Guía de examen de AWS Certified Security - Specialty (SCS-C03)

Introducción

El examen AWS Certified Security - Specialty (SCS-C03) está dirigido a personas que tienen la responsabilidad de proteger las soluciones en la nube. El examen valida la capacidad de un candidato para demostrar eficazmente sus conocimientos sobre seguridad en los productos y servicios de AWS.

En este examen, también se certifica su capacidad para completar las siguientes tareas:

- Aplicar las clasificaciones de datos especializadas y los mecanismos de protección de datos de AWS.
- Implementar métodos de cifrado de datos y mecanismos de cifrado de AWS.
- Implementar los mecanismos de AWS para seguir protocolos de Internet seguros.
- Utilizar los servicios y las características de seguridad de AWS para garantizar entornos de producción seguros.
- Tomar decisiones que tengan en cuenta las compensaciones entre el costo, la seguridad y la complejidad de la implementación para cumplir con un conjunto de requisitos de aplicación.
- Comprender las operaciones y los riesgos de seguridad.

Descripción del candidato objetivo

El candidato objetivo debe tener el equivalente a entre 3 y 5 años de experiencia en la protección de soluciones en la nube.

Conocimientos recomendados de AWS

El candidato objetivo debe tener los siguientes conocimientos de AWS:

- El modelo de responsabilidad compartida de AWS y su aplicación.
- La administración de la identidad a escala.
- La gobernanza de cuentas múltiples.
- La administración de los riesgos de la cadena de suministro de software.
- Las estrategias de prevención y respuesta a incidentes de seguridad.
- La administración de vulnerabilidades en la nube.
- El desarrollo de reglas de firewall a escala para las capas de la 3 a la 7.

- El análisis de la causa raíz del incidente.
- Experiencia en responder a una auditoría.
- Las estrategias de registro y supervisión.
- Metodologías de cifrado de datos, tanto en reposo como en tránsito.
- Los controles de recuperación de desastres, incluidas estrategias de copia de seguridad.

Tareas de trabajo que están fuera del alcance del candidato

A continuación, se muestra una lista que contiene las tareas de trabajo que no se espera que el candidato pueda realizar. Esta lista no es exhaustiva. Estas tareas están fuera del alcance del examen:

- Diseñar algoritmos criptográficos.
- Analizar el tráfico a nivel de paquete.
- Diseñar las implementaciones generales de la nube.
- Administrar los recursos de computación de los usuarios finales.
- Entrenar modelos de machine learning.

Consulte el apéndice A para obtener una lista de los servicios y las características de AWS dentro del alcance y una lista de los servicios y las características de AWS fuera del alcance.

Contenido del examen

Tipos de respuesta

El examen incluye uno o más de los siguientes tipos de preguntas:

- **Opción múltiple:** hay una respuesta correcta y tres incorrectas (distractoras)
- **Respuesta múltiple:** hay dos o más respuestas correctas entre cinco o más opciones.
- **Preguntas de orden:** hay una lista de 3 a 5 respuestas para completar una tarea específica. Debe seleccionar las respuestas correctas y colocarlas en el orden correcto para recibir los créditos por la pregunta.
- **Preguntas de comparación:** hay una lista de respuestas que coinciden con una lista de 3 a 7 peticiones. Debe hacer coincidir todos los pares correctamente para recibir crédito por la pregunta.

Las preguntas no respondidas se califican como incorrectas. No hay penalización por adivinar. El examen incluye 50 preguntas que afectarán el puntaje[1].

Contenido sin puntaje

El examen incluye 15 preguntas sin puntaje que no afectan la puntuación total. AWS recopila información sobre el rendimiento en estas preguntas sin puntaje a fin de evaluarlas para su uso como preguntas con puntaje en el futuro. Estas preguntas sin puntaje no están identificadas en el examen.

Resultados del examen

El examen AWS Certified Security - Specialty (SCS-C03) es un examen que se clasifica como aprobado o reprobado. El puntaje se obtiene según un estándar mínimo que establecen los profesionales de AWS en función de las prácticas recomendadas y las pautas del sector de la certificación.

El informe de los resultados del examen se da en una escala del 100 al 1000. El puntaje mínimo para aprobar es 750. El puntaje muestra cómo le fue en el examen en general y si lo aprobó o no. Los modelos de puntuación en escala ayudan a equiparar las puntuaciones de varios formularios de examen que pueden tener niveles de dificultad un poco diferentes.

El informe de puntaje podría contener una tabla de clasificación de su rendimiento en cada sección. En el examen, se usa un modelo de puntaje compensatorio, lo que significa que no es necesario aprobar cada sección. Solo necesita aprobar el examen general.

