ASIS INTERNATIONAL
Advancing Security Worldwide®

ASIS International

Manual de Certificación

CPP PCI
PSP APP

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

TELÉFONO: **+1 703.519.6200**

SITIO WEB 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

SOBRE ESTE MANUAL

Este manual contiene todas las políticas y procedimientos de los cuatro programas de certificación de ASIS. Todas las personas que postulen a un examen de certificación de ASIS deben cumplir con la información contenida en este manual. *Este manual se actualizó el 6 de enero 2025 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 CPP®, PCI®, PSP®, o APP® transmite a sus compañeros, empleados y empleadores que usted posee experiencia relevante y sustancial, así como competencia demostrada y probada.

PROGRAMA RECONOCIDO INTERNACIONALMENTE Y ACREDITADO GLOBALMENTE

La Junta de Certificación de ASIS se desarrollan y mantienen a través de un proceso riguroso ejemplificado a través de la acreditación del programa por parte de American National Standards Institute (ANSI) de acuerdo con la International Organization for Standardization (ISO) 17024.

THE SAFETY ACT DESIGNATION

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.

JUNTA DE CERTIFICACIÓN PROFESIONAL DE ASIS (PCB)

Los programas de certificación ASIS están regidos por la Junta de Certificación Profesional (PCB). La PCB establece todas las políticas relacionadas con el programa, lo que incluye requisitos de elegibilidad, contenido del examen (Area de Conocimiento- BOK) y desarrollo del examen. Todos los directores del PCB están certificados como CPP, PCI, PSP y/o APP.

Los directores de la 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 directores 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 verdaderamente, necesita una certificación que fomente el crecimiento profesional. Uno que sea reconocido mundialmente como el estándar de profesionalismo. Necesita una certificación de la Junta 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 profesionales.

PROGRAMAS DE CERTIFICACIÓN VS. 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 (CPE) que se pueden usar para prepararse para programas de certificación de ASIS o para renovar la certificación.

¿POR QUÉ ELEGIR 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 su base de conocimientos
- Lo mantiene al día con las mejores prácticas
- Logra reconocimiento global como un experto altamente motivado en su campo.

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

Hoy, profesionales de seguridad de 105 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 CERTIFICACIÓN ES LA ADECUADO PARA USTED?

ASIS ofrece cuatro certificaciones para quienes se desempeñan en campos relacionados con la seguridad:

- Certified Protection Professional (CPP)
- Professional Certified Investigator (PCI)
- Physical Security Professional (PSP)
- Associate Protection Professional (APP)

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

- El programa **Certified Protection Professional (CPP)** está diseñado para aquellos que han demostrado competencia en todas las áreas de gestión de seguridad.
- El programa **Professional Certified Investigator (PCI)** está diseñado para aquellos cuyas responsabilidades incluyan gestión de casos, recopilación de pruebas y preparación de informes y testimonio para fundamentar los hallazgos.
- El programa **Physical Security Professional (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 **Associate Protection Professional (APP)** está diseñado para aquellos con 1 año o más de experiencia en seguridad renumerada.

ASIS recomienda encarecidamente revisar el área de conocimiento de 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 área 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 deben:

- Tener un empleo a tiempo completo en una función relacionada con la seguridad. No se requiere empleo actual.
- Se puede contar hasta un año de experiencia en pasantías para este requisito, siempre que sea directamente relevante para la certificación y de tiempo completo (las pasantías pueden ser no remuneradas para CPP, PCI y PSP).
- 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 41).
- Aceptar cumplir con las políticas de los programas de certificación de ASIS como se describe en este manual y la Guía de Recertificación ASIS.

Los exámenes de certificación de ASIS se basan en la experiencia. La experiencia se define como estar personalmente involucrado en seguridad o prevención de pérdidas a tiempo completo o como un deber primordial. 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.

CAMBIOS EN LOS REQUISITOS DE ELEGIBILIDAD EN 2023

(Actualizado 20 Feb 2024) En 2023, La PCB votó a favor de reducir ligeramente los requisitos de elegibilidad para el programa de certificación APP. Estos cambios se realizaron después de una revisión exhaustiva de la audiencia prevista para la APP, los datos de los candidatos y las tendencias de certificación de la APP. Después del análisis, la PCB votó a favor de cambiar el requisito de experiencia para la APP requiera 1 o más años de experiencia en seguridad compensada, sin educación superior, a partir del 1 de noviembre de 2023.

REQUISITOS DE ELEGIBILIDAD

	APP*	PSP	PCI	CPP
Sin Educación Superior	1 año	5 (4) años	5 (4) años	7 (6) años
Título de Licenciatura	1 año	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

Notes: Nota: Los números entre paréntesis indican los años para aquellos que tienen la certificación APP.
*APP requiere 1 año o más de experiencia en seguridad renumerada.

ASSOCIATE PROTECTION PROFESSIONAL

APP CERTIFICACION EN FUNDAMENTOS 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 **Associate Protection Professional (APP®)** está destinada a aquellos con un año o más años de experiencia renumerada en seguridad. Si ha obtenido otra certificación relacionada aprobada, puede ser elegible para ser aceptado para presentar el examen APP con solo seis meses de experiencia remunerada en seguridad. El examen medirá el conocimiento del profesional sobre los fundamentos de seguridad, las operaciones de negocios, la gestión de riesgos y la gestión de respuesta *(Actualizado el 20 de febrero 2024)*

REQUISITOS DE ELEGIBILIDAD APP

EXPERIENCIA EN SEGURIDAD	EDUCACION
Seis meses	Con una certificación relacionada aprobada
Un año	Sin educación superior

APP IMPACTO EN LOS REQUISITOS DE ELEGIBILIDAD PARA OTRAS CERTIFICACIONES DE ASIS

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

1. Aun se deben cumplir los otros requisitos de elegibilidad para el CPP, PCI o PSP (p. ej., un cargo de responsabilidad o gestión de casos)
2. La designación APP caducara si un candidato obtiene la designación CPP (no se 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**

