



ASIS CAPÍTULO 222, LIMA – PÉRU

BIENVENIDOS AL FUTURO DE LA SEGURIDAD



BIENVENIDOS AL FUTURO DE LA SEGURIDAD

En los últimos años, se ha producido un cambio fundamental en la industria de la seguridad a medida que la seguridad se torna cada vez más globalizada.

Se está transformando en sistemas complejos de interconexiones e interdependencias. Los sucesos sin precedentes que han ocurrido en los últimos tiempos han aumentado la demanda de seguridad para proteger personas, instalaciones, activos y datos. Este nuevo panorama de la seguridad presenta tanto oportunidades como desafíos para el profesional de la seguridad de hoy en día.

BIENVENIDOS AL FUTURO DE LA SEGURIDAD

Mantener el status que ya no basta para promover una carrera profesional y el éxito.

A medida que el mercado del trabajo de seguridad se torna más competitivo, la certificación de la pericia profesional resulta aún más importante. En los últimos años, la certificación profesional se ha integrado cada vez más en áreas como requisitos de empleo, el proceso RFP y las revisiones del desempeño.

BIENVENIDOS AL FUTURO DE LA SEGURIDAD

Los empleadores de hoy en día no sólo están buscando profesionales de seguridad sino la competencia comprobada de profesionales de seguridad certificados por organismos de evaluación. Las empresas ahora otorgan un alto grado de importancia a la contratación, relación y promoción de profesionales de seguridad con credenciales, que estén preparados para afrontar los exigentes desafíos de seguridad de la actualidad, y anticipar los retos de mañana. Existen atractivas oportunidades profesionales para quienes estén preparados para capitalizar la demanda de profesionales de seguridad certificados por organismos de evaluación.

EL VALOR VERDADERO DE CUALQUIER CERTIFICACIÓN DE SEGURIDAD ES LA CREDIBILIDAD

La certificación desempeña un papel importante en la industria de la seguridad al identificar elevadas normas profesionales. Como indicador de calificaciones, la certificación es evidencia documentada de pericia y experiencia. Es un medio objetivo de distinguir a los profesionales de seguridad altamente competentes de aquellos que sólo dicen serlo. En el entorno de seguridad actual, se requiere o prefiere la certificación profesional para aquellos puestos de seguridad de alto nivel más buscados.

EL VALOR VERDADERO DE CUALQUIER CERTIFICACIÓN DE SEGURIDAD ES LA CREDIBILIDAD

Recientemente se ha introducido una gran proliferación de nuevas certificaciones de seguridad para aprovechar la mayor demanda de una certificación profesional.

Muchas son ofrecidas por organizaciones sin conexión previa con las certificaciones de seguridad ni con la seguridad misma. El nivel de conocimientos y experiencia requeridos para estas certificaciones varía ampliamente. Algunas certificaciones sólo requieren la afiliación a una organización y el pago de una cuota.

Bienvenido al futuro de la seguridad!!

MÁS DE 60 AÑOS DE EXPERIENCIA

ASIS International (ASIS) ha establecido normas de certificación en la profesión de seguridad durante más de 25 años. Las certificaciones de ASIS inspiran respeto porque están respaldadas por la credibilidad de ASIS, la organización líder en el mundo para profesionales de seguridad. Desde su fundación en 1955, ASIS ha sido un líder en avanzar la seguridad en todo el mundo. ASIS tiene más de 34.000 miembros y es el educador principal para los profesionales de seguridad.

LA NORMA INTERNACIONAL

La seguridad se ha convertido en un asunto global y las certificaciones de ASIS son reconocidas y aceptadas en todo el mundo como la norma de competencia profesional.

En una era de globalización, son transferibles a través de fronteras y culturas internacionales. Las certificaciones de ASIS proporcionan a las empresas internacionales un idioma común, y aseguran el cumplimiento con las mejores prácticas de la industria de la seguridad. Las compañías multinacionales buscan cada vez más profesionales de seguridad certificados por organismos de evaluación con certificaciones de seguridad aceptadas internacionalmente.

