SSCP®

Systems Security Certified Practitioner

An (ISC)² Certification

Esquema del examen de certificación

Fecha efectiva: Noviembre 2021

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

Sobre SSCP

El Systems Security Certified Practitioner (SSCP®) es la certificación ideal para aquellos con habilidades técnicas probadas y conocimientos prácticos de seguridad en roles operativos de TI. Proporciona la confirmación de la capacidad de un profesional para implementar, monitorear y administrar la infraestructura de TI de acuerdo con las políticas y procedimientos de seguridad de la información que garantizan la confidencialidad, integridad y disponibilidad de los datos.

El amplio espectro de los temas incluidos en el conjunto común de conocimientos (Common Body of Knowledge (CBK®)) de SSCP garantizan su relevancia en todas las disciplinas en el campo de la seguridad de la información. Los candidatos seleccionados son competentes en los siguientes siete dominios:

- Operaciones de seguridad y administración
- Controles de acceso
- Identificación de riesgos, monitoreo y análisis
- Respuesta y recuperación de incidentes
- Criptografía
- Seguridad de redes y comunicaciones
- Seguridad de sistemas y aplicaciones

Requisitos de experiencia

Los candidatos deben tener un mínimo de un año de experiencia laboral acumulada en uno o más de los siete dominios del CBK (conjunto común de conocimientos) del SSCP. A aquellos que presenten un título (licenciatura o maestría) en un programa de ciberseguridad se les otorgará el un año de experiencia de requisito previo.

Un candidato que no tenga la experiencia requerida para convertirse en SSCP puede convertirse en Asociado de (ISC)² al aprobar con éxito el examen SSCP. El Asociado de (ISC)² tendrá dos años para obtener el año de experiencia requerido. Puede conocer más sobre los requisitos de experiencia previa para SSCP y cómo dar cuenta de los trabajos de tiempo parcial y pasantías en www.isc2.org/Certifications/CCSP/experience-requirements.

Acreditación

SSCP cumple con los estrictos requisitos de la norma ANSI/ISO/IEC 17024.

Análisis de tareas laborales (JTA)

(ISC)² tiene la obligación con sus miembros de mantener la relevancia del SSCP. Realizado a intervalos regulares, el análisis de tareas laborales (JTA) es un proceso metódico y crítico para determinar las tareas que realizan los profesionales de seguridad que se dedican a la profesión definida por el SSCP. Los resultados del JTA se utilizan para actualizar el examen. Este proceso garantiza que los candidatos sean evaluados en las áreas temáticas actuales y relevantes para las funciones y responsabilidades de los profesionales de seguridad de la información en la actualidad.

Información del examen SSCP

Duración del examen	4 horas
Cantidad de preguntas	150
Formato de las preguntas	Opción múltiple
Calificación necesaria para aprobar	700 de 1000 puntos
Disponibilidad del examen	Inglés, Japonés, Chino, Coreano, Alemán y Español
Centro de examen	Pearson VUE Testing Center

Ponderación del examen para SSCP

Dominios	Ponderación
1. Operaciones de seguridad y administración	16%
2. Controles de acceso	15%
3. Identificación de riesgos, monitoreo y análisis	15%
4. Respuesta y recuperación de incidentes	14%
5. Criptografía	9%
6. Seguridad de redes y comunicaciones	16%
7. Seguridad de sistemas y aplicaciones	15%
Total:	**100%**

Dominio 1: Operaciones de seguridad y administración

1.1 Cumplir con códigos de ética

» Código de Etica (ISC)²
» Código de ética de la organización

1.2 Comprender conceptos de seguridad

» Confidencialidad
» Integridad
» Disponibilidad
» Responsabilidad
» Privacidad
» No rechazo
» Mínimo privilegio
» Segregación de funciones (SoD)

1.3 Identificar e implementar controles de seguridad

» Controles técnicos (ej: tiempo de espera de la sesión, antigüedad de contraseñas)
» Controles físicos (ej. trampas, cámaras, cerraduras)
» Controles administrativos (ej. políticas de seguridad, estándares, procedimientos, niveles mínimos)
» Evaluar el cumplimiento
» Auditoria y revisión periódica