CPP	Con Maestria	Con Licenciatura	Sin Educación Superior
Experiencia actual requerida	5 años	6 años	7 años
Con APP	4 años	5 años	6 años

PCI	Con Maestria	Con Licenciatura	Sin Educación Superior
Experiencia actual requerida	3 años	4 años	5 años
Con APP	3 años	3 años	4 años

PSP	Con Maestria	Con Licenciatura	Sin Educación Superior
Experiencia actual requerida	3 años	4 años	5 años
Con APP	3 años	3 años	4 años

ÁREAS DE CONOCIMIENTO APP

Para obtener la designación APP, un candidato debe aprobar un examen integral que consta de aproximadamente 125 preguntas de selección múltiple. El candidato seleccionara una respuesta de las cuatro opciones ofrecidas. En total, hay 100 preguntas "en vivo" las cuales serán calificadas y hasta 25 preguntas preliminares no calificadas.

Se evalúan el conocimiento en cuatro áreas principales (dominios).

La importancia de cada dominio y las tareas, conocimientos y habilidades que componen determinan las especificaciones del examen APP. El orden relativo de importancia de los dominios determina el porcentaje de las preguntas totales del examen.

DOMINIO 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

DOMINIO 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

6. 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

1. Principios y técnicas de desarrollo de políticas/procedimientos

2. Normas para el comportamiento individual y corporativo

3. Técnicas de mejora (por ejemplo, programas piloto, educación y capacitación)

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

Conocimiento de

1. Estrategias, métodos y técnicas de comunicación
2. Técnicas para cuantificación de productividad/métricas/indicadores de desempeño clave (KPI, por sus siglas en inglés)
3. Principios, herramientas y técnicas de gestión de proyectos
4. 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

1. Estrategias y metodologías de retención
2. Procesos de análisis de empleo
3. Colaboración multifuncional
4. Estrategias, métodos y técnicas de capacitación
5. Gestión de talentos y planificación de sucesiones
6. 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

1. Técnicas de comunicación y Retroalimentación interpersonales
2. Leyes y reglamentos pertinentes
3. Normas de gobierno y cumplimiento
4. Principios éticos generalmente aceptados
5. 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

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

DOMINIO TRES

GESTIÓN DE RIESGO (25%)

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

Conocimiento de

1. Estrategias de gestión de riesgos (por ejemplo, evitar, asumir/aceptar, transferir, mitigar, etc.)
2. Metodología de gestión de riesgos y análisis de impacto comercial
3. 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

1. Amenazas potenciales a una organización
2. Enfoque holístico para evaluar amenazas de todos los peligros
3. 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

DOMINIO 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

CERTIFIED PROTECTION PROFESSIONAL

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 cumplir 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.

*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 la designación CPP, un candidato debe aprobar un examen integral que consta de aproximadamente 225 preguntas de selección múltiple. El candidato seleccionara una respuesta de las cuatro opciones ofrecidas. En total, hay 200 preguntas "en vivo" los cuales son calificados y hasta 25 preguntas preliminares. Se evalúan el conocimiento en siete áreas principales (dominios).

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

DOMINIO UNO

PRINCIPIOS Y PRÁCTICAS DE SEGURIDAD (22%)

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

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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.)

DOMINIO DOS

BPRINCIPIOS Y PRÁCTICAS COMERCIALES (15%)

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

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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 regulativo

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

Conocimiento 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

DOMINIO TRES

INVESTIGACIONS (9%)

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

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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)

DOMINIO CUATRO

SEGURIDAD PERSONAL (11%)

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

Conocimiento 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).**

Conocimiento 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.**

Conocimiento 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

DOMINIO CINCO

SEGURIDAD FÍSICA (16%)

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

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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

DOMINIO SEIS

SEGURIDAD DE LA INFORMACIÓN (14%)

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

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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)

DOMINIO SIETE

GESTIÓN DE CRISIS (13%)

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

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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.**

Conocimiento 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

PROFESSIONAL CERTIFIED INVESTIGATOR

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 cumplir los siguientes requisitos de elegibilidad:

Sin educación superior:

Cinco (5) años de experiencia en investigaciones (o cuatro años si tiene el APP), 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 tres años si tiene el APP), 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 perdidas, narcóticos, propiedad y accidentes, 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 los cuales son calificados y hasta 15 preguntas preliminares. Se evalúan el conocimiento en tres áreas principales (Dominios).

La importancia de cada dominio 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.

En 2022/2023, ASIS realizó un estudio de análisis de trabajo para garantizar que las áreas de conocimientos PCI aún represente los conocimientos y las habilidades necesarias para ser un investigador exitoso. Las preguntas del examen sobre la nueva información obtenida comenzarán a aparecer en el examen a principios del año 2024 *(Actualizado el 20 de febrero de 2024).*

A continuación, se incluye las áreas de conocimientos actualizado. Para revisar los cambios aprobados,

consulte el documento Especificaciones de la prueba PCI *(Actualizaciones de JA 2023).*

DOMINIO UNO

RESPONSABILIDAD PROFESIONAL (28%)

TAREA 1: **Analizar el caso en busca de conflictos éticos aplicables.**

Conocimiento de

1. Naturaleza/tipos/categorías de temas éticos relacionados con casos (p. ej., abogado-cliente, conflicto de intereses, fiduciario, posible sesgo/discriminación por doble función, competencia en áreas específicas)
2. El papel de leyes, reglamentos, códigos, políticas organizacionales y directrices administrativas aplicables a la realización de investigaciones

TAREA 2: **Evaluar los elementos del caso, estrategias y riesgos.**

Conocimiento de

1. Categorías de casos (p. ej., civiles, cibernéticos, penales, internos, financieros, violencia en el lugar de trabajo)
2. Métodos y herramientas de análisis cualitativos y cuantitativos
3. Análisis estratégico/Operativo
4. Análisis de inteligencia criminal
5. Identificación de riesgos e impacto
6. Identificación de partes interesadas

