ASIS INTERNATIONAL
Advancing Security Worldwide®

ASIS INTERNATIONAL
GUÍA DE RECERTIFICACIÓN

asisonline.org/certification/recertification

CPP® Certified Protection Professional
Board Certified in Security Management

PCI® Professional Certified Investigator
Board Certified, ASIS International

PSP® Physical Security Professional
Board Certified, ASIS International

APP Associate Protection Professional
Board Certified in Security Management Fundamentals

INFORMACIÓN DE CONTACTO DE ASIS INTERNATIONAL

¡ASIS está aquí para ayudar! Esta guía cubre toda la información sobre los tres programas de certificación de ASIS. Si tiene preguntas después de revisar la guía, 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).

Esta guía incluye todas las políticas y procedimientos relacionados con la recertificación de sus designaciones de ASIS. Es su responsabilidad estar al tanto de los procesos y procedimientos que se explican en esta guía y de cumplir con todas las fechas límite requeridas. La versión actualizada de la Guía de Recertificación de ASIS se publicó el 1 de febrero 2022 y reemplaza todas las versiones anteriores.

IMPORTANTE: ASIS SE COMUNICA CON USTED PRINCIPALMENTE POR CORREO ELECTRÓNICO. SI SU INFORMACIÓN CAMBIA, ASEGÚRESE DE ACTUALIZAR SUS REGISTROS DE ASIS EN LÍNEA TAN PRONTO COMO LE SEA POSIBLE

Contenido

Programa de certificación de ASIS International

Las certificaciones de ASIS sirven como un reconocimiento visible de su dominio demostrado de principios y habilidades básicas de seguridad esenciales para la mejor práctica de la gestión de seguridad.

Al obtener una certificación como CPP®, PCI®, PSP®, o APP su empleador, clientes y colegas reconocerán que usted tiene el conocimiento y las habilidades para ser un profesional exitoso en seguridad. Obtener una certificación de ASIS es un logro importante que lo ayudará a obtener sus metas de carrera. Una vez certificado, usted deberá renovar su certificación a través de actividades continuas de educación **cada tres años.**

¿Por qué renovar la certificación?

Renovar su certificación de ASIS cada tres años demuestra que usted ha hecho un compromiso por mantenerse informado sobre las prácticas actuales y las tendencias emergentes en la industria de la seguridad.

¿Cuándo debo renovar la certificación?

Su certificación debe ser renovada cada tres años. Su fecha de vencimiento esta imprimido en su certificado y también puede encontrar esta información en su cuenta Credly.

Ciclo de renovación de certificación

El ciclo de renovación es cada de tres años a partir del momento que aprueba el examen CPP®, PCI®, PSP®, o APP. Por ejemplo, una persona certificada que obtenga la certificación el 15 de abril de 2022 deberá renovar su certificación antes del 30 de abril de 2025.

Certificaciones vencidas - Nueva política

A partir del 1º de enero de 2019, todas las personas certificadas tienen tres meses (no un año) después de sus fechas finales para la recertificación. Durante este periodo de gracia de tres meses, se le permitirá enviar su solicitud; sin embargo, **todos los 60 créditos de CPE se deben completar en su ciclo de certificación de tres años. No puede usar el periodo de gracia de tres meses para acumular créditos adicionales de CPE.** Se aplicará una tarifa de retraso de 40 dólares además de la tarifa de recertificación al momento de enviar la solicitud.

Certificación vencida

Si su solicitud de recertificación **no se envía** antes del término de su periodo de gracia de tres meses, su certificación se vencerá y usted deberá solicitar, tomar y aprobar el examen para obtener de nuevo la certificación.

Certificados de ASIS

Todos los certificados relacionados con las designaciones de CPP, PCI, PSP y/o 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.

Promocionar su certificación

Hay muchas maneras de mostrarles a sus colegas y compañeros que usted ha obtenido con éxito su certificación de ASIS. Proporcionamos información sobre cómo mostrar su credencial y cómo usar los logotipos certificados de ASIS.

Insignias digitales

Una vez que haya obtenido su certificación de ASIS, recibirá un correo electrónico de Credly con instrucciones sobre cómo descargar su insignia digital y certificado. Las insignias digitales son portátiles, verificables e impiden las reproducciones sin autorización de designaciones de CPP, PCI, PSP y APP. Para obtener más información sobre las insignias digitales de ASIS, haga clic aquí.

Requisitos de recertificación

Necesitará completar **60 actividades de Educación Profesional Continua (CPE)** durante el ciclo de certificación de tres años para mantener su certificación.

Todas las actividades de CPE deben relacionarse con la gestión de seguridad/administración de negocios, según lo definido por el cuerpo de conocimientos del examen pertinente. Las personas certificadas deben enlazar cada actividad presentada con un campo del examen. **Vea los campos de CPP, PCI, PSP o APP.**

Los créditos de recertificación están previstos para aprendizaje, enseñanza o servicios relacionados con seguridad o negocios **que no sean parte de los deberes laborales regulares de una persona certificada.** Los créditos de CPE se deben obtener en las siguientes categorías:

- Membresía (24 CPEs Max.)
- Educación
- Instructor (30 CPEs Max.)
- Autor
- Voluntario (30 CPEs Max.)
- Programa de certificación, estándares y normas
- Servicio público
- Otros logros
- Programas relacionados con la seguridad (Safety) (21 CPEs Max.)