Cada sección del examen tiene una ponderación específica, por lo que algunas contienen más preguntas que otras. En la tabla de clasificaciones, se presenta información general que resalta sus fortalezas y debilidades. Interprete los comentarios de cada sección con precaución.

[1] No se aplica a la versión beta del examen. Puede encontrar más información sobre los exámenes beta en general en el sitio web de AWS Certification.

Descripción del contenido

Esta guía de examen incluye ponderaciones, dominios de contenido y tareas para el examen. Sin embargo, no proporciona una lista completa del contenido del examen.

El examen tiene los siguientes dominios de contenido y ponderaciones:

- Dominio de contenido 1: Detección (el 16 % del contenido puntuado)
- Dominio de contenido 2: Respuesta a incidentes (el 14 % del contenido puntuado)
- Dominio de contenido 3: Seguridad de infraestructura (el 18 % del contenido puntuado)
- Dominio de contenido 4: Identity and Access Management (el 20 % del contenido puntuado)
- Dominio de contenido 5: Protección de datos (el 18 % del contenido puntuado)
- Dominio de contenido 6: Aspectos básicos y gobernanza de la seguridad (el 14 % del contenido puntuado)

Dominio de contenido 1: Detección

Tarea 1.1: Diseñe e implemente soluciones de supervisión y alertas para una cuenta u organización de AWS.

Habilidad 1.1.1: Analice las cargas de trabajo para determinar los requisitos de supervisión.
Habilidad 1.1.2: Diseñe e implemente estrategias de supervisión de la carga de trabajo (por ejemplo, mediante la configuración de comprobaciones de estado de los recursos).
Habilidad 1.1.3: Agregue eventos de seguridad y supervisión.
Habilidad 1.1.4: Cree métricas, alertas y paneles para detectar datos y eventos anómalos (por ejemplo, Amazon GuardDuty, Amazon Security Lake, AWS Security Hub, Amazon Macie).
Habilidad 1.1.5: Cree y administre automatizaciones para realizar evaluaciones e investigaciones periódicas (por ejemplo, mediante la implementación de paquetes de conformidad de AWS Config, Security Hub o AWS Systems Manager State Manager).

Tarea 1.2: Diseñe e implemente soluciones de registro.

Habilidad 1.2.1: Identifique las fuentes de ingesta y almacenamiento de registros en función de los requisitos.
Habilidad 1.2.2: Configure el registro para los servicios y aplicaciones de AWS (por ejemplo, configurando una pista de AWS CloudTrail para una organización, creando una cuenta de registro de Amazon CloudWatch dedicada o configurando el agente de Registros de Amazon CloudWatch).
Habilidad 1.2.3: Implemente el almacenamiento de registros y los lagos de datos de registro (por ejemplo, Security Lake) e intégrelos con herramientas de seguridad de terceros.
Habilidad 1.2.4: Utilice los servicios de AWS para analizar los registros (por ejemplo, los hallazgos de CloudWatch Logs Insights, Amazon Athena y Security Hub).
Habilidad 1.2.5: Utilice los servicios de AWS para normalizar, analizar y correlacionar los registros (por ejemplo, OpenSearch, AWS Lambda y Amazon Managed Grafana).
Habilidad 1.2.6: Determine y configure las fuentes de registro adecuadas en función del diseño de la red, las amenazas y los ataques (por ejemplo, los registros de flujo de VPC, los registros de flujo de la puerta de enlace de tránsito y los registros de Amazon Route 53 Resolver).

Tarea 1.3: Solucione problemas con las soluciones de monitoreo, registro y alertas de seguridad.

Habilidad 1.3.1: Analice la funcionalidad, los permisos y la configuración de los recursos (por ejemplo, el registro de funciones de Lambda, el registro de Amazon API Gateway, las comprobaciones de estado y el registro de Amazon CloudFront).
Habilidad 1.3.2: Corrija la mala configuración de los recursos (por ejemplo, solucionando los problemas de configuración del agente de CloudWatch o solucionando los registros faltantes).

Dominio de contenido 2: Respuesta ante incidentes

Tarea 2.1: Diseñe y pruebe un plan de respuesta ante incidentes.