TAREA 3: **Determinar los objetivos de la investigación y elaborar una estrategia.**

Conocimiento de

1. Tipo de caso inicialmente previsto (p. ej., administrativo, penal)
2. Análisis costo-beneficio
3. Opciones de procedimiento
4. Flujo de casos / plan de investigación
5. Métodos de investigación

TAREA 4: **Determinar y gestionar los recursos de investigación.**

Conocimiento de

1. Recursos necesarios (p. ej., equipos, enlaces internos y externos, personal)
2. Asignación de recursos (p. ej., presupuesto, tiempo)
3. Prácticas de gestión de casos (p. ej., procedimientos para la cadena de custodia, requisitos de documentación, cierre de casos)

TAREA 5: **Identificar, evaluar e implementar mejoras en el proceso de investigación.**

Conocimiento de

1. Técnicas de mejora de procesos (p. ej., análisis de brechas (gap), técnicas de gestión de proyectos)
2. Revisión interna (p. ej., recursos humanos, enlaces internos, temas legales, gestión)
3. Revisión externa (p. ej., agencia de acreditación, enlaces externos, organismos reguladores).
4. Recursos de investigación (p. ej., expedientes administrativos, inteligencia de fuentes abiertas (OSINT))

5. Herramientas de investigación (p. ej., software de gestión de casos, software de recopilación de datos, software forense digital)

DOMINIO DOS

TÉCNICAS Y PROCEDIMIENTOS DE INVESTIGACIÓN (52%)

TAREA 1: **Llevar a cabo la vigilancia por medio físicos, conductuales y electrónicos.**

Conocimiento de

1. Autorización y restricciones de la vigilancia (p. ej., consideraciones legales, tipos de vigilancia)
2. Herramientas de vigilancia (p. ej., analítica, equipos, metadatos, software, registros del sistema)
3. Actividades de pre-vigilancia (p. ej., evaluación previa, logística, planificación, recursos)
4. Procedimientos para documentar las actividades de vigilancia (p. ej., soluciones de gestión de casos, consideraciones de privacidad, almacenamiento seguro)

TAREA 2: **Llevar a cabo entrevistas a personas.**

Conocimiento de

1. Tipos de entrevistas (p. ej., asunto, testigo, persona de interés)
2. Técnicas de entrevistas
3. Consideraciones especiales (p. ej., entorno, salud mental del entrevistado, traductor, presencial o remota, etc.)
4. Indicadores de engaño (p. ej., evasión, comunicación no verbal, elección de palabras
5. Documentación de la declaración del sujeto (p. ej., audio, video, escrito)
6. Consideraciones de representación (p. ej., defensa de menores, asesoría legal, representación sindical)

TAREA 3: **Reunir y preservar pruebas.**

Conocimiento de

1. Fuente de las pruebas (p. ej., biológica, digital, física)
2. Métodos/procedimientos para la obtención de diversos tipos de pruebas
3. Métodos/procedimientos para la preservación de diversos tipos de pruebas (p. ej., biológicas, operaciones informáticas, medios digitales)
4. Consideraciones y requisitos de la cadena de custodia (p. ej., física, digital, biológica)

TAREA 4: **Realizar investigaciones por medios físicos, digitales y electrónicos.**

Conocimiento de

1. Métodos de investigación utilizando recursos físicos, de tecnología de la información y tecnología operacional
2. Fuentes de información (p. ej., bases de datos, medios digitales, gobierno, fuentes abiertas, privados)
3. Métodos de análisis de los resultados de la investigación
4. Documentación de investigación (p. ej., conclusiones)

TAREA 5: **Colaborar y obtener información de otras agencias y organizaciones.**

Conocimiento de

1. Fuentes de información externas
2. Desarrollo y mantenimiento de enlaces
3. Técnicas de enlace (p. ej., formal e informal)
4. Técnicas para utilizar y sintetizar información externa (p. ej., documentada vs indocumentada, protección de fuentes y sensibilidades, redacción)

TAREA 6: **Utilizar técnicas de investigación.**

Conocimiento de

1. Consideraciones legales, administrativas y organizativas
2. Conceptos, principios y métodos de grabación de video/audio
3. Conceptos, principios y métodos de análisis forense (p. ej., biológico, digital, físico)
4. Conceptos, principios y métodos de investigaciones encubiertas
5. Conceptos, principios y métodos de evaluación de amenazas y riesgos
6. Conceptos, principios y métodos de aplicación de tecnologías IT/OT
7. Uso de fuentes confidenciales

DOMINIO TRES

PRESENTACIÓN DE CASOS (20%)

TAREA 1: **Prepara un informa para fundamentar los resultados de la investigación.**

Conocimiento de

1. Elementos críticos y formato de un informe de investigación (p. ej., consideraciones de audiencia/legales, tratamiento de la privacidad y confidencialidad, tipos de informe)
2. Terminología de investigación
3. Secuenciación lógica de la información

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

Conocimiento de

1. Tipos de testimonio (p. ej., audiencias administrativas, procedimientos penales y civiles, declaraciones)
2. Preparación para el testimonio (p. ej., ensayo previo al juicio)
3. Mejores prácticas testimoniales

PHYSICAL SECURITY PROFESSIONAL

PSP: CERTIFICACIÓN EN SEGURIDAD FÍSICA

La credencial de **Profesional en Seguridad Física (PSP®)** es una prueba de conocimientos y experiencia en evaluación de seguridad física; aplicación, diseño e integración de sistemas de seguridad física; e implementación 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 cumplir los siguientes requisitos de elegibilidad:

Sin educación superior:

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

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).

