SSCP®

Systems Security Certified Practitioner

ISC2 Certification

Esquema del **examen de certificación**

Fecha de entrada en vigor: Septiembre de 2024

ISC2™

Acerca de SSCP

El certificado Systems Security Certified Practitioner (SSCP®) es la certificación ideal para las personas con aptitudes técnicas demostradas y conocimientos prácticos sobre seguridad en funciones operativas de TI. Confirma la capacidad del profesional para implantar, supervisar y administrar infraestructuras informáticas de acuerdo con políticas y procedimientos de seguridad de la información que garanticen la confidencialidad, integridad y disponibilidad de los datos.

El amplio espectro de temas incluidos en el conjunto de conocimientos del SSCP garantiza su relevancia en todas las disciplinas del campo de la seguridad de la información. Los candidatos seleccionados son competentes en los siguientes ámbitos:

- Conceptos y prácticas de seguridad
- Controles de acceso
- Identificación, supervisión y análisis de riesgos
- Respuesta a incidentes y recuperación
- Criptografía
- Seguridad de redes y comunicaciones
- Seguridad de sistemas y aplicaciones

Requisitos de experiencia

Experiencia requerida: Los candidatos deben tener un mínimo de un año de experiencia a tiempo completo en uno o más de los dominios del actual esquema del SSCP. La obtención de un título de grado (licenciatura o máster) en informática, tecnología de la información (TI) o campos relacionados puede satisfacer hasta un año de la experiencia requerida. Los trabajos a tiempo parcial y las pasantías también pueden contar para el requisito de experiencia.

Acreditación

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

Análisis de tareas de trabajo (JTA)

ISC2 tiene la obligación para con sus miembros de mantener la relevancia del SSCP. Realizado a intervalos regulares, el análisis de tareas de trabajo (JTA) es un proceso metódico y crítico para determinar las tareas que realizan los profesionales de la seguridad que se dedican a la profesión definida por el SSCP. Los resultados de el JTA se utilizan para actualizar el examen. Este proceso garantiza que los candidatos sean evaluados en las áreas temáticas pertinentes para las funciones y responsabilidades de los profesionales de la seguridad de la información en ejercicio en la actualidad.

Información sobre el examen SSCP

Duración del examen	3 horas
Número de preguntas	125
Formato de las preguntas	Opción múltiple
Calificación necesaria para aprobar	700 de 1000 puntos
Disponibilidad del examen	Inglés, japonés, español
Centro examinador	Centro Examinador de Pearson VUE

Ponderaciones del examen SSCP

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

Dominio 1:
Conceptos y prácticas de seguridad

1.1 Cumplir los códigos de ética

» Código de Ética del ISC2
» Código de ética de la organización

1.2 Comprender los conceptos de seguridad

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

1.3 Identificar y aplicar controles de seguridad

» Controles técnicos [por ejemplo, cortafuegos, sistemas de detección de intrusos (IDS), listas de control de acceso (ACL)].
» Controles físicos (por ejemplo, trampas, cámaras, cerraduras)
» Controles administrativos (por ejemplo, políticas de seguridad, normas, procedimientos, líneas de base)
» Evaluar los requisitos de cumplimiento
» Auditoría y revisión periódicas

1.4 Documentar y mantener controles de seguridad funcionales

» Controles disuasorios
» Controles preventivos
» Controles para detectar
» Controles correctivos
» Controles de compensación

1.5 Apoyar y aplicar el ciclo de vida de la gestión de activos (es decir, hardware, software y datos)

- Proceso, planificación, diseño e iniciación
- Desarrollo/Adquisición (por ejemplo, DevSecOps, pruebas)
- Inventario y licencias (por ejemplo, código abierto, código cerrado)
- Aplicación/Evaluación
- Funcionamiento/mantenimiento/final de vida útil (EOL)
- Requisitos de archivo y conservación
- Eliminación y destrucción

1.6 Apoyar y/o aplicar el ciclo de vida de la gestión de cambio

- Gestión de cambio (por ejemplo, funciones, responsabilidades, procesos, comunicaciones, auditoría)
- Análisis del impacto en la seguridad
- Gestión de la configuración (CM)

1.7 Apoyar y/o aplicar la concienciación y la formación en materia de seguridad (por ejemplo, ingeniería social/phishing/ejercicios de simulación/comunicaciones de concienciación).