Habilidad 2.1.1: Diseñe e implemente planes de respuesta y manuales de procedimientos para responder a los incidentes de seguridad (por ejemplo, Systems Manager OpsCenter, cuadernos de IA de Amazon SageMaker AWS).
Habilidad 2.1.2: Utilice las capacidades y características de los servicios de AWS para configurar los servicios a fin de que estén preparados para los incidentes (por ejemplo, aprovisionando el acceso, implementando herramientas de seguridad, minimizando el radio de acción o configurando las protecciones de AWS Shield Advanced).
Habilidad 2.1.3: Recomiende procedimientos para probar y validar la eficacia de un plan de respuesta ante incidentes (por ejemplo, AWS Fault Injection Service, AWS Resilience Hub).
Habilidad 2.1.4: Utilice los servicios de AWS para corregir los incidentes automáticamente (por ejemplo, Systems Manager, Automated Forensics Orchestrator para Amazon EC2, AWS Step Functions, Controlador de recuperación de aplicaciones de Amazon y funciones de Lambda).

Tarea 2.2: Responda a los eventos de seguridad.

Habilidad 2.2.1: Capture y almacene los registros relevantes del sistema y las aplicaciones como artefactos forenses.
Habilidad 2.2.2: Busque y correlacione los registros de eventos de seguridad en las aplicaciones y los servicios de AWS.
Habilidad 2.2.3: Valide los hallazgos de los servicios de seguridad de AWS para evaluar el alcance y el impacto de un evento.
Habilidad 2.2.4: Responda a los recursos afectados conteniendo y erradicando las amenazas, y recuperando los recursos (por ejemplo, mediante la implementación de controles de contención de red o la restauración de las copias de seguridad).
Habilidad 2.2.5: Describa los métodos para realizar un análisis de la causa raíz (por ejemplo, Amazon Detective).

Dominio de contenido 3: Seguridad de la infraestructura

Tarea 3.1: Diseñe, implemente y solucione los problemas de los controles de seguridad para los servicios periféricos de la red.

Habilidad 3.1.1: Defina y seleccione estrategias de seguridad de la periferia en función de las amenazas y los ataques anticipados.
Habilidad 3.1.2: Implemente una protección adecuada de la periferia de red (por ejemplo, encabezados de CloudFront, AWS WAF, políticas de AWS IoT, protección contra las amenazas del OWASP Top 10, intercambio de recursos entre orígenes de Amazon S3 [cross-origin resource sharing, CORS], Shield Advanced).
Habilidad 3.1.3: Diseñe e implemente reglas y controles de la periferia de AWS en función de los requisitos (por ejemplo, la ubicación geográfica, la geolocalización, la limitación de velocidad y la toma de huellas dactilares de los clientes).
Habilidad 3.1.4: Configure las integraciones con los servicios de la periferia de AWS y los servicios de terceros (por ejemplo, mediante la ingesta de datos en formato de marco de trabajo de esquema de ciberseguridad abierto [Open Cybersecurity Schema Framework, OCSF], mediante el uso de reglas de WAF de terceros).

Tarea 3.2: Diseñe, implemente y solucione los problemas de los controles de seguridad para las cargas de trabajo de computación.

Habilidad 3.2.1: Diseñe e implemente AMI de Amazon EC2 e imágenes de contenedores reforzados para proteger las cargas de trabajo de computación e incorporar controles de seguridad (por ejemplo, Systems Manager o EC2 Image Builder).
Habilidad 3.2.2: Aplique los perfiles de instancia, los roles de servicio y los roles de ejecución de forma adecuada para autorizar las cargas de trabajo de computación.
Habilidad 3.2.3: Analice los recursos de computación en busca de vulnerabilidades conocidas (por ejemplo, escanee imágenes de contenedores y funciones de Lambda con Amazon Inspector, supervise los tiempos de ejecución de computación con GuardDuty).
Habilidad 3.2.4: Implemente parches en todos los recursos de computación para mantener entornos seguros y conformes mediante la automatización de los procesos de actualización y la integración de la validación continua (por ejemplo, Administrador de parches de Systems Manager o Amazon Inspector).
Habilidad 3.2.5: Configure el acceso administrativo seguro a los recursos de computación (por ejemplo, Systems Manager Session Manager, EC2 Instance Connect).

Habilidad 3.2.6: Configure las herramientas de seguridad para descubrir y corregir las vulnerabilidades dentro de una canalización (por ejemplo, Amazon Q Developer, Amazon CodeGuru Security).
Habilidad 3.2.7: Implemente protecciones y barreras de protección para las aplicaciones de IA generativa (por ejemplo, aplicando las protecciones de IA generativa del OWASP Top 10 para las aplicaciones de LLM).

Tarea 3.3: Diseñe y solucione los problemas de los controles de seguridad de la red.

