Objetivos del examen de certificación CompTIA Security+

NÚMERO DE EXAMEN: SY0-701

Acerca del examen

El examen de certificación CompTIA Security+ certificará que el candidato aprobado 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 internet de las cosas (IoT).
- Operar con conocimiento de las regulaciones y políticas aplicables, incluso los principios de gobernanza, riesgo y cumplimiento.
- Identificar, analizar y responder a los eventos e incidentes de seguridad.

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 está afiliado 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 más claramente 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 acaten 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 debe comunicarse con CompTIA en examsecurity@comptia.org para confirmar.

RECUERDE

Las listas de ejemplos proporcionadas 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 existentes. Sepa que todos los materiales relacionados de preparación para el examen serán válidos.

DETALLES DE LA PRUEBA

Examen obligatorio	SY0-701
Número de preguntas	90 como máximo
Tipos de preguntas	Selección múltiple y basadas en la ejecución
Tiempo de la prueba	90 minutos
Experiencia recomendada	Un mínimo de 2 años de experiencia en administración de TI enfocado en seguridad, experiencia práctica con seguridad de la información técnica y conocimiento general de los conceptos de seguridad

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	Conceptos generales de seguridad	12%
2.0	Amenazas, vulnerabilidades y mitigaciones	22%
3.0	Arquitectura de seguridad	18%
4.0	Operaciones de Seguridad	28%
5.0	Administración y supervisión de programa de seguridad	20%
Total		**100%**

1.0 Conceptos generales de seguridad

1.1 Comparar y contrastar diversos tipos de controles de seguridad.

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

1.2 Resumir conceptos de seguridad fundamentales.

- **Confidencialidad, integridad, y disponibilidad (CIA)**
- **No repudio**
- **Autenticación, autorización y registro (AAA)**
  - Autenticación de personas
  - Autenticación de sistemas
  - Modelos de autorización
- **Análisis de brecha**
- **Zero Trust**
  - Plano de control
    - Identidad adaptable
    - Reducción de alcance de la amenaza
    - Control de acceso dirigido por políticas
    - Administrador de políticas
    - Motor de políticas
  - Plano de datos
    - Zonas implícitas de confianza
    - Sujeto/Sistema
    - Punto de cumplimiento de políticas
- **Seguridad física**
  - Pilotes
  - Vestíbulo de control de acceso
  - Rejas
  - Vigilancia con video
  - Guardia de seguridad
  - Acceso con gafete
  - Iluminación
  - Sensores
    - Infrarrojo
    - Presión
    - Microondas
    - Ultrasonido
- **Engaño e interrupción tecnológica**
  - Honeypot
  - Honeynet
  - Honeyfile
  - Honeytoken

1.3 Explicar la importancia de los procesos de administración de cambios y el impacto en la seguridad.

- **Procesos de negocios que afectan las operaciones de seguridad**
  - Proceso de aprobación
  - Propiedad
  - Partes interesadas
  - Análisis de impacto
  - Resultados de pruebas
  - Plan de retroceso
  - Ventana de mantenimiento
  - Procedimiento operacional estándar
- **Implicaciones técnicas**
  - Listas permitidas/ listas de rechazo
  - Actividades restringidas
  - Tiempo de inactividad
  - Reinicio de servicio
  - Reinicio de aplicación
  - Aplicaciones heredadas
  - Dependencias
- **Documentación**
  - Actualización de diagramas
  - Actualización de políticas/ procedimientos
- **Control de versiones**

1.4 Explicar la importancia de usar soluciones criptográficas adecuadas.

- **Infraestructura de clave pública (PKI)**
  - Clave pública
  - Clave privada
  - Custodia de claves
- **Cifrado**
  - Nivel
    - Disco completo
    - Partición
    - Archivo
    - Volumen
    - Base de datos
    - Registro
  - Transporte/comunicación
  - Asimétrico
  - Simétrico
  - Intercambio de claves
  - Algoritmos
  - Longitud de la clave
- **Herramientas**
  - Módulo de plataforma confiable (TPM)
  - Módulo de seguridad de hardware (HSM)
  - Sistema de administración de claves
  - Enclave seguro
- **Ofuscación**
  - Esteganografía
  - Tokenización
  - Enmascaramiento de datos
- **Hashing**
- **Salting**
- **Firmas digitales**
- **Expansión de la clave**
- **Blockchain**
- **Libro de public ledger**
- **Certificados**
  - Autoridades de certificados
  - Lista de revocación de certificados (CRL)
  - Protocolo de estado de certificado en línea (OCSP)
  - Auto-firmado
  - Externo
  - Origen de confianza
  - Generación de solicitud de firma de certificado (CSR)
  - Wildcard

