CISSP®

Certified Information Systems Security Professional

La nueva generación de líderes de seguridad

En un mundo cibernético cada vez más complejo hay una necesidad creciente de líderes de seguridad de la información que posean la experiencia amplia y especializada de conocimientos necesarios para crear programas de seguridad integral que aseguren la protección de los activos de información de las organizaciones. Es ahí donde entra el Certified Information Systems Security Professional - CISSP®.

La certificación CISSP es la credencial ideal para aquellas personas con probada y profunda competencia técnica y directiva, habilidades, experiencia y credibilidad para construir y mantener programas de seguridad que protejan a las organizaciones contra ataques cada vez más sofisticados. El CISSP usa un completo y actualizado conjunto global de conocimientos que garantiza a los líderes de seguridad un profundo conocimiento y comprensión de las nuevas amenazas, tecnologías, regulaciones, normas y prácticas.

Respaldado por (ISC)²®, la organización sin ánimos de lucro, reconocida a nivel mundial, dedicada a avanzar en el campo de seguridad de la información, el CISSP fue la primera credencial en el campo de la seguridad de la información a satisfacer los estrictos requisitos de la norma ISO/IEC 17024. No sólo la certificación CISSP es una medida objetiva de excelencia, sino también es un estándar de éxitos reconocido mundialmente.

POR QUÉ SER UN CISSP

El CISSP le ayuda a:

- Validar su probada competencia adquirida a través de años de experiencia en seguridad de la información.
- Demostrar sus conocimientos, habilidades y capacidades técnicas para desarrollar con eficacia un programa de seguridad holística comparado con los estándares aceptados a nivel mundial.
- Diferenciarse de otros candidatos para puestos de trabajo deseables en el cada vez más creciente mercado de seguridad de la información.
- Afirmar su compromiso con el campo y la continua relevancia a través de la formación profesional continua y la comprensión de las mejores prácticas más actuales.
- Acceder a recursos valiosos para su carrera, como crear redes de contactos e intercambiar ideas con sus pares.

CSSLP ayuda a los empleadores a:

- Protegerse contra las amenazas con profesionales calificados que tienen la experiencia necesaria para diseñar, construir y mantener de forma competente un ambiente de negocios seguro.
- Garantizar que los profesionales se mantengan actualizados acerca de nuevas amenazas, tecnologías, regulaciones, normas y prácticas a través de los requerimientos de educación profesional continua.
- Aumentar la confianza de que los candidatos están calificados y comprometidos con la seguridad de la información.
- Asegurar que los empleados usen un lenguaje universal, eludir la ambigüedad con términos y prácticas aceptadas en el sector.
- Aumentar la credibilidad de las organizaciones cuando se trabaja con clientes y proveedores.

CISSP en las Noticias

"La credencial CISSP distingue los profesionales del área de seguridad de TI"

- About.com

"El 56% de los trabajos en ciberseguridad exige CISSP."

- The Washington Post

"Mejor programa de certificación profesional"

- SC Magazine

OPINIONES DEL CISSP

"La certificación CISSP que obtuve después de asistir al seminario oficial de (ISC)² sumó enormemente a mi ventaja competitiva y, como resultado, gané mi posición actual. Ahora estoy haciendo de la certificación (ISC)² un requisito para los miembros de mi equipo, seguro de que sus habilidades son genuinas y actuales"

Daniel, CISSP
Los Países Bajos

"Obtener la certificación CISSP me abrió puertas que creía inviolables. ¡Mi carrera, tanto profesional como académica, creció de forma espectacular!"

Claudi, CISSP, CIA, CISA, CISM
Italia

(ISC)²®

QUIÉN DEBE OBTENER UN CISSP

Los titulares de la credencial CISSP® a menudo ejercen funciones de trabajo incluyendo:

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

EDUCACIÓN OFRECIDA A SU MANERA

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

Este seminario es la revisión más integral y completa de los conceptos de seguridad de sistemas de información y de las mejores prácticas del sector, y el único curso de formación avalado por (ISC)². Como su forma exclusiva de revisar y actualizar sus conocimientos de los dominios y subdominios del CBK CISSP, el seminario le ayudará a identificar las áreas y aplicaciones que necesita estudiar:

- Material didáctico oficial (ISC)²
- Impartido por un instructor autorizado de (ISC)²
- Manual del estudiante
- Colaboración con compañeros de clase
- Escenarios y actividades de aprendizaje del mundo real

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

- **Presencial** Ofrecido en un ambiente de salón de clases durante cinco días, los seminarios de capacitación se imparten en las instalaciones de (ISC)² y en los proveedores oficiales de capacitación de (ISC)² en todo el mundo. Este formato es perfecto para los que prefieren clases prácticas.
- **Privado in situ** Realice su propio seminario de capacitación dentro o fuera de las instalaciones de su organización. Disponible para grupos más numerosos, esta opción a menudo 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 comodidad de su propia computadora. Live OnLine le ofrece el mismo contenido del curso galardonado que los seminarios en salón de clases o los privados in situ y el beneficio de un instructor autorizado de (ISC)².