1.4 Documentar y mantener controles de seguridad funcionales

» Controles disuasivos
» Controles preventivos
» Controles de detectivos
» Controles correctivos
» Controles compensatorios

1.5 Participar en el ciclo de vida de la gestión de activos (hardware, software y datos)

- Proceso, planificación, diseño e iniciación
- Desarrollo/Adquisición
- Inventario y obtención de licencias
- Ejecución/Evaluación
- Operación/Mantenimiento
- Requisitos de archivo y conservación
- Eliminación y destrucción

1.6 Participar en el ciclo de vida de la gestión de cambio

- Gestión de cambio (ej. roles, responsabilidades, procesos)
- Análisis de impacto de seguridad
- Gestión de la configuración (CM)

1.7 Participar en la implementación de la formación y conciencia de seguridad (por ejemplo, la ingeniería social/ phishing)

1.8 Colaborar en las operaciones de seguridad física (ej. evaluación del centro de datos, identificación)

Dominio 2: Controles de acceso

2.1 Implementación y mantenimiento de métodos de autenticación

» Autenticación multifactor (MFA) y factor único (SFA)
» Single sign-on (SSO) (ej. Servicios de Federación de Directorio Activo (ADFS), OpenID Connect)
» Autenticación de dispositivo
» Acceso federado (ej. Autorización abierta 2 (OAuth2), Lenguaje de marcado para confirmaciones de seguridad (SAML))

2.2 Soporte de arquitecturas de confianza de interconexión de redes

» Relaciones de confianza (ej. unilaterales, bilaterales, transitivas, cero)
» Internet, intranet y extranet
» Conexiones a terceros

2.3 Participar en el ciclo de vida de la gestión de identidades

» Autorización
» Verificación
» Aprovisionamiento/Desaprovisionamiento
» Mantenimiento
» Derecho/Legitimación
» Sistemas de gestión de identidades y acceso (IAM)

2.4 Comprender y aplicar controles de acceso

» Obligatorio
» Discrecional
» Basado en roles (ej. atributo, sujeto, basado en objeto)
» Basado en reglas

Dominio 3: Identificación de riesgos, monitoreo y análisis

3.1 Comprender el proceso de gestión de riesgo

» Visibilidad de riesgos e informes (ej. registro de riesgos, intercambio de inteligencia sobre amenazas/ Indicadores de compromiso (IOC), Sistema de puntuación de vulnerabilidades comunes (CVSS))
» Conceptos de gestión de riesgo (ej. evaluación de impacto, modelado de amenazas)
» Marco de gestión de riesgo (ej: Organización Internacional de Normalización (ISO), Instituto Nacional de Estándares y Tecnología (NIST))
» Tolerancia de riesgo (ej. apetito)
» Tratamiento de riesgo (ej. aceptar, transferir, mitigar, evitar, ignorar)

3.2 Comprender consideraciones legales y regulatorias (ej. jurisdicción, límites, privacidad)

3.3 Participar en evaluaciones de seguridad y actividades de gestión de vulnerabilidades

» Pruebas de seguridad
» Revisión de riesgo (ej. interno, proveedor, arquitectura)
» Ciclo de vida de la gestión de vulnerabilidades

3.4 Operar y monitorear plataformas de seguridad (ej. monitoreo continuo)

» Sistemas de origen (ej. aplicaciones, dispositivos de seguridad, dispositivos de red y hosts)
» Eventos de interés (ej. anomalías, intrusiones, cambios sin autorización, monitoreo de cumplimiento)
» Gestión de logs
» Agregación y correlación de eventos

3.5 Analizar resultados de monitoreo

» Nivel mínimo de seguridad y anomalías
» Visualización, métricas y tendencias (ej. notificaciones, tablero, líneas de tiempo)
» Análisis de datos de un evento
» Documentar y comunicar hallazgos (ej. escalado)

Dominio 4:
Respuesta y recuperación de incidentes

4.1 Ciclo de vida de soporte de incidentes (ej: Organización Internacional de Normalización (ISO), Instituto Nacional de Estándares y Tecnología (NIST))

» Preparación
» Detección, análisis, escalado
» Contención
» Erradicación
» Recuperación
» Lecciones aprendidas/Implementación de nuevas contramedidas

