

CISSP®



Conocimientos globalmente reconocidos en el campo de seguridad de la información

Si planea construir una carrera en seguridad de la información, una de las profesiones más visibles de la actualidad, la credencial de Certified Information Systems Security Professional (CISSP®) debería ser el próximo objetivo en su carrera.

Un profesional con certificación CISSP es un profesional en aseguramiento de la información que define la arquitectura, diseño, administración y/o controles que garantizan la seguridad de los entornos comerciales. El amplio campo de conocimiento y la experiencia que se necesita para aprobar el examen es lo que distingue al profesional con certificación CISSP. La credencial demuestra un nivel globalmente reconocido de competencia provisto por (ISC)² CBK®, que cubre temas críticos en la seguridad actual, incluida la computación en la nube, seguridad móvil, seguridad en el desarrollo de aplicaciones, gestión del riesgo y más.

CISSP fue la primera credencial en el campo de la información que cumplió los estrictos requisitos de la Norma ISO/IEC 17024. CISSP no sólo es una medida objetiva de la excelencia, sino también un estándar mundialmente reconocido para medir los logros.

POR QUÉ CONVERTIRSE EN UN CISSP

Beneficios de CISSP para usted

- Demuestra conocimientos laborales sobre la seguridad de la información
- Confirma el compromiso con la profesión
- Ofrece un diferenciador en la carrera, con una mayor credibilidad y capacidad de comercialización
- Le ofrece beneficios exclusivos por ser miembro de (ISC)², incluidos valiosos recursos tales como las relaciones con pares y el intercambio de ideas
- Indica que los profesionales certificados en seguridad de la información obtienen un salario mundial promedio un 25% superior que sus equivalentes no certificados, según el estudio global de la fuerza de trabajo de seguridad de la información
- Cumple los requisitos del gobierno y de la organización para la certificación en seguridad de la información

Beneficios de CISSP para su empleador

- Coloca a los candidatos en un campo de juego nivelado ya que las certificaciones de (ISC)² poseen un reconocimiento internacional
- Ofrece una mayor credibilidad para su organización al trabajar con proveedores y contratistas
- Otorga a los empleados un lenguaje universal, evitando la ambigüedad con términos y prácticas aceptadas en la industria
- Valida el compromiso y los años de experiencia obtenidos en la industria
- Requiere créditos de educación profesional continua (CPE) para asegurar que el personal mantenga actualizados sus conocimientos
- Cumple con los requisitos obligatorios de certificación para proveedores de servicios o subcontratistas

"CISSP lo dice todo: Es una de las mejores calificaciones técnicas del mercado".

TheLadders, mayo de 2011

ASPECTOS DE CISSP

"La certificación CISSP que obtuve después de concurrir al seminario [de revisión] oficial de (ISC)² colaboró significativamente a mi ventaja competitiva y, como resultado, obtuve mi puesto actual. He establecido la certificación de (ISC)² como un requisito para los miembros de mi equipo, confiando que sus conocimientos son genuinos y actuales".

Daniel, CISSP
Países Bajos

"Obtener la certificación CISSP abrió puertas que pensé que eran inalcanzables. ¡Mi carrera, tanto profesional como académica, creció dramáticamente!"

Claudi, CISSP, CIA,
CISA, CISM
Italia

QUIÉN DEBE CONVERTIRSE EN UN CISSP

Los titulares de credenciales CISSP® con frecuencia desempeñan funciones laborales que incluyen:

- Consultor de seguridad
- Analista de seguridad
- Gerente de seguridad
- Ingeniero en sistemas de seguridad
- Director/Gerente de TI
- Gerente de seguridad de la información
- Auditor de seguridad
- Director de seguridad
- Arquitecto de seguridad
- Arquitecto de redes

Los candidatos de CISSP deben tener un mínimo de cinco años de experiencia laboral profesional directa sobre seguridad de tiempo completo en dos o más de los diez dominios de (ISC)²® CISSP CBK®, o cuatro años de experiencia laboral profesional directa sobre seguridad de tiempo completo en dos o más de los diez dominios de CISSP CBK con un título terciario. Alternativamente, existe una reducción de un año al requisito de experiencia profesional por poseer una credencial adicional en la lista aprobada de (ISC)².

