Objetivos del examen de certificación CompTIA Security+

NÚMERO DE EXAMEN: SY0-601

CompTIA

Acerca del examen

Se recomienda que los candidatos usen este documento como ayuda para prepararse para el examen de certificación de CompTIA Security+ (SY0-601). El examen de certificación CompTIA Security+ verificará que el candidato aprovado tenga los conocimientos y las habilidades requeridas para lo siguiente:

- **Evaluar la postura de seguridad de un entorno empresarial y recomendar e implementar soluciones de seguridad apropiadas**
- **Monitorear y asegurar los entornos híbridos, incluso en la nube, móviles y de IoT**
- **Operar con conocimiento de las leyes y políticas aplicables, incluso los principios de gobernanza, riesgo y cumplimiento**
- **Identificar, analizar y responder a los eventos e incidentes de seguridad**

Esto equivale a dos años de trabajo de experiencia práctica en un rol de trabajo de administrador de seguridad/sistemas.

Estos ejemplos de contenido pretenden aclarar los objetivos de la prueba y no se deben interpretar como un listado completo de todos los contenidos de este examen.

DESARROLLO DEL EXAMEN

Los exámenes de CompTIA son resultado de talleres de expertos del área temática y resultados de encuestas de toda la industria con respecto a las habilidades y conocimientos necesarios para un profesional de TI.

POLÍTICA DE USO DE MATERIALES AUTORIZADOS CompTIA

CompTIA Certifications, LLC no encuentra afiliada y no autoriza, aprueba o tolera la utilización de cualquier contenido proporcionado por otros sitios de capacitación no autorizados (conocidos como “brain dumps”). A las personas que utilicen este tipo de materiales en la preparación de cualquier examen CompTIA se les anularán los certificados y será suspendida la realización de futuras pruebas en concordancia con el Acuerdo para Candidatos de CompTIA. En un esfuerzo por comunicar de manera más clara las políticas de exámenes de CompTIA en relación con el uso de materiales de estudio autorizados, CompTIA dirige a todos los candidatos de certificación a las **Políticas de Examen de Certificación CompTIA**. Revise todas las políticas CompTIA antes de comenzar el proceso de estudio para cualquier examen CompTIA. Se requerirá que los candidatos cumplan el **Acuerdo de Candidato CompTIA**. Si un candidato tiene una pregunta acerca de qué materiales de estudio se consideran no autorizados (conocidos como “brain dumps”), él/ella deberá comunicarse con CompTIA al correo electrónico examsecurity@comptia.org para confirmar.

RECUERDE

Las listas de ejemplos proporcionada en formato con viñetas no son listas completas. Otros ejemplos de tecnologías, procesos o tareas relativas a cada objetivo también pueden ser incluidos en el examen, aunque no estén enumerados o cubiertos en este documento de objetivos. CompTIA revisa constantemente el contenido de nuestros exámenes y actualiza las preguntas de las pruebas para asegurar que nuestros exámenes sean actuales y la seguridad de las preguntas esté protegida. Cuando sea necesario, publicaremos exámenes actualizados, basados en objetivos de examen de prueba. Sepa que todos los materiales relacionados de preparación para el examen serán válidos.

DETALLES DE LA PRUEBA

Examen obligatorio	SY0-601
Número de preguntas	90 como máximo
Tipos de preguntas	Selección múltiple y basadas en la ejecución
Longitud de la prueba	90 minutos
Experiencia recomendada	• Al menos 2 años de experiencia de trabajo en la administración de sistemas de TI con un enfoque en la seguridad • Experiencia práctica técnica en seguridad de la información • Conocimiento general de los conceptos de seguridad
Calificación para aprobación	750 (en escala de 100-900)

OBJETIVOS DEL EXAMEN (DOMINIOS)

La siguiente tabla enumera los dominios medidos en este examen y el grado en el que están representados:

DOMINIO	PORCENTAJE DEL EXAMEN
1.0 Ataques, amenazas y vulnerabilidades	24%
2.0 Arquitectura y diseño	21%
3.0 Implementación	25%
4.0 Operaciones y respuesta a incidentes	16%
5.0 Gobernanza, riesgo y cumplimiento	14%
Total	**100%**

1.0 Ataques, amenazas y vulnerabilidades

1.1 Compare y contraste los diferentes tipos de técnicas de ingeniería social.

- **Phishing**
- **Smishing**
- **Vishing**
- **Spam**
- **Spam por mensajería instantánea (SPIM)**
- **Spear phishing**
- **Dumpster diving**
- **Shoulder surfing**
- **Pharming**
- **Tailgating**
- **Obtención de información**
- **Whaling**
- **Prepending**
- **Fraude de identidad**
- **Estafas de facturas**
- **Recolección de credenciales**
- **Reconocimiento**
- **Engaños**
- **Suplantación**
- **Watering hole attack**
- **Typosquatting**
- **Pretexting**
- **Campañas de influencia**
  - Guerra híbrida
  - Redes sociales
- **Principios (motivos de la efectividad)**
  - Autoridad
  - Intimidación
  - Consenso
  - Escasez
  - Familiaridad
  - Confianza
  - Urgencia

1.2 A partir de un escenario, analice los indicadores potenciales para determinar el tipo de ataque.

- **Malware**
  - Ransomware
  - Troyanos
  - Gusanos
  - Programas potencialmente no deseados (PUP)
  - Virus sin archivos
  - Comando y control
  - Bots
  - Criptomalware
  - Bombas lógicas
  - Spyware
  - Keyloggers
  - Troyano de acceso remoto (RAT)
  - Rootkit
  - Puerta trasera
- **Ataques de contraseña**
  - Spraying
  - Diccionario
  - Fuerza bruta
    - Fuera de línea
    - En línea
  - Tablas arcoíris
  - Texto plano/sin cifrar
- **Ataques físicos**
  - Cable Bus Serial Universal (USB) malicioso
  - Unidad de Pendrive maliciosa
  - Clonación de tarjetas
  - Skimming
- **Inteligencia artificial (AI) Adversarial**
  - Datos de entrenamiento contaminados para el aprendizaje automático (ML)
  - Seguridad de los algoritmos de aprendizaje automático
- **Ataques en la cadena de suministro**
- **Ataques basados en la nube vs. ataques on-premise**
- **Ataques criptográficos**
  - Cumpleaños
  - Colisión
  - Degradación