LA NORMA INTERNACIONAL

La obtención de la certificación de ASIS mejora la capacidad de presentarse en el mercado como profesional de seguridad altamente calificado. Para los profesionales expertos, la certificación valida los conocimientos y la experiencia de trabajo en el mundo real.

Para los profesionales con poca experiencia laboral, la misma establece objetivos profesionales a fin de garantizar una comprensión integral de los conocimientos relacionados con el área en cuestión.

UNA CREDENCIAL QUE LOS EMPLEADOS RECONOCEN, RESPETAN Y EXIGEN

La certificación de ASIS es una credencial que es propiedad del individuo, y que amplía las opciones profesionales.

Es una designación que puede transferirse completamente a través de los sectores público y privado. La obtención de la certificación por un organismo de evaluación aumenta el potencial de ascensos profesionales, responsabilidades de mayor nivel y recompensas económicas.

La certificación de ASIS brinda al profesional de seguridad el respeto y la credibilidad necesarios para interactuar de manera eficaz con otros profesionales que toman decisiones.

La obtención de la certificación de ASIS aumenta la seguridad laboral, tanto a corto como a largo plazo.

UNA CREDENCIAL QUE LOS EMPLEADORES RECONOCEN, RESPETAN Y EXIGEN.

Para los profesionales de gobierno, militares o policiales que piensan abandonar el sector público, Para los profesionales Jóvenes que buscan oportunidades de incursionar en la Profesión de la Seguridad Privada, cada vez más especializada y con retos particulares del siglo XXI

La certificación de ASIS brinda una manera de construir sobre la experiencia previa en seguridad, desarrollar una orientación proactiva y realizar la transición hacia una segunda carrera profesional exitosa en el sector privado.

CERTIFICACIONES

ASIS ofrece tres certificaciones de seguridad, que incluyen dos de especialización.

Elija la certificación para la cual mejor esté capacitado, según sus conocimientos, experiencia, aptitud e intereses.



COMPLEMENTOS DE CERTIFICACIONES



GESTION DE NEGOCIOS

SEGURIDAD FÍSICA

INVESTIGACIONES

SEGURIDAD DEL PERSONAL

GESTION DE SEGURIDAD

ADMINISTRACIÓN DE EMERGENCIAS

SEGURIDAD DE LA INFORMACIÓN



CONOCIMIENTO EXIGIDOS PARA OBTENER LA CERTIFICACION CPP

Principales y Practicas de Seguridad

Objetivo 01/01

Conocimiento de
01/01/01
01/01/02

Planificar, organizar, dirigir y administrar el programa de seguridad de la organización para evitar y/o controlar las pérdidas y aplicar los procesos necesarios para proporcionar un entorno de trabajo seguro.

Principios de planificación, organización y control
Teoría de la Seguridad, técnicas y procesos

Objetivo 01/02

Conocimiento de
01/02/01
01/02/02

Desarrollar, gestionar o dirigir el análisis amenaza/vulnerabilidad para determinar la probable incidencia y severidad de los desastres naturales, los provocados por el hombre y la actividad criminal en la rentabilidad de la organización y/o la capacidad de ofrecer productos o servicios.

Evaluación de riesgos cuantitativa y cualitativa
Análisis de Vulnerabilidad

Objetivo 01/03

Conocimiento de
01/03/01
01/03/02
01/03/03

Evaluar los métodos para mejorar los sistemas de seguridad y la prevención de pérdidas en forma continua, a través del uso de auditorías, revisión y evaluación

Métodos de análisis costo-beneficio
Tecnologías de seguridad disponibles
Recopilación de datos y técnicas de análisis de tendencias

Objetivo 01/04

Conocimiento de
01/04/01
01/04/02
01/04/03

Desarrollar y administrar programas de relaciones con organismos de seguridad del Estado u otras organizaciones, con el fin de lograr objetivos de prevención de pérdidas

Roles y responsabilidades de organizaciones y agencias externas
Métodos para crear relaciones de trabajo efectivas
Técnicas y protocolos de enlace

Objetivo 01/05

Conocimiento de
01/05/01
01/05/02

Elaborar y presentar programas de sensibilización de los empleados de seguridad con el fin de conseguir las metas y objetivos organizacionales

