SSCP®

# Systems Security Certified Practitioner

## Certificación de ISC2

# Esquema del examen de certificación

Fecha de entrada en vigor: 1 de octubre de 2025

ISC2™

# Acerca de SSCP

La acreditación *Systems Security Certified Practitioner* (SSCP) es la certificación ideal para quienes cuentan con habilidades técnicas comprobadas y conocimientos prácticos de seguridad aplicados en funciones operativas de TI. Este certificado confirma las capacidades 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 temas incluidos en el temario del examen de SSCP asegura su relevancia en todas las disciplinas dentro del campo de la seguridad de la información. Los candidatos que obtengan esta certificación serán competentes en las siete áreas siguientes:

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

## Requisitos de experiencia previa

Los candidatos deben tener un mínimo de un año de experiencia a tiempo completo en una o más de las áreas del esquema de examen actual de SSCP. La obtención de un título universitario (licenciatura o maestría) en ciencias de la computación, tecnologías de la información (TI) o campos relacionados puede equivaler hasta un año de la experiencia requerida. El trabajo a tiempo parcial y las pasantías también pueden contar para el requisito de experiencia.

## Acreditación

SSCP cumple los requisitos estrictos de la norma ISO/IEC 17024 del Consejo Nacional de Acreditación (ANAB) del Instituto Estadounidense de Normas Nacionales (ANSI).

## Análisis de tareas laborales (ATL)

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

# Información sobre el examen PAC de SSCP

El examen de SSCP usa pruebas adaptativas computarizadas (PAC) para todos los exámenes en inglés, japonés y español moderno. Puede obtener más información sobre el examen PAC de SSCP en www.isc2.org/certifications/computerized-adaptive-testing.

| | |
|---|---|
| **Duración del examen** | 2 horas |
| **Número de preguntas** | 100 - 125 |
| **Formato de las preguntas** | Preguntas de opción múltiple y avanzadas |
| **Calificación necesaria para aprobar** | 700 de 1000 puntos |
| **Disponibilidad del examen** | Inglés, japonés, español |
| **Centro de examen** | Pearson VUE Testing Center |

# Ponderación del examen PAC de SSCP

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

# Área 1:
# Conceptos y prácticas de seguridad

## 1.1 Cumplir con los códigos de ética

- Código de ética de ISC2
- Código de ética de la organización

## 1.2 Comprender los conceptos de seguridad

- Confidencialidad
- Integridad
- Disponibilidad
- Responsabilidad
- No repudio
- Menor privilegio
- Segregación de funciones (SdF)

## 1.3 Identificar e implementar controles de seguridad

- Controles técnicos (ej., cortafuegos, sistemas de detección de intrusos (SDI), lista de control de acceso (LCA))
- Controles físicos (ej., puertas dobles de seguridad, cámaras, candados)
- Controles administrativos (ej., políticas de seguridad, normas, procedimientos, líneas base)
- Evaluación de los requerimientos de cumplimiento regulatorio
- Auditoría y revisiones periódicas

## 1.4 Documentar y mantener controles de seguridad funcionales

- Controles disuasorios
- Controles preventivos
- Controles de detección
- Controles correctivos
- Controles compensatorios

## 1.5 Apoyar e implementar el ciclo de vida de la gestión de activos (ej., hardware, software y datos)

- Proceso, planificación, diseño e iniciación
- Desarrollo / Adquisición (ej., DevSecOps, pruebas)
- Inventario y licencias (ej., código abierto, código cerrado)
- Implementación / Evaluación
- Funcionamiento / Mantenimiento / Fin de la vida útil (EOL)
- Requisitos de archivo y retención
- Eliminación y destrucción

## 1.6 Apoyar e/o implementar el ciclo de vida de la gestión del cambio

- Gestión del cambio (ej. roles, responsabilidades, procesos, comunicaciones, auditoría)
- Análisis del impacto en la seguridad
- Gestión de la configuración (GC)

## 1.7 Apoyar e/o implementar programas de concienciación y capacitación en seguridad (ej., ingeniería social, *phishing*, ejercicios de simulación, comunicaciones de concienciación)