1.3 A partir de un escenario, analice los indicadores potenciales asociados a los ataques de aplicaciones.

- **Escalamiento de privilegios**
- **Cross-site scripting**
- **Inyecciones**
  - Lenguaje de consulta estructurada (SQL)
  - Biblioteca de vínculos dinámicos (DLL)
  - Protocolo ligero de acceso a directorio (LDAP)
  - Lenguaje Extensible de Marcas (XML)
- **Puntero/Objeto sin referencia**
- **Recorrido de directorios**
- **Desbordamientos de búfer**
- **Condiciones de carrera**
  - Tiempo de control/tiempo de uso
- **Manejo de errores**
- **Manejo inapropiado de entradas**
- **Ataque de repetición**
  - Repeticiones de sesiones
- **Desbordamiento de enteros**
- **Falsificaciones de solicitudes**
  - Entre servidores
  - Entre sitios
- **Ataques a la interfaz de programación de aplicaciones (API)**
- **Agotamiento de recursos**
- **Memory leak**
- **Secure Socket Layer (SSL) stripping**
- **Manipulación de drivers**
  - Shimming
  - Refactorización
- **Pass the hash**

1.4 A partir de un escenario, analice los indicadores potenciales asociados a ataques de red.

- **Redes Inalámbricas**
  - Evil twin
  - Rogue access point
  - Bluesnarfing
  - Bluejacking
  - Disociación
  - Interferencia (jamming)
  - Identificación por radiofrecuencia (RFID)
  - Comunicación de campo cercano (NFC)
  - Vector de Inicialización (VI)
- **Ataque en ruta (antes conocido como ataque man-in-the-middle/ ataque man-in-the-browser)**
- **Ataques Capa 2**
  - Envenenamiento del Address Resolution Protocol (ARP)
  - Desbordamiento del Media access control (MAC)
  - Clonación MAC
- **Sistema de nombres de dominio (DNS)**
  - Secuestro de dominio
  - Envenenamiento de DNS
  - Redirección del Uniform Resource Locator (URL)
  - Reputación del dominio
- **Denegación de servicio distribuido (DDoS)**
  - Red
  - Aplicación
  - Tecnología operativa (OT)
- **Código malicioso o ejecución de script**
  - PowerShell
  - Python
  - Bash
  - Macros
  - Visual Basic para Aplicaciones (VBA)

1.5 Explique los diferentes actores de amenazas, vectores y fuentes de inteligencia.

- **Actores y amenazas**
  - Advanced persistent threat (APT)
  - Amenazas internas
  - Actores estatales
  - Hacktivistas
  - Script kiddies
  - Sindicatos criminales
  - Hackers
    - Autorizado
    - No autorizado
    - Semiautorizado
  - Shadow IT
  - Competidores
- **Actores de amenazas**
  - Interno/externo
  - Nivel de sofisticación/capacidad
  - Recursos/financiación
  - Intención/motivación
- **Vectores**
  - Acceso directo
  - Redes inalámbricas
  - Correo electrónico
  - Cadena de suministro
  - Redes sociales
  - Medios extraíbles
  - Cloud
- **Fuentes de inteligencia de amenazas**
  - Open-source intelligence (OSINT)
  - Cerrado/privado
  - Bases de datos de vulnerabilidades
  - Centros de información compartida pública/privada
  - Dark web
  - Indicadores de compromiso
  - Uso compartido de indicadores automatizados (AIS)
    - Expresión estructurada de información sobre amenazas (STIX)/Intercambio automatizado y confiable de información de inteligencia (TAXII)
  - Análisis predictivo
  - Mapas de amenazas
  - Repositorios de archivos/códigos
- **Fuentes de investigación**
  - Sitios web de proveedores
  - Informes de vulnerabilidades
  - Conferencias
  - Artículos académicos
  - Request for comments (RFC)
  - Grupos de industria local
  - Redes sociales
  - Informes sobre amenazas informáticas
  - Tácticas, técnicas y procedimientos del adversario (TTP)

1.6 Explique las preocupaciones de seguridad asociadas con los diferentes tipos de vulnerabilidades.

- **Vulnerabilidades basadas en cloud vs. on-premise**
- **Vulnerabilidades de Zero-day**
- **Configuraciones débiles**
  - Permisos abiertos
  - Cuentas privilegiadas inseguras
  - Errores
  - Cifrado débil
  - Protocolos inseguros
  - Configuraciones predeterminadas
  - Puertos y servicios abiertos
- **Riesgos externos**
  - Gestión de proveedores
    - Integración de sistemas
    - Falta de soporte del proveedor
  - Cadena de suministro
  - Desarrollo Tercerizado
  - Almacenamiento de datos
- **Administración de parches inapropiada o débil**
  - Firmware
  - Sistema operativo (OS)
  - Aplicaciones
- **Plataformas heredadas**
- **Impactos**
  - Pérdida de datos
  - Filtraciones de datos
  - Exfiltración de datos
  - Robo de identidad
  - Financiero
  - Reputación
  - Pérdida de disponibilidad

1.7 Resuma las técnicas que se usan en las evaluaciones de seguridad.

- **Caza de amenazas**
  - Fusión de inteligencia
  - Informes sobre amenazas informáticas
  - Avisos y boletines
  - Maniobras
- **Pruebas de vulnerabilidad**
  - Falsos positivos
  - Falsos negativos
  - Revisiones de bitácoras (logs)
  - Con credenciales vs. sin credenciales
  - Intrusivo vs. no intrusivo
  - Aplicaciones de escritorio
  - Aplicaciones web
  - Redes
  - Vulnerabilidades y exposiciones comunes (CVE)/Sistema de puntuación de vulnerabilidades comunes (CVSS)
  - Revisión de la configuración
- **Syslog/Security information and event management (SIEM)**
  - Informes de revisión
  - Captura de paquetes
  - Entradas de datos
  - Análisis del comportamiento del usuario
  - Análisis de sentimiento
  - Monitoreo de seguridad
  - Agrupadores de bitácoras (logs)
  - Recolectores de bitácoras (logs)
- **Security orchestration, automation, and response (SOAR)**

1.8 Explique las técnicas que se usan en las pruebas de penetración.

- **Pruebas de penetración**
  - Entorno conocido
  - Entorno desconocido
  - Entorno parcialmente conocido
  - Reglas y condiciones
  - Movimiento lateral
  - Escalamiento de privilegios
  - Persistencia
  - Limpieza
  - Recompensa por errores
  - Pivoteo
- **Reconocimiento pasivo y activo**
  - Drones
  - Warflying
  - War driving
  - Footprinting
  - OSINT
- **Tipos de ejercicio**
  - Red team
  - Blue team
  - White team
  - Purple team

2.0 Arquitectura y diseño

2.1 Explique la importancia de los conceptos de seguridad en un entorno empresarial.

- **Gestión de la configuración**
  - Diagramas
  - Configuración inicial
  - Convenciones de nomenclatura estándar
  - Esquema de protocolo de Internet (IP)
- **Soberanía de los datos**
- **Protección de datos**
  - Prevención de pérdida de datos (DLP)
  - Enmascaramiento
  - Cifrado
  - En reposo
  - En tránsito/movimiento
  - En proceso
  - Tokenización
  - Gestión de Privilegios
- **Consideraciones geográficas**
- **Controles de respuesta y recuperación**
- **Inspección del Secure Socket Layer (SSL) / Transport Layer Secuirty (TLS)**
- **Hashing**
- **Consideraciones en las API**
- **Resiliencia del sitio**
  - Hot site
  - Cold site
  - Warm site
- **Engaño e interrupción**
  - Honeypots
  - Honeyfiles
  - Honeynets
  - Telemetría falsa
  - DNS sinkhole