4.2 Comprender y respaldar investigaciones forenses

» Derecho (ej. civil, penal, administrativo) y principios éticos
» Manejo de la evidencia (ej. primera respuesta, triaje, cadena de custodia, preservación de la escena)
» Reporte de análisis

4.3 Comprender y respaldar las actividades del plan de continuidad del negocio (BCP) y del plan de recuperación ante desastres (DRP)

» Planes y procedimientos de respuesta de emergencia (ej. contingencia de sistemas de información, pandemia, desastres naturales, gestión de crisis)
» Estrategias de procesamiento interinas o alternativas
» Plan de restauración
» Implementación de respaldo y redundancia
» Pruebas y simulacros

Dominio 5: Criptografía

5.1 Comprender los fundamentos y requisitos del cifrado

» Confidencialidad
» Integridad y autenticidad
» Sensibilidad de datos (ej. Información de Identificación Personal (PII), propiedad intelectual (IP), información de salud protegida (PHI))
» Mejores prácticas regulatorias e industriales (ej. Estándar de Seguridad de la Información de la Industria de las Tarjetas de Pago (PCI-DSS), Organización Internacional de Normalización (ISO))

5.2 Aplicar conceptos de cifrado

» Hashing
» Salting
» Cifrado simétrico/asimétrico /cifrado de curva elíptica (ECC)
» No repudio (ej. firmas digitales / certificados, código de autenticación de mensajes mediante hash (HMAC), seguimiento de auditoría)
» Robustez de los algoritmos y claves de cifrado (ej. Estándar de cifrado avanzado (AES), Rivest-Shamir-Adleman (RSA), claves de 256-, 512-, 1024-, 2048-bit)
» Ataques criptográficos, criptoanálisis y contramedidas (ej., computación cuántica)

5.3 Comprender e implementar protocolos seguros

» Servicios y protocolos (ej. Seguridad de protocolo de internet (IPsec), Seguridad de la capa de transporte (TLS), Extensiones de Correo de Internet de Propósitos Múltiples / Seguro (S/MIME), Correo identificado por claves de dominio (DKIM)
» Casos de uso habituales
» Limitaciones y vulnerabilidades

5.4 Comprender y soportar sistemas de infraestructura de clave pública (PKI)

» Conceptos fundamentales de gestión de clave (ej. almacenamiento, rotación, composición, generación, destrucción, intercambio, revocación, custodia)
» Web of Trust (WOT) (ej. Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), blockchain)

Dominio 6: Seguridad de redes y comunicaciones

6.1 Comprender y aplicar conceptos fundamentales de redes

- Interconexión de sistemas abiertos (OSI) y modelos de Protocolo de Control de Transmisión/ Protocolo de Internet (TCP/IP)
- Topologías de redes
- Relación de redes (ej. redes de pares (P2P), servidor-cliente)
- Tipos de medios de transmisión (ej. por cable, inalámbrico)
- Redes definidas por software (SDN) (ej. Red de área amplia definida por software (SD-WAN), virtualización de redes, automatización)
- Puertos y protocolos usados habitualmente

6.2 Comprender los ataques de red (ej. Ataque distribuido de denegación de servicio (DDoS), Hombre-en-el-medio (MITM), envenenamiento de servicio de nombres de dominio (DNS) y contramedidas) (ej. Red de entrega de contenidos (CDN))

6.3 Gestionar los controles de acceso a redes

- Controles, estándares y protocolos de acceso a la red (ej. Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) 802.1X, Servicio de autenticación remota de llamadas de usuarios (RADIUS), Sistema plus de control de acceso del controlador de acceso a terminales (TACACS+))
- Operación y configuración de acceso remoto (ej. be thin client, red privada virtual (VPN))

6.4 Gestionar la seguridad de la red

- Ubicación lógica y física de dispositivos de red (ej. en línea, pasivo, virtual)
- Segmentación (ej. física/lógica, plano de control/datos, red virtual de área local (VLAN), lista de control de acceso (ACL), cortafuegos, micro segmentación)
- Gestión de dispositivo seguro

