



# CERTIFIED INFORMATION SYSTEMS AUDITOR®

Guía del candidato para el Examen  
y la Certificación CISA® 2012

## Exámenes CISA 2012— Información importante sobre fechas

### Fecha del examen—9 de junio de 2012

Plazo de inscripción temprana: 8 de febrero de 2012

Plazo de inscripción final: 4 de abril de 2012

**Modificación de inscripciones para el examen:** Entre el 14 y el 20 de abril, se aplica un cargo de US \$50 y no se aceptan cambios después del 20 de abril de 2012

**Reembolsos:** Hasta el 13 de abril de 2012, se aplica un cargo de procesamiento de US \$100 y no se procesan reembolsos después de esa fecha

**Aplazamientos:** Para las solicitudes recibidas el o antes del 20 de abril de 2012 se aplica un cargo de procesamiento de US \$50. Para las solicitudes recibidas del 21 de abril al 24 de mayo de 2012, se aplica un cargo de procesamiento de US \$100. Después del 24 de mayo de 2012, no se permiten aplazamientos.

### Fecha del examen—8 de diciembre de 2012

Plazo de inscripción temprana: 15 de agosto de 2012

Plazo de inscripción final: 3 de octubre de 2012

**Modificación de inscripciones para el examen:** Entre el 6 y el 12 de octubre, se aplica un cargo de US \$50 y no se aceptan cambios después del 12 de octubre de 2012

**Reembolsos:** Hasta el 5 de octubre de 2012, se aplica un cargo de procesamiento de US \$100 y no se procesan reembolsos después de esa fecha

**Aplazamientos:** Para las solicitudes recibidas el o antes del 12 de octubre de 2012 se aplica un cargo de procesamiento de US \$50. Para las solicitudes recibidas del 13 de octubre al 21 de noviembre de 2012 se aplica un cargo de procesamiento de US \$100. Después del 21 de noviembre de 2012, no se permiten aplazamientos.

Todos los plazos vencen a las 5 p.m. de Chicago, Illinois, EE.UU. (hora del centro de los EE.UU.).

*Guía del candidato para el Examen y la Certificación CISA® 2012*  
Impreso en los Estados Unidos de América.

## Tabla de Contenido

Generalidades .....	3
Acreditación del programa CISA renovada	
Bajo ISO/IEC 17024:2003 .....	3
El examen CISA .....	3
Preparación para el examen CISA .....	3
Administración del examen CISA .....	4
Calificación del examen CISA .....	6
Tipos de preguntas en el examen CISA .....	6
Solicitud de Certificación CISA .....	6
Requisitos para obtener la certificación inicial CISA .....	7
Requisitos para mantener la certificación CISA .....	7
Código de Ética Profesional de ISACA .....	7
Revocación de la certificación CISA .....	7
Enunciados de tareas y conocimientos del CISA .....	8

### Acerca de ISACA®

Con más de 95,000 miembros en 160 países, ISACA ([www.isaca.org](http://www.isaca.org)) es un líder mundialmente reconocido, proveedor de conocimiento, certificaciones, comunidad, asesoramiento y educación en seguridad y aseguramiento de sistemas de información (SI), gobierno empresarial, gestión de TI así como riesgos y cumplimiento relacionados con TI. Fundada en 1969, ISACA es una organización no lucrativa e independiente que organiza conferencias internacionales, publica el *ISACA® Journal* y desarrolla estándares internacionales de auditoría y control de sistemas de información que ayudan a sus miembros a garantizar la confianza y el valor de los sistemas de información. También promueve y certifica las habilidades y los conocimientos de TI a través de las mundialmente reconocidas designaciones Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) y Certified in Risk and Information Systems Control™ (CRISC™). ISACA actualiza continuamente COBIT®, lo que ayuda a los profesionales y líderes empresariales a cumplir con sus responsabilidades de gobierno y gestión de TI, particularmente en las áreas de aseguramiento, seguridad, riesgos y control, y aportar valor al negocio.

### Cláusula de exención de responsabilidad

ISACA y el Comité de certificación CISA han diseñado *la Guía del candidato para el Examen y la Certificación CISA® 2012* como guía para quienes aspiran a la certificación CISA. No se establece ninguna afirmación ni garantía por parte de ISACA en relación con estas u otras publicaciones que asegure de ninguna forma que los candidatos aprobarán el examen CISA.

