PIO))

**Tarea 3: Responder a un incidente y gestionarlo.**

Conocimientos de

1. asignación de recursos
2. Principios y prácticas de gestión de EOC
3. Sistemas y protocolos de gestión de incidentes

**Tarea 4: Gestionar la recuperación de incidentes y reanudación de las operaciones.**

Conocimientos de

1. Técnicas de gestión de recursos
2. Estrategias de recuperación a corto y largo plazo
3. Recursos de asistencia para la recuperación (p. ej., ayuda mutua, programa de asistencia al empleado (EAP), asesoramiento)
4. Oportunidades de mitigación en el proceso de recuperación

---

# Investigador Profesional Certificado

---

## PCI: CERTIFICACIÓN EN INVESTIGACIONES

La credencial de Investigador Profesional Certificado (PCI®) es una prueba de conocimientos y experiencia en gestión de casos, reunión de pruebas y preparación de informes y testimonios para fundamentar hallazgos.

Obtener una certificación como PCI proporciona evidencia de un nivel avanzado de conocimientos y habilidades de investigación, que incluyen, entre otros, evaluación de casos y revisión de opciones para estrategias de gestión de casos. Valida su capacidad para reunir información a través del uso efectivo de vigilancia, entrevistas e interrogatorios.

### Requisitos de elegibilidad PCI

Los candidatos que deseen tomar el examen de PCI deben cubrir los siguientes requisitos de elegibilidad:

#### EXPERIENCIA LABORAL

##### Sin educación superior:

Cinco (5) años de experiencia en investigaciones (o si tiene el APP cuatro años), lo que incluye al menos dos años en gestión de casos\*\*

##### Con educación superior:

**Maestría o equivalente internacional** de una institución acreditada de educación superior y tener **tres (3) años de experiencia en investigaciones**, al menos dos (2) años en gestión de casos\*\*

##### O BIEN

**Título de licenciatura o equivalente internacional** de una institución acreditada de educación superior y **tener cuatro (4) años de experiencia en investigaciones**, (o si tiene el APP tres años), al menos dos (2) años en gestión de casos\*\*

\*\*Gestión de casos se define como la coordinación y dirección de una investigación usando diversas disciplinas y recursos, cuyos hallazgos se evaluarían

para establecer los hechos/hallazgos de la investigación como un todo; el proceso de gestión de investigación.

#### La certificación PCI se aplica a una gama amplia de investigaciones especializadas, lo que incluye:

Incendio provocado, Maltrato de menores, Ciencia forense, Videojuegos, Fraude de atención médica, Delitos de alta tecnología, Fraude de seguros, Prevención de pérdidas, narcóticos, Propiedades y siniestros, evaluación de amenazas, Delitos de cuello blanco, Violencia en el lugar de trabajo.

### Área de conocimiento PCI

Para obtener una certificación como PCI, un candidato debe aprobar un examen integral que consta de aproximadamente 140 preguntas de selección múltiple; 125 preguntas "en vivo" con calificación y hasta 15 preguntas previas a la prueba. Se prueba el conocimiento en tres áreas principales (campos).

La importancia de cada campo y las tareas, conocimientos y habilidades dentro de estos determinan las especificaciones del examen de PCI. El orden relativo de importancia de los campos determina el porcentaje de las preguntas totales del examen.

### CAMPO UNO

#### Gestión de casos (35%)

#### TAREA 1: Analizar casos de conflictos éticos correspondientes.

##### Conocimientos de

1. Carácter/tipos/categorías de temas éticos relacionados con casos (fiduciario, conflicto de interés, abogado-cliente, etc.)
2. La función de leyes, códigos, reglamentos y gobernanza organizacional para realizar investigaciones

**TAREA 2: Analizar y evaluar elementos, estrategias y riesgos de casos.**

Conocimientos de

1. Categorías de casos (computadora, cuello blanco, financiero, criminal, violencia en el sitio de trabajo, etc.)
2. Métodos y herramientas de análisis cualitativo y cuantitativo
3. Análisis estratégico/operacional
4. Análisis de inteligencia criminal
5. Identificación e impacto de riesgos
6. Estándar de violencia en el lugar de trabajo de ASIS

**TAREA 3: Determinar metas de investigación y desarrollar estrategias revisando las opciones de procedimiento.**

Conocimientos de

1. Flujo de casos
2. Proceso de negociación
3. Métodos de investigación
4. Análisis costo-beneficio

**TAREA 4: Determinar y gestionar recursos de investigación necesarios para abordar objetivos de casos.**

Conocimientos de

1. Proceso de control de calidad
2. Procedimientos de cadena de custodia
3. Requisitos y asignación de recursos (p. ej., personal, equipos, tiempo, presupuesto, etc.)

**TAREA 5: Identificar, evaluar e implementar oportunidades de mejora del proceso de investigación.**

Conocimientos de

1. Revisión interna (p. ej., gerencia, legal, recursos humanos)
2. Revisión externa (p. ej., entes regulativos, agencia de acreditación, etc.)
3. Recursos de enlace
4. Análisis de causa raíz y técnicas de mejora de procesos

## CAMPO DOS

### Técnicas y procedimientos de investigación (50%)

**TAREA 1: Llevar a cabo vigilancia por medios físicos, conductuales y electrónicos a fin de obtener información relevante.**

Conocimientos de

1. Tipos de vigilancia
2. Equipos de vigilancia
3. Rutinas previas a la vigilancia
4. Procedimientos para documentar actividades de vigilancia

**TAREA 2: Realizar entrevistas a personas para obtener información relevante.**

Conocimientos de

1. Técnicas de entrevistas
2. Indicadores de engaño (p. ej., comunicación no verbal)
3. Documentación de declaración del sujeto

**TAREA 3: Reunir y preservar posibles materiales de pruebas para evaluación y análisis.**

Conocimientos de

1. Oportunidades y recursos de ciencia forense
2. Requisitos de cadena de custodia
3. Métodos/procedimientos para incautación de diversos tipos de pruebas
4. Métodos/procedimientos para preservar diversos tipos de pruebas
5. Conceptos y principios de ciencia forense digital
6. Recuperación, almacenamiento y documentación de información digital
7. Conceptos y principios de operaciones informáticas y medios digitales

**TAREA 4: Realizar investigaciones por medios físicos y electrónicos para obtener información relevante.**

Conocimientos de

1. Métodos de investigación usando recursos físicos
2. Métodos de investigación usando tecnología de la información
3. Métodos de análisis de resultados de investigaciones

4. Documentación de investigación
5. Fuentes de información (p. ej., gobierno, propia, abierta)
6. Capacidades de medios digitales

**TAREA 5: Colaborar con y obtener información de otras agencias y organizaciones que posean información relevante.**

Conocimientos de

1. Fuentes de información externa
2. Técnicas de enlace
3. Técnicas para integrar y sintetizar información externa

**TAREA 6: Usar técnicas especiales de investigación para obtener información relevante.**

Conocimientos de

1. Conceptos y métodos de exámenes con polígrafo
2. Conceptos, principios y métodos de grabaciones de video/audio
3. Conceptos, principios y métodos de análisis de ciencia forense (p. ej., escritura, documentos, huellas digitales, ADN, biometría, productos químicos, fluidos, etc.)
4. Conceptos, principios y métodos de investigaciones encubiertas
5. Conceptos, principios y métodos de evaluación de amenazas
6. Uso de fuentes confidenciales
7. Conceptos, principios y métodos para aplicar equipos de tecnología de la información y herramientas de software

## **CAMPO TRES**

### **Presentación de casos (15%)**

**TAREA 1: Prepararse para informar sobre hallazgos fundamentados de investigaciones.**

Conocimientos de

1. Elementos cruciales y formato de un informe
2. de investigación
3. Terminología de investigación
4. Orden lógico de la información

**TAREA 2: Preparar y presentar testimonios.**

Conocimientos de

1. Tipos de testimonios
2. Preparación para testimonios



---

# Profesional en Seguridad Física

---

## PSP: CERTIFICACIÓN EN SEGURIDAD FÍSICA

La credencial de Profesional en Seguridad Física (PSP®) es una prueba de conocimientos y experiencia en evaluación de amenazas y análisis de riesgos; sistemas integrados de seguridad física; y la identificación, implementación y evaluación continua adecuadas de medidas de seguridad.