Habilidad 3.3.1: Diseñe y resuelva los problemas de los controles de red adecuados para permitir o impedir el tráfico de red según sea necesario (por ejemplo, grupos de seguridad, ACL de red o AWS Network Firewall).
Habilidad 3.3.2: Diseñe una conectividad segura entre redes híbridas y multinube (por ejemplo, AWS Site-to-Site VPN, Amazon AWS Direct Connect, MAC Security [MACSec]).
Habilidad 3.3.3: Determine y configure los requisitos de carga de trabajo de seguridad para la comunicación entre entornos híbridos y AWS (por ejemplo, mediante Acceso verificado de AWS).
Habilidad 3.3.4: Diseñe la segmentación de la red en función de los requisitos de seguridad (por ejemplo, protecciones de tráfico norte/sur y este/oeste, subredes aisladas).
Habilidad 3.3.5: Identifique el acceso innecesario a la red (por ejemplo, los hallazgos de accesibilidad a la red de Acceso verificado de AWS, Network Access Analyzer o Amazon Inspector).

Dominio de contenido 4: Identity and Access Management

Tarea 4.1: Diseñe, implemente y solucione los problemas de las estrategias de autenticación.

Habilidad 4.1.1: Diseñe y establezca soluciones de identidad para la autenticación humana, de aplicaciones y de sistemas (por ejemplo, AWS IAM Identity Center, Amazon Cognito, autenticación multifactor [multi-factor authentication, MFA] e integración con proveedores de identidades [identity provider, IdP]).
Habilidad 4.1.2: Configure los mecanismos para emitir credenciales temporales (por ejemplo, AWS Security Token Service [AWS STS], URL prefirmadas de Amazon S3).

Habilidad 4.1.3: Solución de problemas de autenticación (por ejemplo, CloudTrail, Amazon Cognito, conjuntos de permisos de IAM Identity Center, AWS Directory Service).

Tarea 4.2: Diseñe, implemente y solucione los problemas de las estrategias de autorización.

Habilidad 4.2.1: Diseñe y evalúe los controles de autorización para el acceso humano, de aplicaciones y del sistema (por ejemplo, Amazon Verified Permissions, las rutas de IAM, los roles de IAM Roles Anywhere, las políticas de recursos para el acceso entre cuentas y las políticas de confianza de los roles de IAM).
Habilidad 4.2.2: Diseñe estrategias de control de acceso basado en atributos (attribute-based access control, ABAC) y control de acceso basado en roles (role-based access control, RBAC) (por ejemplo, configurando el acceso a los recursos en función de etiquetas o atributos).
Habilidad 4.2.3: Diseñe, interprete e implemente políticas de IAM siguiendo el principio de mínimo privilegio (por ejemplo, límites de permisos, políticas de sesión).
Habilidad 4.2.4: Analice los errores de autorización para determinar las causas o los efectos (por ejemplo, simulador de políticas de IAM, analizador de acceso de IAM).
Habilidad 4.2.5: Investigue y corrija los permisos, autorizaciones o privilegios no deseados concedidos a un recurso, servicio o entidad (por ejemplo, analizador de acceso de IAM).

Dominio de contenido 5: Protección de datos

Tarea 5.1: Diseñe e implemente controles para los datos en tránsito.

Habilidad 5.1.1: Diseñe y configure mecanismos para solicitar el cifrado al conectarse a los recursos (por ejemplo, configurando las políticas de seguridad de Elastic Load Balancing [ELB] o aplicando las configuraciones de TLS).
Habilidad 5.1.2: Diseñe y configure mecanismos para un acceso seguro y privado a los recursos (por ejemplo, AWS PrivateLink, puntos de conexión de VPC, AWS Client VPN, Acceso verificado de AWS).
Habilidad 5.1.3: Diseñe y configure el cifrado entre recursos en tránsito (por ejemplo, configuraciones de cifrado entre nodos para Amazon EMR, Amazon Elastic Kubernetes Service [Amazon EKS], IA de SageMaker, cifrado Nitro).

Tarea 5.2: Diseñe e implemente controles para los datos en reposo.

Habilidad 5.2.1: Diseñe, implemente y configure el cifrado de datos en reposo en función de requisitos específicos (por ejemplo, seleccionando el servicio de claves de cifrado adecuado, como AWS CloudHSM o AWS Key Management Service [AWS KMS], o seleccionando el tipo de cifrado adecuado, como el cifrado del cliente o el cifrado del servidor).
Habilidad 5.2.2: Diseñe y configure mecanismos para proteger la integridad de los datos (por ejemplo, bloqueo de objetos de S3, bloqueo de almacenes de S3 Glacier, control de versiones, firma de código digital, validación de archivos).
Habilidad 5.2.3: Diseñe soluciones automáticas de administración y retención del ciclo de vida de los datos (por ejemplo, políticas de ciclo de vida de S3, bloqueo de objetos de S3, políticas de ciclo de vida de Amazon Elastic File System [Amazon EFS] y políticas de copia de seguridad de Amazon FSx para Lustre).
Habilidad 5.2.4: Diseñe y configure soluciones seguras de copia de seguridad y replicación de datos (por ejemplo, Amazon Data Lifecycle Manager, AWS Backup, protección contra ransomware, AWS DataSync).