### Reservación de derechos

Copyright © 2011 ISACA. Se prohíbe la reproducción o el almacenamiento en cualquier formato por cualquier razón sin previa autorización de ISACA. No se otorga otra clase de derechos ni permisos en relación con este trabajo. Todos los derechos reservados.

### ISACA

3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 EE.UU.  
Teléfono: +1.847.253.1545  
Fax: +1.847.253.1443  
Correo electrónico: [exam@isaca.org](mailto:exam@isaca.org)  
Página Internet: [www.isaca.org](http://www.isaca.org)

# Guía del candidato para el Examen y la Certificación CISA®

## Generalidades

El símbolo de excelencia de un programa de certificación profesional es el valor y el reconocimiento que concede al individuo que lo obtiene. Desde 1978, el programa Certified Information Systems Auditor (CISA), patrocinado por ISACA, ha sido el estándar de éxito aceptado en todo el mundo entre los profesionales de auditorías, control y seguridad de sistemas de información.

Las destrezas y prácticas técnicas que promueve y evalúa CISA son los pilares del éxito en este campo. Poseer la designación CISA demuestra competencia y es la base de medición en la profesión. Con una demanda creciente de profesionales con destrezas en auditorías, control y seguridad de sistemas de información, CISA se ha convertido en el programa de certificación preferido por individuos y organizaciones en todo el mundo. La certificación CISA significa comprometerse a servir a una organización y la profesión elegida con distinción.

## Acreditación del programa CISA renovada bajo ISO/IEC 17024:2003

El Instituto Nacional de Normalización Estadounidense (ANSI, por sus siglas en inglés) ha acreditado la certificación CISA bajo norma ISO/IEC 17024:2003, Requisitos Generales para los Organismos que Operan Sistemas de Certificación de Personal. ANSI, una organización privada sin fines de lucro que acredita a otras organizaciones para que sirvan como certificadores de productos, sistemas y personal de terceros.

ISO/IEC 17024 especifica los requisitos a cumplir por las organizaciones que certifican a individuos en cuanto a requerimientos específicos. Según ANSI, de ISO/IEC 17024 “se espera que desempeñe un papel vital a la hora de facilitar una estandarización global de la comunidad de certificación, aumentar la movilidad entre países y mejorar la seguridad pública y proteger a los consumidores”.



Programa acreditado por ANSI  
CERTIFICACIÓN DE PERSONAL  
#0694  
ISO/IEC 17024

La acreditación de ANSI:

- Promueve la pericia y las calificaciones exclusivas de las certificaciones que provee ISACA
- Protege la integridad de las certificaciones y brinda defensa legal
- Mejora la confianza del consumidor y del público en cuanto a las certificaciones y las personas que las poseen
- Facilita la movilidad a través de fronteras o entre industrias

La acreditación de ANSI significa que los procedimientos de ISACA cumplen con los requisitos esenciales de ANSI en cuanto a transparencia, equilibrio, consenso y debido proceso. Con esta acreditación, ISACA espera que continúen presentándose oportunidades significativas para los CISA en todo el mundo.

## El examen CISA

### Desarrollo/Descripción del Examen CISA

El Comité de certificación CISA supervisa el desarrollo del examen y garantiza la vigencia del contenido. Las preguntas del examen CISA se desarrollan a través de un proceso exhaustivo diseñado para consolidar la calidad final del examen. El proceso incluye un Subcomité de mejora de exámenes (TES) que trabaja con los redactores de los ítems para desarrollar y revisar las preguntas antes de enviarlas al Comité de certificación CISA para su revisión.

La práctica laboral sirve de base para el examen y para los requisitos de experiencia para obtener la certificación CISA. Esta práctica laboral se actualiza periódicamente y consta de cinco áreas de contenido (dominios). Los dominios y los enunciados de tareas y de conocimiento que los acompañan fueron el resultado de investigaciones y discusiones extensas por parte de expertos de todo el mundo en el área.

Los enunciados de tareas y conocimientos representan las tareas realizadas por los CISA y el conocimiento requerido para realizar estas tareas. Los candidatos al examen se evaluarán de acuerdo a su conocimiento práctico asociado a la realización de estas tareas.