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

# Área 2:
# Controles de acceso

## 2.1 Implementar y mantener métodos de autenticación

- Autenticación única / multifactor (MFA)
- Inicio único de sesión (SSO) (ej., Active Directory Federation Services (ADFS), OpenID Connect)
- Autenticación de dispositivos (ej., certificado, dirección de control de acceso al medio (MAC), módulo de plataforma segura (TPM))
- Acceso federado (ej., Open Authorization 2 (OAuth2), lenguaje de marcado para confirmaciones de seguridad (SAML))

## 2.2 Comprender y brindar soporte a las arquitecturas de confianza de las redes internas

- Relaciones de confianza (ej., unidireccional, bidireccional, transitiva, cero)
- Internet, intranet, extranet y zonas desmilitarizadas (DMZ)
- Conexiones de terceros (ej., (interfaz de programación de aplicaciones (API), extensiones de aplicaciones, *middleware*)

## 2.3 Brindar soporte e/o implementar el ciclo de vida de la gestión de identidades

- Autorización
- Verificación
- Aprovisionamiento / Desaprovisionamiento
- Monitoreo, informes y mantenimiento (ej., cambios de roles, normas nuevas de seguridad)
- Derechos (ej., derechos heredados, recursos)
- Sistemas de gestión de identidades y accesos (IAM)

## 2.4 Comprender y administrar controles de acceso

- Obligatorios
- Discrecionales
- Basados en roles (ej., basados en sujetos, basados en objetos, gestión de accesos privilegiados (PAM))
- Basados en reglas
- Basados en atributos

# Área 3: Identificación, monitoreo y análisis de riesgos

## 3.1 Comprender la gestión de riesgos

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

## 3.2 Comprender los aspectos jurídicos y regulatorios (ej., jurisdicción, limitaciones, privacidad)

## 3.3 Realizar evaluaciones de seguridad y actividades de gestión de vulnerabilidades

- Implementación de marcos de gestión de riesgos
- Pruebas de seguridad
- Revisión de riesgos (ej., internos, proveedores, arquitectura)
- Ciclo de vida de la gestión de vulnerabilidades (ej., escaneo, elaboración de informes, análisis, corrección)

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

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

## 3.5 Analizar los resultados del monitoreo

- Líneas base de seguridad y anomalías (ej., correlación, reducción del ruido)
- Visualizaciones, métricas y tendencias (ej., notificaciones, paneles de control, líneas de tiempo)
- Análisis de datos de eventos
- Documentación y comunicación de hallazgos (ej., escalado)

# Área 4:
# Respuesta y recuperación ante incidentes

## 4.1 Comprender y brindar soporte al ciclo de vida de la respuesta ante incidentes (ej., NIST, ISO)

- Preparación (ej., definición de roles, programas de capacitación)
- Detección, análisis y escalado (ej., comunicación de incidentes, relaciones públicas)
- Contención
- Erradicación
- Recuperación (ej., documentación de incidentes)
- Actividades posteriores al incidente (ej., lecciones aprendidas, nuevas contramedidas, mejora continua)

## 4.2 Comprender y brindar soporte a investigaciones forenses

- Principios jurídicos (ej., civiles, penales, administrativos) y éticos
- Manipulación de pruebas (ej., primer interviniente, triaje, cadenas de custodia, preservación de la escena)
- Informes de análisis
- Cumplimiento de la política de seguridad de la organización

## 4.3 Comprender y brindar soporte para las actividades del Plan de Continuidad de Negocio (PCN) y del Plan de Recuperación ante Desastres (DRP)

- Planes y procedimientos de respuesta ante emergencias (ej., contingencia de sistemas de información, pandemia, catástrofe natural, gestión de crisis)
- Estrategias de procesamiento provisionales o alternativas
- Planificación de la recuperación (ej., tiempo objetivo de recuperación (RTO), punto objetivo de recuperación (RPO), tolerancia máxima de inactividad (MTD))
- Implementación de copias de seguridad y redundancia
- Pruebas y simulacros (ej., manuales de estrategias, ejercicios de simulación, ejercicios de recuperación ante desastres, programación)