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" "en vivo los cuales son calificados y hasta 15 preguntas preliminares. Se evalúan el conocimiento en tres áreas principales (dominios).

La importancia de cada dominio 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.

En 2022, ASIS realizó un estudio de análisis de trabajo para garantizar que las áreas de conocimientos PSP aún represente los conocimientos y las habilidades necesarias para ser un gerente de seguridad física exitoso. Solo se realizaron cambios menores para mayor claridad e indicadas a continuación en color **verde**.

Las preguntas del examen sobre la nueva información obtenida comenzaron a aparecer en el examen a fines de 2023 *(Actualizado el 20 de febrero de 2024).*

DOMINIO UNO

EVALUACIÓN DE LA SEGURIDAD FÍSICA (34%)

TAREA 1: **Desarrollar un plan de evaluación de la seguridad física**

Conocimiento de

1. Area clave o identificación de activos críticos
2. Modelos y consideraciones de evaluación de riesgos (p. ej., evaluación del riesgo de dentro

hacia fuera, de fuera hacia dentro, de un lugar específico, enfoque funcional)

3. Métodos de evaluación cualitativa y cuantitativa

4. Tipos de recursos y directrices necesarios para la evaluación (p. ej., partes interesadas, presupuesto, equipos, políticas, estándares)

TAREA 2: **Identificar los activos para determinar su valor, su criticidad y el impacto de la pérdida.**

Conocimiento de

1. Definiciones y terminología relacionadas con los activos, el valor, el impacto de las pérdidas y la criticidad

2. Naturaleza y tipo de activos (tangibles e intangibles)

3. Cómo determinar el valor de diversos tipos de activos y operaciones comerciales

TAREA 3: **Evaluar la naturaleza de las amenazas y peligros para poder determinar el riesgo.**

Conocimiento de

1. La naturaleza, tipos, gravedad y probabilidad de amenazas y peligros (p. ej., desastres naturales, ciberdelitos, hechos delictivos, terrorismo, sociopolíticos, culturales)

2. Entorno operativo (p. ej., geografía, ambiente socioeconómico, actividad delictiva, contramedidas de seguridad existentes, nivel de riesgos de seguridad)

3. Posible impacto de organizaciones externas (p. ej., competidores, organizaciones en la proximidad inmediata) en el programa de seguridad de la instalación

4. Otros factores internos y externos (p. ej., pérdida de reputación, económicos, cadena de suministro) y su impacto en el programa de seguridad de la instalación.

TAREA 4: **Realizar una evaluación para identificar y cuantificar las vulnerabilidades de la organización.**

Conocimiento de

1. Datos y métodos relevantes para la recopilación (p. ej., encuesta de seguridad entrevistas, informes de incidentes, estadísticas de delitos, asuntos relativos al personal, problemas experimentados por organizaciones similares)

2. Eficacia de las tecnologías/equipos, personal y procedimientos de seguridad actuales

3. Interpretación de planos, dibujos y esquemas del edificio

4. Normas/reglamentos/códigos aplicables y dónde encontrarlos

5. Factores y condiciones ambientales (p. ej., ubicación de las instalaciones, barreras arquitectónicas, iluminación, entradas) que repercuten en la seguridad física

TAREA 5: **Realizar un análisis de riesgos para desarrollar contramedidas.**

Conocimiento de

1. Estrategias y métodos de análisis de riesgos

2. Principios de gestión de riesgos

3. Análisis e interpretación de los datos recopilados

4. Identificación de amenazas/peligros y vulnerabilidades

5. Análisis de perfiles de eventos de pérdida (p. ej., consecuencias)

6. Contramedidas apropiadas relacionadas con riesgos específicos

7. Análisis de costo-beneficio (p. ej., retorno de la inversión [ROI], costo total de propiedad)

8. Consideraciones legales y regulatorias relacionadas con diversas contramedidas/aplicaciones de seguridad (p. ej., videovigilancia, cuestiones de privacidad, información personalmente identificable, seguridad de la vida)

DOMINIO DOS

APLICACIÓN, DISEÑO E INTEGRACIÓN DE SISTEMAS DE SEGURIDAD FÍSICA (35%)

TAREA 1: **Establecer los requisitos de funcionamiento del programa de seguridad.**

Conocimiento de

1. Restricciones de diseño (p. ej., normativas, presupuesto, materiales, compatibilidad de los sistemas)

2. Incorporación de los resultados del análisis de riesgos en el diseño

3. Terminología de seguridad relevante (p. ej., lista de verificación, pruebas de campo)

4. Conceptos de seguridad relevantes (p. ej., CPTED, defensa en profundidad, las 4D: disuadir, detectar, demorar, denegar)

5. Códigos, normas y directrices aplicables

6. Requisitos operativos (p. ej., políticas, procedimientos, dotación de personal)

7. Requisitos funcionales (p. ej., capacidades del sistema, características, tolerancia a fallos)

8. Requisitos de funcionamiento (p. ej., capacidades técnicas, diseño de las capacidades del sistema)

9. Métricas de éxito

TAREA 2: **Determinar las contramedidas de seguridad física apropiadas.**

Conocimiento de

1. Medidas de seguridad estructurales (p. ej., barreras, iluminación, cerraduras, mitigación de explosiones, protección balística)

2. Prevención del delito a través del diseño ambiental (CPTED)

3. Sistemas electrónicos de seguridad (p. ej., control de acceso, videovigilancia, detección de intrusión)

4. Personal de seguridad (p. ej., oficiales, técnicos, gerencia, administración)

5. Inspección de personas, paquetes y vehículos

6. Sistema de notificación de emergencias (p. ej., notificaciones masivas, megafonía, intercomunicador bidireccional)

7. Principios de almacenamiento y gestión de datos (p. ej., en la nube, en la instalación, redundancia, retención, permisos de usuario, información de identificación personal, requisitos reglamentarios)