El análisis actualizado de prácticas de trabajo vigente contiene los siguientes dominios y porcentajes:

- **Proceso de auditoría de sistemas de información (14%)**
- **Gobierno y gestión de TI (14%)**
- **Adquisición, desarrollo e implementación de sistemas de información (19%)**
- **Operaciones, mantenimiento y soporte de sistemas de información (23%)**
- **Protección de los activos de información (30%)**

**Nota:** Los porcentajes que aparecen en los dominios indican el énfasis o porcentaje de preguntas que aparecerán en el examen en cada dominio. Para obtener una descripción de los enunciados de tareas y conocimientos de cada dominio, consulte las páginas 8-11.

El examen consta de 200 preguntas de selección múltiple y se administra dos veces al año; en junio y diciembre, durante una sesión de cuatro horas. Los candidatos pueden elegir presentar el examen en uno de varios idiomas. Si desea una lista actualizada de idiomas, visite [www.isaca.org/cisaterminology](http://www.isaca.org/cisaterminology).

## Preparación para el examen CISA

Se puede lograr la aprobación del examen CISA mediante un plan de estudios organizado. A fin de brindar apoyo a las personas con el desarrollo de un plan de estudio exitoso, ISACA ofrece guías de estudio y cursos de repaso para los candidatos al examen. Vaya a [www.isaca.org/cisaguide](http://www.isaca.org/cisaguide) para conocer las guías de estudio de ISACA que pueden ayudarlo en su preparación para el examen. Envíe su orden con anticipación, ya que el tiempo de entrega puede ser de una a cuatro semanas dependiendo de la ubicación geográfica y las prácticas aduaneras. Para información actualizada sobre envíos, refiérase a [www.isaca.org/shipping](http://www.isaca.org/shipping).

# Guía del candidato para el Examen y la Certificación CISA®



ISACA también ofrece el Curso de Repaso en línea CISA®. El curso incluye ejercicios interactivos, casos de estudio, herramientas de repaso y preguntas de práctica. Visite [www.isaca.org/elearning](http://www.isaca.org/elearning) para obtener más información y una vista preliminar del curso.

En el *Manual de preparación al examen CISA 2012* se ofrece una lista completa de referencias recomendadas para el estudio.

Puede encontrar una lista de los acrónimos que los candidatos deberían conocer y una lista adicional de acrónimos que pudiera ser de interés para los candidatos en [www.isaca.org/cisaguide](http://www.isaca.org/cisaguide).

Para ayudar a los candidatos con la terminología técnica, se ha confeccionado una lista de los términos técnicos más frecuentemente utilizados en inglés junto con su traducción en otros idiomas, disponible en el sitio web de ISACA en [www.isaca.org/cisaguide](http://www.isaca.org/cisaguide).

ISACA posee un glosario de términos, así como glosarios específicos de cada certificación. Estos glosarios están disponibles en [www.isaca.org/glossary](http://www.isaca.org/glossary).

*No se establece ninguna afirmación ni garantía por parte de ISACA ni la Junta de Certificación CISA en relación con estas u otras publicaciones o cursos que asegure de alguna forma que los candidatos aprobarán el examen.*

## Administración del examen CISA

ISACA utiliza una agencia examinadora profesional reconocida internacionalmente para que ayude en la construcción, administración y calificación del examen CISA.

Los candidatos que deseen hacer comentarios sobre las condiciones de administración de las pruebas pueden hacerlo al concluir la sesión de la prueba llenando el "Cuestionario de administración de pruebas". El Cuestionario de administración de pruebas se presenta al final del cuadernillo del examen, y sus respuestas al cuestionario se deben ingresar en las casillas P a S de la sección Códigos especiales (Esquema No. 4) al frente de su Hoja de respuestas.

Los candidatos que deseen expresar comentarios o inquietudes adicionales sobre la administración de exámenes, incluyendo las condiciones del sitio o el contenido del examen, deben comunicarse con la sede internacional de ISACA por correo postal o electrónico ([exam@isaca.org](mailto:exam@isaca.org)). Esos comentarios e inquietudes deben ser recibidos por ISACA en un plazo de 2 semanas después de la fecha del examen. En sus comentarios, incluya la siguiente información: Número de ID del examen, lugar de la prueba, fecha de la prueba y detalles relevantes sobre el tema en cuestión. Sólo serán considerados en el proceso de calificación del examen los comentarios recibidos por ISACA durante las 2 primeras semanas posteriores a la aplicación del examen.