2.0 Amenazas, vulnerabilidades y mitigaciones

2.1 Comparar y contrastar actores de amenazas y motivaciones comunes.

- **Actores de amenazas**
  - Nation-state
  - Atacante sin habilidades
  - Hacktivistas
  - Amenazas internas
  - Crimen organizado
  - Shadow IT
- **Actores de amenazas**
  - Interno/externo
  - Recursos/financiación
  - Nivel de sofisticación/capacidad
- **Motivaciones**
  - Exfiltración de datos
  - Espionaje
  - Interrupción del servicio
  - Extorsión
  - Beneficio financiero
  - Creencias filosóficas/políticas
  - Éticas
  - Venganza
  - Alteración/caos
  - Guerra

2.2 Explicar vectores de amenazas y superficies de ataque comunes.

- **Basado en mensajes**
  - o Correo electrónico
  - o Servicio de Mensajes Cortos (SMS)
  - o Mensajería instantánea (IM)
- **Basado en imagen**
- **Basado en archivo**
- **Llamada de voz**
- **Dispositivos extraíbles**
- **Software vulnerable**
  - o Basado en cliente vs. sin agentes
- **Sistemas y aplicaciones no soportadas**
- **Redes inseguras**
  - Redes inalámbricas
  - Con cable
  - Bluetooth
- **Puertos de servicio abiertos**
- **Credenciales predeterminadas**
- **Cadena de suministro**
  - Proveedores de servicio administrado (MSP)
  - Proveedores
  - Vendedores
- **Vectores humanos/ ingeniería social**
  - Phishing
  - Vishing
  - Smishing
  - Mala información/ desinformación
  - Suplantación
  - Compromiso de correo de negocios
  - Pretexting
  - Watering hole
  - Suplantación de marca
  - Typosquatting

2.3 Explicar diversos tipos de vulnerabilidades.

- **Aplicación**
  - Inyección de memoria
  - Desbordamiento de búfer
  - Condiciones de carrera
    - Tiempo de control (TOC)
    - Tiempo de uso (TOU)
  - Actualización maliciosa
- **Basado en sistemas operativos (OS)**
- **Basado en la web**
  - Structured Query Language injection (SQLi)
  - Secuencias de comandos entre sitios (XSS)
- **Hardware**
  - Firmware
  - Final de la vida
  - Heredado
- **Virtualización**
  - Escape de máquina virtual (VM)
  - Reutilización de recursos
- **Específico de la nube**
- **Cadena de suministro**
  - Proveedor de servicio
  - Proveedor de hardware
  - Proveedor de software
- **Criptográfico**
- **Mala configuración**
- **Dispositivo móvil**
  - Carga lateral
  - Jailbreaking
- **Día cero**

2.4 A partir de un escenario, analizar indicadores de actividad maliciosa.

- **Ataques de malware**
  - Ransomware
  - Troyanos
  - Gusano
  - Spyware
  - Bloatware
  - Virus
  - Keylogger
  - Bomba lógica
  - Rootkit
- **Ataques físicos**
  - Fuerza bruta
  - Clonación de identificación por radiofrecuencia (RFID)
  - Ambiental
- **Ataques de red**
  - Denegación de servicio distribuido (DDoS)
    - Amplificado
    - Reflejado
  - Ataques de Sistema de nombres de dominio (DNS)
  - Redes inalámbricas
  - En ruta
  - Repetición de credencial
  - Código malicioso
- **Ataques de aplicación**
  - Inyección
  - Desbordamiento de búfer
  - Repetición
  - Escalamiento de privilegios
  - Falsificación
  - Directory traversal
- **Ataques criptográficos**
  - Degradación
  - Colisión
  - Cumpleaños
- **Ataques de contraseña**
  - Spraying
  - Fuerza bruta
- **Indicadores**
  - Bloqueo de cuenta
  - Uso concurrente de la sesión
  - Contenido bloqueado
  - Viaje imposible
  - Consumo de recursos
  - Inaccesibilidad de recursos
  - Out-of-cycle logging
  - Publicado/documentado
  - Registros faltantes