Obtener una certificación como PSP demuestra su experiencia para realizar estudios de seguridad física a fin de identificar vulnerabilidades y realizar análisis de costos para la selección de medidas integradas de seguridad física. Asimismo, confirma su conocimiento especializado en adquisición de sistemas, pruebas de aceptación final y procedimientos de implementación.

### Requisitos de elegibilidad PSP

Los candidatos que deseen tomar el examen de PSP deben cubrir los siguientes requisitos de elegibilidad:

#### EXPERIENCIA LABORAL

##### Sin educación superior:

Cinco años de experiencia en el campo de seguridad física\* (o si tiene el APP cuatro años)

##### Con educación superior:

**Maestría o equivalente internacional** de una institución acreditada de educación superior y tener **tres (3) años de experiencia en seguridad física\***

##### O BIEN

**Título de licenciatura o equivalente internacional** de una institución acreditada de educación superior y tener **cuatro (4) años de experiencia en seguridad física\***, (o si tiene el APP tres años).

\* Seguridad física se define como las diversas medidas físicas diseñadas para salvaguardar el personal, la propiedad y la información a tiempo completo (no se

permiten pasantías) o que lo tiene como un deber principal.

- a.) Experiencia como profesional de seguridad en la protección de activos en el sector público o en el privado, el sistema de justicia penal, inteligencia gubernamental o agencias de investigación.
- b.) Experiencia con compañías, asociaciones, gobierno u otras organizaciones que presten servicios o productos, lo que incluye firmas de asesoría, siempre y cuando los deberes y responsabilidades se relacionen de manera sustancial con el diseño, la evaluación y la aplicación de sistemas, programas o equipos, o con el desarrollo y operación de servicios para la protección de activos en el sector público o en el privado.
- c.) Experiencia como educador a tiempo completo en la facultad de una institución educativa acreditada, siempre que las responsabilidades de los cursos y otros deberes se relacionen principalmente con áreas de conocimiento pertinentes a la gestión y operación de programas de activos en el sector público o en el privado.

### Área de conocimiento PSP

Para obtener una certificación como PSP, un candidato debe aprobar un examen integral que consta de aproximadamente 140 preguntas de selección múltiple; 125 preguntas "en vivo" con calificación y hasta 15 preguntas previas a la prueba. Se prueba el conocimiento en tres áreas principales (campos).

La importancia de cada campo y las tareas, conocimientos y habilidades dentro de estos determinan las especificaciones del examen de PSP. El orden relativo de importancia de los campos determina el porcentaje de las preguntas totales del examen.

## CAMPO UNO

### Evaluación de seguridad física (34%)

#### **TAREA 1:** Desarrollar un plan de evaluación de seguridad física.

##### Conocimientos de

1. Modelos y consideraciones de evaluación de riesgos
2. Métodos de evaluación cualitativa y cuantitativa
3. Áreas clave de la instalación o activos que pueden estar involucrados en la evaluación
4. Tipos de recursos necesarios para la evaluación

#### **TAREA 2:** Identificar activos para determinar su valor, criticidad e impacto de pérdidas.

##### Conocimientos de

1. Definiciones y terminología relacionados con activos, valor, impacto de pérdidas y criticidad
2. El carácter y los tipos de activos (tangibles e intangibles)
3. Cómo determinar el valor de diversos tipos de activos y operaciones comerciales

#### **TAREA 3:** Evaluar el carácter de las amenazas a fin de que se pueda determinar el alcance del problema.

##### Conocimientos de

1. El carácter, los tipos, la gravedad y la probabilidad de amenazas y peligros (p. ej., desastres naturales, cibernéticos, eventos criminales, terrorismo, sociopolíticos, culturales, etc.)
2. Ambiente de operación (p. ej., geografía, ambiente socioeconómico, actividad criminal, etc.)
3. Posible impacto de organizaciones externas (p. ej., competidores, cadena de suministro, organizaciones en la cercanía inmediata, etc.) sobre el programa de seguridad de la instalación
4. Otros factores externos (p. ej., legal, pérdida de reputación, económicos, etc.) y su impacto en el programa de seguridad de la instalación

#### **TAREA 4:** Realizar una investigación para identificar y cuantificar vulnerabilidades de la organización.

##### Conocimientos de

1. Datos y métodos relevantes para la recopilación (p. ej., estudio de seguridad, entrevistas, informes de incidentes previos, estadísticas delictivas, problemas de empleados, problemas sufridos por otras organizaciones similares, etc.)
2. Métodos cualitativos y cuantitativos para evaluar vulnerabilidades ante posibles amenazas y peligros
3. Equipos existentes, sistemas de seguridad física, personal y procedimientos
4. Efectividad de tecnologías y equipos de seguridad implementados actualmente
5. Interpretación de planos, dibujos y esquemas de edificios
6. Estándares/reglamentos/códigos pertinentes y dónde encontrarlos
7. Factores y condiciones ambientales (p. ej., ubicación de la instalación, barreras arquitectónicas, iluminación, entradas, etc.) que afectan la seguridad física

#### **TAREA 5:** Realizar un análisis de riesgos para que se puedan desarrollar las medidas compensatorias correspondientes.

##### Conocimientos de

1. Estrategias y métodos de análisis de riesgos
2. Principios de gestión de riesgos
3. Métodos para análisis e interpretación de datos reunidos
4. Identificación de amenazas y vulnerabilidad
5. Análisis de perfiles de eventos de pérdida
6. Medidas compensatorias correspondientes relacionadas a amenazas específicas
7. Análisis de costo-beneficio (p. ej., análisis de rentabilidad [ROI], costo total de tenencia, etc.)
8. Asuntos legales relacionados con diversas aplicaciones de medidas compensatorias/seguridad (p. ej., vigilancia por video, asuntos de privacidad, información personalmente identificable, etc.)

## CAMPO DOS

### Aplicación, diseño e integración de sistemas de seguridad física (34%)

#### **TAREA 1:** Establecer requisitos de desempeño de programas de seguridad.

### Conocimientos de

1. Limitaciones de diseño (p. ej., reglamentos, presupuesto, costo, materiales, equipos y compatibilidad de sistema)
2. Aplicabilidad de resultados de análisis de riesgo
3. Terminología y conceptos de seguridad relevantes
4. Códigos, estándares y normas correspondientes
5. Requisitos funcionales (p. ej., capacidades de sistema, características, tolerancia de fallos, etc.)
6. Requisitos de desempeño (p. ej., capacidad técnica, capacidades de diseño de sistemas, etc.)
7. Requisitos operativos (p. ej., políticas, procedimientos, dotación de personal, etc.)
8. Mediciones de éxito

**TAREA 2:** Determinar medidas adecuadas de seguridad física.

### Conocimientos de

1. Medidas de seguridad estructural (p. ej., barreras, iluminación, candados, migración de explosiones, protección balística, etc.)
2. Prevención de delitos a través de conceptos de diseño ambiental (crime prevention through environmental design concepts)
3. Sistemas de seguridad electrónica (p. ej., control de acceso, vigilancia por video, detección de intrusión, etc.)
4. Dotación de personal de seguridad (p. ej., oficiales, técnicos, gerencia, etc.)
5. Selección de personal, paquetes y vehículos
6. Sistemas de notificación de emergencia
7. Principios de datos y administración de datos
8. Principios de infraestructura y seguridad de redes
9. Comunicaciones de audio de seguridad (p. ej., radio, teléfono, intercomunicador, audio IP, etc.)
10. Sistemas de seguimiento y visualización (centros/consolas de control)
11. Fuentes de alimentación alternativa de redundancia de sistemas (p. ej., batería, UPS, generadores, protección contra sobretensión, etc.)
12. Métodos de transmisión de señales y datos
13. Consideraciones concernientes a la información personalmente identificable (física/lógica/biométrica)

14. Sistemas de control de visitantes y circulación

**TAREA 3:** Diseñar sistemas físicos y preparar la documentación de construcción y adquisición.

### Conocimientos de

1. Diseñar fases (fase previa al diseño, diseño esquemático, desarrollo de diseño, documentación de construcción, etc.)
2. Elementos de diseño (cálculos, bosquejos, especificaciones, revisión de presentaciones y datos técnicos de fabricantes, etc.)
3. Estándares de especificación de construcción (p. ej., Instituto de Especificaciones de Construcción, estándares de equipos del propietario, American Institute of Architects MasterSpec, etc.)
4. Integración de sistemas (enfoque técnico, conexión con sistemas que no sean de seguridad, etc.)
5. Conceptos de gestión de proyectos
6. Programación (p. ej., gráficos de Gantt, gráficos de PERT, hitos y objetivos, etc.)
7. Estimación de costos y análisis costo-beneficio de opciones de diseño
8. Ingeniería de valor

## **CAMPO TRES**

### **Implementación de medidas de seguridad física (32%)**

**TAREA 1:** Definir criterios para la reunión antes de la oferta a fin de garantizar la integridad e idoneidad de la implementación.