### Boleto de admisión

Aproximadamente de dos a tres semanas antes de la fecha del examen CISA, se le enviará a los candidatos un boleto físico de admisión y un boleto electrónico por parte de ISACA. Los candidatos al examen pueden descargar una copia del boleto de admisión en la página [exam@isaca.org](http://exam@isaca.org) > MyISACA. Los boletos indicarán la fecha, hora de inscripción y la localización del examen, programa de eventos de ese día y una lista de los materiales que los candidatos deben llevar para tomar el examen CISA. Con la excepción de los cambios relacionados con la información de contacto, los candidatos no deben escribir nada en el boleto de admisión.

**Por favor, tenga en cuenta:** Para recibir un boleto de admisión, se deben pagar todos los cargos. Los boletos de admisión se envían en copia impresa y por correo electrónico a la dirección postal actual y a la dirección de correo electrónico que aparecen en el registro. Sólo se admitirán a examen los candidatos que tengan un boleto de admisión y un documento de identificación aceptable emitido por el Gobierno, y el nombre que aparece en el boleto de admisión deberá coincidir con el que aparece en dicho documento de identificación. La copia impresa del boleto de admisión o la copia impresa del boleto electrónico son válidas para ser admitido en el examen. Si la dirección de correo postal o la dirección de correo electrónico del candidato cambian, el candidato deberá actualizar su perfil en el sitio web de ISACA ([www.isaca.org](http://www.isaca.org)) o ponerse en contacto con [exam@isaca.org](mailto:exam@isaca.org).

**Es imperativo que los candidatos anoten las fechas específicas de registro y del examen en su boleto de admisión. NO SE PERMITIRÁ A NINGUN CANDIDATO INGRESAR AL CENTRO DE PRUEBA UNA VEZ QUE EL JEFE EXAMINADOR HAYA COMENZADO A DAR LAS INSTRUCCIONES ORALES, APROXIMADAMENTE 30 MINUTOS ANTES QUE COMIENZE EL EXAMEN.** No se permitirá tomar el examen a ningún candidato que llegue después del comienzo de la lectura de las instrucciones, y perderá el valor de su inscripción. Un boleto de admisión sólo se puede utilizar en el centro de prueba designado en el boleto de admisión. Los documentos de identificación se verificarán durante la administración del examen.

### Arreglos especiales

Al solicitarlo, ISACA hará los arreglos que sean razonables en sus procedimientos de examen para los candidatos con incapacidades documentadas o compromisos religiosos. Estos candidatos pueden solicitar que se consideren las modificaciones que sean razonables en el formato, presentación, comida y bebida en el lugar del examen, u horario de examen. Los pedidos de comida o bebida en el lugar del examen deben estar acompañados por una nota de un médico, de lo contrario, **no se permiten ni comida ni bebidas en ninguno de los lugares de examen.** Las solicitudes de consideraciones especiales se deben enviar a la Oficina central internacional de ISACA por escrito, junto con los documentos apropiados, antes del 4 de abril de 2012 para el examen de junio de 2012, y antes del 3 de octubre de 2012, para el examen de diciembre de 2012.

### Sea puntual

La inscripción empezará a la hora indicada en el boleto de admisión en cada centro. Todos los candidatos tienen que estar registrados y encontrarse dentro de la sala de examen cuando el examinador principal comience a leer las instrucciones en voz alta. **NO SE ADMITIRÁ A NINGÚN CANDIDATO EN EL CENTRO DE PRUEBA DESPUÉS DE QUE EL JEFE EXAMINADOR HAYA COMENZADO A DAR LAS INSTRUCCIONES ORALES, APROXIMADAMENTE 30 MINUTOS ANTES DE QUE COMIENZE EL EXAMEN.**

**Recuerde traer el Boleto de admisión**

# Guía del candidato para el Examen y la Certificación CISA®

Los candidatos pueden utilizar su boleto de admisión (bien sea su boleto electrónico o físico) sólo en el centro de prueba designado. Los candidatos serán admitidos al centro de prueba solamente si tienen un boleto de admisión válido y una forma aceptable de identificación. La forma de identificación aceptable debe estar actualizada y debe ser un certificado original emitido por el gobierno que contenga el nombre del candidato, como aparece en el boleto de admisión, y la fotografía del candidato. La información del documento de identidad no puede estar escrita a mano. Todas estas características deben ser demostradas por una única prueba de identificación suministrada. Los ejemplos incluyen, pero no se limitan a, un pasaporte, una licencia de conducir, una identificación militar, una identificación estatal, una tarjeta de inmigración y un documento de identificación nacional. El candidato que no provea una forma de identificación aceptable no podrá tomar el examen y perderá el valor de su inscripción.