Metodologías de entrenamiento
Estrategias, técnicas y métodos de comunicación

CONOCIMIENTO EXIGIDOS PARA OBTENER LA CERTIFICACION CPP

Seguridad del Personal

Objetivo 04/01	Desarrollar, implementar y administrar, las investigaciones de antecedentes para validar a los individuos para la contratación, promoción o retención
Conocimiento de 04/01/01	Investigaciones de antecedentes y técnicas de selección de personal
04/01/02	Calidad y tipo de fuentes de información
Objetivo 04/02	Desarrollar, implementar, administrar y evaluar políticas, procedimientos, programas y métodos para proteger a las personas en el lugar de trabajo contra el hostigamiento, amenazas
Conocimiento de 04/02/01	Métodos y técnicas de seguridad
04/02/02	Análisis de evaluación de amenazas
04/02/03	Tácticas de intervención y respuesta
04/02/04	Diseño e implementación de programas educativos y de sensibilización
04/02/05	Seguridad en programas de viajes
Objetivo 04/03	Desarrollar, implementar y administrar programas de protección de ejecutivo
Conocimiento de 04/03/01	Métodos y técnicas de protección de ejecutivos
04/03/02	Análisis de Riesgos
04/03/03	Técnicas de enlace y gestión de recursos
04/03/04	Selección, costos y efectividad de tener personal de protección de ejecutivos propios o externos
04/03/05	Seguridad en programas de viajes

Seguridad de la Información

Objetivo 06/01

Estudio de seguridad de las instalaciones, los procesos y los sistemas para evaluar el estado de: la seguridad Física, la seguridad de los sistemas de información, los procedimientos de seguridad, la sensibilización de los empleados y la capacidad de destrucción y recuperación de la información

Conocimiento de
06/01/01
06/01/02
06/01/03
06/01/04

Estudio de seguridad y metodología de evaluación de riesgos, análisis de riesgos cualitativo y cuantitativo y análisis costo-beneficio de las medidas de Seguridad.
Procedimientos, equipos y tecnología de seguridad
Metodología actual que compromete la información
Planos, diseños y esquemas del edificio y de los sistemas

Objetivo 06/02

Desarrollar e implementar las políticas y normas para asegurar que la información esté protegida contra todas las formas de acceso, uso, divulgación, modificación, destrucción o negación, no autorizado/inadvertido

Conocimiento de
06/02/01
06/02/02
06/02/03
06/02/04
06/02/05

Principios de Administración
Teoría y terminología de seguridad de la información
Leyes relativas a la protección de la información confidencial y de la propiedad intelectual
Medidas de seguridad, equipos y técnicas; incluyendo los procesos de seguridad de la información, los sistemas de acceso físico, el control de datos y el manejo y destrucción de la información
Técnicas y tendencias actuales que comprometen la información

Objetivo 06/03

Desarrollar y gestionar un programa de controles de seguridad integrado, para garantizar la confidencialidad, integridad, disponibilidad, autenticación, reconocimiento, contabilidad, auditoría, capacidad de recuperación de información sensible y los recursos tecnológicos asociados, los activos y las investigaciones

Conocimiento de
06/03/01
06/03/02
06/03/03
06/03/04
06/03/05
06/03/06
06/03/07
06/03/08
06/03/09
06/03/10

Teoría y metodología de seguridad de la información
Análisis de la evaluación de amenazas y vulnerabilidades y su mitigación
Técnicas de integración de sistemas
Metodología de análisis de costo-beneficio
Técnicas de administración de proyectos
Proceso de desarrollo de la proyección presupuestaria
Proceso de evaluación y selección de proveedores
Aceptación final y procedimiento de pruebas, sistemas de información, evaluación y programa de seguridad de la documentación
Tecnología de seguridad, equipamiento, investigaciones y procedimientos
Metodología y procedimientos de entrenamiento y sensibilización

Objetivo 06/04

Evaluar la efectividad de los controles de un programa integrado de seguridad de la información, que incluya las políticas, procedimientos y planes para asegurar la coherencia con la estrategia de la organización, sus metas y objetivos