2.5 Explicar el objetivo de las técnicas de mitigación usadas para asegurar la empresa.

- **Segmentación**
- **Control de acceso**
  - Lista de control de acceso (ACL)
  - Permisos
- **Lista de aplicaciones permitidas**
- **Aislamiento**
- **Parches**
- **Cifrado**
- **Monitoreo**
- **Mínimo privilegio**
- **Cumplimiento de la configuración**
- **Dar de baja**
- **Técnicas de endurecimiento**
  - Cifrado
  - Instalación de protección de endpoint
  - Firewall basado en el host
  - Sistema de Prevención de Intrusión Basado en Host (HIPS)
  - Deshabilitar puertos/protocolos
  - Cambios de contraseñas predeterminadas
  - Eliminación de software innecesario

3.0 Arquitectura de seguridad

3.1 Comparar y contrastar implicaciones de seguridad de los diferentes modelos de arquitectura.

- **Conceptos de infraestructura y arquitecura**
  - Nube
    - Matriz de responsabilidad
    - Consideraciones híbridas
    - Proveedor de terceros
  - Infraestructura como código (IaC)
  - Sin servidor
  - Microservicios
  - Infraestructura de red
    - Aislamiento físico
      - Air-gapped
    - Segmentación lógica
    - Redes definidas por software (SDN)
  - En sitio
  - Centralizado vs. descentralizado
  - Contenedorización
  - Virtualización
  - IoT
  - Sistemas de control industrial (ICS)/Supervisión, Control y Adquisición de Datos (SCADA)
  - Sistema operativo en tiempo real (RTOS)
  - Sistemas embebidos
  - Alta disponibilidad
- **Consideraciones**
  - Disponibilidad
  - Resiliencia
  - Costo
  - Reactividad
  - Escalabilidad
  - Facilidad de implementación
  - Transferencia de riesgos
  - Facilidad de recuperación
  - Disponibilidad de parches
  - Imposibilidad de aplicar parches
  - Energía
  - Computadora

3.2 A partir de un escenario, aplicar principios de seguridad para asegurar la infraestructura de la empresa.

- **Consideraciones de infraestructura**
  - Colocación de dispositivos
  - Zonas de seguridad
  - Superficie de ataque
  - Conectividad
  - Modos de falla
    - Fail-open
    - Fail-closed
  - Atributo de dispositivo
    - Activo vs. pasivo
    - En línea vs. tap/monitor
  - Dispositivos de red
    - Servidor de salto
    - Servidor proxy
    - Sistema de prevención de intrusión (IPS)/Sistema de detección de intrusión (IDS)
    - Balanceador de carga
    - Sensores
  - Seguridad de puertos
    - 802.1X
    - Protocolo de Autenticación Extensible (EAP)
  - Tipos de firewall
    - Firewall de aplicación web (WAF)
    - Administración de amenazas unificadas (UTM)
    - Firewall de próxima generación (NGFW)
    - Capa 4/Capa 7
- **Comunicación/acceso seguro**
  - Red Privada Virtual (VPN)
  - Acceso remoto
  - Tunelización
    - Transport Layer Security(TLS) TLS
    - Seguridad del Protocolo de Internet (IPSec)
  - Red de área amplia definida por software (SD-WAN)
  - Sector de servicio de acceso seguro (SASE)
- **Selección de controles efectivos**

3.3 Comparar y contrastar conceptos y estrategias para proteger los datos.

- **Tipos de datos**
  - Regulado
  - Secreto comercial
  - Propiedad intelectual
  - Información legal
  - Información financiera
  - Legible por humanos y no humanos
- **Clasificaciones de datos**
  - Sensibles
  - Confidenciales
  - Públicos
  - Restringidos
  - Privados
  - Críticos
- **Consideraciones generales de datos**
  - Estados de datos
    - Datos en reposo
    - Datos en tránsito
    - Datos en uso
  - Soberanía de los datos
  - Geolocalización
- **Métodos para asegurar datos**
  - Restricciones geográficas
  - Cifrado
  - Hashing
  - Enmascaramiento
  - Tokenización
  - Ofuscación
  - Segmentación
  - Restricciones de permisos