2.2 Resuma los conceptos de virtualización y computación en la nube.

- **Modelos en la nube**
  - Infraestructura como Servicio (IaaS)
  - Plataforma como Servicio (PaaS)
  - Software como Servicio (SaaS)
  - Todo como Servicio (XaaS)
  - Público
  - Comunitario
  - Privado
  - Híbrido
- **Proveedores de servicios en la nube**
- **Proveedor de servicios administrados (MSP)/proveedor de servicios de seguridad administrada (MSSP)**
- **On-premise vs. off-premise**
- **Fog computing**
- **Edge computing**
- **Cliente ligero**
- **Contenedores**
- **Microservicios/API**
- **Infraestructura como código**
  - Redes definidas por software (SDN)
  - Visibilidad definida por software (SDV)
- **Arquitectura sin servidor**
- **Integración de servicios**
- **Políticas de recursos**
- **Tránsito de puerta de enlace**
- **Virtualización**
  - Evitar la expansión de máquinas virtuales (VM)
  - Protección de escape de VM

2.3 Resuma los conceptos de desarrollo de aplicación, implementación y automatización segura.

- **Entorno**
  - Desarrollo
  - Prueba
  - Implementación
  - Producción
  - Aseguramiento de la calidad (QA)
- **Aprovisionamiento y desaprovisionamiento**
- **Medición de la integridad**
- **Técnicas de codificación seguras**
  - Normalización
  - Procedimientos almacenados
  - Ofuscación/camuflaje
  - Reutilización de código/ código muerto
  - Ejecución y validación del lado del cliente vs. el lado del servidor
  - Administración de memoria
  - Uso bibliotecas externas y software development kits (SDK)
  - Exposición de datos
- **Open Web Application Security Project (OWASP)**
- **Diversidad de software**
  - Compilador
  - Binario
- **Automatización/secuencias de comandos**
  - Cursos de acción automatizados
  - Monitoreo continuo
  - Validación continua
  - Integración continua
  - Entrega continua
  - Despliegue continuo
- **Elasticidad**
- **Escalabilidad**
- **Control de versiones**

2.4 Resuma los conceptos de diseño de autenticación y autorización.

- **Métodos de autenticación**
  - Servicios de directorio
  - Federación
  - Confirmación
  - Tecnologías
    - Contraseña de un solo uso basada en el tiempo (TOTP)
    - Contraseña de un solo uso basada en HMAC (HOTP)
    - Servicio de Mensajes Cortos (SMS)
    - Clave token
    - Códigos estáticos
    - Aplicaciones de autenticación
    - Notificaciones push
    - Llamada telefónica
  - Autenticación de tarjetas inteligentes
- **Biométricos**
  - Huella digital
  - Retina
  - Iris
  - Facial
  - Voz
  - Venas
  - Análisis de movimiento humano
  - Tasas de eficacia
  - Falsa aceptación
  - Falso rechazo
  - Tasa de error cruzado
- **Factores y atributos de autenticación de multifactores (MFA)**
  - Factores
    - Algo que sabe
    - Algo que tiene
    - Algo que es
  - Atributos
    - Un lugar donde está
    - Algo que puede hacer
    - Algo que puede mostrar
    - Alguien que conoce
- **Autenticación, autorización y registro (AAA)**
- **Requisitos en la nube vs. on-premise**

2.5 A partir de un escenario, implemente la resiliencia de ciberseguridad.

- **Redundancia**
  - Dispersión geográfica
  - Disco
    - Niveles de Redundant array of inexpensive disks (RAID)
    - Multipath
  - Red
    - Balanceadores de carga
    - Emparejamiento de la tarjeta de interfaz de red (NIC)
  - Energía
    - Fuente de alimentación ininterrumpida (UPS)
    - Generador
    - Suministro doble
    - Unidades de distribución de energía administrada (PDU)
- **Replicación**
  - Red de área de almacenamiento
  - Máquina virtual (VM)
- **On-premise vs. cloud**
- **Tipos de copia de seguridad**
  - Completa
  - Incremental
  - Instantánea
  - Diferencial
  - Cinta
  - Disco
  - Copia
  - Network-attached storage (NAS)
  - Red de área de almacenamiento (SAN)
  - Nube
  - Imagen
  - En línea vs. fuera de línea
  - Almacenamiento fuera del sitio
    - Consideraciones de distancia
- **No persistencia**
  - Volver al estado conocido
  - Última configuración válida conocida
  - Live boot media
- **Alta disponibilidad**
  - Escalabilidad
- **Orden de restauración**
- **Diversidad**
  - Tecnologías
  - Proveedores
  - Criptografía
  - Controles

2.6 Explique las implicaciones de seguridad de los sistemas embebidos y especializados.

- **Sistemas embebidos**
  - Raspberry Pi
  - Field-programmable gate array (FPGA)
  - Arduino
- **Supervisión, Control y Adquisición de Datos (SCADA)/sistema de control industrial (ICS)**
  - Instalaciones
  - Industrial
  - Manufactura
  - Energía
  - Logística
- **Internet de las cosas (IoT)**
  - Sensores
  - Dispositivos inteligentes
  - Wearables
  - Automatización de las instalaciones
  - Configuraciones predeterminadas débiles
- **Especializado**
  - Sistemas médicos
  - Vehículos
  - Aeronaves
  - Medidores inteligentes
- **Voz sobre IP (VoIP)**
- **Calefacción, Ventilación, Aire Acondicionado (HVAC)**
- **Drones**
- **Impresora multifunción (MFP)**
- **Sistema operativo en tiempo real (RTOS)**
- **Sistemas de vigilancia**
- **Sistema en un chip (SoC)**
- **Consideraciones de comunicación**
  - 5G
  - Narrow-band
  - Radio de banda base
  - Tarjetas del módulo de identidad del suscriptor (SIM)
  - Zigbee
- **Restricciones**
  - Energía
  - Computadora
  - Red
  - Criptografía
  - Imposibilidad de aplicar parches
  - Autenticación
  - Rango
  - Costo
  - Confianza implícita