A continuación, se explica la información adicional sobre cada una de estas categorías y la documentación que deberá presentar en su solicitud de recertificación.

Proceso de solicitud y revisión de recertificación

Todas sus actividades completadas y documentos de soporte deben ser almacenados y subidos en su portal ASIS. El portal le permite cargar sus créditos de CPE a medida que los obtiene; sin embargo, el personal de ASIS ya no revisará sus créditos de CPE hasta que haya presentado su solicitud de recertificación. Las actividades se mostrarán como **"pending"** hasta que haya completado el proceso de recertificación.

Llame o envíe un correo electrónico a ASIS si tiene preguntas sobre sus créditos de CPE. Además, recomendamos (pero no exigimos) que presente créditos adicionales de CPE si los tiene.

Revisión de su Solicitud

Su recertificación no está completa cuando envía su solicitud de recertificación. ASIS requiere de 2-3 semanas para revisar y aprobar su solicitud de recertificación. Recibirá una notificación una vez que la revisión se ha completado por correo electrónico de ASIS. El correo electrónico informará si cumplió con

los requisitos de recertificación o si necesitamos información adicional. **Si no ha recibido esta notificación después de tres semanas, sírvase comunicarse con el personal de certificación.**

Recertificación antes de la fecha de vencimiento

Su solicitud de recertificación se puede enviar en cualquier momento en su tercer ciclo de certificación. Una vez que se hayan revisado sus créditos de CPE, **su nuevo ciclo de certificación comenzará donde finalizó su ciclo de tres años** (es decir, usted no obtendrá un nuevo inicio de ciclo y fecha final). Todos los créditos de CPE se deben obtener durante el ciclo de tres años. Si usted solicita la recertificación temprana en su tercer año y si algún CPE no es aprobado, usted tendrá hasta el final de su ciclo de tres años para enviar sus CPE faltantes.

Una vez que su solicitud de recertificación ha sido aprobada, **cualquier crédito de CPE obtenido después de la recertificación, pero antes de que inicie un nuevo ciclo, no se acumulará para su nuevo ciclo de certificación.**

Tenga en cuenta que, durante el primer y segundo año de su ciclo de certificación, puede usar el portal para almacenar, monitorear y revisar sus CPEs a medida que son acumulados.

Ventajas de ser miembro de ASIS

No es necesario que sea miembro de ASIS para volver a certificar su designación, ¡pero si es socio, tendrá una amplia gama de recursos para recertificarse! Solo por ser miembro recibirá cuatro créditos de CPE por año por un total de 12 créditos de CPE durante su ciclo de tres años. Los roles de liderazgo del Capítulo y el Consejo de ASIS, el trabajo voluntario en ASIS, los seminarios en línea solo para miembros y más lo ayudarán a alcanzar sus objetivos de recertificación y se aplicarán descuentos solo para miembros.

Créditos CPE patrocinado por ASIS

La mayoría de las actividades patrocinados por ASIS se cargará a su cuenta de certificación en línea. Estas incluyen una membresía de ASIS, el liderazgo como voluntario de ASIS, Global Access Live y el Global Security Exchange (GSX), cursos en línea y nuestros seminarios web en directo y bajo demanda. Usted recibirá de su líder de ASIS un certificado de culminación para todas las otras actividades relacionadas con ASIS. Este certificado, el cual usted cargará en su cuenta, será un crédito de CPE garantizado.

Por favor permita al personal de ASIS de cuatro a seis semanas después de la conclusión de la actividad para que los CPEs aparezcan en su cuenta. Para seminarios en línea, su participación será cargada en un periodo de 48 horas al término del seminario en línea.

Eventos por Capítulo/Región

Los créditos por actividades de Capítulo de ASIS/Región no se cargan automáticamente en su cuenta en línea. En el Capítulo/Región, hay dos opciones para conformar los créditos de CPE obtenidos por asistir a un evento que califica. Haga clic aquí para obtener más información (versión en inglés).

Enviar actividades de recertificación

El sistema de reporte de CPE en línea de ASIS se mejoró recientemente, permitiendo que usted presente las actividades de CPE desde su página de perfil en el enlace rápido "My Certifications". Vea las instrucciones para cargar sus créditos de CPE y enviar su solicitud.

NOTA: La primera vez que acceda a su cuenta en línea, haga clic en el botón “Calculate” para totalizar cualquier CPE que hayamos importado de la base de datos ASIS anterior (si no ve ningún CPE después que haga clic en "calculate", entonces su aplicación está actualizada).

Documentación de respaldo

Se requiere documentación de respaldo para todas las actividades (excepto las actividades de CPE cargadas por el personal de ASIS). Todas las actividades deben alinearse con los campos y los conocimientos y enunciados de tareas para la certificación que está renovando. **Su documentación debe incluir una prueba de que asistió a la sesión y descripción de los objetivos aprendidos** Su documentación puede incluir una copia de un certificado/carta de culminación y agenda, la cual contenga las horas de asistencia en el salón de clases. Toda la documentación de respaldo debe estar en inglés y en español. Cualquier envío en idiomas extranjeros debe estar acompañado con una traducción en inglés.

Se debe cargar al menos un documento por actividad CPE que autoinforme y el sistema permite hasta tres cargas para cada entrada.