### Conocimientos de

1. Componentes del paquete de oferta
2. Criterios para evaluación de ofertas
3. Criterios de cumplimiento técnico
4. Éticas en la contratación

**TAREA 2:** Adquirir sistema e implementar soluciones recomendadas para resolver problemas identificados.

### Conocimientos de

1. Funciones y procesos de gestión de proyectos a lo largo del ciclo de vida del sistema
2. Cualificación previa del proveedor (entrevistas y diligencia debida)
3. Proceso de compra

**TAREA 3:** Realizar pruebas de aceptación final e implementar/proporcionar procedimientos para seguimiento continuo y evaluación de las medidas.

Conocimientos de

1. Técnicas de inspección de instalación/mantenimiento
2. Integración de sistemas
3. Puesta en marcha
4. Resolución de problemas de instalación (listas de tareas)
5. Gestión de configuración de sistemas
6. Criterios para las pruebas de aceptación final
7. Requisitos de capacitación del usuario final

**TAREA 4:** Implementar procedimientos para seguimiento y evaluación continuos a lo largo del ciclo de vida del sistema.

Conocimientos de

1. Técnicas de inspección de mantenimiento
2. Criterios de pruebas y aceptación
3. Tipos de garantías
4. Mantenimiento, inspecciones y actualizaciones continuos
5. Requisitos de capacitación continua
6. Procesos de eliminación y reemplazo de sistemas

**TAREA 5:** Desarrollar requisitos para el personal involucrado en el apoyo del programa de seguridad.

Conocimientos de

1. Funciones, responsabilidades y limitaciones del personal de seguridad (lo que incluye personal propio [interno] y contratado)
2. Gestión de recursos humanos
3. Capacitación, desarrollo y certificación de personal de seguridad
4. Órdenes generales, posteriores y especiales
5. Uniformes y equipos de personal de seguridad
6. Procesos de revisión y mejora de desempeño del personal
7. Métodos para proporcionar capacitación y educación en concienciación sobre seguridad para personal que no sea de seguridad

## ¡ANUNCIANDO EXÁMENES SUPERVISADOS DE FORMA REMOTA!

¡ASIS ahora ofrece exámenes supervisados de forma remota que puede realizar en la comodidad de su hogar u oficina! Los exámenes serán del mismo calibre que siempre han sido, pero ahora no tiene que viajar a un centro de pruebas de Prometric para rendir el examen. Cuando programe su examen, decidirá si tomara el examen en un centro de pruebas de Prometric o mediante la opción ProProctor de Prometric. Aunque no habrá diferencia en los exámenes en sí, existen requisitos técnicos adicionales que debe tener presente si selecciona la opción ProProctor.

Lea la información sobre [Requisitos Técnicos y Otras Preguntas Frecuentes](#) e [infórmese que esperar el día del examen](#) antes de decidir qué método de prueba es mejor para usted.

## SOLICITUD DE EXÁMENES

La solicitud de certificación se puede llenar [en línea](#) .

Una vez que se haya revisado y aprobado su solicitud, recibirá un correo de Autorización para la Prueba con instrucciones sobre cómo programar su examen. Considere aproximadamente de dos a tres semanas para que su solicitud sea revisada.

**Asegúrese de que el nombre con el que envía su solicitud corresponda EXACTAMENTE al nombre de su identificación con foto emitida por el gobierno. Si no corresponden, no se le permitirá tomar el examen.**

### Documentos de solicitud que necesitará:

- ◆ Transcripción no oficial de una institución acreditada de educación superior (si corresponde)
- ◆ *Resumé* o currículum que detalle su experiencia laboral en la industria de seguridad y que se alinee con los campos del examen de certificación que usted está solicitando
- ◆ Nombres e información de contacto de tres referencias que puedan verificar su experiencia laboral
- ◆ Nombre de supervisor que pueda verificar su empleo

## Recordatorios de fechas límite

ASIS enviará recordatorios periódicos sobre las fechas límite (p. ej., programar un examen, solicitudes de información adicional, etc.); **sin embargo, cubrir y adherirse a las fechas límite son en última instancia responsabilidad del solicitante.** ASIS no puede garantizar que usted haya recibido ni leído cualquier correspondencia.

Asegúrese de que su información de contacto, especialmente su dirección de correo electrónico esté al día en su cuenta en línea. También asegúrese de colocar en lista blanca los correos electrónicos de [asisonline.org](#).

## TARIFAS DE SOLICITUD

Los exámenes de ASIS se ofrecen en centros de prueba Prometric alrededor del mundo o a través de la plataforma ProProctor de Prometric, el cual permite tomar el examen desde su casa u oficina.

Los costos de presentar una solicitud de certificación como **CPP, PCI o PSP** son:

**335 dólares miembros de ASIS**

**485 dólares no miembros**

El costo de presentar una solicitud de certificación como **APP** es:

**200 dólares miembros de ASIS**

**350 dólares no miembros**

Para recibir el descuento, [hágase miembro](#) ANTES de enviar su solicitud de examen.

**Nota: Los materiales de estudio de ASIS, que se recomiendan, pero no son obligatorios, deben comprarse por separado.**

## Reembolso

Si se rechaza su solicitud por cualquier motivo, recibirá un reembolso de su tarifa de solicitud menos una tarifa de procesamiento no reembolsable de 135 dólares.

Si se aprueba su solicitud y usted no programa o no toma el examen dentro del periodo de elegibilidad de dos años (candidatura), usted perderá tanto la tarifa de solicitud como la de la prueba.

## Retomar el examen

Los candidatos solo pueden tomar el examen tres veces en sus periodos de elegibilidad de dos años.

Asimismo, debe haber 90 días entre cada fecha de pruebas. Aquellos que no aprueben el examen tres veces pueden volver a solicitar tomar el examen después de que finalice su periodo de elegibilidad.

#### **TARIFAS PARA RETOMAR EL EXAMEN:**

**Miembros de ASIS: 225 dólares**  
**No miembros: 225 dólares**  
**(APP costo: 150 dólares)**

#### **Notificación de aprobación de ASIS**

Si usted recibe la aprobación para tomar un examen de certificación de ASIS, se le enviará por correo electrónico una carta de Autorización para la Prueba. Esta carta incluirá:

- ◆ Su identificación de elegibilidad, la cual necesitará para programar la fecha de su examen
- ◆ Instrucciones para programar su examen
- ◆ Sugerencias para estudiar

Tiene dos años y hasta tres intentos a partir de la fecha de Autorización para la Prueba para tomar y pasar su examen antes de volver a presentar una solicitud.

**Recuerde que el nombre en su identificación corresponda EXACTAMENTE al nombre en su carta de Autorización para la Prueba.**

#### **Apelar una solicitud rechazada**

Las apelaciones se considerarán en el transcurso de 30 días posteriores a la recepción por parte del solicitante de la notificación de una decisión adversa, con el día uno como la fecha del correo electrónico de notificación al solicitante. Siga las siguientes instrucciones cuando presente una apelación:

- ◆ Se debe enviar una carta en la que se explique la acción que se está solicitando a [certification@asisonline.org](mailto:certification@asisonline.org)
- ◆ Las apelaciones se deben enviar por correo postal o correo electrónico. Si se envían por correo postal, ASIS sugiere encarecidamente enviarlas por correo certificado o expreso para que se pueda rastrear el paquete
- ◆ Las apelaciones se deben enviar a la atención del Comité de Relaciones para Personas Certificadas del PCB
- ◆ Las apelaciones deben identificar la decisión adversa que se está apelando e indicar los motivos de la apelación. Además, en las cartas se debe incluir cualquier información nueva o adicional a ser considerada

#### **Las apelaciones se deben enviar a:**

PCB Certificant Relations Committee  
c/o ASIS International  
1625 Prince Street  
Alexandria, VA 22314  
Attn: Certification Department  
[certification@asisonline.org](mailto:certification@asisonline.org)

#### **Proceso de apelación relacionada para personas certificadas de la PCB**

El Comité de Relaciones para Personas Certificadas de la PCB revisará y considerará una apelación debidamente presentada a través de teleconferencia o durante sus reuniones anuales.