# Área 5: Criptografía

## 5.1 Comprender las razones y los requerimientos de la criptografía

- Confidencialidad
- Integridad y autenticidad
- Sensibilidad de los datos (ej., información personalmente identificable (PII), propiedad intelectual (PI), información médica protegida (PHI))
- Prácticas recomendadas del sector y regulatorias (ej., Estándar de Seguridad de la Información de la Industria de las Tarjetas de Pago (PCI-DSS), ISO)
- Entropía criptográfica (ej., criptografía cuántica, distribución de claves cuánticas)

## 5.2 Aplicar conceptos de criptografía

- Algoritmos hash
- Algoritmos salt
- Cifrado simétrico y asimétrico / Criptografía de curva elíptica (ECC)
- No repudio (ej., firmas o certificados digitales, código de autenticación de mensajes mediante hash (HMAC), rastros de auditoría)
- Fuerza de los algoritmos de cifrado y claves (ej., Estándares de Cifrado Avanzado (AES), Rivest-Shamir-Adleman (RSA))
- Ataques criptográficos y criptoanálisis

## 5.3 Comprender e implementar protocolos seguros

- Servicios y protocolos (ej., Seguridad del Protocolo de Internet (IPsec), Seguridad de la Capa de Transporte (TLS), Extensiones de Correo de Internet de Propósitos Múltiples/Seguros (S/MIME), Correo identificado por Claves de Dominio (DKIM))
- Casos de uso comunes (ej., procesamiento de tarjetas de crédito, transferencia de archivos, cliente web, redes privadas virtuales (VPN), transmisiones de datos personales)
- Limitaciones y vulnerabilidades

## 5.4 Comprender y brindar soporte a los sistemas de infraestructura de clave pública (PKI)

- Conceptos fundamentales de gestión de claves (ej., almacenamiento, rotación, composición, generación, destrucción, intercambio, revocación, custodia)
- Redes de confianza (WOT) (ej., Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), *blockchain*)

# Área 6: Seguridad de redes y comunicaciones

## 6.1 Comprender y aplicar los conceptos fundamentales sobre redes

- Modelos de Interconexión de Sistemas Abiertos (OSI) y de Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP)
- Topologías de red
- Relaciones de redes (ej., entre pares (P2P), cliente-servidor)
- Tipos de medios de transmisión (ej., por cable o inalámbricos)
- Redes definidas por software (SDN) (ej., redes de área amplia definidas por software (SD-WAN), virtualización de redes, automatización)
- Puertos y protocolos más utilizados

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

- Contramedidas (ej., redes de entrega de contenidos (CDN), cortafuegos, controles de acceso a la red, sistemas preventivos de detección de intrusos (SPDI))

## 6.3 Gestionar controles de acceso a la red

- Controles de acceso a la red, normas y protocolos (ej., Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) 802.1X, Servicio de Autenticación Remota de Llamadas de Usuarios (RADIUS), Sistema Plus de Control de Accesos del Controlador de Accesos a Terminales (TACACS+))
- Operación y configuración de accesos remotos (ej., cliente ligero, VPN, infraestructura de escritorio virtual)

## 6.4 Gestionar la seguridad de la red

- Ubicación lógica y física de los dispositivos de red (ej., en línea, pasivos, virtuales)
- Segmentación (ej., física/lógica, plano de datos/control, red virtual de área local (VLAN), LCA, zonas de cortafuegos, microsegmentación)
- Gestión de dispositivos seguros

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

- Cortafuegos y proxies (ej., métodos de filtrado, cortafuegos de aplicación-web (WAF), agente de seguridad de acceso a la nube (CASB))
- Sistemas de detección de intrusos (SDI) y sistemas de prevención de intrusos (SPI)
- Enrutadores y conmutadores
- Dispositivos de modelos de tráfico (ej., optimización de redes de área amplia (WAN), equilibrio de cargas)
- Control de acceso de red (NAC)
- Prevención de pérdida de datos (DLP)
- Gestión unificada de amenazas (UTM)