1.8 Colaborar con las operaciones de seguridad física (por ejemplo, evaluación de centros de datos/instalaciones, gestión de credenciales y visitantes, restricciones de dispositivos personales).

Dominio 2:
Controles de acceso

2.1 Aplicar y mantener métodos de autenticación

» Autenticación única o multifactor (MFA)
» Inicio de sesión único (SSO) (por ejemplo, Servicios de Federación de Directorio Activo (ADFS), OpenID Connect)
» Autenticación del dispositivo (por ejemplo, certificado, dirección MAC (Media Access Control), TPM (Módulo de plataforma segura))
» Acceso federado (por ejemplo, Autorización abierta 2 (OAuth2), Lenguaje de marcado para confirmaciones de seguridad (SAML))

2.2 Comprender y apoyar las arquitecturas de confianza de la red interna

» Relaciones de confianza (por ejemplo, unidireccionales, bidireccionales, transitivas, nulas)
» Internet, intranet, extranet y zona desmilitarizada (DMZ)
» Conexiones de terceros (por ejemplo, interfaz de programación de aplicaciones (API), extensiones de aplicaciones, middleware)

2.3 Apoyar y/o aplicar el ciclo de vida de gestión de identidades

» Autorización
» Verificación
» Aprovisionamiento/desaprovisionamiento
» Supervisión, informes y mantenimiento (por ejemplo, cambios de funciones, nuevas normas de seguridad)
» Derechos (por ejemplo, derechos heredados, recursos)
» Sistemas de gestión de identidades y accesos (IAM)

2.4 Comprender y administrar los controles de acceso

» Obligatorio
» Discrecional
» Basado en roles (por ejemplo, basado en sujetos, basado en objetos, Gestión de Acceso Privilegiado (PAM))
» Basado en reglas
» Basado en atributos

Dominio 3:
Identificación, supervisión y análisis de riesgos

3.1 Comprender la gestión de riesgos

- Visibilidad de los riesgos y elaboración de informes (por ejemplo, registro de riesgos, intercambio de información sobre amenazas, indicadores de compromiso (IOC), sistema de puntuación de vulnerabilidades comunes (CVSS), socialización, modelo MITRE/ATT&CK).
- Conceptos de gestión de riesgos (por ejemplo, evaluaciones de impacto, modelización de amenazas, alcance).
- Marcos de gestión de riesgos (por ejemplo, Organización Internacional de Normalización (ISO), Instituto Nacional de Normas y Tecnología (NIST)).
- Tolerancia al riesgo (por ejemplo, apetito, cuantificación del riesgo)
- Tratamiento del riesgo (por ejemplo, aceptar, transferir, mitigar, evitar, ignorar)

3.2 Comprender los aspectos legales y normativos (por ejemplo, jurisdicción, limitaciones, privacidad)

3.3 Realizar evaluaciones de seguridad y actividades de gestión de vulnerabilidades

- Aplicación de marcos de gestión de riesgos
- Pruebas de seguridad
- Revisión de riesgos (por ejemplo, internos, de proveedores, de arquitectura)
- Ciclo de vida de la gestión de vulnerabilidades (por ejemplo, exploración, elaboración de informes, análisis, corrección).