Los documentos enviados deben incluir:

- Nombre de la persona certificada
- Nombre del tema
- Nombre del programa patrocinador
- Descripción del curso del programa patrocinador (esto se usará para verificar que el curso esté alineado con los campos de la certificación)
- Fecha de asistencia o culminación (dentro del periodo de certificación de 3 años)
- Número de horas de enseñanza adjudicadas o la agenda
- Certificado/carta de culminación

(Consulte **Categorías de CPE y documentación requerida** más adelante para documentación específica necesaria para cada categoría de crédito).

Notificaciones/recordatorios de renovación de certificación

Su certificación debe ser renovada cada tres años. Su fecha final está impresa en su certificado y también se puede encontrar en su perfil en línea.

ASIS hace todos los esfuerzos posibles por mantenerlo informado sobre sus fechas límites para la recertificación. Se enviarán notificaciones por correo electrónico a la dirección principal en su cuenta en línea. **Asegúrese de tener actualizada su dirección de correo electrónico y colocar en la "lista blanca" todos los correos de asisonline.org para ayudar a seguir los recordatorios de recertificación.** En última instancia, sin embargo, usted es responsable de mantenerse al día sobre las fechas límites de recertificación y enviar la documentación correspondiente. **No recibir las notificaciones de ASIS no es un motivo razonable para dejar pasar fechas límites de solicitud.**

Políticas de extensión

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

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

Tarifas de recertificación

En enero 2022, la Junta Directiva Global de ASIS votó para aumentar las tarifas de certificación como se describe a continuación. La Junta de ASIS también 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.

Miembro de ASIS: $170
Mercado Emergente 1: $130
Mercado Emergente 2: $120

No miembro de ASIS: $210
Mercado Emergente 1: $160
Mercado Emergente 2: $150

Se aplicará una tarifa de retraso si la solicitud se recibe durante los tres meses de gracia. Las tarifas se deben pagar en dólares estadounidenses y están sujetas a cambio. Tarifas no son reembolsables.

Miembro de ASIS: $250
Mercado Emergente 1: $190
Mercado Emergente 2: $175

No miembro de ASIS: $290
Mercado Emergente 1: $220
Mercado Emergente 2: $205

Durante el tercer año de su ciclo de certificación, usted puede enviar en cualquier momento su solicitud de recertificación. Cuando se haya revisado su solicitud, recibirá una notificación por correo electrónico.

Categorías de CPE y documentación requerida

Se deben presentar sesenta (60) créditos de CPE para cada certificación. Si tiene más de una certificación de ASIS, necesitará enviar una solicitud de recertificación por cada una de ellas. Tome en cuenta que en algunos casos se puede presentar una actividad de CPE para más de una certificación, siempre y cuando la descripción de la actividad se alinee con los campos de la certificación.

Con el nuevo proceso de solicitud en línea de ASIS, se le solicitará enviar documentación de respaldo con cada actividad de CPE presentada. Consulte a continuación la documentación aceptable por categoría de crédito.

Categoría 1: Crédito de Membresía (24 CPEs Max.)

Si usted es un miembro de ASIS International, se cargarán automáticamente 4 créditos de CPE en su cuenta en línea una vez al año. También puede informar sobre su membresía en otras asociaciones relacionadas con la seguridad. En su ciclo de certificación de tres años, se pueden presentar un máximo de 24 créditos de CPE (4 créditos de CPE por año de membresía) para membresías individuales en:

- Organización o asociación de seguridad profesional, o relacionadas con seguridad, sin fines de lucro.
- Organización o asociación relacionada con administración de negocios sin fines de lucro

No se aceptan membresías de corporaciones

Documentación requerida

- Recibo de tarifas pagadas de membresía que incluya los años de membresía
- Carta de la organización confirmando los años de membresía (membrete de la organización)
- Copia de directorio de membresía que incluya su nombre y años de membresía

Categoría 2: Crédito Educativo

Las personas que renueven la certificación pueden reclamar el tiempo directo que pasaron en una actividad educativa. ASIS acepta horas completas o parciales, pero todas las sesiones deben tener una duración mínima de 30 minutos. Por ejemplo, si asiste a una sesión de 90 minutos, usted informaría 1.5 horas reloj. Si asiste a una sesión de 45 minutos, usted informaría 0.75 horas reloj. **No se debe incluir el tiempo para comidas, recesos, reuniones sociales, sesiones de planificación, reuniones de negocios y actividades similares.**

CÁLCULO DE HORAS DE CPE

Actividad educativa	Horas reales
9:00 a.m.– 5:00 p.m.	8
Menos: Dos recesos de 15 minutos	0.50
Menos: Almuerzo	1
TOTAL	**6.5**

El crédito educativo se puede obtener por las siguientes actividades:

- **Seminario/conferencia:** programas de uno o varios días.
- **Seminarios en línea (en vivo o archivados):** comprados a través de ASIS (suscripción de seminario en línea o compra única) o seminarios en línea patrocinados por otros. Los seminarios en línea deben relacionarse con seguridad y alinearse con uno de los campos para los cuales está renovando la certificación. Se requiere certificado de culminación o prueba de asistencia y descripción de la sesión. Nota: seminarios en línea de ASIS visto después del 1º de agosto de 2019 serán cargados en su cuenta. Los seminarios en línea de ASIS vistos antes de esa fecha debe ser auto-reportados.
- **Otras certificaciones relacionadas con la seguridad:** Si usted posee una certificación de otra organización, usted puede reclamar 20 CPEs siempre y cuando ha obtenido la certificación durante su ciclo de renovación de tres años. El PCB ha aprobado esta lista de otros programas de certificación que son elegibles.
- **Reuniones de Capítulos de ASIS International:** Los programas educativos deben tener un orador o facilitador formal y relacionarse directamente con las competencias (campos) de las certificaciones correspondientes
- **Cursos por correspondencia, en línea y de estudio independiente:** Preparación a través de una institución que requiera un examen final y donde el patrocinador del curso emita un certificado de culminación en el que se indiquen las horas de enseñanza alcanzadas.
- **Cursos universitarios acreditados:** Cursos universitarios acreditados relacionados con la gestión de seguridad o administración de negocios se pueden reclamar y calcular a la tasa de siete créditos de CPE por cada hora de semestres completada. Esto incluye aprendizaje en Internet/a distancia u otros programas de estudio independiente que tengan como resultado créditos universitarios. **Solo se pueden reclamar 21 créditos de CPE por semestre para cursos de administración de negocios:**

- **Solo exposiciones y participación como expositor:** Se pueden adjudicar tres créditos de CPE por la participación o asistencia a cada exposición relacionada con seguridad.
- **"Best of GSX" bundles:** ASIS ofrece paquetes de temas específicos seleccionados de las sesiones de GSX. Los créditos se otorgan en base a la longitud del paquete.

Documentación requerida

- Una descripción del curso, certificado o carta de culminación y una agenda que incluya las horas en el salón de clases
- Una transcripción que muestre la culminación de los cursos universitarios
- Insignia que muestre "Solo exposición" o "Expositor"
- Para seminarios en línea archivados: una captura de pantalla de la primera y la última página de la presentación o carta o certificado de culminación.

Categoría 3: Crédito de Instructor (30 CPEs Max.)

Los temas de los cursos deben ser pertinentes a la práctica de gestión de seguridad o administración de negocios (p. ej., los campos para cada examen de certificación).

CPE	Actividad de instructor
20	Por tema, preparación inicial o modificaciones importantes del trabajo de curso para actuar como instructor u orador principal para un curso relacionado con la gestión de seguridad o administración de negocios en una universidad o instituto universitario acreditado.
12	Cursos de estudio de certificación de Capítulo: Planificar el curso de estudio completo, lo que incluye varias reuniones.
9	Cursos de estudio de certificación de Capítulo documentados (ser mentor de un estudiante durante un curso de estudio completo o cumplir un papel específico en la realización del curso). Solo se permiten programas de tutoría aprobados por ASIS.
9	Programa Mentor ASIS - Los mentores recibirán 9 CPE por año por cada programa de mentoría activo. Cada programa debe tener una duración mínima de 6 meses.
9	Programa Mentor ASIS - Los aprendices pueden registrar 5 CPE cada tres años. Programa de tutoría debe de alinear deben enlazar por lo menos con uno del campo del examen de la certificación apropiada. Se requiere una carta de su mentor, explicando el propósito de la tutoría y cómo se alinea con los Dominios.
3	Por hora participante, como un instructor, orador o panelista en un programa educativo relacionado con seguridad o de administración de negocios.

Documentación requerida

- La programación del curso debe incluir objetivos de aprendizaje, hora, fecha y ubicación del curso
- Carta del presidente del Capítulo confirmando el rol del instructor
- Un certificado o carta de agradecimiento del patrocinador del programa

Categoría 4: Crédito de Autor

Los temas deben ser pertinentes a la práctica de gestión de seguridad o administración de negocios (p. ej., los campos para cada examen de certificación).

CPE	Artículos y publicaciones escritos (sin límite)
45	Por libro relacionado con la gestión de seguridad o libro de administración de negocios.
9	Por artículo relacionado con la gestión de seguridad o administración de negocios en periódico reconocido.
9	Por monografía, folleto o contribución de capítulo de un libro relacionado con la gestión de seguridad o temas de administración de negocios
3	Cada revisión de libro publicada en un periódico reconocido
1-2	Por traducción de un artículo relacionado con cualquier campo de seguridad que haya sido publicado originalmente y/o posteriormente en una revista de gestión de seguridad u otra publicación relacionada con seguridad.[1]

Documentación requerida

- La copia del artículo debe incluir nombre, fecha de publicación y firma del autor
- Carta de la editorial (en el encabezado) que autentique la contribución

Categoría 5: Servicio de Voluntariado (Max. 30 CPEs)

CPE (créditos por año)	Actividades de voluntariado (un máximo de 30 créditos de CPE por ciclo de certificación de tres años)
30	Miembro de un Comité Ejecutivo nacional o internacional de una Junta de directores de una organización o asociación certificada relacionada con seguridad (p.ej., miembros del comité ejecutivo de ASIS Global Board, CSO, Foundation, PCB, y PSB).
25	Miembro de una junta nacional o internacional de directores de una organización autorizada relacionada con seguridad (p.ej., ASIS Global Board Directors; Regional Board/Advisory Committee; and Directors of the ASIS CSO, Foundation, PCB, y PSB).
18	Servicio como ASIS Senior Regional Vice President o Council Vice President (*Community Vice President) de una organización o asociación certificada relacionada con seguridad.
15	Servicio como ASIS Regional Vice President, Council Chairman, o Vice Chairman (*Steering Committee Chair or Vice Chair), o Chapter Chair, o un rol similar de una organización o asociación certificada relacionada con seguridad.
12	Servicio como ASIS Assistant Regional Vice President, Council Member (*Steering Committee Member), Chapter Vice Chair, Secretary o Treasurer GSX Host Committee Chair, o Awards Committee, o rol similar de una organización o asociación certificada relacionada con seguridad.