Tarea 5.3: Diseñe e implemente controles para proteger datos confidenciales, credenciales, secretos y materiales de claves criptográficas.

Habilidad 5.3.1: Diseñe la administración y rotación de credenciales y secretos (por ejemplo, AWS Secrets Manager).
Habilidad 5.3.2: Administre y use el material de claves importado (por ejemplo, administrando y rotando el material de claves importado, administrando y configurando almacenes de claves externos).
Habilidad 5.3.3: Describa las diferencias entre el material de claves importado y el material de claves generado por AWS.
Habilidad 5.3.4: Enmascare la información confidencial (por ejemplo, las políticas de protección de datos de Registros de CloudWatch o la protección de datos de mensajes de Amazon Simple Notification Service [Amazon SNS]).
Habilidad 5.3.5: Cree y administre claves y certificados de cifrado en una sola región de AWS o en varias regiones (por ejemplo, las claves de AWS KMS administradas por el cliente de AWS KMS o AWS Private Certificate Authority).

Dominio de contenido 6: Aspectos básicos y gobernanza de la seguridad

Tarea 6.1: Desarrolle una estrategia para implementar y administrar las cuentas de AWS de forma centralizada.

- Habilidad 6.1.1: Implemente y configure organizaciones mediante AWS Organizations.
- Habilidad 6.1.2: Implemente y administre AWS Control Tower en entornos nuevos y existentes, e implemente controles opcionales y personalizados.
- Habilidad 6.1.3: Implemente políticas de la organización para administrar los permisos (por ejemplo, SCP, RCP, políticas de exclusión de servicios de IA, políticas declarativas).
- Habilidad 6.1.4: Administre de forma centralizada los servicios de seguridad (por ejemplo, cuentas de administrador delegado).
- Habilidad 6.1.5: Administre las credenciales de los usuarios raíz de las cuentas de AWS (por ejemplo, centralizando el acceso raíz para las cuentas de miembros, administrando MFA y diseñando procedimientos innovadores).

Tarea 6.2: Implemente una estrategia de implementación segura y coherente para los recursos en la nube.

- Habilidad 6.2.1: Utilice la infraestructura como código (infrastructure as code, IaC) para implementar los recursos de la nube de forma coherente y segura en todas las cuentas (por ejemplo, conjuntos de pilas de CloudFormation, herramientas de IaC de terceros, CloudFormation Guard, cfn-lint).
- Habilidad 6.2.2: Use etiquetas a fin de organizar los recursos de AWS en grupos para su administración (por ejemplo, agrupándolos por departamento, centro de costos o entorno).
- Habilidad 6.2.3: Implemente y aplique políticas y configuraciones desde una fuente central (por ejemplo, AWS Firewall Manager).
- Habilidad 6.2.4: Comparta recursos de forma segura entre cuentas de AWS (por ejemplo, AWS Service Catalog, AWS Resource Access Manager [AWS RAM]).

Tarea 6.3: Evalúe el cumplimiento de los recursos de AWS.

Habilidad 6.3.1: Cree o habilite reglas para detectar y corregir los recursos de AWS no conformes y para enviar notificaciones (por ejemplo, mediante el uso de AWS Config para agregar alertas y corregir los recursos no conformes, Security Hub).
Habilidad 6.3.2: Utilice los servicios de auditoría de AWS para recopilar y organizar las pruebas (por ejemplo, AWS Audit Manager o AWS Artifact).
Habilidad 6.3.3: Utilice los servicios de AWS para evaluar la arquitectura y comprobar el cumplimiento de las Prácticas recomendadas para la seguridad de AWS (por ejemplo, la herramienta Marco de AWS Well-Architected).

Apéndice A

Tecnologías y conceptos que pueden aparecer en el examen

En la siguiente lista, se enumeran las tecnologías y conceptos que pueden aparecer en el examen. Esta lista no es exhaustiva y está sujeta a cambios. El orden y la ubicación de los elementos de esta lista no indican su peso ni importancia relativos en el examen:

- AWS CLI
- SDK de AWS
- Consola de administración de AWS
- Acceso remoto seguro
- Administración de certificados
- Infraestructura como código (IaC)

Servicios y características de AWS dentro del alcance

Nota: La seguridad afecta a todos los servicios de AWS. Muchos servicios no aparecen en esta lista porque el servicio general está fuera del alcance, pero los aspectos de seguridad del servicio están dentro del alcance. Por ejemplo, a un candidato de este examen no se le preguntará sobre los pasos para configurar la replicación en un bucket de S3. Sin embargo, es posible que se le pregunte sobre la configuración de una política de bucket de S3.