Cuando sea necesario, el Comité de Relaciones con Personas Certificadas de la PCB tiene la autoridad de buscar asesoría legal concerniente a cualquier aspecto de la apelación del solicitante.

El personal de certificación de ASIS, en nombre del Comité de Relaciones para Personas Certificadas del PCB solo notificará al solicitante sobre la decisión del Comité de Relaciones para Personas Certificadas del PCB y los motivos de esta, de acuerdo con lo especificado en el plazo de apelaciones. (Se debe proporcionar una respuesta inicial en el transcurso de 30 días, acusando el recibo de la queja. Debe haber un proceso de revisión de investigación de 60 días, renovable por otro periodo de 60 días con base en los hallazgos).

La decisión del Comité de Relaciones para Personas Certificadas del PCB es definitiva.

#### **PROGRAMACIÓN DE SU EXAMEN**

Después de recibir la carta de autorización, los candidatos deben dirigirse a la sede [Prometric](#) y programar su fecha de examen.

Ahora hay dos formas de realizar el examen. Usted tendrá la opción de:

1. Realizar el examen en un **centro de pruebas Prometric.**  
**O**
2. Realizar el examen utilizando su computadora personal a través de la **plataforma supervisada remota ProProctor de Prometric.** Si opta por realizar el examen con ProProctor, asegúrese de cumplir estos [requisitos técnicos](#).

**LAS COMPUTADORAS DE EMPRESA TIENEN OPCIONES DE SEGURIDAD AVANZADAS QUE NO LE PERMITEN UTILIZAR EL SOFTWARE PROPROCTOR. POR LO TANTO, NO UTILICE,**



## EL DÍA DEL EXAMEN, LA COMPUTADORA DE SU COMPAÑÍA

Nuestros exámenes se ofrecen todo el año. Recuerde que no puede programar un examen hasta que no haya recibido la aprobación para tomar el examen y haya recibido la carta de Autorización para la Prueba.

## Hacer su cita para el examen

### Programación en línea

Se puede acceder al examen en línea [prometric.com/asis](http://prometric.com/asis)

Le pedirán:

- ◆ Su identificación de elegibilidad (número de ASIS), la cual puede encontrar en su carta de Autorización para la Prueba
- ◆ Las primeras cuatro letras de su apellido.

### Programación por teléfono

Prometric: +1.800.699.4975, de lunes a viernes, de 8:00 am a 8:00 pm (EST) y sábados de 8:00 am a 4:00 pm (EST)

Prometric lo ayudará a seleccionar la fecha y ubicación óptimas para la prueba (centro de examen o remota) y responderá preguntas sobre el proceso de pruebas.

Los candidatos recibirán un número de confirmación para llevar al centro de pruebas en el momento del examen. Si programa un examen supervisado de forma remota, deberá tener este número de confirmación disponible para proporcionárselo a su supervisor.

### Confirmación de Prometric por correo electrónico

Una vez que se haya confirmado la cita de su examen, Prometric le enviará un correo electrónico con la hora del examen y el número de confirmación. **Asegúrese de imprimir esta carta y tenerla con usted el día del examen junto con dos identificaciones con foto emitidas por el gobierno** (p. ej., licencia de conducir, pasaporte, tarjeta de identificación de empleado o tarjeta de identificación estatal). Las formas aceptables de identificación secundaria incluyen tarjeta de crédito, tarjeta de cheques, tarjeta de cajero automático y ambas deben tener la firma del candidato.

### Escoger su examen (inglés o español)

Los exámenes de CPP, PCI, PSP, y APP se administran en inglés y en español. Si usted decide tomar el examen usando la plataforma remota ProProctor, **tenga en cuenta que actualmente Prometric no tiene**

**Agente de Preparación o Proctor de Examen que hablen español.** Por lo tanto, si elige esta opción deberán firmar esta exención ([Formulario de exención](#)). Para los exámenes en español, usted también recibe una traducción en inglés. Durante el proceso de solicitud en línea, usted elegirá el idioma en que desea tomar el examen (Inglés o español).

## Adaptaciones de pruebas para candidatos con discapacidades y otras consideraciones especiales

Todos los programas de ASIS cumplen con la Ley sobre estadounidenses con Discapacidades y no son discriminatorios. Si se necesitan arreglos específicos para las pruebas debido a una condición de discapacidad, los candidatos pueden solicitar adaptaciones especiales marcando la casilla "Acceso especial/para personas con discapacidad requerido" cuando completen sus aplicaciones. **Las adaptaciones especiales para pruebas deben ser aprobadas por ASIS antes de la programación de su examen. Se le solicitará proporcionar documentación antes de que ASIS pueda aprobar su solicitud.** Las solicitudes se revisan y manejan caso por caso.

## Políticas de extensión – Solicitudes de examen

ASIS no concede extensiones debido a exigencias laborales, presupuestos de compañías, condición de empleado, finanzas personales, cambios de estado civil, cambio en la dirección postal y otros motivos personales o profesionales. Se pueden conceder extensiones si hay una dificultad seria, tal como una emergencia médica importante en la familia inmediata, un desastre natural o si está en servicio militar activo y es destinado a un área remota o peligrosa. El solicitante está obligado a proporcionar documentación de las circunstancias atenuantes (p. ej., nota del médico). El personal militar deberá comprobar su situación de despliegue a través de una copia de las órdenes oficiales de despliegue. Esto no aplica a individuos que sean contratistas militares. La dificultad seria se debe documentar y debe ser verificable.

Las políticas de extensión pueden ser modificadas en corto plazo, en tiempos de crisis que afecta a muchas personas al mismo tiempo (por ejemplo, pandemia, emergencias nacionales, desastres naturales), Todos los afectados por la crisis serán notificados de los cambios de política.

## Política de cancelación

**Nota: Las políticas de cancelación se aplican a ambos centros de pruebas y de forma remota.**

Debido a cancelaciones frecuentes y reprogramaciones con notificaciones de poca antelación, Prometric ha indicado que puede haber capacidad inadecuada en los centros donde se administran los exámenes de ASIS International. Gestionar el proceso de programar y reprogramar citas es crucial para garantizar que todos los candidatos puedan obtener una cita para tomar la prueba en la fecha y hora solicitadas.

Para ofrecer la mejor experiencia para todos los candidatos, Prometric cobrará una tarifa de reprogramación/cancelación. Esta tarifa se valorará bien sea en [Prometric.com/ASIS](http://Prometric.com/ASIS) si el candidato reprograma o cancela en línea, o vía telefónica al +1.800.699.4975 a través del servicio al cliente de Prometric.

Si un candidato reprograma o cancela 31 días o antes del día programado para la prueba, no hay ningún cargo.

Si un candidato reprograma o cancela entre 4 y 30 días antes del día programado para la prueba, se aplica una tarifa de 62.50 dólares por reprogramación. Candidatos no pueden reprogramar su fecha de examen faltando tres o menos días para la prueba. Todas las tarifas de reprogramación o cancelación se deben pagar directamente a través de Prometric.

Si un candidato no se presenta y no se adhiere a los procedimientos anteriores, se pierde por completo la tarifa para tomar la prueba y este debe enviar una solicitud de certificación a ASIS junto con la tarifa de 200 dólares para volver a presentar la prueba.