8. Principios de infraestructura de red y seguridad física de la red (p. ej., red en anillo o token ring, LAN/WAN, VPN, DHCP versus estática, TCP/IP)

9. Seguridad en comunicaciones de audio (p. ej., radio, teléfono, intercomunicador, audio IP)

10. Monitorización y visualización de sistemas (p. ej., centros/consolas de control, estación central de monitoreo)

11. Fuentes de energía primaria y de respaldo (p. ej., red, batería, UPS, generadores, alternativa/renovable)

12. Métodos de transmisión de señales y datos (p. ej., cobre, fibra, inalámbrico)

13. Políticas de gestión de visitantes y proveedores

TAREA 3: **Diseño de sistemas de seguridad física y documentación del proyecto.**

Conocimiento de

1. Fases del diseño (p. ej., prediseño, desarrollo esquemático, construcción, documentación)

2. Elementos de diseño (p. ej., cálculos, planos, especificaciones, revisión, datos técnicos)

3. Normas de especificaciones de construcción (p. ej., Instituto de Especificaciones de la Construcción, Normas de equipamiento del propietario, Instituto Norteamericano de Arquitectos (AIA), MasterSpec)

4. Integración de sistemas

5. Conceptos de gestión de proyectos

6. Planificación (p. ej., carta Gantt, malla PERT, hitos y objetivos)

7. Estimación de costos y análisis costo-beneficio de las opciones de diseño (p. ej., ingeniería de valor)

DOMINIO TRES

IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD FÍSICA (31%)

TAREA 1: **Bosquejar los criterios para la reunión previa a la licitación.**

Conocimiento de

1. Proceso de Licitación (p. ej., visitas al sitio, solicitud de información (RFI), solicitudes de sustitución, reunión previa a la licitación)

2. Tipos de paquetes de licitación (p. ej., solicitud de propuesta (RFP), solicitud de presupuesto (RFQ), llamado a licitación (IFB), proveedor único)

3. Componentes del paquete de licitación (p. ej., cronograma del proyecto, costos, personal, documentación, alcance del trabajo)

4. Criterios para evaluación de ofertas (p. ej., costo, experiencia, cronograma, certificación, recursos)

5. Criterios de conformidad técnica

6. Ética en la contratación

TAREA 2: **Desarrollar un plan de adquisición de bienes y servicios.**

Conocimiento de

1. Evaluación y selección de proveedores (p. ej., entrevistas, proceso de debida diligencia, comprobación de referencias)

2. Funciones y procesos de gestión de proyectos

3. Proceso de Adquisición

TAREA 3: Gestionar la implementación de bienes y servicios.

Conocimiento de

1. Técnicas de instalación e inspección
2. Integración de sistemas
3. Puesta en marcha
4. Resolución de problemas de instalación (p. ej., listas de comprobación)
5. Gestión de la configuración de los sistemas (p. ej., planos de obra terminada)
6. Criterios de la prueba de aceptación final (p. ej., prueba de aceptación del sistema, prueba de aceptación en fábrica)
7. Requisitos de capacitación de los usuarios finales

TAREA 4: Establecer requisitos para el personal involucrado en el apoyo del programa de seguridad.

Conocimiento de

1. Funciones, responsabilidades y limitaciones del personal de seguridad (incluido el personal de seguridad propio [interno] y contratado).
2. Gestión de recursos humanos (p. ej., establecimiento de indicadores clave de rendimiento (KPI), revisión del desempeño, procesos de mejora, contratación, incorporación, disciplina progresiva)
3. Desarrollo profesional del personal de seguridad (p. ej., formación, certificación)
4. Órdenes generales, de puesto y especiales
5. Uniformes y equipo del personal de seguridad
6. Capacitación y educación en materia de seguridad para el personal que no es de seguridad

TAREA 5: Supervisar y evaluar el programa a lo largo del ciclo de vida del sistema.

Conocimiento de

1. Mantenimiento de sistemas y de hardware (p. ej., preventivo, correctivo, actualizaciones, calibración, acuerdos del servicio)
2. Tipos de garantía (p. ej., fabricante, instalación, piezas de recambio, extendida)
3. Capacitación continua sobre el sistema (p. ej., actualizaciones del sistema, certificación del fabricante)
4. Evaluación del sistema y proceso de sustitución

TOMANDO 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 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.

DEBIDO A LAS SEGURIDADES DE FIREWALL NO SE RECOMIENDA QUE PRESENTE SU EXAMEN SUPERVISADO DE FORMA REMOTA EN LA COMPUTADORA DE SU COMPAÑÍA. 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.

Los problemas comunes que se encuentran durante un examen supervisado de forma remota incluyen:

- Conexión a Internet débil o problemas de ancho de banda.
- La cámara o el micrófono no funcionan.
- Identificación adecuada no proporcionada al Supervisor

Si su ancho de banda de Internet es deficiente y pierde la conexión a Internet y/o su cámara web y micrófono no funcionan y no puede completar su examen, perderá la tarifa de examen pagada y deberá pagar una tarifa de repetición del examen para realizar el examen dentro de su período de elegibilidad de dos años. **Solicitudes aceptadas a partir del 6 de enero de 2025, se aprobarán con un período de elegibilidad de un año.** *(Actualizado el 1 de octubre de 2024)*

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

Documentación en idiomas extranjeros debe estar acompañado con una traducción en inglés.

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 certification@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.

La Junta Global de ASIS aprobó tarifas especiales para aquellas personas que viven en Mercados Emergentes, según lo identificado por el Banco Mundial.

Consulte la lista de países identificados como mercados emergentes por el Banco Mundial.

Para recibir el descuento, hágase miembro ANTES de enviar su solicitud de examen.