[1] No se otorgarán créditos por traducciones pagadas de artículos. Un crédito de CPE otorgado por artículos de hasta 1.000 palabras y dos créditos de CPE otorgados por artículos de más de 1.000 palabras. Se pueden otorgar cuatro créditos de CPE por año, con un máximo de 12 créditos de CPE por ciclo de recertificación de tres años. Para recibir créditos, la persona certificada debe enviar una copia del artículo original, junto con una copia del artículo publicado traducido. Ambas copias deben indicar claramente la publicación y la fecha. Para recibir un crédito por una traducción, la persona certificada debe ser nombrada o acreditada en la traducción. De no ser así, la persona certificada debe enviar una verificación por escrito de la editorial indicando que la persona certificada fue responsable de la traducción.

9	Servicio como miembro del ASIS GSX Host Committee o Awards Committee, Chapter Committee Chair, o rol similar de otra conferencia anual de una organización o asociación certificada relacionada con seguridad.
4	Servicio como miembro de ASIS Chapter Committee o servicio equivalente en una organización o asociación certificada relacionada con seguridad

***Nuevos grupos de interés y títulos entraran en vigor el 1 de enero 2021.**

Documentación requerida

- Carta de la organización que autentique el rol del voluntario y las fechas de servicio.

Categoría 6: Servicio de Programa de Certificación, Estándares y Normas

CPE (créditos por año)	Actividades de Certificación y de Estándares y Normas (Standards & Guidelines-S&G) de ASIS
15	Por evento, Grupo de Desarrollo de Ítems (Item Development Group, IDG) o preparación de descripción de rol (análisis de trabajo).
12	Por evento, estudio de punto de aprobación.
5	Por evento, evaluación de Llamado de Presentaciones para GSX de ASIS International.
2/reunión	Por evento, miembros del Comité Técnico de Estándares y Normas de ASIS; la asistencia/participación es obligatoria.
1/reunión	Por evento, miembros del Grupo de Trabajo de Estándares y Normas de ASIS; la asistencia/participación es obligatoria.

Documentación requerida

- Carta de la organización que autentique su rol del voluntario y las fechas de servicio.

Categoría 7: Servicio Público

A criterio de la PCB, actividades relacionadas con los campos de gestión de seguridad o de administración de negocios, según lo descrito en los campos de cada examen, pueden ser elegibles para créditos. Las actividades elegibles pueden incluir aquellas para una organización de caridad, religiosa, gubernamental o comunitaria que opere *pro-bono*. Ejemplos son auditorías de seguridad de edificios de escuelas públicas; plan de seguridad para evento de recaudación de fondos u otra actividad grande; o evaluación de la gestión de emergencia para una agencia pública. La PCB determinará los puntos que se otorgaran con base en el alcance de la actividad, el valor para el receptor, los logros de objetivos cara a cara y el tiempo invertido.

Documentación requerida

- Carta de la organización que autentique su rol en el servicio público, las fechas de servicio, las horas invertidas, una breve descripción del servicio *pro-bono* prestado y el número de créditos solicitados

Categoría 8: Otros Logros

A criterio de la PCB, actividades especiales relacionadas con los campos de gestión de seguridad o administración de negocios, según lo descrito en los campos de cada examen, pueden ser elegibles para créditos. La PCB determinará los puntos que se otorgarán con base en el alcance de la actividad y otros factores relevantes.

Documentación requerida

- Carta al PCB que autentique su actividad especial, fechas de la actividad y el número de créditos solicitados

Categoría 9: Programas Relacionadas con Seguridad (Safety-Max. 21 CPES)

Solo se puede reclamar 21 créditos CPE por término por asistir o hablar/enseñar en las áreas de seguridad (Safety), protección medioambiental contra incendios y protección personal de seminarios de uno o varios días y se pueden reclamar conferencias.

Documentación requerida

- Un certificado o carta de culminación y una agenda que incluya las horas del seminario o tiempo de conferencia.
- Copia del programa en el sitio que muestra su papel como orador.
- Carta de la organización anfitriona que acredite su participación en un seminario o conferencia.

Cómo Postular Para la Recertificación por Examen

Un certificado actual en su tercer año puede volver a certificarse tomando el examen (en lugar de presentar CPE). Para recertificar tomando el examen, debe comunicarse con el departamento de sus intenciones. El equipo de certificación deberá rescindir su certificación actual para que pueda enviar una solicitud de examen. Se le pedirá que siga todas las políticas con respecto a la presentación de una solicitud de examen y las tarifas correspondientes. Nota, si el candidato **no aprueba** el examen, perderá su certificación actual.

La persona certificada que toma el examen nuevamente y **lo aprueba**, su fecha de inicio y ciclo de certificación comenzara en la fecha en la que aprobó nuevamente el examen.