**Las políticas de cancelación se aplican tanto al centro de pruebas como a los exámenes supervisados de forma remota. Prometric NO hace ninguna excepción a esta regla.**

### “No presentación”

Si usted no cancela ni reprograma su examen, se considerará que no se presentó y perderá todas las tarifas para tomar la prueba. ASIS comprende que las emergencias ocurren. Si no aparece para su examen por cualquiera de los siguientes motivos, tendrá 14 días a partir de la fecha de la cita para proporcionar la siguiente documentación y reprogramar su examen:

1. Fallecimiento en la familia inmediata
  - ◆ Certificado de defunción o nota del médico, los cuales deben estar firmados por un médico o director de funeraria autorizados e incluir información de contacto
2. Lesión grave o incapacitante (para usted o un miembro de la familia inmediata)  
Nota del médico con fecha de la visita médica.  
La documentación:
  - ◆ Debe explicar que el inicio de la enfermedad o lesión fue 24 horas antes del examen
  - ◆ Debe estar firmado por un médico autorizado e incluir información de contacto
  - ◆ No necesita incluir detalles de la enfermedad o emergencia, pero el médico debe indicar que la condición evitó que el candidato tomará el examen
3. Comparecencia en tribunal o deber de jurado
  - ◆ Comparecencias ante el tribunal o como jurado, citaciones, las cuales deben incluir la fecha y su nombre
4. Servicio militar activo
  - ◆ Carta de servicio activo, la cual debe incluir la fecha y su nombre

ASIS se reserva el derecho de solicitar pruebas adicionales para respaldar su motivo para no presentarse para el examen. Si ASIS y Prometric aceptan la explicación, se le permitirá programar una cita nueva dentro de su periodo de elegibilidad sin pagar la tarifa de reprogramación.

## EL DÍA DEL EXAMEN

No importa si está tomando el examen en un centro de pruebas o lo realiza mediante supervisión remota, se le pedirá que siga procedimientos de registro específicos.

### Procedimientos de Registro en un Centro Prometric

Planifique llegar 30 minutos antes de la cita para permitir tiempo para el proceso de registración. Si va a manejar, identifique la localización exacta del centro, la mejor ruta y donde estacionar.

Si llega con más de 15 minutos de retraso, el personal del centro de pruebas de Prometric puede decidir no otorgarle asiento si hacerlo interrumpiría a los otros participantes. Si esto ocurre, **no se reembolsarán** sus



tarifas de inscripción. **No hay excepciones a esta regla.**

### Qué Llevar y qué No Llevar

Por motivos de seguridad de la prueba, todos los objetos personales como bolsos, bolsas de libros, etc. se deben colocar en un casillero durante el examen, así que limite lo que lleve al centro de pruebas.

Las joyas que no sean anillos de boda o compromiso están prohibidas y todos los accesorios para el cabello están sujetos a inspección. Absténgase de usar pinzas, peines, pasadores, cintillos y otros accesorios ornamentales para el cabello, dado que le pueden prohibir usarlos en el salón del examen y se le solicitará que los guarde en su casillero. La violación del protocolo de seguridad puede tener como consecuencia confiscación de dispositivos prohibidos y presentación de un informe ante las autoridades locales.

### Procedimiento de Registro para el Examen Supervisado Remoto

Los candidatos que realicen el examen supervisado de forma remota deben permitir 15 minutos para preparar el entorno donde presentara el examen.

El registro para los exámenes supervisados de forma remota es un proceso de dos pasos:

#### PRIMER PASO – Verificación de sus Documentos de Identificación

**Captura de Imágenes** – utilizando el software ProProctor, usted tomara y capturara una imagen de su rostro.

**Captura de ID** – Luego, usted capturara una foto de sus dos documentos de identificación. (Ver Documentos de Identificación Aceptables)

**Lista de Control** – Para asegurarse de que está listo para lanzar el examen revise la lista de control que aparecerá en su pantalla

#### SEGUNDO PASO – Conozca a su Agente de Preparación

**Verificación de Información Personal** – Tendrá un chat de video con el agente para confirmar su información personal

**Control Ambiental 360°** – Usando su cámara web, le mostrará al agente un escaneo de 360 grados de su habitación y su mesa. Usted necesitara un espejo de

mano de tamaño mediano o grande para que el agente pueda ver su computador. **IMPORTANTE: SU COMPUTADOR PORTATIL NO DEBE DE ESTAR CONECTADO A LA BASE DE CONEXION.**

**Verificación de la persona candidata** - El agente le pedirá que se ponga de pie para hacer un escaneo de su persona. Este escaneo incluirá, pero no se limita a, la realización de una revisión de la manga, el bolsillo y los anteojos. Además, se le pedirá que dé la vuelta a todos los bolsillos. **NOTA: VACÍE SUS BOLSILLOS ANTES DE INICIAR EL PROCESO DE REGISTRO.**

### Documentos de Identificación Aceptables

Debe contar con lo siguiente, o de lo contrario no será admitido al examen:

**Dos formas de identificación**, una de las cuales debe ser una identificación con foto emitida por el gobierno (tal como pasaporte, licencia de conducir, ID de empleado); **ambas deben tener la firma del candidato.**

Solo su primer nombre y apellido en su carta de aprobación de ASIS y las identificaciones debe corresponder EXACTAMENTE o NO le será permitido el ingreso a la prueba. Esto incluye nombres abreviados o separados con guion.

**Correo electrónico y número de confirmación de Prometric** (del correo electrónico que recibe cuando programa su examen).

Si va a realizar la prueba fuera de su país de residencia, debe contar con pasaporte válido. Si va a realizar la prueba en su país de residencia, puede presentar pasaporte, licencia de conducir, o una ID nacional (ID militar es no aceptable) No se aceptarán identificaciones vencidas.

**Si no trae la identificación adecuada, no se le permitirá tomar el examen y perderá la tarifa del examen.**

### Medidas de seguridad

El personal para la presentación de pruebas de Prometric no tiene permitido palpar a un candidato durante el proceso de registro de entrada y usarán una vara de seguridad (similar a las que usan en aeropuertos) para comprobar que los candidatos no llevan ningún tipo de dispositivo para hacer trampa. Esto además de pedirles a los candidatos que volteen los bolsillos de sus pantalones.

- ◆ El desempeño de los candidatos se supervisa y se puede analizar para detectar fraude. ASIS no validará las calificaciones de exámenes de

candidatos que violen las medidas de seguridad.

- ◆ Si ofrece o recibe ayuda durante el examen, será acompañado fuera del centro de pruebas y se le informará a la PCB. No se calificará su examen, no se reembolsarán las tarifas del examen y se le prohibirá tomar el examen de nuevo.
- ◆ Todos los materiales del examen, lo que incluye todas las preguntas y todas las formas del examen, están protegidos por copyright y son propiedad de ASIS. Cualquier distribución de estos materiales a través de reproducción o comunicación oral o por escrito está estrictamente prohibida y es penada por la ley.

#### **Alternativas para distracciones sonoras**

Los candidatos pueden llevar sus propios tapones pequeños para oídos al centro. Debe presentar los tapones a los supervisores del centro para que los examinen antes de ingresar al salón de la prueba. Tome en cuenta que los candidatos no pueden traer sus propios reductores de ruido estilo audífonos sin una adaptación especial.

Los candidatos pueden optar por usar audífonos reductores de ruido disponibles en los sitios de Prometric. Estos son audífonos grandes estilo "aeropuerto" y pueden ser incómodos cuando se usan por un periodo largo. No hay reductores de ruido estilo tapón pequeño disponibles en los centros Prometric.

No está permitido comer, beber ni fumar durante el examen. Si trae un abrigo o suéter, se le solicitará que lo lleve puesto en todo momento en el salón del examen. No se permiten visitantes en el centro de pruebas y no se proporciona cuidado de niños.

#### **Durante el examen**

Una vez que haya completado el proceso de registro de entrada, se le asignará una estación de prueba o un agente remoto.

#### **En la estación de prueba**

- ◆ Se le proporcionará, dos pizarras que se pueden borrar para tomar notas y marcadores de borrado en seco.
- ◆ No se permiten hojas sueltas, diccionarios, libros, notas ni otras ayudas personales en el área de la prueba.
- ◆ Para usar el baño, los candidatos deben notificárselo al administrador del centro de

pruebas o al agente remoto; sin embargo, si toma un receso, no se detiene el tiempo del examen.

- ◆ No hay ningún receso programado.
- ◆ No se permite ninguna conversación sobre la prueba con el agente ni otros examinandos.

#### **Su oficina u hogar debe cumplir con los siguientes requisitos**

- ◆ El lugar donde tomara el examen debe ser en un cuarto, bien iluminado, libre de ruidos e interrupciones.
- ◆ Otra persona no debe estar presente en el cuarto durante el examen. Si esto ocurre, su examen se terminará y/o sus resultados serán invalidados.
- ◆ Su mesa y el área circundante deben estar libres de bolígrafos, papel, dispositivos electrónicos.
- ◆ Se permite dos pañuelos de papel en su mesa, pero será inspeccionado por el agente antes que empiece el examen.