3.4 Explicar la importancia de la resiliencia y la recuperación en la arquitectura de seguridad.

- **Alta disponibilidad**
  - Balanceo de carga vs. clustering
- **Consideraciones de sitio**
  - Hot
  - Cold
  - Warm
  - Dispersión geográfica
- **Diversidad de plataformas**
- **Sistemas multi-nube**
- **Continuidad de operaciones**
- **Planificación de capacidad**
  - Personas
  - Tecnología
  - Infraestructura
- **Prueba**
  - Ejercicio de simulación
  - Falla
  - Simulaciones
  - Procesamiento paralelo
- **Copias de seguridad**
  - En el sitio/fuera del sitio
  - Frecuencia
  - Cifrado
  - Instantánea
  - Recuperación
  - Replicación
  - Journaling
- **Energía**
  - Generadores
  - Fuente de alimentación ininterrumpida (UPS)

4.0 Operaciones de Seguridad

4.1 A partir de un escenario, aplicar técnicas comunes de seguridad a los recursos computacionales.

- **Puntos de partida de seguridad**
  - Establecer
  - Implementar
  - Mantener
- **Endurecimiento de objetivos**
  - Dispositivos móviles
  - Estaciones de trabajo
  - Switches
  - Enrutadores
  - Infraestructura de nube
  - Servidores
  - ICS/SCADA
  - Sistemas embebidos
  - RTOS
  - Dispositivos IoT
- **Dispositivos inalámbricos**
  - Consideraciones de instalación
    - Encuestas del sitio
    - Mapas de calor
- **Soluciones móviles**
  - Gestión de dispositivos móviles (MDM)
  - Modelos de implementación
    - Trae Tu Propio Dispositivo (BYOD)
    - De propiedad corporativa y habilitada , personalmente (COPE)
    - Elija su propio dispositivo (CYOD)
  - Métodos de conexión
    - Celular
    - Wi-Fi
    - Bluetooth
- **Configuración de seguridad inalámbrica**
  - Acceso Protegido Wi-Fi 3 (WPA3)
  - Servidor de Autenticación AAA/Remota de Usuario por Acceso Telefónico (RADIUS)
  - Protocolos criptográficos
  - Protocolos de autenticación
- **Seguridad de la aplicación**
  - Validación de entrada
  - Cookies seguras
  - Análisis de código estático
  - Firma del código
- **Sandboxing**
- **Monitoreo**

4.2 Explicar las implicaciones de seguridad de la administración adecuada de activos de hardware, software y datos.

- **Proceso de adquisición/compra**
- **Asignación/contabilidad**
  - Propiedad
  - Clasificación
- **Monitoreo/seguimiento de activos**
  - Inventario
  - Enumeración
- **Eliminación/dada de baja**
  - Desinfección
  - Destrucción
  - Certificación
  - Retención de datos

4.3 Explicar diversas actividades asociadas con la administración de vulnerabilidades.

- **Métodos de identificación**
  - Escaneo de vulnerabilidad
  - Seguridad de la aplicación
    - Análisis estático
    - Análisis dinámico
    - Monitoreo de paquetes
  - Informes sobre amenazas informáticas
    - Inteligencia de código abierto (OSINT)
    - Propietario/terceros
    - Organización que comparte información
    - Dark web
  - Pruebas de penetración
  - Programa de divulgación responsable
    - Recompensa por errores
  - Auditoría de sistema/procesos
- **Análisis**
  - Confirmación
    - Falso positivo
    - Falso negativo
  - Priorización
  - Sistema de puntuación de vulnerabilidades comunes (CVSS)
  - Enumeración de vulnerabilidades comunes (CVE)
  - Clasificación de vulnerabilidades
  - Factor de exposición
  - Variables ambientales
  - Impacto organizacional/ en la industria
  - Tolerancia al riesgo
- **Respuesta y remediación de vulnerabilidades**
  - Parches
  - Seguros
  - Segmentación
  - Controles de compensación
  - Excepciones
- **Validación de remediación**
  - Reescaneo
  - Auditoría
  - Verificación
- **Informes**