2.7 Explique la importancia de los controles de seguridad física.

- **Bolardo (poste corto)/barricadas**
- **Vestíbulos de control de acceso**
- **Gafetes**
- **Alarmas**
- **Señalización**
- **Cámaras**
  - Reconocimiento del movimiento
  - Detección de objetos
- **Televisión de Circuito Cerrado (CCTV)**
- **Camuflaje industrial**
- **Personal**
  - Guardias
  - Centinelas robot
  - Recepción
  - Integridad/control de dos personas
- **Cerraduras**
  - Biométricas
  - Electrónicas
  - Físicas
  - Candados de cable
- **Bloqueador de datos USB**
- **Iluminación**
- **Rejas**
- **Supresión de incendios**
- **Sensores**
  - Detección del movimiento
  - Detección del ruido
  - Lector de proximidad
  - Detección de la humedad
  - Tarjetas
  - Temperatura
- **Drones**
- **Registros de visitantes**
- **Jaulas de Faraday**
- **Air gap**
- **Subred filtrada (antes conocida como zona desmilitarizada)**
- **Distribución protegida de cables**
- **Áreas seguras**
  - Air gap
  - Bóveda
  - Caja fuerte
  - Pasillo caliente
  - Pasillo frío
- **Destrucción segura de datos**
  - Quemar
  - Triturar
  - Destruir
  - Pulverizar
  - Desmagnetizar
  - Soluciones externas

2.8 Resuma los aspectos básicos de los conceptos criptográficos.

- **Firmas digitales**
- **Longitud de la clave**
- **Expansión de la clave**
- **Salting**
- **Hashing**
- **Intercambio de claves**
- **Criptografía de Curva Elíptica**
- **Secreto perfecto hacia adelante**
- **Cuántico**
  - Comunicaciones
  - Computación
- **Poscuántico**
- **Efímero**
- **Modos de operación**
  - Autenticado
  - No autenticado
  - Contador
- **Blockchain**
  - Public ledgers
- **Suites de cifrado**
  - Transmisión
  - Bloque
- **Simétrico vs. asimétrico**
- **Criptografía ligera**
- **Esteganografía**
  - Audio
  - Video
  - Imagen
- **Cifrado homomórfico**
- **Casos de uso comunes**
  - Dispositivos de energía baja
  - Latencia baja
  - Resiliencia alta
  - Confidencialidad
  - Integridad
  - Ofuscación
  - Autenticación
  - No repudio
- **Limitaciones**
  - Velocidad
  - Tamaño
  - Claves débiles
  - Tiempo
  - Longevidad
  - Predictibilidad
  - Reutilización
  - Entropía
  - Sobrecarga computacional
  - Restricciones de recursos vs. de seguridad

3.0 Implementación

3.1 A partir de un escenario, implemente protocolos de seguridad.

- **Protocolos**
  - Extensiones de seguridad para el sistema de nombres de dominio (DNSSEC)
  - SSH
  - Extensiones de Correo de Internet de Propósitos Múltiples/Seguro (S/MIME)
  - Protocolo de transporte seguro en tiempo real (SRTP)
  - Protocolo ligero de acceso a directorio por SSL (LDAPS)
  - Protocolo de transferencia segura de archivos (FTPS)
  - Protocolo de Transferencia de Archivos SSH (SFTP)
  - Protocolo de Administración de Red Simple, versión 3 (SNMPv3)
  - Protocolo de transferencia de hipertexto por SSL/TLS (HTTPS)
  - IPSec
    - Encabezado de Autenticación (AH)/Encapsulating Security Payload (ESP)
    - Túnel/transporte
  - Protocolo de Oficina de Correo (POP)/ Protocolo de Acceso a Mensajes de Internet (IMAP)
- **Casos de uso**
  - Voz y video
  - Sincronización del tiempo
  - Correo electrónico y web
  - Transferencia de archivos
  - Servicios de directorio
  - Acceso remoto
  - Resolución de nombre de dominio
  - Routing y switching
  - Asignación de dirección de red
  - Servicios de suscripción

3.2 A partir de un escenario, implemente soluciones de seguridad para el host o la aplicación.

- **Endpoint protection**
  - Antivirus
  - Antimalware
  - Detección y respuesta de endpoints (EDR)
  - DLP
  - Firewall de próxima generación (NGFW)
  - Sistema de Prevención de Intrusión Basado en Host (HIPS)
  - Sistema de Detección de Intrusión Basado en Host (HIDS)
  - Firewall basado en el host
- **Boot integrity**
  - Seguridad de arranque/Interfaz de Firmware Extensible Unificada (UEFI)
  - Measured boot
  - Boot attestation
- **Base de datos**
  - Tokenización
  - Salting
  - Hashing
- **Seguridad de la aplicación**
  - Validaciones de entrada
  - Cookies seguras
  - Encabezados del Protocolo de Transferencia de Hipertexto (HTTP)
  - Firma del código
  - Lista de permisos
  - Lista de bloqueo/Lista de rechazo
  - Prácticas de codificación segura
  - Análisis de código estático
    - Revisión manual de código
  - Análisis dinámico de código
  - Fuzzing
- **Protección**
  - Puertos y servicios abiertos
  - Registro
  - Cifrado de disco
  - Sistema operativo (OS)
  - Gestión de parches
    - Actualizaciones externas
    - Actualización automática
- **Unidad de autocifrado (SED)/Cifrado de disco completo (FDE)**
  - Opal
- **Hardware root of trust**
- **Módulo de Plataforma Confiable (TPM)**
- **Sandboxing**

3.3 A partir de un escenario, implemente diseños seguros de red.

- **Balanceo de carga**
  - Activo/activo
  - Activo/pasivo
  - Programación
  - IP virtual
  - Persistencia
- **Segmentación de red**
  - Red de Área Local Virtual (VLAN)
  - Subred filtrada (antes conocida como zona desmilitarizada)
  - Tráfico este-oeste
  - Extranet
  - Intranet
  - Zero trust
- **Red Privada Virtual (VPN)**
  - Siempre activa
  - Túnel dividido vs. túnel completo
  - Acceso remoto vs. de sitio a sitio
  - IPSec
  - SSL/TLS
  - HTML5
  - Protocolo de Túnel de Capa 2 (L2TP)
- **DNS**
- **Network access control (NAC)**
  - Con agente y sin agente
- **Administración fuera de banda**
- **Seguridad de puertos**
  - Prevención de tormentas de difusión
  - Protección de la Unidad de Datos de Protocolo Bridge (BPDU)
  - Prevención de bucles
  - Snooping de Protocolo de Configuración Dinámica de Servidor (DHCP)
  - Filtrado de Desbordamiento del control de acceso al medio (MAC)
- **Dispositivos de red**
  - Servidores jump
  - Servidores proxy
    - Hacia adelante
    - Hacia atrás
  - Sistema de detección de intrusión basado en red (NIDS)/ Sistema de prevención de intrusión basado en red (NIPS)
    - Basado en firma
    - Heurístico/comportamiento
    - Anomalías
    - En línea vs. pasivo
  - HSM
  - Sensores
  - Colectores
  - Agregadores
  - Firewalls
    - Firewall de aplicación web (WAF)
    - NGFW
    - Con estado (Stateful)
    - Sin estado
    - Administración de Amenazas Unificadas (UTM)
    - Puerta de enlace de traducción de dirección de red (NAT)
    - Filtro de contenido/URL
    - Open-source vs. propietario
    - Hardware vs. software
    - Appliance vs. basado en host vs. virtual
- **Lista de Control de Acceso (ACL)**
- **Route security**
- **Calidad de servicio (QoS)**
- **Implicaciones de IPv6**
- **Port spanning/port mirroring**
  - Port taps
- **Monitoreo de servicios**
- **Monitoreo de integridad de archivos**