Un tutorial de 15 minutos en pantalla lo orientará en las características del ambiente de prueba computarizada. Cuando haya completado el tutorial, usted comenzará el examen.

#### **Consejos para tomar la prueba**

- ◆ ¡Relájese! Reducir el estrés físico lo ayudará a estar más alerta.
- ◆ Encuentre el ritmo correcto de trabajo. No se apure ni vaya demasiado lento. Encuentre un ritmo que sea cómodo.
- ◆ Siga las instrucciones y trabaje con cuidado.
- ◆ Lea todas las opciones para cada pregunta antes de marcar la respuesta.
- ◆ Salte las preguntas difíciles. Puede marcar las preguntas para regresar más adelante. Si todavía no está seguro, haga una suposición informada.
- ◆ Las preguntas sin contestar y las preguntas incorrectas se cuentan ambas como respuestas incorrectas. Su calificación se basa en el número total de respuestas correctas.
- ◆ Esté atento al cronómetro del examen (en su pantalla). Si no entrega la prueba antes de que se acabe el tiempo, el examen se apagará automáticamente cuando se acabe el tiempo.

## Resultados del examen

Una vez que entregue su examen, será dirigido a una encuesta corta antes de que reciba su calificación. Recibirá el resultado preliminar de su calificación por correo electrónico en el correo electrónico que proporcionó a Prometric (permite hasta cinco horas para recibir su resultados). Su calificación oficial le será enviada aproximadamente tres semanas después de haber tomado el examen También puede llamar a servicios al cliente de Prometric al +1.800.853.6769 para que le envíen su informe de calificaciones.

**Si no recibe un informe de calificación, debe contactar al departamento de certificación de ASIS en el transcurso de cinco (5) días calendario a partir de la fecha de la prueba. No hacerlo dentro del tiempo especificado tendrá como consecuencia una tarifa para reemplazar el informe de calificaciones.**

### Encuesta al final del examen

Después de que entregue su examen y **antes de que reciba sus resultados preliminares**, se le pedirá que complete una encuesta corta. Esta es una oportunidad para contarle tanto a ASIS como a Prometric sobre su experiencia en la prueba. Sus comentarios no incidirán en la calificación de su examen. ASIS usa los resultados de esta encuesta para mejorar sus procedimientos de certificación.

## Emergencias por clima

Si el clima severo, desastres naturales u otros incidentes similares hacen que el centro de pruebas sea inaccesible o inseguro, puede que se re programe o cancele el examen (sin costo alguno para el candidato). Para verificar su centro de pruebas, consulte el sitio web con cierres de ubicaciones de Prometric en <https://www.prometric.com/closures>

## ¿CÓMO ESTÁN ESTRUCTURADOS LOS EXÁMENES?

Todos los exámenes de certificación de ASIS son de selección múltiple. Usted tendrá cuatro respuestas posibles, de las cuales solo una será la correcta. A continuación, se presenta el número de ítems (preguntas) por examen y el tiempo máximo que tiene para completar y entregar el examen:

- ◆ CPP – 200 “en vivo” (calificables) y 25 ítems previos a la prueba (sin calificar). 4 horas.
- ◆ PSP – 125 “en vivo” (calificables) y 15 ítems previos a la prueba (sin calificar). 2.5 horas.

- ◆ PCI – 125 “en vivo” (calificables) y 15 ítems previos a la prueba (sin calificar). 2.5 horas.
- ◆ APP – 100 “en vivo” (calificables) y 25 ítems previos a la prueba (sin calificar), 2 horas

Habrán un cronómetro en la pantalla de su computadora mostrándole cuánto tiempo le queda. Asegúrese de haber contestado todos los ítems. Cualquier ítem sin contestar se marcará como incorrecto.

## Calificación del examen

Todos los exámenes de ASIS usan el método de “**calificación escalada**” para determinar el punto de aprobación de cada pregunta del examen. Antes de que se presente una pregunta en el examen, se hace una prueba previa. Esto le permite a los psicometristas ponderar el desempeño de cada pregunta y su nivel de dificultad.

Las preguntas individuales reciben una puntuación ponderada/escalada con base en el nivel de dificultad. Una puntuación escalada se transforma en una puntuación bruta del examen (el número de preguntas del examen contestadas correctamente). Para interpretar cualquier calificación del examen, se requiere un marco de referencia uniforme. Las puntuaciones escaladas proporcionan ese marco de referencia con base en el estándar adoptado por ASIS concerniente al nivel de conocimientos necesarios para aprobar los exámenes sin consideración de la versión del examen tomada.

Esto explica por qué cada examen tiene un número diferente de preguntas por campo. **Se requiere una calificación escalada de al menos 650 para aprobar el examen.** Una calificación escalada no es ni el número de preguntas que usted contestó correctamente ni el porcentaje de preguntas que contestó correctamente.

La puntuación para aprobar se estableció a través de un procedimiento sistemático (estudio de establecimiento de estándar) que empleó el juicio de un grupo representativo de profesionales certificados por ASIS con la asistencia de expertos de desarrollo de exámenes de Prometric. Este grupo de expertos en la materia recomendó un estándar a ASIS sobre lo que un profesional de seguridad mínimamente competente necesita saber sobre el contenido evaluado para obtener una calificación aprobatoria. Cada **ÍTEM** de la prueba computarizada se califica de manera electrónica con base en cómo se desempeñó el ítem durante la prueba previa. Debido a este

método es virtualmente imposible que la calificación de su examen sea incorrecta; por tanto, **los exámenes computarizados no son elegibles para una calificación manual.**

## ESTUDIAR PARA EL EXAMEN

Los exámenes de certificación de ASIS se basan en la experiencia. Por tanto, mientras más experiencia práctica tenga relacionada con el cuerpo de conocimientos, más éxito tendrá en el examen. Todo el mundo tiene una preferencia de estudio diferente: a algunos les gusta estudiar por su cuenta y otros prefieren un enfoque de estudio en grupo. ASIS no requiere ningún método de estudio, pero sí ofrecemos las siguientes recomendaciones:

Comience con el cuerpo de conocimientos. Lea cada campo con atención y haga una evaluación honesta de su propia experiencia. Esto lo ayudará a decidir dónde necesita concentrar sus esfuerzos de estudio.

- ◆ [Autoevaluación de ASIS para Exámenes de CPP, PCI, PSP o APP](#)
- ◆ ASIS ofrece además [Conjuntos de referencia](#) para cada certificación. Nuestros escritores y revisores de ítems usan estos mismos materiales para consultar las respuestas correctas en nuestros exámenes\*
- ◆ ASIS ofrece muchas oportunidades de estudio para cada examen. Visite nuestra sección [Education](#) del sitio web [asisonline.org](#) para obtener más información. \*
- ◆ Muchos [Capítulos de ASIS](#) ofrecen grupos de estudio.
- ◆ \* ASIS no garantiza el éxito en los exámenes porque usted estudie usando nuestros materiales.

## Recursos de preparación para el examen

ASIS ofrece una cantidad de recursos para ayudarlo a estudiar para su certificación. Se invita a los candidatos a consultar el siguiente material de referencia mientras se preparan para su examen de CPP, PCI o PSP. Después de revisar con atención los campos de estudio e identificar necesidades individuales de aprendizaje, los candidatos pueden usar referencias y oportunidades de estudio adicionales según sea necesario.

### PROFESIONAL CERTIFICADO EN PROTECCIÓN

La *Protección de Activos* (POA) y el set de estándares y normas de ASIS componen el material de referencia de la certificación como CPP. Cada uno está

disponible para compra individual o como el conjunto que se describe a continuación.

#### • Protección de activos

POA es una referencia completa que cubre una gama de temas técnicos y de gestión que proporcionan la soluciones necesarias para satisfacer las demandas de seguridad del siglo 21. El POA se actualizó [en junio de 2021](#).

- [POA en línea](#)
- [POA impresa](#)

#### • Estándares y Normas

Los estándares ASIS son recomendado por la industria prácticas sobre preocupaciones específicas inherentes a la seguridad industria y proporcionar herramientas y procesos para implementación. Junto con POA, estos siete estándares y normas constituyen la referencia de CPP. Estándares: CSO, ORM.1, WVPI AA, PAP; Normas: GSRA, IAP, PBS

- [Free Online Access for ASIS Members](#)
- [Standards & Guidelines CPP softcover bundle](#)

### INVESTIGADOR PROFESIONAL CERTIFICADO

Dos publicaciones componen ahora los materiales de referencia para la certificación como PCI.