4.4 Explicar los conceptos y las herramientas de alertas de seguridad y monitoreo.

- **Monitoreo de recursos computacionales**
  - Sistemas
  - Aplicaciones
  - Infraestructura
- **Actividades**
  - Agrupadores de bitácoras
  - Alertas
  - Escanear
  - Informes
  - Archivo
  - Respuesta de alertas y remediación/validación
    - Cuarentena
    - Ajuste de alerta
- **Herramientas**
  - Protocolo de automatización de contenido de seguridad (SCAP)
  - Referencias
  - Agentes/sin agente
  - Gestión de información y eventos de seguridad (SIEM)
  - Antivirus
  - Prevención de pérdida de datos (DLP)
  - Protocolo simple de gestión de red (SNMP)
  - NetFlow
  - Escáneres de vulnerabilidad

4.5 A partir de un escenario, modificar las capacidades de la empresa para aumentar la seguridad.

- **Firewall**
  - Reglas
  - Listas de acceso
  - Puertos/protocolos
  - Subredes analizadas
- **IDS/IPS**
  - Tendencias
  - Firmas
- **Filtro web**
  - Basado en agente
  - Proxy centralizado
  - Escaneo del Universal Resource Locator (URL)
  - Categorización del contenido
  - Reglas de bloqueo
  - Reputación
- **Seguridad del sistema operativo**
  - Política de grupo
  - SELinux
- **Implementación de protocolos seguros**
  - Selección de protocolos
  - Selección de puerto
  - Método de transporte
- **Filtro DNS**
- **Seguridad de correo electrónico**
  - Autenticación de mensajes basada en dominios (DMARC)
  - DomainKeys Identified Mail (DKIM)
  - Marco de políticas de remitente (SPF)
  - Puerta de enlace
- **Monitoreo de integridad de archivos**
- **DLP**
- **Control de acceso de red (NAC)**
- **Detección y respuesta de endpoint (EDR)/Detección y respuesta extendida (XDR)**
- **Análisis del comportamiento del usuario**

4.6 A partir de un escenario, implementar y mantener la administración de identidad y acceso.

- **Asignación/desasignación de cuenta de usuario**
- **Asignación de permisos e implicaciones**
- **Prueba de identidad**
- **Federación**
- **Inicio de sesión único (SSO)**
  - Protocolo ligero de acceso a directorio (LDAP)
  - Autorización abierta (OAuth)
  - Lenguaje de marcado de aserción de seguridad (SAML)
- **Interoperabilidad**
- **Confirmación**
- **Controles de Acceso**
  - Obligatorio
  - Discrecional
  - Basado en roles
  - Basado en reglas
  - Basado en atributos
  - Restricciones de hora del día
  - Mínimo privilegio
- **Autenticación de multifactores**
  - Implementaciones
    - Biométrica
    - Tokens de autenticación hard/soft
    - Claves de seguridad
  - Factores
    - Algo que sabe
    - Algo que tiene
    - Algo que es
    - Un lugar donde está
- **Conceptos de contraseñas**
  - Mejores prácticas de contraseñas
    - Longitud
    - Complejidad
    - Reutilización
    - Vencimiento
    - Edad
  - Administradores de contraseñas
  - Sin contraseña
- **Herramientas de administración de acceso privilegiado**
  - Permisos a tiempo
  - Bóvedas de contraseñas
  - Credenciales efímeras

4.7 Explicar la importancia de la automatización y orquestación relacionada a las operaciones de seguridad.

- **Usar casos de automatización y secuencia de comandos**
  - Aprovisionamiento de usuario
  - Aprovisionamiento de recursos
  - Guard rails
  - Grupos de seguridad
  - Creación de ticket
  - Escalamiento
  - Habilitar/deshabilitar servicios y acceso
  - Integración y pruebas continuas
  - Interfaces de programación de aplicación e integraciones (API)
- **Beneficios**
  - Eficiencia/ahorro de tiempo
  - Enforcing baselines
  - Configuraciones de infraestructura estándar
  - Escalar en forma segura
  - Retención de empleados
  - Tiempo de reacción
  - Multiplicador de fuerza de trabajo
- **Otras consideraciones**
  - Complejidad
  - Costo
  - Punto único de fallo
  - Deuda técnica
  - Soportabilidad continua