PARTICIPE MIENTRAS OBTIENE LA EXPERIENCIA



Asociado de (ISC)² para CISSP

No es necesario que pase años en el campo para demostrar su competencia en seguridad informática. Conviértase en asociado de (ISC)², y ya formará parte de una organización con reputación y credibilidad, obteniendo el reconocimiento de empleadores y pares por el conocimiento de la industria que ya ha obtenido.

Requisitos de participación

El estado de asociado de (ISC)² está disponible para quienes poseen conocimientos en áreas clave de conceptos de la industria pero que no poseen experiencia laboral. Como candidato, puede tomar el examen de CISSP y suscribirse al Código de Ética de (ISC)². Sin embargo, para obtener la credencial CISSP tendrá que adquirir los años necesarios de experiencia profesional necesaria, presentar una prueba de ello y contar con el endoso de un miembro vigente de (ISC)². Si trabaja para obtener esta credencial, tendrá un máximo de seis años desde la fecha en que aprueba su examen para adquirir los cinco años necesarios de experiencia profesional. Se aplica un arancel anual de mantenimiento (AMF) de US\$ 35 y se deben obtener 20 créditos de educación profesional continua (CPE) cada año para mantenerse vigente.

Para obtener más información sobre cómo convertirse en asociado de (ISC)², visite www.isc2.org/associate.

AVANCE MÁS ALLÁ DE CISSP

Concentraciones de CISSP

Después de la concepción original de CISSP y la evolución continua de la seguridad de la información, (ISC)² descubrió la necesidad de desarrollar credenciales que cubran las necesidades específicas de nuestros miembros. Considerando esto, hemos producido nuestras concentraciones de CISSP para ofrecer una ruta de carrera que abra nuevas oportunidades a los titulares de credenciales CISSP. Específicamente, estas credenciales permiten funciones más demandantes en empresas de mayor tamaño y reconocen los talentos especializados de los CISSP.



- Profesional en Arquitectura en Seguridad de los Sistemas de Información (CISSP-ISSAP®)
- Profesional en Ingeniería en Seguridad de los Sistemas de Información (CISSP-ISSEP®)
- Profesional en Administración en Seguridad de los Sistemas de Información (CISSP-ISSMP®)

Para obtener la credencial CISSP-ISSAP, CISSP-ISSEP o CISSP-ISSMP, el CISSP debe mantener vigente su credencial y aprobar el examen de concentración correspondiente. Cada una de las tres concentraciones posee sus propios dominios CBK.

Para obtener más información, visite www.isc2.org/concentrations.

Los dominios de CISSP® se extraen de varios temas de seguridad de la información dentro de (ISC)²® CBK®. Actualizados anualmente, los dominios reflejan las mejores prácticas más actualizadas de todo el mundo, mientras se establece un marco común de términos y principios para discutir, debatir y resolver cuestiones relacionadas con la profesión.



El CISSP CBK incluye los diez dominios siguientes:

- **Control de acceso:** una colección de mecanismos que funcionan en conjunto para crear una arquitectura de seguridad para proteger los activos del sistema de información.
 - Conceptos/metodologías/técnicas
 - Efectividad
 - Ataques
- **Seguridad de telecomunicaciones y redes:** analiza las estructuras de redes, los métodos de transmisión, los formatos de transporte y las medidas de seguridad utilizadas para proporcionar disponibilidad, integridad y confidencialidad.
 - Arquitectura y diseño de red
 - Canales de comunicación
 - Componentes de redes
 - Ataques de redes
- **Administración de la seguridad de la información y gestión de riesgos:** la identificación de los activos de información de una organización y el desarrollo, documentación e implementación de políticas, estándares, procedimientos y lineamientos.
 - Administración y políticas de seguridad
 - Clasificación/propiedad de la información
 - Acuerdos contractuales y procesos de compra
 - Conceptos de gestión de riesgos
 - Seguridad del personal
 - Educación, capacitación e información sobre la seguridad
 - Certificación y acreditación
- **Seguridad en el desarrollo de software:** se refiere a los controles que se incluyen dentro del software de sistemas y aplicaciones y los pasos usados en su desarrollo.
 - Ciclo de vida del desarrollo de sistemas (SDLC)
 - Entorno de aplicaciones y controles de seguridad
 - Efectividad de la seguridad de aplicaciones
- **Criptografía:** los principios, medios y métodos de ocultar la información para garantizar su integridad, confidencialidad y autenticidad.
 - Conceptos de cifrado
 - Firmas digitales
 - Ataques criptanalíticos
 - Infraestructura de clave pública (KPI)
 - Alternativas para ocultar información
- **Arquitectura y diseño de seguridad:** contiene los conceptos, principios, estructuras y estándares usados para diseñar, implementar, supervisar y asegurar sistemas operativos, equipos, redes, aplicaciones y los controles usados para aplicar varios niveles de confidencialidad, integridad y disponibilidad.
 - Conceptos fundamentales de los modelos de seguridad
 - Capacidades de los sistemas de información (por ejemplo, protección de memorias, virtualización)
 - Principios de contramedidas
 - Vulnerabilidades y amenazas (por ejemplo, computación en la nube, agregación, control del flujo de datos)
- **Seguridad de las operaciones:** utilizada para identificar los controles sobre el hardware, medios y los operadores con privilegios de acceso a cualquiera de estos recursos.
 - Protección de recursos
 - Respuesta ante incidentes
 - Prevención y respuesta ante ataques
 - Administración de parches y vulnerabilidad
- **Continuidad comercial y planificación para la recuperación de desastres:** cubre la preservación del negocio en caso de interrupciones importantes a las operaciones comerciales normales.
 - Análisis del impacto comercial
 - Estrategia de recuperación
 - Proceso de recuperación de desastres
 - Proporcionar capacitación
- **Leyes, regulaciones, investigaciones y cumplimiento:** cubre las leyes y reglamentaciones sobre delitos informáticos; las medidas de investigación y técnicas que se pueden usar para determinar si se ha cometido un delito y los métodos para recopilar evidencia.
 - Cuestiones legales
 - Investigaciones
 - Procedimientos de argumentaciones
 - Requisitos/procedimientos de cumplimiento
- **Seguridad física (ambiental):** cubre las amenazas, vulnerabilidades y contramedidas que se pueden utilizar para proteger físicamente los recursos y la información sensible de una empresa.
 - Consideraciones sobre el diseño del sitio/las instalaciones
 - Seguridad del perímetro
 - Seguridad interna
 - Seguridad de las instalaciones

Descargue el Boletín de información para candidatos de CISSP at www.isc2.org/cib.

CISSP®

EDUCACIÓN OFRECIDA A SU MANERA

Seminario de revisión oficial de (ISC)²® CISSP® CBK®

Este seminario de revisión oficial es la revisión más integral y completa de conceptos de seguridad de los sistemas de información y las mejores prácticas de la industria, y el único curso de revisión que cuenta con el endoso de (ISC)². Como su forma exclusiva de revisar y actualizar su conocimiento sobre los dominios y sub-dominios de CISSP CBK, el seminario lo ayudará a identificar las áreas que necesita estudiar; e incluye:

- Material 100% actualizado
- Una descripción del campo de seguridad de la información
- Contribuciones de CISSP, instructores autorizados de (ISC)² y expertos en el tema
- Autoevaluación posterior al seminario

El seminario de revisión oficial de CISSP CBK se ofrece en los formatos siguientes:

- **En días múltiples en un entorno de salón de clases.** El material del curso se concentra en cubrir los diez dominios de CISSP. Disponible en todo el mundo en instalaciones de (ISC)² y filiales autorizadas de educación de (ISC)².
- **Privado en el sitio.** Disponible para grupos de mayor tamaño, esta opción con frecuencia ahorra tiempo y gastos de viaje de los empleados. Precios para grupos también disponibles a organizaciones con 15 o más empleados que planean tomar el examen.
- **Programa Live OnLine.** Aprenda desde la conveniencia de su propia computadora. Live OnLine le ofrece el mismo contenido del curso galardonado que los seminarios en salón de clases o los seminarios privados en el sitio y el beneficio de un instructor autorizado de (ISC)².

Visite www.isc2.org/cissprevsem para obtener más información o para registrarse.