- [POA Investigations volume](#) (reemplaza Manual del Investigador Profesional)
- ASIS Estándar de investigaciones como referencia.
  - [Free Online Access for ASIS Members](#)
  - [Investigations Standard for nonmembers](#)

### PROFESIONAL EN SEGURIDAD FÍSICA

Las publicaciones indicadas a continuación componen el material de referencia para la certificación como PSP. Disponible en set de tapa dura o tapa blanda. Cada título está disponible para compra individual.

- POA Physical Security volume (Reemplaza Seguridad Física Principios)
- [Implementación de Sistemas de Protección Física: Una Guía Práctica](#), 2ª edición
- **ASIS Business Continuity Guideline: A Practical Approach**
  - [Free Online Access for ASIS Members](#)
  - [Guideline for nonmembers](#)
- **ASIS Physical Asset Protection Standard (Reemplaza ASIS Facilities Physical Security Measures Guideline)**
  - [Free download for ASIS members](#)
  - [Standard for nonmembers](#)

## PROFESIONAL DE PROTECCION ASOCIADO

Las publicaciones a continuación componen el material de referencia de la certificación APP, el cual incluye cinco Normas y tres volúmenes de los libros de Protección de activos de ASIS.

Las publicaciones están disponibles individualmente o en paquetes.

### Cinco Normas

- Physical Asset Protection
- Security and Resilience in Organizations and their Supply Chains - Requirements with Guidance
- Investigations
- Workplace Violence and Active Assailant – Prevention, Intervention, and Response
- Risk Assessment

### Protection of Assets Volumes (actualizado [en junio de 2021](#))

- Protection of Assets: Business Principles
- Protection of Assets: Crisis Management
- Protection of Assets: Security Management (Nota: Reemplaza el POA Information Security volume)

### ASIS offers three pricing bundles for the APP:

- [APP Standards Bundle](#)
- [Protection of Assets Bundle for the APP Certification](#)
- [APP Complete Reference Set](#)

ASIS ofrece otros elementos preparatorios (como flash Cards y manuales de estudio. Obtenga estas publicaciones en [ASIS Store](#).

### CURSOS DE REPASO

ASIS ofrece tanto cursos presenciales como de revisión en línea para ayudarlo a prepararse para el examen. Muchos Capítulos de ASIS ofrecen además grupos de estudio. Comuníquese con el Capítulo de ASIS en su área para obtener más información.

*Ni la Junta de Certificación Profesional (PCB) ni el personal de certificación de ASIS tienen alguna involucración en los cursos de revisión de ASIS. Los instructores de los cursos de revisión no tienen acceso a preguntas reales del examen.*

### Herramientas gratuitas de estudio

Los exámenes de práctica contienen ítems que alguna vez aparecieron en exámenes reales de certificación, pero que ya no aparecen. Use estos exámenes de

práctica para familiarizarse con cómo aparecen los ítems en los exámenes actuales.

[Examen de práctica CPP](#)

[Examen de práctica PCI](#)

[Examen de práctica PSP](#)

## APROBÉ EL EXAMEN, ¿AHORA QUÉ?

Después de completar con éxito el examen, recibirá un certificado con su nombre y número de certificación.

Además, recibirá un correo electrónico de Acclaim (socio de acreditación digital de ASIS) con el título "You've earned a badge from ASIS International". El mensaje le proporcionará una invitación e instrucciones para reclamar su insignia digital. Considere dos a cuatro semanas para recibir su certificado y credencial digital.

¡Lleve ahora su certificación con orgullo! ¡Agréguela a las firmas de sus correos electrónicos, tarjetas de presentación y cuentas de redes sociales!

### Recertificación

Todas las personas que tengan una certificación de ASIS deben **renovar la recertificación cada tres años** obteniendo créditos de Educación Profesional Continua. La recertificación les indica a sus colegas, compañeros y empleador que usted está comprometido con mantenerse al día en la profesión de seguridad. Para obtener más información sobre los requisitos de recertificación, descargue la [Guía de recertificación](#).

## POLÍTICAS DE SOLICITUD Y DE PERSONAS CERTIFICADAS DE ASIS

### Declaración de Imparcialidad

La Junta de Certificación Profesional de ASIS (PCB) y el personal de certificación comprenden la importancia de la imparcialidad y los conflictos en la gestión de actividades de certificación. Cuando se hacen negocios con miembros y personas que no son miembros, todas las personas implicadas en el proceso de certificación mantendrán un nivel alto de conducta ética y evitarán conflictos de interés relacionados con el desempeño de sus deberes.

Se evitará cualquier acción o compromiso que podrían dar la apariencia de:

- ◆ Usar cargos para ganancia personal



- ◆ Dar tratamiento preferencial inadecuado
- ◆ Obstaculizar la eficiencia
- ◆ Perder independencia o imparcialidad
- ◆ Afectar de manera adversa la confianza de los miembros de ASIS en la integridad de las operaciones de certificación.

La PCB y el personal de certificación se asegurarán de que, al tratar con sus miembros, son y permanecerán imparciales y confidenciales.

### **Código de Responsabilidad Profesional de la Certificación de ASIS**

- ◆ Los profesionales de seguridad certificados de ASIS y los solicitantes de certificación debe acatar el Código de Responsabilidad Profesional y aceptar:
- ◆ Realizar deberes profesionales en conformidad con la ley y los más altos principios morales. El no cumplimiento incluye cualquier acto u omisión que equivalga a conducta no profesional y se considere perjudicial para la certificación.
- ◆ Observar los preceptos de honradez, honestidad e integridad.
- ◆ Ser leales, competentes y diligentes al asumir sus deberes profesionales.
- ◆ Salvaguardar información confidencial y privilegiada y ejercitar el cuidado debido para evitar su divulgación inadecuada.
- ◆ No dañar maliciosamente la reputación profesional ni la práctica de colegas, clientes o empleados.

Cualquier acto que se considere perjudicial para la certificación puede resultar en la denegación de la aprobación para tomar el examen de certificación o medidas disciplinarias de la Junta de Certificación Profesional (PCB), que podría incluir la revocación de la certificación. Entre tales actos se pueden encontrar, entre otros:

- ◆ Dar declaraciones o información falsas o engañosas cuando solicite tomar el examen de certificación o renovar la certificación.
- ◆ Cualquier acto u omisión que viole las disposiciones del Código de Responsabilidad Profesional de la Certificación de ASIS.
- ◆ Cualquier acto que viole las leyes penales o civiles de cualquier jurisdicción.
- ◆ Cualquier acto que sea la base adecuada para la suspensión o revocación de una licencia profesional.

- ◆ Cualquier acto u omisión que viole las Reglas y Procedimientos Disciplinarios de la PCB.
- ◆ No cooperar con la Junta de Revisión Profesional de la PCB para el desempeño de sus labores de investigación de cualquier acusación contra un solicitante o persona certificada actual.
- ◆ Dar declaraciones falsas o engañosas a la PCB concernientes a un solicitante o persona certificada actual.

### **Declaración de Elegibilidad Continua para Certificación**

**Todos los solicitantes de un examen de ASIS firmarán la siguiente declaración sobre la solicitud.**

Mediante mi firma, declaro que la información que presento aquí dentro o en cualquier documentación acompañante o posterior requerida es verdadera y precisa a mi leal saber y entender.

Comprendo que las personas que solicitan certificación como Profesional Certificado en Protección (CPP), Investigador Profesional Certificado (PCI) o Profesional en Seguridad Física (PSP) o personas que hayan sido certificadas por ASIS International, están sujetas a los requisitos de elegibilidad de ASIS International para certificación, recertificación y el Código de Responsabilidad Profesional de Certificación de ASIS.

Comprendo que a fin de mantener mi certificación debo renovar la certificación cada tres años al presentar una cantidad de créditos de Educación Profesional Continua (Continuing Professional Education, CPE), de conformidad con la política y procedimientos de ASIS para presentar dichos informes. Comprendo que los créditos de CPE se pueden obtener a través de programas educativos, cursos y otras actividades, y que toda la CPE debe adecuarse a los requisitos especificados en la Guía de Recertificación de ASIS International. Comprendo además que cada cierto tiempo ASIS International puede modificar sus requisitos, políticas y procedimientos para incluir certificación inicial, recertificación y el Código de Responsabilidad Profesional.