## Lea las Reglas del Centro de prueba

- No se permite a los candidatos ingresar al centro de prueba después de que se haya comenzado a dar las instrucciones orales.
- Los candidatos deben tener varios lápices No. 2 o HB (mina blanda) con punta y un buen borrador. No habrá lápices ni borradores disponibles en el centro de prueba. Debido a que los lugares de celebración del examen varían, se harán todos los esfuerzos posibles para tener un control confortable del clima en cada lugar del examen. Es conveniente que los candidatos vistan como se sientan más cómodos.
- No se permite a los candidatos traer a la sala de examen material de referencia, hojas en blanco, libretas ni diccionarios de idiomas.
- No se permite a los candidatos ingresar con calculadoras ni utilizarlas en el centro de prueba.
- No se permite que los candidatos traigan ningún tipo de dispositivo de comunicaciones (por ejemplo teléfonos celulares, PDAs, Blackberries) al centro de prueba. **Si se detecta que los candidatos al examen tienen un dispositivo de este tipo durante la administración del examen, sus exámenes se invalidarán y se les solicitará que abandonen de inmediato la sala de examen.**
- No se permiten visitantes en el centro de prueba.
- No se permite el consumo de comida ni bebidas en la sala de examen (sin la autorización previa de ISACA).

## Faltas de conducta

Se descalificará como candidatos, y podrán tomarse acciones legales contra ellos, a quienes se descubra involucrados en algún tipo de conducta no aceptable, tal como proporcionar o recibir ayuda; utilizar notas, papeles u otro tipo de ayuda; intentar tomar el examen en lugar de otra persona; utilizar cualquier tipo de dispositivo de comunicación, incluyendo teléfonos móviles, durante la administración del examen; o llevándose el folleto de examen, hoja de respuestas o notas fuera de la sala de examen. Los candidatos que salgan de la sala de examen sin autorización o sin ir acompañados de un supervisor no podrán volver a la sala de examen y serán objeto de descalificación. La agencia que administra las pruebas informará sobre tales irregularidades al Comité de Certificación CISA de ISACA.

La Política de Pertenencias Personales completa está disponible en [www.isaca.org/cisabelongings](http://www.isaca.org/cisabelongings). Ni ISACA ni el proveedor de la prueba son responsables de las pertenencias personales de los candidatos.

## Llene la Hoja de respuestas con mucho cuidado

- Antes de que los candidatos comiencen el examen, el jefe examinador del centro de prueba leerá en voz alta las instrucciones sobre cómo ingresar la información de identificación en la hoja de respuestas. El número de identificación del candidato, como aparece en el boleto de admisión, y el resto de la información requerida se deben ingresar apropiadamente, de lo contrario es posible que las calificaciones se retrasen o se reporten incorrectamente.
- Existe un supervisor que habla el idioma primario utilizado en cada centro de prueba. Si un candidato desea presentar el examen en otro idioma que no sea el del centro de prueba, el supervisor pudiera no comunicarse en la lengua elegida. Sin embargo, habrá instrucciones escritas en el idioma del examen.
- Se instruye a los candidatos para que lean todas las instrucciones cuidadosamente antes de intentar responder a las preguntas. Los candidatos que omitan las instrucciones o las lean rápidamente pudieran perder información importante y posiblemente perder crédito.
- Se debe marcar las respuestas en el círculo apropiado en la hoja de respuestas. Los candidatos deben asegurarse de no marcar más de una respuesta por pregunta y de que respondan a las preguntas en la fila de respuestas apropiada. Si es necesario cambiar una respuesta, el candidato tiene que borrar la respuesta incorrecta completamente antes de marcar una nueva.
- Se debe responder a todas las preguntas. **No se penalizan las respuestas incorrectas. Las calificaciones se basan únicamente en el número de preguntas respondidas correctamente, por lo que se debe responder a todas las preguntas.**
- Después de terminar, los candidatos deben entregar sus hojas de respuestas y el cuadernillo de la prueba.