3.4 Operar y supervisar plataformas de seguridad (por ejemplo, supervisión continua)

- Sistemas de origen (por ejemplo, aplicaciones, dispositivos de seguridad, dispositivos de red, servidores anfitriones)
- Eventos de interés (por ejemplo, errores, omisiones, anomalías, cambios no autorizados, incumplimiento, fallos de las políticas)
- Gestión de registros (por ejemplo, política, integridad, conservación, arquitecturas, configuración, agregación, ajuste)
- Gestión de eventos e información de seguridad (SIEM) (por ejemplo, supervisión en tiempo real, análisis, seguimiento, auditoría)

3.5 Analizar los resultados del seguimiento

- Líneas de base de seguridad y anomalías (por ejemplo, correlación, reducción del ruido)
- Visualizaciones, métricas y tendencias (por ejemplo, notificaciones, cuadros de mando, líneas de tiempo)
- Análisis de datos de sucesos
- Documentar y comunicar los resultados (por ejemplo, asuntos derivados a niveles superiores)

Dominio 4:
Respuesta a incidentes y recuperación

4.1 Comprender y apoyar el ciclo de vida de respuesta a incidentes (por ejemplo, Instituto Nacional de Normas y Tecnología (NIST), Organización Internacional de Normalización (ISO))

- Preparación (por ejemplo, definición de funciones, programas de formación)
- Detección, análisis y derivación a niveles superiores (por ejemplo, comunicación de incidentes, relaciones públicas)
- Contención
- Erradicación
- Recuperación (por ejemplo, documentación de incidentes)
- Actividades posteriores al incidente (por ejemplo, lecciones aprendidas, nuevas contramedidas, mejora continua)

4.2 Comprender y apoyar las investigaciones forenses

- Principios jurídicos (por ejemplo, civiles, penales, administrativos, etc.) y éticos
- Manipulación de pruebas (por ejemplo, primer interviniente, triaje, cadena de custodia, preservación de la escena))
- Informe de análisis
- Cumplimiento de la política de seguridad de la organización

4.3 Comprender y apoyar las actividades del plan de continuidad de la empresa (BCP) y el plan de recuperación ante desastres (DRP)

- Planes y procedimientos de respuesta en caso de emergencia (por ejemplo, contingencia de sistemas de información, pandemia, catástrofe natural, gestión de crisis).
- Estrategias de tratamiento provisionales o alternativas
- Planificación de la restauración (por ejemplo, tiempo objetivo de restauración (RTO), punto objetivo de restauración (RPO), tolerancia máxima de inactividad (MTD)).
- Implantación de copias de seguridad y redundancia
- Pruebas y simulacros (por ejemplo, libro de jugadas, ejercicios de simulación, ejercicios de recuperación en caso de catástrofe, programación).

Dominio 5: Criptografía

5.1 Comprender las razones y los requisitos de la criptografía

» Confidencialidad
» Integridad y autenticidad
» Sensibilidad de los datos (por ejemplo, información personal identificable (PII), propiedad intelectual (IP), información sanitaria protegida (PHI)).
» Mejores prácticas regulatorias y de la industria (por ejemplo, normas de seguridad de datos de la industria las tarjetas de pago (PCI-DSS), Organización Internacional de Normalización (ISO)).
» Entropía criptográfica (por ejemplo, criptografía cuántica, distribución de claves cuánticas)

5.2 Aplicar conceptos de criptografía

» Hashing
» Salting (agregar algo al final de las contraseñas)
» Cifrado simétrico/asimétrico/Criptografía de curva elíptica (ECC)
» No rechazo (por ejemplo, firmas/certificados digitales, código de autenticación de mensajes basado en hash (HMAC), registros de auditoría).
» Fuerza de los algoritmos de cifrado y claves (por ejemplo, Estandar de cifrado avanzado (AES), Rivest-Shamir-Adleman (RSA)
» Ataques criptográficos y criptoanálisis

5.3 Comprender y aplicar protocolos seguros

» Servicios y protocolos (por ejemplo, seguridad del protocolo de Internet (IPsec), seguridad en 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 comunes (por ejemplo, procesamiento de tarjetas de crédito, transferencia de archivos, cliente web, red privada virtual (VPN), transmisión de datos PII).
» Limitaciones y vulnerabilidades