Apelar una solicitud rechazada

Las apelaciones se considerarán en el transcurso de 30 días posteriores a la solicitud de recertificación de la persona certificada o de la denegación de actividad de CPE, con el día uno siendo la fecha del correo electrónico de notificación enviado al solicitante. Siga las siguientes instrucciones cuando presente una apelación:

- Las apelaciones se deben enviar por correo postal o por correo electrónico al Comité de Relaciones con Personas Certificadas de la Junta de Certificación Profesional (PCB), a la dirección que se indica más adelante. Si se envían por correo postal, ASIS sugiere usar un método de envío rastreable (p. ej., correo certificado o expreso).
- Las apelaciones deben identificar la decisión adversa e indicar los motivos de la apelación. Además, en la apelación se debe incluir cualquier información nueva o adicional a ser considerada.

Las apelaciones se deben enviar a:

PCB Certificant Relations Committee
c/o ASIS International
1625 Prince Street
Alexandria, VA 22314

Attn: Certification Department
certification@asisonline.org

Proceso de Apelación del Comité de Relaciones de Personas Certificadas del PCB

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

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

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

La decisión del PCB es final

Certificación de Por Vida (jubilado)

ASIS ofrece una certificación de por vida a personas certificadas que:

- Tengan una certificación como CPP, PCI, PSP, o APP en buena situación (no se ha vencido ni ha expirado)
- Haber mantenido una certificación por 12 años consecutivos precedentes a la fecha de solicitud
- Haberse retirado (se define como el cese por completo de cualquier empleo o práctica relacionados con seguridad o representación de empleo o práctica semejantes) y no tener interés legal, financiero ni comercial con cualquier forma de empleo o práctica relacionados con seguridad, según lo definido en el campo de examen de certificación correspondiente (CPP, PCI, PSP, o APP)
- Haber pagado la tarifa de recertificación para el periodo actual

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

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.**

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), PCI – Certificado de por vida (jubilado) o PSP – Certificado de por vida (jubilado). No puede usar la designación sin estas descripciones calificativas.

De conformidad con los Estándares ANSI ISO 17024, ASIS se reserva el derecho de revocar su certificación de por vida si se descubre que usted ya no está jubilado. Si se revoca su certificación de por vida, se le pedirá que regrese su certificado de por vida.

Conviértase en Voluntario de ASIS

ASIS depende de sus voluntarios para todos los aspectos de sus programas de certificación (p. ej., elaboración del examen, establecer la calificación o análisis del trabajo). Todos los aspectos de las

certificaciones como CPP, PCI, PSP, y APP son creados y luego mantenidos por profesionales dedicados que ofrecen su experiencia y tiempo para garantizar que nuestros programas reflejen el conocimiento y las habilidades necesarias para ser un profesional de gestión de seguridad.

Para ser un voluntario, usted debe:

- Estar certificado por ASIS
- Aceptar adherirse al Código de Responsabilidad Profesional de ASIS
- Firmar un contrato de no divulgación
- No participar, coordinar, albergar ni enseñar clases de preparación o revisión para la certificación de ASIS, y no aceptar hacerlo por al menos dos años después de haber completado su asignación como voluntario
- Estar de acuerdo con no solicitar ni tomar un examen de certificación de ASIS por al menos dos años después de haber completado su asignación como voluntario

ASIS recluta periódicamente voluntarios para:

- Escribir o revisar preguntas de examen
- Sentarse en un panel de estudio de análisis de trabajo
- Sentarse en un panel de establecimiento de estándares
- Prestar su experiencia para proyectos especiales

Todos aquellos escogidos para ser voluntarios del programa de certificación de ASIS recibirán créditos de CPE por su participación.

Si está interesado en ser voluntario, descargue y complete el formulario de voluntariado y envíelo a certification@asisonline.org .

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 concernientes a los requisitos de elegibilidad, la programación de pruebas, las políticas y procedimientos del programa de certificación de ASIS, el personal de certificación u otra persona certificada se pueden presentar por escrito al director de certificación. Envíe su queja por escrito y por correo postal o correo electrónico a certification@asisonline.org. Las quejas anónimas no serán revisadas.

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

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 constituyentes 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 constituyentes son y permanecerán imparciales y confidenciales.

Código Profesional de Conducta

Los profesionales de seguridad certificados de ASIS y los solicitantes de certificación debe acatar el Código Profesional de Conducta, 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 conducto no profesional y se considere perjudicial para la certificación.
- Observar los preceptos de honradez, honestidad e integridad.
- Ser leales, competentes y diligentes al asumir sus deberes profesionales.
- Salvaguardar información confidencial y privilegiada y ejercitar el cuidado debido para evitar su divulgación inadecuada.
- No dañar maliciosamente la reputación profesional ni la práctica de colegas, clientes o empleados.

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

- Dar declaraciones o información falsas o engañosas cuando solicite tomar el examen de certificación o renovar la certificación.
- Cualquier acto u omisión que viole las disposiciones del Código de Responsabilidad Profesional de 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 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

En conformidad con los Estándares ANSI ISO 17024, si ASIS revoca su certificación, se le pedirá que regrese su certificado.