3.4 A partir de un escenario, instale y configure parámetros de seguridad inalámbrica.

- **Protocolos criptográficos**
  - Acceso Protegido Wi-Fi 2 (WPA2)
  - Acceso Protegido Wi-Fi 3 (WPA3)
  - Protocolo Counter-Mode/ CBC-MAC (CMP)
  - Autenticación simultánea de iguales (SAE)
- **Protocolos de autenticación**
  - Protocolo de Autenticación Extensible (EAP)
  - Protocolo de Autenticación Extensible (EAP)
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1X
  - Remote Authentication Dial-in User Service (RADIUS) Federation
- **Métodos**
  - Clave precompartida (PSK) vs. Empresarial vs. Abierta
  - Acceso Protegido Wi-Fi (WPS)
  - Portales cautivos
- **Consideraciones de instalación**
  - Site surveys
  - Mapas de calor
  - Analizadores de WiFi
  - Channel overlaps
  - Colocación de punto de acceso inalámbrico (WAP)
  - Seguridad del controlador y del punto de acceso

3.5 A partir de un escenario, implemente soluciones móviles seguras.

- **Métodos de conexión y receptores**
  - Celular
  - WiFi
  - Bluetooth
  - NFC
  - Infrarrojo
  - USB
  - Punto a punto
  - Punto a multipunto
  - Sistema de Posicionamiento Global (GPS)
  - RFID
- **Gestión de dispositivos móviles (MDM)**
  - Gestión de aplicaciones
  - Gestión del contenido
  - Limpieza remota
  - Geofencing
  - Geolocalización
  - Bloqueo de pantalla
  - Notificaciones push
  - Contraseñas y PIN
  - Biométricos
  - Autenticación basada en contexto
  - Contenedorización
  - Segmentación del almacenamiento
  - Cifrado de dispositivo completo
- **Dispositivos móviles**
  - Módulo de seguridad de hardware MicroSD (HSM)
  - MDM/Administración unificada de endpoints (UEM)
  - Gestión de aplicaciones móviles (MAM)
  - SEAndroid
- **Ejecución y monitoreo de lo siguiente:**
  - Tiendas de aplicaciones externas
  - Rooting/jailbreaking
  - Sideloading
  - Firmware personalizado
  - Desbloqueo del operador
  - Actualizaciones de firmware por aire (OTA)
  - Uso de cámara
  - SMS/Servicios de mensajería multimedia (MMS)/Servicios de comunicación enriquecida (RCS)
  - Medios externos
  - USB On-The-Go (USB OTG)
  - Micrófono de grabación
  - Etiquetado de GPS
  - WiFi directo/ad hoc
  - Anclaje de red
  - Hotspot
  - Métodos de pago
- **Modelos de despliegue**
  - Trae Tu Propio Dispositivo (BYOD)
  - De propiedad corporativa y habilitada personalmente (COPE)
  - Elija su propio dispositivo (CYOD)
  - De propiedad corporativa
  - Infraestructura de escritorio virtual (VDI)

3.6 A partir de un escenario, aplique soluciones de ciberseguridad en la nube.

- **Controles de seguridad en la nube**
  - Alta disponibilidad entre zonas
  - Políticas de recursos
  - Gestión de secretos
  - Integración y auditoría
  - Almacenamiento
    - Permisos
    - Cifrado
    - Replicación
    - Alta disponibilidad
  - Red
    - Redes virtuales
    - Subredes públicas y privadas
    - Segmentación
    - Inspección e integración API
  - Computadora
    - Grupos de seguridad
    - Asignación de recursos dinámicos
    - Reconocimiento de instancias
    - Endpoint de nube privada virtual (VPC)
    - Seguridad de contenedor
- **Soluciones**
  - CASB
  - Seguridad de la aplicación
  - Secure Web Gateway (SWG) de próxima generación
  - Consideraciones de firewall en un entorno en la nube
    - Costo
    - Necesidad de segmentación
    - Capas de Interconexión de Sistemas Abiertos (OSI)
- **Controles nativos en la nube vs. soluciones externas**

3.7 A partir de un escenario, implemente controles de identidad y administración de cuentas.

- **Identidad**
  - Proveedor de identidad (IdP)
  - Atributos
  - Certificados
  - Tokens
  - Claves SSH
  - Tarjetas inteligentes
- **Tipos de cuentas**
  - Cuentas de usuario
  - Cuentas/credenciales compartidas y genéricas
  - Cuentas de invitado
  - Cuentas de servicio
- **Políticas de la cuenta**
  - Complejidad de contraseñas
  - Historial de contraseñas
  - Reutilización de contraseñas
  - Ubicación de red
  - Geofencing
  - Geoetiquetado
  - Geolocalización
  - Inicios de sesión basados en el tiempo
  - Políticas de acceso
  - Permisos de la cuenta
  - Auditorías de cuentas
  - Riesgos de inicio de sesión por tiempo de viaje imposible
  - Bloqueo
  - Inhabilitación

3.8 A partir de un escenario, implemente soluciones de autenticación y autorización.

- **Gestión de la autenticación**
  - Claves de contraseñas
  - Bóvedas de contraseñas
  - TPM
  - HSM
  - Autenticación basada en el conocimiento
- **Autenticación/autorización**
  - EAP
  - Challenge-Handshake Authentication Protocol (CHAP)
  - Protocolo de Autenticación de Contraseña (PAP)
  - 802.1X
  - RADIUS
  - Inicio de sesión único (SSO)
  - Lenguaje de marcado de aserción de seguridad (SAML)
  - Terminal Access Controller Access Control System Plus (TACACS+)
  - OAuth
  - OpenID
  - Kerberos
- **Esquemas de control de acceso**
  - Control de acceso basado en atributos (ABAC)
  - Control de acceso basado en roles
  - Control de acceso basado en reglas
  - MAC
  - Control de Acceso Discrecional (DAC)
  - Acceso condicional
  - Administración de acceso privilegiado
  - Permisos del sistema de archivos