TARIFAS PARA EL EXAMEN CPP, PCI, Y PSP *(Actualizado 6 de enero 2025):*

Miembro de ASIS: $580

Mercado Emergente 1: $480

Mercado Emergente 2: $460

No miembro de ASIS: $910

Mercado Emergente 1: $720

Mercado Emergente 2: $680

TARIFA PARA EL EXAMEN APP ES *(Actualizado 6 de enero 2025):*

Miembro de ASIS: $300

Mercado Emergente 1: $270

Mercado Emergente 2: $260

No miembro de ASIS: $620

Mercado Emergente 1: $510

Mercado Emergente 2: $490

Nota: Todas las tarifas incluyen $160 no reembolsables *(Actualizado 6 de enero 2025).*

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 $160 dólares *(Actualizado 6 de enero 2025).*

No se emitirá reembolsos 90 días después de la fecha de aprobación de la solicitud. *(Actualizado el 1 de octubre 2024)*

RETOMAR EL EXAMEN

Los candidatos solo pueden tomar el examen tres veces en su periodo de elegibilidad de un año. Asimismo, debe haber 60 días entre cada fecha de pruebas. Aquellos que no reprueben el examen tres veces o cuyo periodo de elegibilidad finalice, pueden volver a postular presentado una nueva solicitud *(Actualizado el 6 de enero 2025)*.

Los candidatos que paguen la tarifa para retomar el examen recibirán una carta de Autorización por correo electrónico con instrucciones para programar nuevamente su examen en la plataforma de Prometric.

TARIFA PARA RETOMAR EL EXAMEN CPP, PCI, Y PSP *(Actualizado 6 de enero 2025).*

Miembro y No miembro de ASIS: $480

Mercado Emergente 1: $360

Mercado Emergente 2: $330

TARIFA PARA RETOMAR EL EXAMEN APP:

Miembro y No miembro de ASIS: $250

Mercado Emergente 1: $240

Mercado Emergente 2: $220

NORMAS DE AJUSTE DE TARIFAS

Las tarifas de certificación y recertificación de ASIS se evaluarán cada dos años.

Se considerará en la evaluación de tarifas los contratos con los proveedores, las tasas de inflación de los Estados Unidos y otros costos operativos. Los ajustes de tarifas se enfocarán en recuperar los costos operativos de certificación y recertificación, mantener o mejorar el procesamiento de solicitudes y las métricas de servicio al cliente, mientras se minimiza el impacto en los candidatos y certificantes *(Actualizado 1 de octubre 2024)*

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 (ASIS ID), 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 que reciba la carta de Autorización para tomar y pasar su examen antes de volver a presentar una nueva solicitud.

Solicitudes aceptadas a partir del 6 de enero de 2025, se aprobarán con un período de elegibilidad de un año y los candidatos deben esperar 60 días entre cada fecha de examen. *(Actualizado el 1 de octubre de 2024)*

Recuerde que el nombre en su identificación oficial corresponda EXACTAMENTE al nombre en su carta de Autorización.

APELAR UNA DECISION

Hay un procedimiento de apelación disponible para cualquier persona que haya solicitado o recibido una certificación de ASIS y desee impugnar cualquier decisión adversa. Esta política se aplica únicamente a los aspectos procesales del proceso de acreditación. Las áreas que no están sujetas a apelación se identifican con más detalle en la sección titulada “Principios generales relacionados con las apelaciones” al final de esta sección. Cualquier persona que no presente una solicitud por escrito de apelación dentro del plazo requerido renunciará al derecho de apelación. La presentación de una apelación no dará lugar a ninguna acción discriminatoria contra el apelante.

Durante el proceso de certificación, las personas pueden apelar ciertas decisiones tomadas por ASIS. Algunos ejemplos de apelaciones incluyen:

- Decisiones sobre elegibilidad
- Límites de tiempo para la elegibilidad
- Interpretaciones de CPE para la recertificación
- Condenas penales
- Uso no autorizado

Para apelar una decisión sobre su certificación, se requiere:

- 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.

- Se debe enviar una carta en la que se explique la acción que se está solicitando a certification@asisonline.org.

    - Se deben enviar a la atención del Comité del Certificant Relations 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

Proceso de Apelación del Comité del Certificant Relations del PCB

- Una vez recibido la apelación por escrito, el Equipo de Certificación de ASIS registrará la apelación en la base de datos correspondiente.

- El Director de Certificación evaluará la apelación para verificar que cumpla con las políticas de presentación de apelaciones de ASIS.

- La apelación y los materiales relacionados se enviarán al Comité del Certificant Relations del PCB para tomar una decisión. El comité hará su mejor esfuerzo para tomar una decisión dentro de los 90 días posteriores a la recepción de la apelación. ASIS puede hacer que un asesor legal revise esta decisión antes de enviarla al apelante.

- La decisión de la apelación se registrará en la hoja de hoja de seguimiento de apelaciones y en la cuenta del apelante.

- Siempre que sea posible, el apelante recibirá informes de progreso del proceso y se le notificará por escrito la decisión del Comité de Relaciones con Certificadores de PCB y las razones de esa decisión dentro de los 30 días posteriores a la revisión.

- Las decisiones del comité son definitivas y no pueden ser apeladas.

Principios generales relacionados con las apelaciones

- Se considerarán las apelaciones por dificultades según se describe en las Politicas de Extensión de ASIS.

- Se considerarán las apelaciones si el apelante considera que el personal de ASIS cometió un error en la revisión de la solicitud.

- Los requisitos de elegibilidad de ASIS, así como las demás políticas del programa de certificación, no son apelables.

- La puntuación de aprobación del examen no se puede apelar.

PROGRAMACIÓN DE SU EXAMEN

Después de recibir la carta de autorización, los candidatos deben dirigirse a la sede de Prometric para programar su fecha de examen.

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

1. Presentar el examen en un **centro de pruebas Prometric**. O

2. Presentar el examen utilizando su computador personal a través de la **plataforma de supervisión a distancia ProProctor de Prometric**. Si opta por realizar el examen por este medio, asegúrese de poder cumplir estos requisitos técnicos.