"Nuestra capacitación y nuestro instructor fueron excelentes. Los diez dominios se cubrieron con conocimiento exacto y experiencia que transmitió comprensión. El uso de Dennis de preguntas difíciles para prepararnos para el examen me permitió aprobar".

Joe, CISSP
Virginia, EE. UU.

"Tengo la certificación CISSP desde 2005 y espero obtener la certificación CISSP-ISSAP este año. Los beneficios de la formalización de mis conocimientos sobre el dominio siempre han sido claros, CISSP es reconocido en todo el mundo, y cuando los colegas y clientes ven esas letras en mi tarjeta de presentación, visiblemente sienten que están hablando con un experto en el dominio, y lo que es más importante, con una persona en quien pueden confiar. La capacitación de (ISC)² a la que concurrí siempre fue dirigida por instructores capacitados y amables con experiencia en el mundo real para compartir."

Rik, CISSP
Reino Unido

FILIALES DE EDUCACIÓN



Los seminarios de revisión oficial de (ISC)² CBK están disponibles en todo el mundo en las instalaciones de (ISC)² y por medio de filiales de educación autorizadas de (ISC)². Los seminarios de revisión oficial de (ISC)² CBK son realizados solamente por instructores autorizados de (ISC)² que son expertos en su campo y han demostrado su conocimiento sobre los dominios cubiertos.

No confíe en proveedores de capacitación no autorizados por (ISC)². Asegúrese de que su instructor ostente el logotipo de oficial de proveedor autorizado de (ISC)² para asegurar que experimente los mejores y más actuales programas disponibles.

Ganador del premio de la revista SC de 2011 – Mejor programa de capacitación de profesionales, (ISC)² Educación

Ganador del premio de la revista SC de 2012 – Mejor programa de certificación profesional, CISSP



**AWARDS
2012
WINNER**
Honored in the U.S.



Boletín de información para candidatos - gratuito

Su principal recurso en sus esfuerzos de estudio por convertirse en CISSP®. El CIB contiene un resumen del examen que describe los temas principales y los subtemas dentro de los dominios, una lista sugerida de referencias para un posterior estudio, información sobre el examen y políticas e instrucciones de registro/administración. www.isc2.org/cib



Guía oficial de (ISC)²® para CISSP CBK®

El libro de texto es un libro guía sobre seguridad de la información basado en CISSP CBK, un compendio global de las mejores prácticas de seguridad. El libro de texto está disponible en versión en papel o como libro electrónico y contiene información obligatoria, redactada y compilada por expertos de primer nivel con certificación CISSP - un elemento esencial para quienes buscan obtener la certificación CISSP. www.isc2.org/store



Autoevaluación studIScope

Experimente el examen de certificación CISSP lo más cerca posible antes de tomarlo. Cada studIScope de 100 preguntas ofrece el aspecto del examen, al tiempo que identifica los dominios clave a estudiar. Incluso recibirá un plan de estudio personalizado. www.isc2.org/studiscope



Vista previa de dominios CBK: Canal gratuito de webcasts

Vea una serie de breves webcasts que ofrecen una descripción detallada de cada dominio de CISSP, el valor de la certificación y cómo estudiar para el examen. www.isc2.org/previews



Aprendizaje electrónico

Estas conferencias y ejercicios dinámicos de aprendizaje electrónico con ritmo propio se basan en los comprobados seminarios de revisión de CBK. Ofrecidos con un acceso de 60 o 120 días en un formato de internet fácil de usar, estas conferencias y ejercicios se dividen en módulos de revisión de dominios individuales para un estudio enfocado. Cada paquete de aprendizaje electrónico presenta preguntas de revisión de fin del dominio y fin del curso modeladas después del examen de certificación. El aprendizaje electrónico también otorga créditos de educación profesional continua (CPE) para los miembros de (ISC)². www.isc2.org/self-paced