En la siguiente lista, se enumeran los servicios y las características de AWS que están dentro del alcance del examen. Esta lista no es exhaustiva y está sujeta a cambios. Las ofertas de AWS aparecen en categorías que se alinean con las funciones principales de las ofertas:

Análisis:

- Amazon Athena
- Amazon OpenSearch Service

Integración de aplicaciones:

- Amazon Simple Notification Service (Amazon SNS)
- AWS Step Functions

Computación:

- Amazon API Gateway
- Amazon EC2 (incluidos EC2 Image Builder y EC2 Instance Connect)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon EMR
- AWS Lambda
- Amazon Data Lifecycle Manager

Herramientas para desarrolladores

- AWS Fault Injection Service

Internet de las cosas

- AWS IoT Core

Machine learning:

- Amazon Bedrock
- Seguridad de Amazon CodeGuru
- Amazon Q Business
- Amazon Q Developer
- IA de Amazon SageMaker

Administración y gobernanza:

- AWS CloudFormation
- AWS CloudTrail
- AWS CloudTrail Lake
- Amazon CloudWatch
- AWS Config
- AWS Control Tower
- Amazon Managed Grafana
- AWS Organizations
- AWS Resilience Hub
- AWS Resource Access Manager (AWS RAM)
- AWS Service Catalog
- AWS Systems Manager
- AWS Trusted Advisor
- Notificaciones de usuarios de AWS
- Herramienta de AWS Well-Architected

Redes y entrega de contenido:

- Controlador de recuperación de aplicaciones de Amazon
- Amazon VPC
    - Analizador de acceso a la red
    - ACL de red
    - Grupos de seguridad
    - Puntos de conexión de VPC
    - AWS Site-to-Site VPN
    - Registros de flujo
    - Puntos de conexión de VPC
    - Acceso verificado de AWS
- AWS Client VPN
- Amazon CloudFront
- Amazon Verified Permissions
- Amazon Route 53 (incluido el firewall de DNS de Route 53 Resolver)
- AWS Direct Connect
- Elastic Load Balancing (ELB)
- Analizador de acceso a la red
- AWS Transit Gateway

Seguridad, identidad y cumplimiento:

- AWS Artifact
- AWS Audit Manager
- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Cognito
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- Automated Forensics Orchestrator para Amazon EC2
- Amazon GuardDuty
- AWS IAM Identity Center
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- AWS Key Management Service (AWS KMS)
- Amazon Macie
- AWS Network Firewall

- AWS Private Certificate Authority
- AWS Secrets Manager
- AWS Security Hub
- Amazon Security Lake
- AWS Security Token Service (AWS STS)
- AWS Shield
- AWS Shield Advanced
- AWS WAF

Almacenamiento y administración de datos:

- Amazon S3
- AWS Backup
- AWS DataSync
- Amazon Elastic File System (Amazon EFS) (incluidas las políticas de ciclo de vida de EFS)
- Amazon FSx para Lustre

Servicios y características de AWS fuera del alcance

En la siguiente lista, se enumeran los servicios y las características de AWS que están fuera del alcance del examen. Esta lista no es exhaustiva y está sujeta a cambios. Las ofertas de AWS que no tienen ninguna relación con los roles laborales objetivo para el examen se excluyen de esta lista:

Integración de aplicaciones:

- Amazon Managed Workflows para Apache Airflow (Amazon MWAA)

Seguridad, identidad y cumplimiento:

- AWS Payment Cryptography

Apéndice B: Comparación entre SCS-C02 y SCS-C03

Comparación en paralelo

En la siguiente tabla, se muestran los dominios y el porcentaje de preguntas con puntaje en cada dominio para el examen SCS-C02 (en uso hasta el 1 de diciembre de 2025) y el examen SCS-C03 (en uso a partir del 2 de diciembre de 2025).

Dominio de SCS-C02	Dominio de SCS-C03
Dominio 1: Detección de amenazas y respuesta ante incidentes (14 %)	Dominio de contenido 1: Detección (el 16 % del contenido puntuado)
Dominio 2: Registro y monitoreo de seguridad (18 %)	Dominio de contenido 2: Respuesta ante incidentes (14 %)
Dominio 3: Seguridad de la infraestructura (20 %)	Dominio de contenido 3: Seguridad de la infraestructura (18 %)
Dominio 4: Identity and Access Management (16 %)	Dominio de contenido 4: Identity and Access Management (20 %)
Dominio 5: Protección de datos (18 %)	Dominio de contenido 5: Protección de datos (18 %)
Dominio 6: Administración y gobernanza de seguridad (14 %)	Dominio de contenido 6: Aspectos básicos y gobernanza de la seguridad (14 %)

Adiciones de contenido para SCS-C03

En la tarea 2.2.3, se agregó el siguiente contenido:

- 2.2.3 Valide los hallazgos de los servicios de seguridad de AWS para evaluar el alcance y el impacto de un evento.