Conocimiento de
06/04/01
06/04/02

06/04/03
06/04/04
06/04/05

Metodología de encuesta/evaluación de seguridad
Metodología de análisis de costo-beneficio, incluyendo la identificación y valoración de activos, el análisis de amenazas, la evaluación de la vulnerabilidad y la identificación de consecuencias/impacto
Tecnología/equipamiento de sistemas de seguridad
Técnicas de monitoreo, auditoría y pruebas
Investigaciones/auditorías (Due Diligence) para programas, proyectos y transacciones específicas (por ejemplo, fusiones, adquisiciones, evaluación de proveedores, contratos con terceros, etc.), cláusulas contractuales para proteger los activos de información y los sistemas (por ejemplo, relaciones con proveedores, vendedores, socios, consultores, subcontratistas y otros).

Investigación

Objetivo 08/01

Conocimiento de
08/01/01
08/01/02
08/01/03
08/01/04

Desarrollar y administrar programas de investigación
Principios y técnicas de desarrollo de políticas y procedimientos
Objetivos de la organización y enlace entre departamentos
Las fuentes de investigación
Métodos de preservación de la evidencia

Objetivo 08/02

Conocimiento de
08/02/01
08/02/02
08/02/03
08/02/04

Administrar o llevar a cabo la recolección y conservación de evidencias que apoyen acciones posteriores a una investigación (disciplina laboral, procedimientos criminales o civiles, arbitraje)
Técnicas de colección de evidencias
Protección/preservación de la escena del crimen
Requisitos de la cadena de custodia
Métodos de preservación de la evidencia

Objetivo 08/03

Conocimiento de
08/03/01
08/03/02

Administrar o llevar a cabo procesos de vigilancia
Técnicas de vigilancia
Recursos humanos, tecnológicos/equipamiento

Objetivo 08/04

Conocimiento de
08/04/01
08/04/02
08/04/03

Administrar y realizar investigaciones especializadas
Roles y responsabilidades de organizaciones y agencias externas
Métodos para crear relaciones de trabajo efectivas
Técnicas y protocolos de enlace

Objetivo 08/05

Conocimiento de
08/05/01
08/05/02
08/05/03
08/05/04
08/05/05

Administrar o realizar entrevistas de investigación
Métodos y técnicas de obtención de información
Técnicas para detectar el engaño
La comunicación no verbal
El uso de códigos de derechos humanos en declaraciones de advertencia
Componentes necesarios para las declaraciones escritas

Investigación

Objetivo 07/01

Conocimiento de

07/01/01

07/01/02

07/01/03

07/01/04

07/01/04

Evaluar y priorizar los riesgos para mitigar las posibles consecuencias de los incidentes

Todas las amenazas por tipo, probabilidad de ocurrencia y sus consecuencias

Análisis costo-beneficio

Estrategias de mitigación

Administración de riesgos y metodología de análisis de impacto en el negocio

Elaboración de un caso de negocios para la dirección

Objetivo 07/02

Conocimiento de

07/02/01

07/02/02

07/02/03

07/02/04

07/02/05

07/02/06

Preparar planificar cómo la organización responderá a los incidentes

Técnicas de administración de recursos

Técnicas de planificación de emergencias

Técnicas de comunicación

Técnicas entrenamiento y ejercicios

Concepto y diseño de Centro de operaciones de emergencia (EOC)

Funciones básicas y deberes en una estructura de comando de incidentes

Objetivo 07/03

Conocimiento de

07/03/01

07/03/02

Respuesta y gestión de un incidente

Técnicas de administración de recursos

Gestión, principios y prácticas de un centro de operaciones de emergencia (EOC)

Objetivo 07/04

Conocimiento de

07/04/01

07/04/02

07/04/03

07/04/04

Recuperarse de incidentes administrando la recuperación y la reanudación de funciones

Técnicas de administración de recursos

Estrategias de recuperación de corto y largo plazo

Recursos de apoyo para la recuperación

Oportunidades de mitigación en el proceso de recuperación

CONOCIMIENTO EXIGIDOS PARA OBTENER LA CERTIFICACION CPP



Protection of Assets



Standards & Guidelines



ASIS INTERNATIONAL



www.asisonline.org



ASIS Capítulo 222, Lima – Perú



www.asis.org.pe
informes@asis.org.pe