LISTA DE VERIFICACIÓN PARA LA CERTIFICACIÓN

- ✓ **Obtenga la experiencia requerida:** Para la certificación CISSP®, cinco años de experiencia laboral profesional directa de tiempo completo en seguridad en dos o más de los diez dominios de (ISC)²® CISSP CBK®, o cuatro años de experiencia laboral profesional directa de tiempo completo en seguridad en dos o más de los diez dominios de CISSP CBK con un título terciario. Si usted no cuenta con la experiencia necesaria, aún puede tomar un examen y convertirse en asociado de (ISC)² hasta obtener la experiencia necesaria.
- ✓ **Estudie para el examen:** Utilice estas herramientas educativas opcionales para aprender acerca de CISSP CBK.
 - Boletín de información para candidatos
 - Webcasts de vista previa de dominios de CBK
 - Libro de texto oficial
 - Autoevaluación studIScope
 - aprendizaje electrónico con ritmo propio
 - Seminario de revisión oficial
- ✓ **Regístrese para el examen**
 - Visite www.isc2.org/certification-register-now para programar una fecha de examen
 - Enviar el arancel del examen
- ✓ **Apruebe el examen:** Apruebe el examen CISSP con un puntaje escalado de 700 puntos o más. Lea las preguntas más frecuentes sobre los puntajes de examen en www.isc2.org/exam-scoring-faqs.
- ✓ **Complete el proceso de endoso:** Una vez que se le ha informado que ha aprobado con éxito el examen, tendrá nueve meses a partir de la fecha en que tomó el examen para completar el siguiente proceso de endoso:
 - Complete un formulario de endoso de solicitud
 - Suscríbase al código de ética de (ISC)²
 - Solicite el endoso de su formulario a un miembro de (ISC)²La credencial puede ser otorgada una vez que se han completado los pasos anteriores y su formulario ha sido enviado. * Consulte los lineamientos y obtenga el formulario en www.isc2.org/endorsement.
- ✓ **Mantenga la certificación :** Se requiere una nueva certificación cada tres años, con requisitos continuos para mantener las credenciales en vigencia. Esto se logra principalmente obteniendo 120 créditos de Educación profesional continua (CPE) cada tres años, con un mínimo de 20 CPE obtenidos después de cada certificación. Si no se cumplen los requisitos de CPE, los CISSP deben volver a tomar el examen para mantener la certificación. Los CISSP también deben pagar un arancel anual de mantenimiento (AMF) de US\$ 85.

Para obtener más información sobre CISSP, visite www.isc2.org/cissp.

**Aviso de auditoría: Los candidatos que aprueban el examen serán seleccionados al azar y auditados por (ISC)² antes de la emisión de los certificados. Las certificaciones múltiples pueden resultar en que un candidato sea auditado más de una vez.*

(ISC)² es la más grande entidad de membresía sin afanes de lucro formada por profesionales certificados en seguridad de la información en todo el mundo, con más de 80.000 miembros en más de 135 países. Globalmente reconocido como Estándar Industrial, (ISC)² emite credenciales de Certified Information Systems Security Professional (CISSP®) y concentraciones relacionadas, así como el Certified Secure Software Lifecycle Professional (CSSLP®), Certified Authorization Professional (CAP®) y Systems Security Certified Practitioner (SSCP®) a los candidatos elegibles. Las certificaciones de (ISC)² fueron unas de las primeras credenciales sobre seguridad de la información que cumplieron con los estrictos requisitos de la Certificación ISO/IEC 17024, un hito global para evaluar y certificar al personal. (ISC)² también ofrece programas y servicios educativos basados en su CBK®, un compendio de temas de seguridad de la información. Puede encontrar más información en www.isc2.org.



BENEFICIOS PARA MIEMBROS

GRATUITO:

Serie de liderazgo en seguridad
Iniciativas de la industria
Verificación de la certificación
Programa de capítulos
Recepciones de (ISC)²/oportunidades para el establecimiento de relaciones
Programa global de premios de (ISC)²
Foro en línea
Simposio electrónico
ThinkTANK
Estudio global de la fuerza de trabajo de seguridad de la información
Revista *InfoSecurity Professional*
SecurityTalk
Oportunidades para voluntarios de seguridad en línea
Herramientas para la carrera
InterSeC
Grupos de medios sociales de primer nivel

CON DESCUENTO:

Conferencias de la industria
el periódico de (ISC)²

Mantenga la certificación con los CPE y AMF requeridos