En la tarea 3.1.4, se agregó el siguiente contenido:

- 3.1.4 Configure las integraciones con los servicios de la periferia de AWS y los servicios de terceros (por ejemplo, mediante la ingesta de datos en formato de marco de trabajo de esquema de ciberseguridad abierto [Open Cybersecurity Schema Framework, OCSF], mediante el uso de reglas de WAF de terceros).

En la tarea 3.2.7, se agregó el siguiente contenido:

- 3.2.7 Implemente protecciones y barreras de protección para las aplicaciones de IA generativa (por ejemplo, aplicando las protecciones de IA generativa del OWASP Top 10 para las aplicaciones de LLM).

En la tarea 5.1.3, se agregó el siguiente contenido:

- 5.1.3 Diseñe y configure el cifrado entre recursos en tránsito (por ejemplo, configuraciones de cifrado entre nodos para Amazon EMR, Amazon Elastic Kubernetes Service [Amazon EKS], IA de SageMaker, cifrado Nitro).

En la tarea 5.3.3, se agregó el siguiente contenido:

- 5.3.3 Describa las diferencias entre el material de claves importado y el material de claves generado por AWS.

En la tarea 5.3.4, se agregó el siguiente contenido:

- 5.3.4 Enmascare la información confidencial (por ejemplo, las políticas de protección de datos de Registros de CloudWatch o la protección de datos de mensajes de Amazon Simple Notification Service [Amazon SNS]).

En la tarea 5.3.5, se agregó el siguiente contenido:

- 5.3.5 Cree y administre claves y certificados de cifrado en una sola región de AWS o en varias regiones (por ejemplo, las claves de AWS KMS administradas por el cliente de AWS KMS o AWS Private Certificate Authority).

Eliminaciones de contenido para SCS-C03

En la tarea 6.4, se eliminó el siguiente contenido:

- Identificar las brechas de seguridad mediante revisiones de arquitectura y análisis de costos.

En la tarea 1.1, se eliminó el siguiente contenido:

- Formato AWS Security Finding

En la tarea 1.3, se eliminó el siguiente contenido:

- guía de respuesta ante incidentes de seguridad de AWS

En la tarea 2.5, se eliminó el siguiente contenido:

- formato y componentes de registro (por ejemplo, registros de CloudTrail)

En la tarea 3.3, se eliminó el siguiente contenido:

- seguridad basada en host (por ejemplo, firewalls, refuerzo)
- activar los mecanismos de seguridad basados en el host (por ejemplo, los firewalls basados en el host)

En la tarea 3.4, se eliminó el siguiente contenido:

- cómo analizar la conectividad (por ejemplo, mediante VPC Reachability Analyzer y Amazon Inspector)
- conceptos fundamentales de redes TCP/IP (por ejemplo, UDP en comparación con TCP, puertos, modelo de interconexión de sistemas abiertos [Open Systems Interconnection, OSI], utilidades del sistema operativo de red)
- identificar, interpretar y priorizar los problemas de conectividad de red (por ejemplo, mediante conexiones de red de Amazon Inspector)

En la tarea 4.2, se eliminó el siguiente contenido:

- componentes e impacto de una política (por ejemplo, entidad principal, acción, recurso, condición)

En la tarea 5.1, se eliminó el siguiente contenido:

- conceptos de TLS
- diseñar redes entre regiones mediante el uso de VIF privados y públicos

En la tarea 5.2, se eliminó el siguiente contenido:

- Configure el alojamiento web de sitios web estáticos de S3.

Recategorizaciones del contenido para SCS-C03

Durante la transición de SCS-C02 a SCS-C03 se han producido las siguientes reorganizaciones importantes de contenido:

Los dominios 1 y 2 de SCS-C02 se han reestructurado:

- "Detección de amenazas y respuesta ante incidentes" y el "Registro y monitoreo de seguridad" ahora son:
  - Dominio 1: Detección
  - Dominio 2: Respuesta ante incidentes

Se cambió el nombre del dominio 6 para SCS-C03:

- De "Administración y gobernanza de la seguridad" a "Aspectos básicos y gobernanza de la seguridad"

Se recategorizaron los siguientes enunciados de tareas:

El enunciado de la tarea 1.1 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 1.1 Diseñe e implemente la supervisión y las alertas para una cuenta u organización de AWS.
- 1.2 Diseñe e implemente el registro.
- 2.1 Diseñe y pruebe un plan de respuesta ante incidentes.
- 2.2 Responda a los eventos de seguridad.