3.9 A partir de un escenario, implemente una infraestructura de clave pública.

- **Infraestructura de Clave Pública (PKI)**
  - Administración de claves
  - Autoridad Certificadora (CA)
  - CA intermedia
  - Autoridad de registro (RA)
  - Lista de Revocación de Certificados (CRL)
  - Atributos del certificado
  - Protocolo de estado de certificado en línea (OCSP)
  - Solicitud de firma de certificado (CSR)
  - CN
  - Nombre alternativo del sujeto
  - Vencimiento
- **Tipos de certificados**
  - Wildcard
  - Nombre alternativo del sujeto
  - Firma del código
  - Auto-firmado
  - Máquina/computadora
  - Correo electrónico
  - Usuario
  - Root
  - Validación del dominio
  - Validación extendida
- **Formatos de certificado**
  - Reglas de codificación distinguidas (DER)
  - Correo con Privacidad Mejorada (PEM)
  - Intercambio de información personal (PFX)
  - .cer
  - P12
  - P7B
- **Conceptos**
  - CA en línea vs. fuera de línea
  - Stapling
  - Pinning
  - Modelo de confianza
  - Custodia de claves
  - Encadenamiento de certificados

4.0 Operaciones y respuesta a incidentes

4.1 A partir de un escenario, use la herramienta apropiada para evaluar la seguridad de la organización.

- **Reconocimiento y descubrimiento de red**
  - tracert/traceroute
  - nslookup/dig
  - ipconfig/ifconfig
  - nmap
  - ping/pathping
  - hping
  - netstat
  - netcat
  - Escáneres de IP
  - arp
  - route
  - curl
  - theHarvester
  - sn1per
  - scanless
  - dnsenum
  - Nessus
  - Cuckoo
- **Manipulación de archivos**
  - head
  - tail
  - cat
  - grep
  - chmod
  - logger
- **Entornos de shell y scripts**
  - SSH
  - PowerShell
  - Python
  - OpenSSL
- **Captura y repetición de paquetes**
  - Tcpreplay
  - Tcpdump
  - Wireshark
- **Análisis forense**
  - dd
  - Memdump
  - WinHex
  - FTK imager
  - Autopsy
- **Frameworks de explotación**
- **Decodificadores de contraseñas**
- **Sanitización de datos**

4.2 Resuma la importancia de las políticas, los procesos y los procedimientos de respuesta a incidentes.

- **Planes de respuesta ante incidentes**
- **Proceso de respuesta ante incidentes**
  - Preparación
  - Identificación
  - Contención
  - Erradicación
  - Recuperación
  - Lecciones aprendidas
- **Ejercicios**
  - Tabletop
  - Walkthroughs
  - Simulaciones
- **Frameworks de ataque**
  - MITRE ATT&CK
  - The Diamond Model of Intrusion Analysis
  - Cyber Kill Chain
- **Administración de stakeholder**
- **Plan de comunicaciones**
- **Plan de recuperación ante desastres**
- **Plan de continuidad de negocio**
- **Plan de continuidad operativa (COOP)**
- **Equipo de respuesta a incidentes**
- **Políticas de retención**

4.3 A partir de un incidente, use las fuentes de datos apropiadas para respaldar una investigación.

- **Resultados de escaneo de vulnerabilidades**
- **Tableros SIEM**
  - Sensor
  - Sensibilidad
  - Tendencias
  - Alertas
  - Correlación
- **Archivos de bitácora**
  - Red
  - Sistema
  - Aplicación
  - Seguridad
  - Web
  - DNS
  - Autenticación
  - Archivos dump
  - VoIP y gestor de llamadas
  - Tráfico del Protocolo de Inicio de Sesión (SIP)
- **syslog/rsyslog/syslog-ng**
- **journalctl**
- **NXLog**
- **Monitores de ancho de banda**
- **Metadatos**
  - Correo electrónico
  - Móvil
  - Web
  - Archivo
- **Netflow/sFlow**
  - Netflow
  - sFlow
  - IPFIX
- **Resultado del analizador de protocolo**

4.4 A partir de un incidente, aplique técnicas de mitigación o controles para asegurar un entorno.

- **Reconfigurar las soluciones de seguridad de endpoint**
  - Lista de aplicaciones aprobadas
  - Lista de aplicaciones bloqueadas/rechazadas
  - Cuarentena
- **Cambios de configuración**
  - Reglas de firewall
  - MDM
  - DLP
  - Filtro de contenido/filtro de URL
  - Actualización o revocación de certificados
- **Aislamiento**
- **Contención**
- **Segmentación**
- **SOAR**
  - Runbooks
  - Playbooks

4.5 Explique los aspectos clave del análisis forense digital.

- **Documentación/evidencia**
  - Retención legal
  - Video
  - Admisibilidad
  - Cadena de custodia
  - Cronogramas de la secuencia de eventos
    - Marcas de tiempo
    - Compensación del tiempo
  - Etiquetas
  - Informes
  - Registros de eventos
  - Entrevistas
- **Adquisición**
  - Orden de volatilidad
  - Disco
  - Memoria de acceso aleatorio (RAM)
  - Swap/pagefile
  - Sistema operativo (OS)
  - Dispositivo
  - Firmware
  - Instantánea
  - Caché
  - Red
  - Artefactos
- **On-premises vs. cloud**
  - Cláusula de derecho de auditoría
  - Regulatorio/jurisdicción
  - Leyes de notificación de filtración de datos
- **Integridad**
  - Hashing
  - Checksums
  - Procedencia
- **Preservación**
- **E-discovery**
- **Recuperación de datos**
- **No repudio**
- **Inteligencia/contrainteligencia estratégica**

5.0 Gobernanza, riesgo y cumplimiento

5.1 Compare y contraste diversos tipos de controles.

- **Categorías**
  - Gerencial
  - Operacional
  - Técnica
- **Tipos de control**
  - Preventivo
  - Detectivo
  - Correctivo
  - Disuasivo
  - Compensatorio
  - Físico

5.2 Explique la importancia de las regulaciones, los estándares o los frameworks aplicables que afectan la postura de la seguridad de la organización.

- **Regulaciones, estándares y legislación**
  - Reglamento General de Protección de Datos (GDPR)
  - Leyes nacionales, territoriales o estatales
  - Payment Card Industry Data Security Standard (PCI DSS)
- **Frameworks principales**
  - Center for Internet Security (CIS)
  - Risk Management Framework (RMF)/ Cybersecurity Framework (CSF) del National Institute of Standards and Technology (NIST)
  - International Organization for Standardization (ISO) 27001/27002/27701/31000
  - SSAE SOC 2 Tipo I/II
  - Cloud security alliance
    - Matriz de control en la nube
    - Arquitectura de referencia
- **Guías de referencias/ configuración segura**
  - Guías de plataformas/ específicas del proveedor
    - Servidor web
    - Sistema operativo (OS)
    - Servidor de aplicaciones
    - Dispositivos de infraestructura de red