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

HACER SU CITA PARA EL EXAMEN

Programación en línea

Ya sea que desee realizar el examen en un centro de prueba o la plataforma de supervisión a distancia programe su cita de examen en línea en pro-metric.com/asis

Le pedirán:

- Su número de ASIS, el cual puede encontrar en su carta de Autorización.
- 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 examen.

Los candidatos recibirán un número de confirmación para llevar al centro de pruebas el día del examen. Si programa un examen de supervisión a distancia, deberá tener este número de confirmación disponible.

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 fecha de examen, hora, localización (centro de prueba o supervisada a distancia) y el número de confirmación exclusivo de 16 digitos. **Asegúrese de imprimir esta carta y tenerla con usted el día del examen junto con dos identificaciones oficiales 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. 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 (ingles o español). Si usted decide tomar el examen en el idioma español será asignado un agente de Preparación o Proctor de Examen que hable 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 PRORROGA

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, o ciertas circunstancias tales como, nacimiento de un niño, adopción, o aceptación de un niño en cuidado de crianza. El solicitante está obligado a proporcionar documentación de las circunstancias atenuantes (p. ej., nota del médico o otra prueba apropiada de las circunstancias). 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. Las dificultades graves deben ser documentadas y ser verificables. Candidatos y personas certificadas que deseen solicitar una extensión deben comunicarse con el personal de certificación de ASIS a más tardar 60 días antes que termine su fecha de elegibilidad o certificación. Extensiones para las personas certificadas solo serán consideradas si al momento de la solicitud ha completado el 50% o más los créditos CPE requeridos durante su ciclo de certificación actual. Ejemplo:

Ciclo de Certificación actual: 1 de mayo 2021 – 31 de mayo 2024

- *Prórroga de seis meses: 30 de noviembre 2024 para obtener y reportar CPE*
- *Nuevo Ciclo de Certificación para el próximo ciclo: 1 de diciembre 2024 – 31 diciembre 2027*

En tiempo de crisis que afecta a muchas personas al mismo tiempo (por ejemplo, pandemia, emergencias nacionales, desastres naturales), las políticas de extensión pueden ser modificadas en corto plazo. Todos los afectados por la crisis serán notificados de los cambios de política. *(Actualizado el 20 de febrero 2024)*

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 cobrará bien sea en 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 de:

- 31 días o antes del día programado para la prueba, no hay ningún cargo.
- Cuatro a 30 días antes del día programado para la prueba, se aplica una tarifa de $62.50 por reprogramación.
- **Candidatos no pueden reprogramar su fecha de examen faltando tres o menos día 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, perderá por completo la tarifa. Para programar otro examen deberá pagar la tarifa de repetición.

Las políticas de cancelación se aplican tanto al centro de pruebas como a los exámenes de supervisión a distancia. Prometric NO hace ninguna excepción a esta regla.

"NO PRESENTARSE"

Si usted no cancela o 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:

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

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

COMPARECENCIA EN TRIBUNAL O DEBER DE JURADO

- Comparecencias ante el tribunal o como jurado, citaciones, las cuales deben incluir la fecha y su nombre

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.

PROCEDIMIENTO DE REGISTRO EN UN CENTRO DE PRUEBA DE 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 A DISTANCIA

Los candidatos que realicen el examen supervisado a distancia deben permitir 15 minutos para preparar el entorno donde presentara el examen. Tenga en cuenta que los baños NO son entornos de prueba aceptables *(Actualizado el 6 de enero 2025)*. Debido al aumento de los protocolos de seguridad, recomendamos encarecidamente NO realizar el examen en una computadora propiedad de la empresa.

El registro para los exámenes supervisados a distancia es un proceso de dos pasos:

PRIMER PASO – VERIFICANDO SU IDENTIFICACION

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

Captura de ID – Luego, usted capturara una foto de su 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

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. Si su computador no tiene cámara web, 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.

Revision del candidato – 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 son requeridos en el centro de examen (una forma de identificación es requerido para los que presenten el examen en forma remota), una de las cuales debe ser una identificación con foto emitida por el gobierno (tal como pasaporte, licencia de conducir, ID de empleado); La segunda forma de identificación aceptable incluyen tarjeta de crédito, tarjeta de cheque, o tarjeta ATM y todas deben tener la firma del candidato.

Solo su primer nombre y apellido en su carta de aprobación de ASIS y las identificaciones deben 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 EN EL CENTRO DE PRUEBAS

El personal del centro 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 DE 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 CONFIGURACIÓN REMOTA DEBE CUMPLIR CON LOS SIGUIENTES REQUISITOS

- El lugar donde tomara el examen debe ser en un cuarto (con paredes), 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.

Revise la Guía del Usuario de ProProctor de Prometric para información adicional.

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, recibirá el resultado preliminar de su calificación en el correo electrónico que proporcionó a Prometric (permita hasta cinco horas para recibir su resultado). Su calificación oficial le será enviada aproximadamente tres semanas después de haber tomado el examen También puede visitar la sede de Prometric para obtener su resultado del examen. Tenga a la mano su número de confirmación de 16 dígitos).

ENCUESTA POSTERIOR AL EXAMEN

Cuando reciba su informe de calificación oficial de ASIS, se le proporcionará un enlace para completar una encuesta posterior a la administración sobre su experiencia en el examen. Esta es su oportunidad de compartir con a ASIS y a Prometric sobre su experiencia en el examen. Sus comentarios no tendrán ninguna influencia en su calificación en el examen. ASIS utiliza los resultados de esta encuesta para mejorar nuestros 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 reprograme 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

Habrá 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 puntaje para aprobar el examen. Antes de que se presente una pregunta en el examen, se hace una prueba previa. Esto le permite a los psicométricos evaluar el rendimiento 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 del 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** *(Actualizado el 20 de febrero 2024).*

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 área de conocimientos. Lea cada dominio 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 preguntas utilizan estos mismos materiales para hacer referencia a 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 PSP o APP. Después de revisar con atención los dominios de estudio e identificar necesidades individuales de aprendizaje, los candidatos pueden usar referencias y oportunidades de estudio adicionales según sea necesario. (Los materiales de referencia están disponible en el idioma inglés solamente)

PROFESIONAL CERTIFICADO EN PROTECCIÓN

El Protection of Assets (POA) y el set de estándares y normas de ASIS componen el material de referencia para la certificación 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 las soluciones necesarias para satisfacer las demandas de seguridad del siglo 21. El POA se actualizó en junio de 2021.