6.5 Operar y configurar dispositivos de seguridad basados en red

- Cortafuegos y proxies (ej. método de filtrado, cortafuego de aplicación web (WAF))
- Sistema de detección de intrusos (IDS) y sistema de prevención de intrusiones (IPS)
- Enrutadores y conmutadores
- Dispositivo de modelado de tráfico (ej. optimización de red de área amplia (WAN), balanceo de carga)

6.6 Comunicaciones inalámbricas seguras

- Tecnologías (ej. red móvil, Wi-Fi, Bluetooth, comunicación de campo cercano (NFC))
- Protocolos de autenticación y cifrado (ej. Privacidad Equivalente a Cableado (WEP), acceso Wi-Fi protegido (WPA), protocolo de autenticación extensible (EAP))
- Internet de las cosas (IoT)

Dominio 7:
Seguridad de sistemas y aplicaciones

7.1 Identificar y analizar el código malicioso y la actividad

- Malware (ej. rootkits, spyware, scareware, secuestro de datos, troyanos, virus, gusanos, trapdoors, puerta trasera, fileless
- Contramedidas de malware (ej. escáneres, antimalware, firma de código)
- Actividad maliciosa (ej. amenaza de información privilegiada, robo de datos, Ataque distribuido de denegación de servicio (DDoS), botnet, exploits de día cero, ataques basados en la web, amenaza persistente avanzada (APT))
- Contramedidas ante actividad maliciosa (ej. conocimiento de los usuarios, bebastionado del sistema, parcheo, aislamiento, prevención de pérdida de datos (DLP))
- Ingeniería social (ej. phishing, suplantación de identidad)
- Análisis de comportamiento (ej. aprendizaje automático, Inteligencia artificial (AI), análisis de datos)

7.2 Implementar y operar la seguridad en dispositivos finales

- Sistema de Prevención de Intrusiones en un Host (HIPS)
- Cortafuegos basados en host
- Aplicaciones autorizadas
- Cifrado de Endpoint (ej. cifrado del disco completo)
- Módulo de plataforma de confianza (TPM)
- Navegación segura
- Detección y respuesta en el Endpoint (EDR)

7.3 Administrar la gestión de dispositivos móviles (MDM)

- Técnicas de aprovisionamiento (ej. dispositivos corporativos, habilitado personalmente (COPE), Bring Your Own Device (BYOD))
- Uso de contenedores
- Cifrado
- Gestión de aplicación móvil (MAM)

7.4 Comprender y configurar la seguridad en la nube

- Modelos de implementación en la nube (ej.: pública, privada, híbrida, comunidad, nube múltiple)
- Categorías de servicios en la nube (ej.: Software como servicio (SaaS), Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS))
- Virtualización (ej. hipervisor)
- Conceptos legales y regulatorios (ej. privacidad, vigilancia, propiedad de datos, jurisdicción, eDiscovery)
- Almacenamiento, procesamiento y transmisión de datos (ej. archivo, recuperación, resiliencia)
- Requisitos de terceros/externalización (ej., Acuerdos de nivel de servicio, portabilidad de datos, destrucción de datos, auditoría)
- Modelos de responsabilidad compartida

7.5 Operar y mantener entornos virtuales seguros

- Hipervisor
- Dispositivos virtuales
- Containers
- Continuidad y resiliencia
- Ataques y contramedidas
- Almacenamiento compartido

Información adicional del examen

Referencias suplementarias

Se fomenta a los candidatos a complementar su educación y experiencia revisando los recursos relevantes que pertenecen al CBK e identificando áreas de estudio que pueden necesitar atención adicional.

Puede encontrar la lista completa de referencias suplementarias en www.isc2.org/certifications/References.

Políticas y procedimientos para tomar el examen

(ISC)² recomienda que los candidatos a SSCP revisen las políticas y procedimientos de forma previa al registro para el examen. Lea la información completa en www.isc2.org/Register-for-Exam.

Información legal

Para cualquier consulta relacionada con las políticas legales de(ISC)² , por favor contactar con el Departamento Legal de (ISC)² en legal@isc2.org.

Consultas a:

(ISC)² Americas
Tel: +1.866.331.ISC2 (4722)
Correo electrónico: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Correo electrónico: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0) 203 300 1625
Correo electrónico: info-emea@isc2.org