5.3 Explique la importancia de las políticas para la seguridad de la organización.

- **Personal**
  - Política de uso aceptable
  - Rotación de trabajo
  - Vacaciones obligatorias
  - Separación de tareas
  - Mínimo privilegio
  - Política de escritorio limpio
  - Verificaciones de antecedentes
  - Acuerdo de no divulgación (NDA)
  - Análisis de redes sociales
  - Incorporación
  - Desvinculación
  - Capacitación del usuario
    - Gamificación
    - Capture the flag (CTF)
    - Campañas de phishing
      - Simulaciones de phishing
    - Capacitación basada en computadora (CBT)
    - Capacitación basada en roles
- **Diversidad de las técnicas de capacitación**
- **Administración de riesgos externos**
  - Proveedores
  - Cadena de suministro
  - Socios comerciales
  - Acuerdo de Nivel de Servicio (SLA)
  - Memorándum de entendimiento (MOU)
  - Análisis de sistemas de medición (MSA)
  - Acuerdo de Asociación Comercial (BPA)
  - End of life (EOL)
  - End of service life (EOSL)
  - Acuerdo de no divulgación (NDA)
- **Datos**
  - Clasificación
  - Gobernanza
  - Retención
- **Políticas de credenciales**
  - Personal
  - Externo
  - Dispositivos
  - Cuentas de servicio
  - Cuentas de administrador/root
- **Políticas organizativas**
  - Administración de cambios
  - Control de cambios
  - Administración de activos

5.4 Resuma los conceptos y procesos de la gestión de riesgos.

- **Tipos de riesgos**
  - Externo
  - Interno
  - Sistemas heredados
  - Multiparty
  - Robo de propiedad intelectual
  - Cumplimiento/licencias de software
- **Estrategias de gestión de riesgos**
  - Aceptar
  - Evitar
  - Transferir
    - Seguro de ciberseguridad
  - Mitigar
- **Análisis de riesgo**
  - Registro de riesgos
  - Matriz de riesgo/mapa de calor
  - Evaluación de control del riesgo
  - Autoevaluación de control del riesgo
  - Conocimiento del riesgo
  - Riesgo inherente
  - Riesgo residual
  - Riesgo de control
  - Apetito al riesgo
  - Regulaciones que afectan la postura de riesgo
  - Tipos de evaluación de riesgos
    - Cualitativo
    - Cuantitativo
  - Probabilidad de ocurrencia
  - Impacto
  - Valor del activo
  - Expectativa de Pérdida Simple (SLE)
  - Expectativa de Pérdida Anualizada (ALE)
  - Tasa de Ocurrencia Anualizada (ARO)
- **Desastres**
  - Ambientales
  - Humanos
  - Internos vs. externos
- **Análisis de impacto al negocio (BIA)**
  - Tiempo objetivo de recuperación (RTO)
  - Punto objetivo de recuperación (RPO)
  - Tiempo medio de reparación (MTTR)
  - Tiempo medio entre fallos (MTBF)
  - Planes de recuperación funcional
  - Punto único de fallo
  - Plan de recuperación de desastres (DRP)
  - Funciones esenciales de la misión
  - Identificación de los sistemas críticos
  - Evaluación de riesgos del sitio

5.5 Explique los conceptos de privacidad y datos sensibles en relación con la seguridad.

- **Consecuencias organizacionales de las filtraciones de privacidad y datos**
  - Daño a la reputación
  - Robo de identidad
  - Sanciones
  - Robo de propiedad intelectual
- **Notificaciones de las infracciones**
  - Escalamiento
  - Notificaciones y divulgaciones públicas
- **Tipos de datos**
  - Clasificaciones
    - Públicos
    - Privados
    - Sensibles
    - Confidenciales
    - Críticos
    - Propietarios
  - Información de Identificación Personal (PII)
  - Información médica
  - Información financiera
  - Datos gubernamentales
  - Datos de clientes
- **Tecnologías de mejora de la privacidad**
  - Minimización de datos
  - Enmascaramiento de datos
  - Tokenización
  - Anonimización
  - Pseudo-anonimización
- **Roles y responsabilidades**
  - Propietarios de datos
  - Controlador de datos
  - Procesador de datos
  - Custodio/administrador de datos
  - Delegado de Protección de Datos (DPO)
- **Ciclo de vida de la información**
- **Evaluación del impacto**
- **Términos del acuerdo**
- **Aviso de privacidad**

Lista de acrónimos de Security+ (SY0-601)

A continuación, hay una lista de siglas que aparecen en el examen de CompTIA Security+. Se insta a los candidatos a revisar la lista completa y alcanzar un conocimiento práctico de todas las siglas listadas, como parte de un programa completo de preparación para el examen.

ACRÓNIMO	DEFINICIÓN
3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization, and Accounting
ABAC	Attribute-based Access Control
ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
AES256	Advanced Encryption Standards 256bit
AH	Authentication Header
AI	Artificial Intelligence
AIS	Automated Indicator Sharing
ALE	Annualized Loss Expectancy
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
ASP	Active Server Pages
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AUP	Acceptable Use Policy
AV	Antivirus
BASH	Bourne Again Shell
BCP	Business Continuity Planning
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BPA	Business Partnership Agreement
BPDU	Bridge Protocol Data Unit
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart

ACRÓNIMO	DEFINICIÓN
CAR	Corrective Action Report
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining
CBT	Computer-based Training
CCMP	Counter-Mode/CBC-MAC Protocol
CCTV	Closed-Circuit Television
CERT	Computer Emergency Response Team
CFB	Cipher Feedback
CHAP	Challenge-Handshake Authentication Protocol
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CIS	Center for Internet Security
CMS	Content Management System
CN	Common Name
COOP	Continuity of Operations Planning
COPE	Corporate-owned Personally Enabled
CP	Contingency Planning
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Cloud Security Alliance
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
CSP	Cloud Service Provider
CSR	Certificate Signing Request
CSRF	Cross-Site Request Forgery
CSU	Channel Service Unit
CTM	Counter-Mode
CTO	Chief Technology Officer
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CYOD	Choose Your Own Device
DAC	Discretionary Access Control
DBA	Database Administrator
DDoS	Distributed Denial-of-Service
DEP	Data Execution Prevention

ACRÓNIMO	DEFINICIÓN
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHE	Diffie-Hellman Ephemeral
DKIM	Domain Keys Identified Mail
DLL	Dynamic-link Library
DLP	Data Loss Prevention
DMARC	Domain Message Authentication Reporting and Conformance
DNAT	Destination Network Address Transaction
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial-of-Service
DPO	Data Protection Officer
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
ECB	Electronic Code Book
ECC	Elliptic-curve Cryptography
ECDHE	Elliptic-curve Diffie-Hellman Ephemeral
ECDSA	Elliptic-curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
EFS	Encrypted File System
EIP	Extended Instruction Pointer
EOL	End of Life
EOS	End of Service
ERP	Enterprise Resource Planning
ESN	Electronic Serial Number
ESP	Encapsulating Security Payload
ESSID	Extended Service Set Identifier
FACL	File System Access Control List
FDE	Full Disk Encryption
FIM	File Integrity Monitoring
FPGA	Field Programmable Gate Array
FRR	False Rejection Rate
FTP	File Transfer Protocol
FTPS	Secured File Transfer Protocol
GCM	Galois/Counter Mode
GDPR	General Data Protection Regulation
GPG	GNU Privacy Guard
GPO	Group Policy Object
GPS	Global Positioning System
GPU	Graphics Processing Unit
GRE	Generic Routing Encapsulation
HA	High Availability
HDD	Hard Disk Drive
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HMAC	Hash-based Message Authentication Code
HOTP	HMAC-based One-time Password