## 6.6 Comunicaciones inalámbricas seguras

- Tecnologías (ej., redes celulares, Wi-Fi, Bluetooth, Comunicación de Campo Cercano (NFC))
- Protocolos de autenticación y cifrado (ej., 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 monitorear el Internet de las Cosas (IoT) (ej., configuración, aislamiento de la red, actualizaciones de *firmware*, gestión de fin de la vida útil)

# Área 7: Seguridad de sistemas y aplicaciones

## 7.1 Identificar y analizar códigos y actividades maliciosas

- *Malware* (ej., *rootkits*, *spyware*, *scareware*, *ransomware*, troyanos, virus, gusanos, puertas trampa, puertas traseras, ataques sin archivos, vulnerabilidades de aplicaciones/código/sistemas operativos (SO)/código móvil)
- Contramedidas contra *malware* (ej., escáneres, software anti-*malware*, contención y remediación, seguridad de software)
- Tipos de actividad maliciosa (ej., amenazas internas, robo de datos, ataque distribuido de denegación de servicio (DDoS), *botnets*, *exploits* de día cero, ataques basados en web, amenazas persistentes avanzadas (APT))
- Contramedidas para actividades maliciosas (ej., concienciación/capacitación de usuarios, refuerzo de sistemas, aplicación de parches, aislamiento, prevención de pérdida de datos (DLP))
- Métodos de ingeniería social (ej., correos electrónicos spam, *phishing*/*smishing*/*vishing*, suplantación de identidad, tácticas de escasez, cacería de ballenas)
- Analítica de comportamiento (ej., aprendizaje automático, inteligencia artificial (IA), análisis de datos)

## 7.2 Implementar y operar la seguridad de dispositivos de endpoint

- Sistema de prevención de intrusos en el host (SPIH)
- Sistema de detección de intrusos en el host (SDIH)
- Cortafuegos basados en el host
- Lista blanca de aplicaciones
- Cifrado de endpoint (ej., cifrado de disco completo)
- Módulo de plataforma segura (TPM) (ej., gestión del módulo de seguridad de hardware)
- Navegación segura (ej., certificados digitales)
- Detección y respuesta en el endpoint (EDR)

## 7.3 Detección y respuesta en el endpoint (EDR)

- Técnicas de aprovisionamiento (ej., dispositivos de propiedad de una corporación habilitados personalmente (COPE), traiga su propio dispositivo (*Bring Your Own Device*, 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 (ej., pública, privada, híbrida, comunitaria)
- Modelos de servicio (ej., infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS))
- Virtualización (ej., hipervisor, nube privada virtual (VPC))
- Asuntos jurídicos y regulatorios (ej., privacidad, vigilancia, propiedad de los datos, jurisdicción, eDiscovery, TI en la sombra)
- Requerimientos de terceros/externalización (ej., acuerdos de nivel de servicio (SLA), portabilidad/privacidad/destrucción/auditoría de datos)
- Modelos de responsabilidad compartida
- Almacenamiento, procesamiento y transmisión de datos (ej., archivo, copias de seguridad, recuperación, resiliencia)

## 7.5 Operar y dar mantenimiento a entornos virtuales seguros

- Hipervisores (tipo 1 (*bare metal*), tipo 2 (software))
- Dispositivos virtuales
- Contenedores
- Continuidad y resiliencia
- Gestión del almacenamiento (ej., dominio de datos)
- Amenazas, ataques y contramedidas (ej., ataques de fuerza bruta, escape de máquinas virtuales, cacería 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 esquema de examen de SSCP e identificando las áreas de estudio que puedan requerir atención adicional.

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

## Políticas y procedimientos de examen

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

## Información legal

Si tiene alguna pregunta relacionada con las políticas legales de ISC2, comuníquese con el Departamento Legal de ISC2 a través del correo legal@isc2.org.

## ¿Alguna pregunta?

Comuníquese con el área de Servicios para Candidatos de ISC2 en su región:

**América**
Tel.: +1 866 331 ISC2 (4722), presione 1
Correo electrónico: membersupport@isc2.org

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

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