4.8 Explicar las actividades adecuadas de respuesta a incidentes.

- **Proceso**
  - Preparación
  - Detección
  - Análisis
  - Contención
  - Erradicación
  - Recuperación
  - Lecciones aprendidas
- **Capacitación**
- **Prueba**
  - Ejercicio de simulación
  - Simulaciones
- **Análisis de causa raiz**
- **Caza de amenazas**
- **Forense digital**
  - Retención legal
  - Cadena de custodia
  - Adquisición
  - Informes
  - Preservación
  - E-discovery

4.9 A partir de un escenario, usar las fuentes de datos para respaldar una investigación.

- **Datos de registro**
  - Registros de firewall
  - Registros de aplicación
  - Registros de endpoint
  - Registros de seguridad específicos de SO
  - Registros de IPS/IDS
  - Registros de red
  - Metadatos
- **Fuentes de datos**
  - Escaneos de vulnerabilidad
  - Informes automatizados
  - Tableros
  - Capturas de paquetes

5.0 Administración y supervisión de programa de seguridad

5.1 Resumir elementos de gobernanza efectiva de seguridad.

- **Pautas**
- **Políticas**
  - Política de Uso Aceptable (AUP)
  - Políticas de seguridad de la información
  - Continuidad empresarial
  - Recuperación de desastres
  - Respuesta a incidentes
  - Ciclo de vida del desarrollo de software (SDLC)
  - Administración de cambios
- **Estándares**
  - Contraseña
  - Control de acceso
  - Seguridad física
  - Cifrado
- **Procedimientos**
  - Administración de cambios
  - Incorporación/desvinculación
  - Playbooks
- **Consideraciones externas**
  - Regulatorias
  - Legal
  - Industrial
  - Local/regional
  - Nacional
  - Global
- **Monitoreo y revisión**
- **Tipos de estructuras de gobernanza**
  - Juntas
  - Comités
  - Entidades gubernamentales
  - Centralizado/descentralizado
- **Roles y responsabilidades por sistemas y datos**
  - Propietarios
  - Controladores
  - Procesadores
  - Custodios/administradores

5.2 Explicar elementos del proceso de administración de riesgos.

- **Identificación de riesgos**
- **Evaluación de riesgos**
  - Adhoc
  - Recurrente
  - Una vez
  - Continua
- **Análisis de riesgo**
  - Cualitativo
  - Cuantitativo
  - Expectativa de pérdida simple (SLE)
  - Expectativa de pérdida anualizada (ALE)
  - Tasa de ocurrencia anualizada (ARO)
  - Probabilidad
  - Posibilidad
  - Factor de exposición
  - Impacto
- **Registro de riesgos**
  - Indicador clave de riesgo
  - Propietarios de riesgo
  - Umbral de riesgo
- **Tolerancia al riesgo**
- **Apetito al riesgo**
  - Expansionario
  - Conservador
  - Neutro
- **Estrategias de gestión de riesgos**
  - Transferir
  - Aceptar
    - Exención
    - Excepción
  - Evitar
  - Mitigar
- **Informes de riesgo**
- **Análisis de impacto al negocio**
  - Tiempo objetivo de recuperación (RTO)
  - Punto objetivo de recuperación (RPO)
  - Tiempo medio de reparación (MTTR)
  - Tiempo medio entre fallos (MTBF)

5.3 Explicar los procesos asociados con la evaluación y administración de riesgos de terceros.

- **Evaluación de proveedores**
  - Pruebas de penetración
  - Cláusula de derecho de auditoría
  - Evidencia de auditorías internas
  - Evaluaciones independientes
  - Análisis de la cadena de suministro
- **Selección de proveedores**
  - Debida diligencia
  - Conflicto de interés
- **Tipos de acuerdo**
  - Acuerdo de Nivel de Servicio (SLA)
  - Memorándum del Acuerdo (MOA)
  - Memorándum de entendimiento (MOU)
  - Acuerdo de servicio maestro (MSA)
  - Orden de trabajo (WO)/ declaración de trabajo (SOW)
  - Acuerdo de no divulgación (NDA)
  - Acuerdo de Asociación Comercial (BPA)
- **Monitoreo de proveedores**
- **Cuestionarios**
- **Reglas y condiciones**