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

PROVEEDORES OFICIALES DE CAPACITACIÓN

Los seminarios oficiales de capacitación CBK de (ISC)² están disponibles en todo el mundo en las instalaciones de (ISC)² y por medio de proveedores oficiales de capacitación de (ISC)². Los seminarios oficiales de capacitación CBK de (ISC)² son impartidos solamente por instructores autorizados de (ISC)² que son expertos en su campo y han demostrado su conocimiento sobre los dominios cubiertos. Encuentre su proveedor oficial de capacitación más cercano en **www.isc2.org/educationaffiliates.aspx.**

(ISC)² OFFICIAL TRAINING PROVIDER

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

SC MAGAZINE AWARDS 2014 WINNER Honored in the U.S. 2013 2012 2011 2010 2009 2007 2006

Ganador del premio de la revista SC de 2014 – Mejor programa de certificación profesional, CISSP

Ganador del premio de la revista SC de 2013 – Mejor programa de capacitación profesional, Educación (ISC)²

EL CBK CISSP

Los dominios del CISSP® proceden de diversos temas de seguridad de la información dentro del CBK® de (ISC)²®. Actualizados anualmente, los dominios reflejan las mejores y más actualizadas prácticas en todo el mundo.

El CBK CISSP abarca los siguientes ocho dominios: (Efectivo desde 15 de abril de 2015)

- **Gestión de seguridad y riesgos** (Seguridad, riesgo, cumplimiento, leyes, reglamentos y continuidad del negocio)
  - Conceptos de confidencialidad, integridad y disponibilidad
  - Principios de gobernanza de la seguridad
  - Cumplimiento
  - Cuestiones legales y regulatorias
  - Ética profesional
  - Políticas, estándares, procedimientos y directrices de seguridad
  - Requerimientos para la continuidad del negocio
  - Políticas de seguridad del personal
  - Conceptos de gestión de riesgo
  - Modelado de amenazas
  - Consideraciones de riesgo
  - Educación, capacitación y concienciación en seguridad
- **Seguridad de activos** (Protección de la seguridad de activos)
  - Clasificación de la información y de activos
  - Propiedad (por ej. propietarios de datos, de sistemas)
  - Protección de la privacidad
  - Retención apropiada
  - Controles de seguridad de los datos
  - Requisitos de manejo (por ej. marcado, etiquetas, almacenamiento)
- **Ingeniería de seguridad** (Ingeniería y administración de la seguridad)
  - Procesos de ingeniería usando principios de diseño seguro
  - Conceptos básicos de modelos de seguridad
  - Modelos de evaluación de seguridad
  - Capacidades de seguridad de sistemas de información
  - Vulnerabilidades de las arquitecturas de seguridad, del diseño y de los elementos de las soluciones de seguridad
  - Vulnerabilidades de los sistemas basados en la web
  - Vulnerabilidades de los sistemas móviles
  - Vulnerabilidades de los dispositivos integrados y de sistemas ciber-físicos
  - Criptografía
  - Principios de seguridad para diseño de sitios e instalaciones
  - Seguridad física
- **Seguridad de comunicaciones y redes** (Diseño y protección de la seguridad de redes)
  - Diseño de la arquitectura de red segura (por ej. protocolos IP y no IP, segmentación)
  - Componentes de red segura
  - Canales de comunicación segura
  - Ataques de red
- **Gestión de identidad y acceso** (Control de acceso y gestión de identidad)
  - Control de activos físicos y lógicos
  - Identificación y autenticación de personas y dispositivos
  - Identidad como servicio (por ej. identidad en la nube)
  - Servicios de identidad de terceros (por ej. en la sede)
  - Ataques a controles de acceso
  - Ciclo de vida del aprovisionamiento de identidad y acceso (por ej. revisión del aprovisionamiento)
- **Evaluación y pruebas de seguridad** (Diseño, ejecución y análisis de pruebas de seguridad)
  - Estrategias de evaluación y pruebas
  - Datos de proceso de seguridad (por ej. controles de gestión y operativos)
  - Pruebas de control de seguridad
  - Resultados de pruebas (por ej. automatizado, manual)
  - Vulnerabilidades de arquitecturas de seguridad
- **Operaciones de seguridad** (Conceptos básicos, investigación, gestión de incidentes y recuperación de desastres)
  - Apoyo a las investigaciones y requisitos
  - Registro y seguimiento de las actividades
  - Aprovisionamiento de recursos
  - Conceptos básicos de operaciones de seguridad
  - Técnicas para la protección de recursos
  - Gestión de incidentes
  - Medidas de prevención
  - Gestión de correcciones y vulnerabilidades
  - Procesos de gestión de cambios
  - Estrategias de recuperación
  - Planes y procesos para la recuperación de desastres
  - Planificación y ejercicios de continuidad del negocio
  - Seguridad física
  - Preocupaciones de seguridad del personal
- **Seguridad en el desarrollo de software** (Entendimiento, aplicación y cumplimiento de la seguridad del software)
  - Seguridad en el ciclo de vida de desarrollo del software
  - Controles de seguridad del ambiente de desarrollo
  - Efectividad de la seguridad del software
  - Impacto en la seguridad del software adquirido