- e-Book (paquete completo)

- Print (paquete completo)

STÁNDARES 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 el POA, estos siete estándares y normas constituyen el conjunto de referencia para la certificación como CPP

Estándares:

- Senior Security Executive

- Security and Resilience in Organizations and Their

- Supply Chains—Requirements with Guidance

- Workplace Violence Prevention and Intervention

- Physical Asset Protection

Normas:

- General Security Risk Assessment Guideline

- Information Asset Protection Guideline

- Preemployment Background Screening Guideline

Socio de ASIS tienen acceso gratuito a todos los Standards and Guidelines.

- Free eBook 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

- ASIS International's Investigations Standard (Acceso gratuito al libro electrónico para ASIS Socios)

PROFESIONAL EN SEGURIDAD FÍSICA

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

- POA Physical Security Volume
- Implementing Physical Protection Systems: A Practical Guide, 3rd Ed

Estándares:

- ASIS Physical Asset Protection Standard (Acceso gratuito al libro electrónico para ASIS socios)

Normas:

- Business Continuity Management Guideline (Acceso gratuito al libro electrónico para ASIS socios)

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 Junio 2021)

- Protection of Assets: Business Principles
- Protection of Assets: Crisis Management
- Protection of Assets: Security Management (Note: Replaces POA Information Security volume)

ASIS OFRECE DOS PAQUETES DE PRECIOS:

- Protection of Assets Bundle for the APP Certification
- APP Complete Reference Set

Para aquellos que tienen la certificación APP y están estudiando para el CPP, ASIS ofrece un paquete de Transición de APP que incluye los volúmenes de Investigaciones, Seguridad Física. y Personal del POA. También se ofrece un conjunto de referencia completo de APP a CPP.

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

PREPARACION ADICIONAL PARA LA CERTIFICACION

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 preguntas que alguna vez aparecieron en exámenes reales de certificación, pero han sido removidas. Use estos exámenes de práctica para familiarizarse con cómo aparecen los ítems en los exámenes actuales. Nota: Debido a que estas preguntas ya no aparecen en el examen, es posible que ya no sean precisas. Estas preguntas solo están destinadas a que vea cómo se formularán las preguntas del examen.

Examen de práctica CPP

Examen de práctica PCI

Examen de práctica PSP

APROBÉ EL EXAMEN, ¿AHORA QUÉ?

Al completar con éxito el examen, recibirá un certificado con su nombre, las fechas de inicio y finalización del ciclo de certificación y el número de certificación. Espere al menos cuatro semanas para recibir su certificado.

Además, recibirá un correo electrónico de Credly (asociado 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 e imprimir su certificado. Considere dos a cuatro semanas para recibir su 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

(Actualizado el 20 de febrero 2024) Además del Código de Ética y el Código de Conducta de ASIS International, todos 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.

Además, 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.

Según las normas ANAB ISO 17024, si su certificación ASIS se revoca, es posible que se le solicite que devuelva su certificado.

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), Profesional en Seguridad Física (PSP) o Asociado Profesional de Protección (APP) 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.

Certifico que he completado todos los requisitos de certificación y/o recertificación según lo descrito en el manual de Certificación de la Junta Internacional de ASIS o la Guía de Recertificación de la Junta, según corresponda. *(Actualizado el 20 de febrero 2024)*

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 (p. ej., el estatus es “actual” y no “vencida” o “expirada”

- Haber mantenido una certificación por 12 años consecutivos precedentes a la fecha de solicitud

- El candidato debe estar actualmente retirado de cualquier tipo de empleo o práctica de seguridad, o recibir una compensación por ello, según lo definido por el dominio del examen de certificación correspondiente.

- Haber pagado la tarifa de recertificación para el periodo actual

Las personas designadas de por vida y en buen estado están sujetas a las mismas condiciones que los demás certificados, excepto que no será necesaria la recertificación y la recertificación no se cobrarán honorarios.

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, deberá enviar una solicitud. Se aplica tarifas de solicitud.

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.

De acuerdo con las normas ANSI ISO 17024, ASIS se reserva el derecho de revocar cualquier certificación de por vida si se descubre que el certificador ya no está jubilado. Si se revoca una certificación de por vida, el certificado de por vida debe devolverse a ASIS.

Para solicitar una certificación de por vida, completé y envié la solicitud por correo electrónico a 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 Professional 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 certificante; y no comparte información con terceros.

PRESENTAR UNA QUEJA

Las quejas relacionadas con los requisitos de elegibilidad, la programación de exámenes, las políticas y los procedimientos del programa de certificación de ASIS, el personal de certificación u otro certificador pueden presentarse por escrito según las instrucciones de la Sección III: Proceso para presentar una queja. La confidencialidad tanto del denunciante como de la persona a quien se presenta la queja están protegidas por los acuerdos de confidencialidad de ASIS.

Proporcione suficientes pruebas objetivas para fundamentar la queja. Todas las quejas serán revisadas por el director de certificación y/o miembros del Comité de Relaciones con Personas Certificadas por la PCB.

Siempre que sea posible, ASIS elaborara informes de progreso tanto a la persona que presenta la queja como a la persona a quien se presenta la queja. 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. La política de quejas completa de ASIS se puede encontrar **aquí**.

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.