5.4 Comprender y apoyar los sistemas de infraestructura de clave pública (PKI)

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

Dominio 6: Seguridad de redes y comunicaciones

6.1 Comprender y aplicar los conceptos fundamentales de las redes

- » Modelos de interconexión de sistemas abiertos (OSI) y protocolo de control de transmisión/protocolo de Internet (TCP/IP)
- » Topologías de red
- » Relaciones de red (por ejemplo, entre iguales (P2P), cliente-servidor)
- » Tipos de medios de transmisión (por ejemplo, por cable o inalámbricos)
- » Redes definidas por software (SDN) (por ejemplo, red de área amplia definida por software SD-WAN), virtualización de redes, automatización)
- » Puertos y protocolos más utilizados

6.2 Comprender los ataques a la red (por ejemplo, ataque distribuido de denegación de servicio (DDoS), ataque de intermediario (MITM), envenenamiento de caché del Sistema de Nombres de Dominio (DNS))

» Contramedidas (por ejemplo, redes de distribución de contenidos (CDN), cortafuegos, controles de acceso a la red, sistemas de prevención y de intrusiones (IDPS)).

6.3 Gestionar los controles de acceso a la red

- » Controles de acceso a la red, normas y protocolos (por ejemplo, Institute of Electrical and Electronics Engineers (IEEE) 802.1X, servicio de autenticación remota de llamadas de usuario (RADIUS), sistema plus de control de acceso al controlador de acceso a terminales (TACACS+)).
- » Funcionamiento y configuración del acceso remoto (por ejemplo, cliente ligero, red privada virtual (VPN), infraestructura de escritorio virtual).

6.4 Gestionar la seguridad de la red

- » Ubicación lógica y física de los dispositivos de red (por ejemplo, en línea, pasivos, virtuales).
- » Segmentación (p. ej., física/lógica, plano de datos/control, red de área local virtual (VLAN), lista de control de acceso (ACL), zonas de cortafuegos, microsegmentación).
- » Gestión segura de dispositivos

6.5 Operar y configurar dispositivos y servicios de seguridad basados en red

- » Cortafuegos y proxies (por ejemplo, métodos de filtrado, cortafuegos de aplicaciones web (WAF), agente de seguridad de acceso a la nube (CASB))
- » Sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS)
- » Enrutadores y conmutadores
- » Dispositivos de modelado del tráfico (por ejemplo, optimización de redes de área amplia (WAN), equilibrio de carga).
- » Controles de acceso a la red (NAC)
- » Prevención de pérdida de datos (DLP)
- » Gestión unificada de amenazas (UTM)

6.6 Comunicaciones inalámbricas seguras

- » Tecnologías (por ejemplo, red celular, Wi-Fi, Bluetooth, comunicación de campo cercano (NFC))
- » Protocolos de autenticación y cifrado (por ejemplo, acceso Wi-Fi protegido (WPA), protocolo de autenticación extensible (EAP), acceso Wi-Fi protegido 2 (WPA2), acceso Wi-Fi protegido 3 (WPA3))

6.7 Proteger y supervisar la Internet de las cosas (IoT) (por ejemplo, configuración, aislamiento de la red, actualizaciones de firmware , gestión del fin de vida útil (EOL))

Dominio 7: Seguridad de sistemas y aplicaciones

7.1 Identificar y analizar código y actividad maliciosos

- Malware (por ejemplo, rootkits, spyware, scareware, ransomware, troyanos, virus, gusanos, trampillas, puertas traseras, vulnerabilidades sin archivos, aplicaciones/códigos/sistemas operativos (SO)/códigos móviles)
- Contramedidas contra el malware (por ejemplo, escáneres, antimalware, contención y corrección, seguridad del software)
- Tipos de actividad maliciosa (por ejemplo, amenazas internas, robo de datos, denegación de servicio distribuido (DDoS), botnet, exploits de día cero, ataques basados en web, amenazas persistentes avanzadas (APT))
- Contramedidas para actividades maliciosas (por ejemplo, concienciación/capacitación del usuario, refuerzo del sistema, parches, aislamiento, prevención de pérdida de datos (DLP))
- Métodos de ingeniería social (por ejemplo, correo electrónico no deseado, phishing/smishing/vishing, suplantación de identidad, escasez, caza de ballenas)
- Análisis de comportamiento (por ejemplo, aprendizaje automático, inteligencia artificial (IA), análisis de datos)