El enunciado de la tarea 1.2 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 1.1 Diseñe e implemente la supervisión y las alertas para una cuenta u organización de AWS.
- 1.2 Diseñe e implemente el registro.

El enunciado de la tarea 1.3 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 2.1 Diseñe y pruebe un plan de respuesta ante incidentes.
- 2.2 Responda a los eventos de seguridad.

El enunciado de la tarea 2.1 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 1.1 Diseñe e implemente la supervisión y las alertas para una cuenta u organización de AWS.

El enunciado de la tarea 2.2 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 1.1 Diseñe e implemente la supervisión y las alertas para una cuenta u organización de AWS.
- 1.2 Diseñe e implemente el registro.
- 1.3 Solucione problemas con el monitoreo, el registro y las alertas de seguridad.

El enunciado de la tarea 2.3 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 1.2 Diseñe e implemente el registro.

El enunciado de la tarea 2.4 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 1.2 Diseñe e implemente el registro.
- 1.3 Solucione problemas con el monitoreo, el registro y las alertas de seguridad.

El enunciado de la tarea 2.5 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 1.2 Diseñe e implemente el registro.

El enunciado de la tarea 3.1 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 1.2 Diseñe e implemente el registro.
- 3.1 Diseñe, implemente y solucione los problemas de los controles de seguridad para los servicios periféricos de la red.

El enunciado de la tarea 3.2 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 1.2 Diseñe e implemente el registro.
- 3.3 Diseñe y solucione los problemas de los controles de seguridad de la red.
- 5.1 Diseñe e implemente controles para los datos en tránsito.
- 6.2 Implemente una estrategia de implementación segura y coherente para los recursos en la nube.

El enunciado de la tarea 3.3 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 3.2 Diseñe, implemente y solucione los problemas de los controles de seguridad para las cargas de trabajo de computación.
- 5.3 Diseñe e implemente controles para proteger datos confidenciales, credenciales, secretos y materiales de claves criptográficas.

El enunciado de la tarea 3.4 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 1.2 Diseñe e implemente el registro.
- 3.3 Diseñe y solucione los problemas de los controles de seguridad de la red.

El enunciado de la tarea 4.1 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 4.1 Diseñe, implemente y solucione los problemas de las estrategias de autenticación.

El enunciado de la tarea 4.2 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 4.2 Diseñe, implemente y solucione los problemas de las estrategias de autorización.

El enunciado de la tarea 5.1 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 3.2 Diseñe, implemente y solucione los problemas de los controles de seguridad para las cargas de trabajo de computación.
- 3.3 Diseñe y solucione los problemas de los controles de seguridad de la red.
- 5.1 Diseñe e implemente controles para los datos en tránsito.

El enunciado de la tarea 5.2 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 4.2 Diseñe, implemente y solucione los problemas de las estrategias de autorización.
- 5.2 Diseñe e implemente controles para los datos en reposo.

El enunciado de la tarea 5.3 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 5.2 Diseñe e implemente controles para los datos en reposo.

El enunciado de la tarea 5.4 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 5.2 Diseñe e implemente controles para los datos en reposo.
- 5.3 Diseñe e implemente controles para proteger datos confidenciales, credenciales, secretos y materiales de claves criptográficas.

El enunciado de la tarea 6.1 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 4.2 Diseñe, implemente y solucione los problemas de las estrategias de autorización.
- 6.1 Desarrolle una estrategia para implementar y administrar las cuentas de AWS de forma centralizada.

El enunciado de la tarea 6.2 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 6.2 Implemente una estrategia de implementación segura y coherente para los recursos en la nube.

El enunciado de la tarea 6.3 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 1.1 Diseñe e implemente la supervisión y las alertas para una cuenta u organización de AWS.
- 5.2 Diseñe e implemente controles para los datos en reposo.
- 6.3 Evalúe el cumplimiento de los recursos de AWS.

El enunciado de la tarea 6.4 de SCS-C02 se asigna a las siguientes tareas en SCS-C03:

- 2.1 Diseñe y pruebe un plan de respuesta ante incidentes.
- 1.1 Diseñe e implemente la supervisión y las alertas para una cuenta u organización de AWS.
- 6.3 Evalúe el cumplimiento de los recursos de AWS.

Encuesta

¿Qué tan útil fue esta guía de examen? Complete nuestra encuesta para informarnos.