Declaración de Continuidad en la elegibilidad para la Certificación

Todo los que se aplican para la recertificación de su certificación firmará la siguiente declaración sobre la aplicación

Con mi firma, doy fe de que la información que presento en este documento o en la documentación adjunta o subsiguientemente requerida es verdadera y exacta según mi conocimiento.

Entiendo que las personas que solicitan la certificación como Certified Protection Professional (CPP), Professional Certified Investigator (PCI), Physical Security Professional (PSP), o Associate Protection Professional (APP), o personas que hayan sido certificadas por ASIS International, están sujetas a los requisitos de elegibilidad de ASIS Internacional para la certificación, recertificación y al Código de Certificación de Responsabilidad Profesional de ASIS.

Entiendo que, con el fin de mantener mi certificación, debo recertificar cada tres años informando un número específico de créditos de Educación Profesional Continua (CPE), en conformidad con la política y los procedimientos de ASIS para la presentación de dichos informes. Comprendo que los créditos de CPE pueden ser obtenidos a través de programas y cursos de formación y también por otras actividades, y que todos los CPEs deben ajustarse a los requisitos especificados en la Guía de ASIS Internacional para Recertificación. Además, entiendo que ASIS Internacional podrá modificar sus requisitos, políticas y procedimientos incluyendo la certificación inicial, recertificación, y el Código de Responsabilidad Profesional.

También entiendo que podré estar sujeto a una auditoría en cualquier momento y que ASIS International se reserva el derecho de tomar medidas en caso de incumplimiento de los procedimientos de auditoría.

Mientras mantenga la certificación de ASIS Internacional, acuerdo notificar a ASIS Internacional por escrito inmediatamente si fallo en cumplir con cualquiera de los requisitos para obtener o mantener la certificación o recertificación, tales como, pero no sólo limitado a, ya no estar en la profesión, haber interrumpido mi status de Retirado habiendo regresado a un empleo de tiempo completo, no obtener el número de créditos CPE necesarios para mantener la certificación o para ser recertificado, o haber sido sancionado -incluyendo suspensión, expulsión o pérdida de la credencial – violando el Código de Responsabilidad Profesional de ASIS. También estoy de acuerdo con notificar a ASIS Internacional por escrito acerca de cualquier cambio de dirección o de nombre dentro de los treinta (30) días después de que el cambio se haga efectivo.

Si así lo solicitara, ASIS Internacional podrá verificar el estado de mi certificación.

Junta de Certificación Profesional de ASIS (PCB)

La Junta de Certificación Profesional (PCB) de ASIS rige los programas de certificación de ASIS. La PCB establece todas las políticas relacionadas con el programa, lo que incluye requisitos de elegibilidad, contenido del examen (cuerpo de conocimientos) y desarrollo de exámenes. Todos los miembros de la PCB tienen certificación de ASIS.

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

APP: Áreas de Conocimiento

CAMPO UNO

Principios de la seguridad (35 %)

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

Conocimiento de

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

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

Conocimiento de

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

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

Conocimiento de:

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

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

Conocimiento de

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

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

Conocimiento de

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

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

Conocimiento de

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

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

Conocimiento de

1. Investigaciones de antecedentes y técnicas de selección de personal
2. Calidad y tipos de fuentes de información y datos

3. Leyes y procedimientos penales, civiles y laborales

Tarea 8: Desarrollar, implementar, coordinar y evaluar políticas, procedimientos, programas y métodos para protección de personas de amenazas humanas en el lugar de trabajo (por ejemplo, acoso, violencia, etc.)

Conocimiento de

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

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

Conocimiento de

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

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

Conocimiento de

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

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

Conocimiento de

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

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

Conocimiento de

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

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

Conocimiento de

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

CAMPO DOS

Operaciones comerciales (22 %)

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

Conocimiento de

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

CAMPO 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

CAMPO CUATRO

Gestión de respuestas (18 %)

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

Conocimiento de

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

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

Conocimiento de

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

Tarea 3: Llevar a cabo una revisión posterior al incidente

Conocimiento de

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

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

Conocimiento de

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

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

Conocimiento de

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

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

Conocimiento de

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

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

Conocimiento de

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

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

Conocimiento de

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

Tarea 9: Supervisar la eficacia de la respuesta a incidentes

Conocimiento de

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

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

Conocimiento de

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

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

Conocimiento de

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

CPP: Áreas de Conocimiento

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

CAMPO UNO

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

CAMPO DOS

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

1. Conceptos clave en la preparación de solicitudes de propuestas y revisiones/evaluaciones de ofertas
2. Términos, medición e informes de Acuerdos de Nivel de Servicio (Service Level Agreements, SLA)
3. Principios de ley contractual, indemnización y seguro de responsabilidad

4. Procesos de supervisión para garantizar que se estén cubriendo necesidades de la organización y requisitos contractuales

CAMPO TRES

Investigaciones (9% -- fue 10%)

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

1. Delitos financieros y relacionados con fraudes
2. Delitos de propiedad intelectual y espionaje industrial
3. Delitos contra propiedades (p.ej., incendio provocado, vandalismo, robo, sabotaje)
4. Delitos cibernéticos (p.ej., denegación de servicio distribuida (DDoS), phishing, ransomware)
5. **Delitos contra personas (p.ej., violencia en el trabajo, el tráfico de personas, el acoso)**

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

Conocimientos de

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

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

Conocimientos de

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

CAMPO CUATRO

Seguridad personal (11% -- fue 12%)