7.2 Implementar y operar la seguridad de dispositivos endpoint

- Sistema de prevención de intrusiones basado en host (HIPS)
- Sistema de detección de intrusiones basado en host (HIDS)
- Cortafuegos basados en host
- Lista blanca de aplicaciones
- Cifrado de endpoint (por ejemplo, cifrado de disco completo)
- Módulo de plataforma segura (TPM) (por ejemplo, gestión del módulo de seguridad de hardware)
- Navegación segura (por ejemplo, certificados digitales)
- Detección y respuesta en el endpoint (EDR)

7.3 Detección y respuesta en el endpoint (EDR)

- Técnicas de aprovisionamiento (por ejemplo, propiedad corporativa, habilitado personalmente (COPE), traiga su propio dispositivo (BYOD), gestión de dispositivos móviles (MDM)).
- Contenerización
- Cifrado
- Gestión de aplicaciones móviles

7.4 Comprender y configurar la seguridad en la nube

- Modelos de implementación (por ejemplo, público, privado, híbrido, comunitario)
- Modelos de servicio (por ejemplo, infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS))
- Virtualización (por ejemplo, hipervisor, nube privada virtual (VPC))
- Cuestiones jurídicas y normativas (por ejemplo, privacidad, vigilancia, propiedad de los datos, jurisdicción, eDiscovery, tecnologías de la información (TI) en la sombra).
- Requisitos de terceros/externalización (por ejemplo, acuerdo de nivel de servicio (SLA), portabilidad/privacidad/destrucción/auditoría de datos).
- Modelo de responsabilidad compartida
- Almacenamiento, tratamiento y transmisión de datos (por ejemplo, archivo, copia de seguridad, recuperación, resistencia)

7.5 Operar y mantener entornos virtuales seguros

- Hipervisor (es decir, Tipo 1 (por ejemplo, bare metal), Tipo 2 (por ejemplo, software))
- Dispositivos virtuales
- Contenedores
- Continuidad y resiliencia
- Gestión del almacenamiento (por ejemplo, dominio de datos)
- Amenazas, ataques y contramedidas (por ejemplo, ataque de fuerza bruta, escape de máquinas virtuales, caza de amenazas).

Información adicional sobre el examen

Referencias complementarias

Se sugiere a los candidatos que complementen su formación y experiencia revisando los recursos pertinentes relacionados con el conjunto de conocimientos e identificando las áreas de estudio que puedan necesitar atención adicional.

Consulte la lista completa de referencias complementarias en www.ISC2.org/certifications/References.

Políticas y procedimientos del examen

ISC2 recomienda que los candidatos revisen las políticas y procedimientos del examen antes de inscribirse en el examen. Lea el amplio desglose de esta importante información en www.ISC2.org/Register-for-Exam.

Información legal

Para cualquier pregunta relacionada con las políticas legales de ISC2, póngase en contacto con el Departamento Legal de ISC2 en legal@isc2.org.

¿Tiene alguna pregunta?

Póngase en contacto con ISC2 Candidate Services en su región:

América
Tel: +1.866.331.ISC2 (4722), pulse 1
Correo electrónico: membersupport@isc2.org

Asia-Pacífico
Tel: +852-5803-5662
Correo electrónico: isc2asia@isc2.org

Europa, Oriente Medio y África
Tel: +44 (0)203-960-7800
Correo electrónico: info-emea@isc2.org