También comprendo que puedo estar sujeto a una auditoría en cualquier momento y que ASIS International se reserva el derecho de emprender acciones si no cumplo con los procedimientos de auditoría.

Mientras soy titular de una certificación de ASIS International, acepto notificarle a ASIS International de inmediato por escrito si no cumplo con alguno de sus requisitos para obtener o mantener una certificación o renovarla, lo que incluye casos como, entre otros, no trabajar más en la profesión, no tener más la condición de retirado de por vida debido a que regresé a trabajar a tiempo completo, no obtener el número de créditos de CPE necesarios para mantener o renovar una certificación o haber sido sancionado –lo que incluye suspensión, expulsión o pérdida de credencial– como resultado de que se haya determinado que he violado el Código de Responsabilidad Profesional. También acepto notificarle a ASIS International por escrito sobre cualquier cambio de dirección o nombre en el transcurso de treinta (30) días a partir de que el cambio se haga efectivo.

Si me lo solicitan, ASIS International puede verificar mi condición de certificación.

## REVOCACIÓN DE CERTIFICACIÓN

Las certificaciones están sujetas a revocación por cualquiera de las siguientes causas:

- ◆ La persona certificada no debió haber sido elegible para recibir dicha certificación, independientemente de si se conocía los hechos o no o pudieran ser comprobados por la PCB al momento de la emisión de dicha certificación.
- ◆ La persona certificada haya hecho alguna declaración falsa de hechos en la solicitud de dicha certificación o cualquier otra declaración o representación conectada con la solicitud de certificación.
- ◆ Se ha hallado que la persona certificada ha adoptado prácticas poco éticas o ha sido condenada por un delito grave.

No se revocará ninguna certificación a menos que se sigan los siguientes procedimientos:

- ◆ Se haya enviado por correo registrado a la persona certificada una copia de los cargos en su contra y la información concerniente al evento o eventos de los cuales surgieron dichos cargos. Dicha notificación deberá indicar que no se tomarán acciones contra la persona certificada hasta después de una audiencia, a menos que la persona no solicite una audiencia o no ofrezca una defensa en el transcurso de 15 días.
- ◆ La persona certificada tiene al menos 15 días para preparar una defensa.

- ◆ Se celebra una audiencia por dichos cargos, ante un panel designado, momento en el cual la persona recibe una oportunidad completa de ser escuchada en su propia defensa, lo que incluye el derecho de ser presentado por consejo, de interrogar testigos y de examinar materiales que documenten dichos cargos. Se proporcionará apoyo de adaptaciones para las personas elegibles.
- ◆ El panel determinará inicialmente si la certificación de la persona se debe revocar o no. La determinación inicial del panel, lo que incluye toda la evidencia presentada en la audiencia, será revisada. Después de la revisión, la PCB puede afirmar, revertir, modificar o devolver la determinación original del panel.
- ◆ Si la determinación inicial del panel es revocar la certificación de la persona, y la mayoría de la PCB, en sesión oficial, afirma la determinación del panel de que la persona no es elegible para mantener la certificación, entonces se emitirá una notificación. Si se revoca su certificación, se le pedirá que regrese su certificado y deje de usar la designación.

## DESIGNACIÓN DE POR VIDA.

Los CPP, PCI o PSP pueden ser considerados para una designación de por vida, si la persona cumple con los siguientes criterios:

- ◆ Ser un CPP, PCI o PSP en buena situación
- ◆ Haber mantenido una certificación por doce años consecutivos precedentes a la fecha de solicitud
- ◆ Estar jubilado actualmente (“jubilado” se define como el cese por completo de cualquier empleo o práctica relacionados con seguridad o representación de empleo o práctica semejantes) y no tener interés legal, financiero ni comercial con cualquier forma de empleo o práctica relacionadas con seguridad, según lo definido en el campo de examen de certificación correspondiente.
- ◆ Haber pagado la tarifa de recertificación para el periodo actual

Si una persona certificada de por vida vuelve a la práctica profesional después del término de su último periodo de certificación regular, debe presentar una solicitud de recertificación demostrando la culminación exitosa de sesenta (60) créditos CPE en el periodo previo de tres años o de volver a tomar y aprobar con éxito el examen de certificación correspondiente. Las personas certificadas de por

vida son elegibles automáticamente para presentar el examen de sus certificaciones previas, sin la necesidad de enviar materiales de respaldo adicionales.

Si le conceden una certificación de por vida, usted recibirá un nuevo certificado con su nueva designación. Para mostrar esta nueva designación, usted usará los siguientes: CPP – Certificado de por vida (jubilado), PSP – Certificado de por vida (jubilado) o PCI – Certificado de por vida (jubilado). No puede usar la designación sin estas descripciones calificativas.

**Para solicitar una certificación de por vida**, complete y envíe la [solicitud](#) por correo electrónico a [certification@asisonline.org](mailto:certification@asisonline.org). **Hay una tarifa de \$100 para aplicar.**

## **DIVULGACIÓN DE INFORMACIÓN DE CANDIDATOS Y PERSONAS CERTIFICADAS**

Está prohibida la divulgación a terceros de información confidencial de candidatos y personas certificadas de ASIS, a menos que ASIS obtenga un permiso por escrito del candidato o de la persona certificada para hacerlo. El consentimiento de divulgar información debe incluir a quién se le puede divulgar la información del candidato o persona certificada y cuál información se puede divulgar.

## **CERTIFICADOS DE ASIS**

Todos los certificados relacionados con las designaciones de CPP, PCI, PSP y APP son propiedad exclusiva de ASIS International. Los certificados suspendidos y revocados deben ser devueltos a los directores de certificación de ASIS International en el transcurso de 15 días posteriores a haber recibido la notificación de suspensión o revocación. La persona previamente certificada debe dejar de usar de inmediato las designaciones de ASIS International y eliminarlas de todas sus comunicaciones impresas, electrónicas o de otro tipo.

## **INTERVENCIÓN DE TERCEROS**

La Junta Profesional de Certificación (PCB) establece las políticas de los programas de certificación ASIS. Existe un "muro" apropiado y requerido entre las actividades de certificación de ASIS y la Junta Global de ASIS, el personal de ASIS y el CEO de ASIS. Solo el PCB puede adjudicar asuntos de certificación.

Debido a que los programas de certificación ASIS están acreditados por ANSI según la norma ISO / 17024, involucrar a terceros para tratar de cambiar una decisión tomada por el PCB está en contra de los requisitos de acreditación de ANSI y esto pone en peligro el estado de acreditación de ASIS como un organismo de certificación internacional. Además, ASIS se esfuerza por aplicar consistentemente sus políticas para ser justos con todos. Admitir "reglas" especiales para algunos simplemente no es justo para los más de 10,000 certificados que siguen las políticas. Finalmente, debido a los requisitos de confidencialidad, el PCB y el equipo de certificación solo pueden comunicarse directamente con el certificador; y no comparte información con terceros.

## **PRESENTAR UNA QUEJA**

Las quejas concernientes a los requisitos de elegibilidad, la programación de pruebas, las políticas y procedimientos del programa de certificación de ASIS, el personal de certificación u otra persona certificada se le pueden presentar por escrito al director de certificación. Envíe su queja por escrito y por correo postal o correo electrónico a [certification@asisonline.org](mailto:certification@asisonline.org).

Proporcione suficientes pruebas objetivas para fundamentar la queja. El director de certificación o los miembros del Comité de Relaciones con Personas Certificadas de la PCB revisarán todas las quejas. Se le enviará el acuse de recibo de su queja e incluirá acciones que ASIS tomará para solventar la situación. Cuando se haya resuelto la queja, la persona que la presentó recibirá una notificación con los resultados de la revisión.

## **SOBRE NUESTRO SOCIO DEL EXAMEN**

Prometric es una compañía independiente de realización de pruebas actualmente bajo contrato con ASIS para administrar los exámenes de certificación de ASIS. Los expertos en Prometric trabajan de cerca con ASIS y la Junta de Certificación Profesional (PCB) para desarrollar exámenes que evalúen con precisión el conocimiento que el candidato tiene sobre la profesión de seguridad. Prometric califica el examen, envía los resultados a ASIS y almacena los registros de exámenes. El personal de ASIS y la PCB supervisan las actividades de Prometric para garantizar que todos los aspectos del proceso de examen cubran los estándares de certificación.