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

CAMPO CINCO

Seguridad física (16% -- fue 25%)

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

CAMPO SEIS

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

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

Conocimientos de

1. Elementos de un programa de seguridad de la información, que incluye seguridad física; seguridad de procedimientos; seguridad de sistemas de información; sensibilización de empleados; y capacidades destrucción de información y recuperación
2. Técnicas de realización de estudios
3. Evaluaciones cuantitativas y cualitativas de riesgo
4. Estrategias de mitigación de riesgos (p. ej., tecnología, personal, proceso, diseño de instalaciones, etc.)
5. Métodos de análisis costo-beneficio
6. Tecnología, equipos y procedimientos de protección (p. ej., interoperabilidad)
7. Amenazas de seguridad de la información
8. integración de instalaciones, planes del sistema, dibujos y esquemas

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

Conocimientos de

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

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

Conocimientos de

1. Seguridad de la información que incluye confidencialidad, integridad y disponibilidad
2. Metodología de sistemas de seguridad de la información
3. Técnicas de autenticación (p. ej., multifactorial, biometría)
4. Programas de evaluación y mejora continua
5. Técnicas y prácticas de pruebas éticas de piratería y ataques
6. Técnicas de codificación y ocultación de datos (p. ej., criptografía)
7. Técnicas de integración de sistemas (p. ej., interoperabilidad, licencias, redes)
8. Metodología de análisis costo-beneficio
9. Técnicas de gestión de proyectos
10. Proceso de revisión del presupuesto (p. ej., ciclo de vida de desarrollo del sistema)
11. Proceso de evaluación y selección de proveedor
12. Aceptación final y procedimientos de pruebas
13. Tecnología de protección e investigaciones forenses

14. Programas de capacitación y sensibilización para mitigar amenazas y vulnerabilidades (p. ej., phishing, ingeniería social, ransomware, amenazas internas)

CAMPO SIETE

Gestión de crisis (13% -- fue 10%)

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

Conocimientos de

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

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

Conocimientos de

1. Técnicas de gestión de recursos (p. ej., acuerdos de ayuda mutua, MOUs)
2. Técnicas de planificación de emergencia
3. Técnicas de evaluación de priorización y daños
4. Técnicas de comunicación y protocolos de notificación (p. ej., interoperabilidad, términos operativos comunes, sistema de notificación de emergencia)
5. Técnicas de capacitación y ejercicios (p. ej., ejercicios de mesa y de gran escala)
6. Conceptos y diseño de centros de operaciones de emergencia (emergency operations center, EOC)
7. Funciones y deberes principales en una estructura de comando de incidente (p. ej., difusión de información, enlace, oficial de información pública (PIO))

Tarea 3: Responder a un incidente y gestionarlo.

Conocimientos de

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

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

Conocimientos de

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

PCI: Áreas de Conocimiento

CAMPO UNO

Gestión de casos (35%)

TAREA 1: Analizar casos de conflictos éticos correspondientes.

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

CAMPO DOS

Técnicas y procedimientos de investigación (50%)

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

1. Métodos de investigación usando recursos físicos
2. Métodos de investigación usando tecnología de la información
3. Métodos de análisis de resultados de investigaciones
4. Documentación de investigación
5. Fuentes de información (p. ej., gobierno, propia, abierta)
6. Capacidades de medios digitales

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

Conocimientos de

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

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

Conocimientos de

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

CAMPO TRES

Presentación de casos (15%)

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

Conocimientos de

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

TAREA 2: Preparar y presentar testimonios.

Conocimientos de

1. Tipos de testimonios
2. Preparación para testimonios

PSP: Áreas de Conocimiento

CAMPO UNO

Evaluación de seguridad física (34%)

Tarea 1: Desarrollar un plan de evaluación de seguridad física.

Conocimientos de

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

Tarea 2: Identificar activos para determinar su valor, criticidad e impacto de pérdidas.

Conocimientos de

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

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

Conocimientos de

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

Tarea 4: Realizar una investigación para identificar y cuantificar vulnerabilidades de la organización.

Conocimientos de

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

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

Conocimientos de

1. Estrategias y métodos de análisis de riesgos

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

CAMPO DOS

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

Tarea 1: Establecer requisitos de desempeño de programas de seguridad.

Conocimientos de

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

Tarea 2: Determinar medidas adecuadas de seguridad física.

Conocimientos de

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

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

Conocimientos de

1. Diseñar fases (fase previa al diseño, diseño esquemático, desarrollo de diseño, documentación de construcción, etc.)
2. Elementos de diseño (cálculos, bosquejos, especificaciones, revisión de presentaciones y datos técnicos de fabricantes, etc.)

3. Estándares de especificación de construcción (p. ej., Instituto de Especificaciones de Construcción, estándares de equipos del propietario, American Institute of Architects MasterSpec, etc.)
4. Integración de sistemas (enfoque técnico, conexión con sistemas que no sean de seguridad, etc.)
5. Conceptos de gestión de proyectos
6. Programación (p. ej., gráficos de Gantt, gráficos de PERT, hitos y objetivos, etc.)
7. Estimación de costos y análisis costo-beneficio de opciones de diseño
8. Ingeniería de valor

CAMPO TRES

Implementación de medidas de seguridad física (32%)

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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

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

Conocimientos de

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