Descargue una copia de la Descripción del Examen CISSP en **www.isc2.org/exam-outline.**

(ISC)²®

LISTA DE VERIFICACIÓN PARA LA CERTIFICACIÓN

✓ **Obtenga la experiencia necesaria** - Para la certificación CISSP® los candidatos deben tener un mínimo de cinco años acumulativos de experiencia laboral profesional remunerada a tiempo completo en dos o más de los ocho dominios del CBK® CISSP de (ISC)²®, o cuatro años de experiencia laboral profesional remunerada acumulativos a tiempo completo en dos o más de los ocho dominios del CBK CISSP además de una licenciatura. Si usted no cuenta con la experiencia necesaria, aún puede tomar el examen y convertirse en Asociado de (ISC)² hasta obtener la experiencia necesaria. Visite **www.isc2.org/associate** para saber más.

✓ **Estudie para el examen** - Utilice estas herramientas educativas opcionales para aprender acerca de CBK CISSP.

- Descripción del examen - **www.isc2.org/exam-outline**
- Manual oficial - **www.isc2.org/store**
- Seminario de capacitación oficial - **www.isc2.org/cissprevsem**

✓ **Regístrese para el examen**

- Visite **www.pearsonvue.com/isc2** para programar una fecha de examen
- Envie el pago de la tasa de examen

✓ **Apruebe el examen** - Apruebe el examen de 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 informado que usted aprobó 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 el formulario de solicitud de endoso
- Suscríbase al código de ética de (ISC)²
- Solicite el endoso de su formulario a un miembro de (ISC)²

La credencial puede ser otorgada una vez que se han completado los pasos anteriores y su formulario ha sido enviado.* Consulte las directrices 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 obteniendo y publicando un mínimo de 40 créditos de Educación Profesional Continua (CPE) de los 120 créditos exigidos en el ciclo de certificación de tres años, y pagando la tasa anual de mantenimiento (AMF) de US$ 85 durante cada año del ciclo de certificación de tres años antes de la fecha de aniversario de su certificación o recertificación anual. Para saber más, visite **www.isc2.org/maintaining-your-credential**.

BENEFICIOS PARA MIEMBROS

GRATUITOS:

Eventos (ISC)² de un día sobre seguridad de información (SecureEvents)
Iniciativas de la industria
Verificación de la certificación
Programa de Capítulos
Oportunidades de networking/Recepciones de (ISC)²
Programa Internacional de Premios (ISC)²
Foro en línea
Webinars e-Symposium (ISC)²
ThinkTANK
Estudio Global de la Fuerza de Trabajo de Seguridad de la Información
Revista InfoSecurity Professional
Oportunidades de voluntariado en el programa Safe and Secure Online
InterSeC

CON DESCUENTO:

(ISC)² Security Congress
Eventos (ISC)² locales de dos días sobre seguridad de información
Conferencias de la industria
Manuales (ISC)²
El periódico de (ISC)²

Mantenga la certificación con los CPEs y AMFs requeridos.

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

**Aviso de auditoría - Los candidatos que aprueban el examen serán seleccionados aleatoriamente 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..*

*Creado en 1989, (ISC)²® es la más grande entidad de membresía sin ánimos de lucro formada por profesionales certificados en seguridad de software e información en todo el mundo, con más de 100.000 miembros en más de 160 países. Globalmente reconocido como Estándar de Oro, (ISC)² emite credenciales de Certified Information Systems Security Professional (CISSP®) y Concentraciones relacionadas, así como el Certified Secure Software Lifecycle Professional (CSSLP®), Certified Cyber Forensics Professional (CCFPSM), el Certified Authorization Professional (CAP®), HealthCare Information Security and Privacy Practitioner (HCISPPSM) y Systems Security Certified Practitioner (SSCP®) a candidatos cualificados. Las certificaciones de (ISC)² fueron unas de las primeras credenciales de tecnología de la información que cumplieron con los estrictos requisitos de la Norma ISO/IEC 17024, un estándar de referencia global para evaluar y certificar al personal. (ISC)² también ofrece programas y servicios educativos basados en su CBK®, un compendio de temas e información sobre seguridad de software. Puede encontrar más información en **www.isc2.org**.*

(ISC)²®

CIS.0
(02/15)