ACRÓNIMO	DEFINICIÓN
HSM	Hardware Security Module
HSMaaS	Hardware Security Module as a Service
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation, Air Conditioning
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDEA	International Data Encryption Algorithm
IDF	Intermediate Distribution Frame
IdP	Identity Provider
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP4	Internet Message Access Protocol v4
IoC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IR	Incident Response
IRC	Internet Relay Chat
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISFW	Internal Segmentation Firewall
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSO	Information Systems Security Officer
ITCP	IT Contingency Plan
IV	Initialization Vector
KDC	Key Distribution Center
KEK	Key Encryption Key
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
MaaS	Monitoring as a Service
MAC	Media Access Control
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MBR	Master Boot Record
MD5	Message Digest 5
MDF	Main Distribution Frame
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Multifunction Device
MFP	Multifunction Printer
ML	Machine Learning

ACRÓNIMO	DEFINICIÓN
MMS	Multimedia Message Service
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
MSA	Measurement Systems Analysis
MS-CHAP	Microsoft Challenge-Handshake Authentication Protocol
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAS	Network-attached Storage
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NFC	Near-field Communication
NFV	Network Function Virtualization
NGFW	Next-generation Firewall
NG-SWG	Next-generation Secure Web Gateway
NIC	Network Interface Card
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards & Technology
NOC	Network Operations Center
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
OSI	Open Systems Interconnection
OSINT	Open-source Intelligence
OSPF	Open Shortest Path First
OT	Operational Technology
OTA	Over-The-Air
OTG	On-The-Go
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
P12	PKCS #12
P2P	Peer-to-Peer
PaaS	Platform as a Service
PAC	Proxy Auto Configuration
PAM	Privileged Access Management
PAM	Pluggable Authentication Modules
PAP	Password Authentication Protocol
PAT	Port Address Translation
PBKDF2	Password-based Key Derivation Function 2
PBX	Private Branch Exchange
PCAP	Packet Capture

ACRÓNIMO	DEFINICIÓN
PCI DSS	Payment Card Industry Data Security Standard
PDU	Power Distribution Unit
PE	Portable Executable
PEAP	Protected Extensible Authentication Protocol
PED	Portable Electronic Device
PEM	Privacy Enhanced Mail
PFS	Perfect Forward Secrecy
PGP	Pretty Good Privacy
PHI	Personal Health Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PoC	Proof of Concept
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Preshared Key
PTZ	Pan-Tilt-Zoom
PUP	Potentially Unwanted Program
QA	Quality Assurance
QoS	Quality of Service
PUP	Potentially Unwanted Program
RA	Registration Authority
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory
RAS	Remote Access Server
RAT	Remote Access Trojan
RC4	Rivest Cipher version 4
RCS	Rich Communication Services
RFC	Request for Comments
RFID	Radio Frequency Identification
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROI	Return on Investment
RPO	Recovery Point Objective
RSA	Rivest, Shamir, & Adleman
RTBH	Remotely Triggered Black Hole
RTO	Recovery Time Objective
RTOS	Real-time Operating System
RTP	Real-time Transport Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAE	Simultaneous Authentication of Equals
SAML	Security Assertions Markup Language
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol

ACRÓNIMO	DEFINICIÓN
SCEP	Simple Certificate Enrollment Protocol
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDLM	Software Development Life-cycle Methodology
SDN	Software-defined Networking
SDP	Service Delivery Platform
SDV	Software-defined Visibility
SED	Self-Encrypting Drives
SEH	Structured Exception Handling
SFTP	SSH File Transfer Protocol
SHA	Secure Hashing Algorithm
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service-level Agreement
SLE	Single Loss Expectancy
SMB	Server Message Block
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol Secure
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation, Response
SoC	System on Chip
SOC	Security Operations Center
SPF	Sender Policy Framework
SPIM	Spam over Instant Messaging
SQL	Structured Query Language
SQLi	SQL Injection
SRTP	Secure Real-time Transport Protocol
SSD	Solid State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXpression
STP	Shielded Twisted Pair
SWG	Secure Web Gateway
TACACS+	Terminal Access Controller Access Control System
TAXII	Trusted Automated eXchange of Intelligence Information
TCP/IP	Transmission Control Protocol/Internet Protocol
TGT	Ticket Granting Ticket
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOTP	Time-based One Time Password
TPM	Trusted Platform Module
TSIG	Transaction Signature
TTP	Tactics, Techniques, and Procedures
UAT	User Acceptance Testing
UDP	User Datagram Protocol
UEBA	User and Entity Behavior Analytics
UEFI	Unified Extensible Firmware Interface
UEM	Unified Endpoint Management
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Universal Resource Locator
USB	Universal Serial Bus
USB OTG	USB On-The-Go
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VBA	Visual Basic for Applications
VDE	Virtual Desktop Environment
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VLSM	Variable-length Subnet Masking
VM	Virtual Machine
VoIP	Voice over IP
VPC	Virtual Private Cloud
VPN	Virtual Private Network
VTC	Video Teleconferencing
WAF	Web Application Firewall
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WORM	Write Once Read Many
WPA	WiFi Protected Access
WPS	WiFi Protected Setup
XaaS	Anything as a Service
XML	Extensible Markup Language
XOR	Exclusive OR
XSRF	Cross-site Request Forgery
XSS	Cross-site Scripting

Lista propuesta de hardware y software para Security+

CompTIA ha incluido esta lista de muestra de hardware y software para apoyar a los candidatos en su preparación para el examen de Security+. Esta lista también puede ser útil para las empresas de capacitación que desean crear un componente de laboratorio en su oferta de capacitación. Las listas con viñetas debajo de cada tema son listas de muestra y no están completas.

HARDWARE

- Computadora portátil con acceso a Internet
- NIC inalámbrico separado
- WAP
- Firewall
- UTM
- Dispositivo móvil
- Servidor físico o servidor cloud
- Dispositivos IoT

SOFTWARE

- Software de virtualización
- Sistemas operativos para pruebas de penetración/distribuciones (por ej., Kali Linux, Parrot OS)
- SIEM
- Wireshark
- Metasploit
- tcpdump

OTRO

- Acceso a CSP