5.4 Resumir elementos de cumplimiento efectivo de seguridad.

- **Informe de cumplimiento**
  - Interno
  - Externo
- **Consecuencias del incumplimiento**
  - Multas
  - Sanciones
  - Daño a la reputación
  - Pérdida de licencia
  - Impactos contractuales
- **Monitoreo de cumplimiento**
  - Debida diligencia/cuidado
  - Confirmación y agradecimiento
  - Internos y externos
  - Automatización
- **Privacidad**
  - Implicaciones legales
    - Local/regional
    - Nacional
    - Global
  - Tema de datos
  - Controlador vs. procesador
  - Propiedad
  - Inventario de datos y retención
  - Derecho a ser olvidado

5.5 Explicar tipos y objetivos de auditorías y evaluaciones.

- **Confirmación**
- **Interno**
  - Cumplimiento
  - Comité de auditoría
  - Autoevaluaciones
- **Externo**
  - Regulatorias
  - Exámenes
  - Evaluación
  - Auditoría independiente de terceros
- **Pruebas de penetración**
  - Físico
  - Ofensivo
  - Defensivo
  - Integrada
  - Entorno conocido
  - Entorno parcialmente conocido
  - Entorno desconocido
  - Reconocimiento
    - Pasivo
    - Activo

5.6 A partir de un escenario, implementar prácticas de conocimiento de seguridad.

- **Phishing**
  - Campañas
  - Reconocer un intento de phishing
  - Responder a mensajes sospechosos reportados
- **Reconocimiento de comportamientos anómalos**
  - Riesgoso
  - Inesperado
  - No intencional
- **Guía y capacitación del usuario**
  - Política/manuales
  - Conocimiento situacional
  - Amenazas internas
  - Administración de contraseñas
  - Medios extraíbles y cables
  - Ingeniería social
  - Seguridad operacional
  - Entornos laborales remotos/híbridos
- **Reportes y monitoreo**
  - Inicial
  - Recurrente
- **Desarrollo**
- **Ejecución**

CompTIA Lista de siglas de Security+ SY0-701

A continuación hay una lista de siglas que aparecen el examen de CompTIA Seguridad+ SY0-701. 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.

Sigla	Frase completa
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AES-256	Advanced Encryption Standards 256-bit
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
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 Partners Agreement
BPDU	Bridge Protocol Data Unit
BYOD	Bring Your Own Device
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CAR	Corrective Action Report
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining
CCMP	Counter Mode/CBC-MAC Protocol
CCTV	Closed-circuit Television
CERT	Computer Emergency Response Team
CFB	Cipher Feedback

Sigla	Frase completa
CHAP	Challenge Handshake Authentication Protocol
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CMS	Content Management System
COOP	Continuity of Operation Planning
COPE	Corporate Owned, Personally Enabled
CP	Contingency Planning
CRC	Cyclical Redundancy Check
CRL	Certificate Revocation List
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 Vulnerability Enumeration
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
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHE	Diffie-Hellman Ephemeral
DKIM	DomainKeys Identified Mail
DLL	Dynamic Link Library
DLP	Data Loss Prevention
DMARC	Domain Message Authentication Reporting and Conformance
DNAT	Destination Network Address Translation
DNS	Domain Name System
DoS	Denial of Service
DPO	Data Privacy Officer

Sigla	Frase completa
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
ERP	Enterprise Resource Planning
ESN	Electronic Serial Number
ESP	Encapsulated Security Payload
FACL	File System Access Control List
FDE	Full Disk Encryption
FIM	File Integrity Management
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	Hashed Message Authentication Code
HOTP	HMAC-based One-time Password
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation Air Conditioning
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
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

Sigla	Frase completa
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP	Internet Message Access Protocol
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
ISO	International Standards Organization
ISP	Internet Service Provider
ISSO	Information Systems Security Officer
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	Mandatory Access Control
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MBR	Master Boot Record
MD5	Message Digest 5
MDF	Main Distribution Frame
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Dispositivo Multifuncional
MFP	Multifunction Printer
ML	Machine Learning
MMS	Multimedia Message Service
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multi-protocol Label Switching
MSA	Master Service Agreement
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure

Sigla	Frase completa
MTTR	Mean Time to Recover
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NFC	Near Field Communication
NGFW	Next-generation Firewall
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards & Technology
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OAUTH	Open Authorization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
OSINT	Open-source Intelligence
OSPF	Open Shortest Path First
OT	Operational Technology
OTA	Over the Air
OVAL	Open Vulnerability Assessment Language
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
PCI DSS	Payment Card Industry Data Security Standard
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PED	Personal Electronic Device
PEM	Privacy Enhanced Mail
PFS	Perfect Forward Secrecy
PGP	Pretty Good Privacy
PHI	Personal Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-shared Key
PTZ	Pan-tilt-zoom
PUP	Potentially Unwanted Program
RA	Recovery Agent
RA	Registration Authority
RACE	Research and Development in Advanced Communications Technologies in Europe
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Server
RAT	Remote Access Trojan
RBAC	Role-based Access Control
RBAC	Rule-based Access Control
RC4	Rivest Cipher version 4
RDP	Remote Desktop Protocol
RFID	Radio Frequency Identifier
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
SAN	Storage Area Network
SAN	Subject Alternative Name
SASE	Secure Access Service Edge
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCEP	Simple Certificate Enrollment Protocol
SD-WAN	Software-defined Wide Area Network
SDK	Software Development Kit
SDLC	Software Development Lifecycle
SDLM	Software Development Lifecycle Methodology

Sigla	Frase completa
SDN	Software-defined Networking
SE Linux	Security-enhanced Linux
SED	Self-encrypting Drives
SEH	Structured Exception Handler
SFTP	Secured File Transfer Protocol
SHA	Secure Hashing Algorithm
SHTTP	Secure Hypertext Transfer Protocol
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SLA	Service-level Agreement
SLE	Single Loss Expectancy
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
SOW	Statement of Work
SPF	Sender Policy Framework
SPIM	Spam over Internet Messaging
SQL	Structured Query Language
SQLi	SQL Injection
SRTP	Secure Real-Time Protocol
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXchange
SWG	Secure Web Gateway
TACACS+	Terminal Access Controller Access Control System
TAXII	Trusted Automated eXchange of Indicator Information
TCP/IP	Transmission Control Protocol/ Internet Protocol
TGT	Ticket Granting Ticket
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOC	Time-of-check
TOTP	Time-based One-time Password
TOU	Time-of-use
TPM	Trusted Platform Module
TTP	Tactics, Techniques, and Procedures
TSIG	Transaction Signature
UAT	User Acceptance Testing
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UEM	Unified Endpoint Management
UPS	Uninterruptable 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
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
WO	Work Order
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
WTLS	Wireless TLS
XDR	Extended Detection and Response
XML	Extensible Markup Language
XOR	Exclusive Or
XSRF	Cross-site Request Forgery
XSS	Cross-site Scripting

Lista de hardware y software para CompTIA Security+ SY0-701

CompTIA ha incluido esta lista de muestra de hardware y software para asistir a los candidatos mientras se preparan para el examen de certificación Security+ SY0-701. Esta lista también puede ser útil para las empresas de capacitación que desean crear un componente de laboratorio en su capacitación ofertada. Las listas con viñetas debajo de cada tema son listas de muestra y no están completas.

Equipos
- Tableta
- Computadora portátil
- Servidor web
- Firewall
- Enrutador
- Switch
- IDS
- IPS
- Punto de acceso inalámbrico
- Máquinas virtuales
- Sistema de correo electrónico
- Acceso a Internet
- Servidor de DNS
- Dispositivos IoT
- Token de hardware
- Teléfono inteligente

Hardware de repuesto
- NICs
- Fuentes de energía
- GBIC
- SFPs
- Switch administrado
- Punto de acceso inalámbrico
- UPS

Herramientas
- Analizador WiFi
- Mapeador de red
- Analizador de NetFlow

Software
- Windows OS
- Linux OS
- Kali Linux
- Software de captura de paquetes
- Software para pruebas con lápiz
- Herramientas de análisis dinámico y estático
- Escáner de vulnerabilidad
- Emuladores de red
- Código de muestra
- Editor de código
- SIEM
- Keyloggers
- Software MDM
- VPN
- Servicio DHCP
- Servicio DNS

Otra
- Acceso a entorno en la nube
- Documentación/diagramas de red de muestra
- Registros de muestra

CompTIA