## Administre el tiempo

- El examen, con una duración de cuatro horas, permite detenerse en cada pregunta por más de un minuto. Se aconseja a los candidatos mantener un mismo ritmo durante todo el examen. Los candidatos deben responder un promedio de 50 preguntas por hora.
- Se recomienda a los candidatos colocar inmediatamente sus respuestas en la hoja de respuestas. **No se otorgará tiempo adicional para transferir o registrar respuestas una vez concluido el tiempo del examen, en caso de que el candidato marque las respuestas en el cuadernillo de la prueba.**

## Mantenga una conducta apropiada

- Para proteger la seguridad del examen y mantener la validez de las calificaciones, se pide a los candidatos firmar la hoja de respuestas.
- El Comité de Certificación CISA se reserva el derecho de descalificar a cualquier candidato que sea descubierto en cualquier tipo de conducta inapropiada o violación de las reglas del examen, como recibir o dar ayuda; utilizar notas, papeles u otro tipo de ayuda; intentar resolver el examen de otro candidato; o sacar materiales o notas del examen fuera de la sala de examen. La agencia examinadora proporcionará al Comité de Certificación CISA los registros correspondientes a tales irregularidades para su revisión y tomar una decisión.

## Razones para la expulsión o descalificación

- Admisión desautorizada al centro de prueba.

# Guía del candidato para el Examen y la Certificación CISA®

- El candidato perturba o da o recibe ayuda.
- El candidato intentar sacar materiales o notas de la prueba fuera del centro de prueba.
- El candidato suplanta a otro candidato.
- El candidato ingresa elementos no permitidos al centro de prueba.
- Posesión por parte del candidato de cualquier dispositivo de comunicación (es decir, teléfono móvil, PDA, BlackBerry®) durante la administración del examen
- Salida no autorizada del candidato de la sala de examen.

**Si un candidato es observado con un dispositivo de comunicación (es decir, teléfono móvil, PDA, BlackBerry®) durante la administración del examen, su examen se invalidará y se le solicitará que abandone de inmediato la sala de examen.**

## Calificación del examen CISA

El examen CISA consta de 200 preguntas de selección múltiple. Las calificaciones del candidato se reportan como calificaciones escaladas. La calificación escalada es la conversión de la calificación bruta del candidato en un examen a una escala común. ISACA utiliza y reporta las calificaciones en una escala común de 200 a 800. Por ejemplo, una calificación de 800 en esta escala representa una puntuación perfecta, ya que se respondieron todas las preguntas correctamente; una calificación de 200 en esta escala constituye la clasificación más baja posible y significa que sólo se respondió correctamente un número muy bajo de respuestas. Un candidato deberá recibir una calificación de 450 o mayor para aprobar el examen. Una calificación de 450 representa una norma consistente mínima de conocimiento de acuerdo a lo establecido por el Comité de Certificación CISA de ISACA. El candidato que recibe una calificación aprobatoria, puede entonces solicitar certificación si cumple con el resto de los requisitos.

El examen CISA contiene algunas preguntas que se incluyen solamente con propósitos de investigación y análisis. Estas preguntas no están identificadas ni separadas, tampoco se utilizan para calcular la calificación final de los candidatos.

**Aproximadamente ocho semanas después de la fecha del examen, los resultados oficiales del examen se enviarán por correo a los candidatos.**

Además, con el consentimiento del candidato durante el proceso de registro, se enviará al candidato un mensaje de correo electrónico con el estado de aprobación/reprobación y la calificación del candidato. Esta notificación por correo electrónico se enviará solamente a la dirección especificada en el perfil del candidato al momento de la divulgación inicial de los resultados. Para garantizar la confidencialidad de las calificaciones, los resultados del examen no se informarán por teléfono ni fax. Para evitar que la notificación por correo electrónico sea enviada a las carpetas de correo no solicitado (spam), los candidatos deberán agregar *exam@isaca.org* a su directorio de direcciones, lista de direcciones aprobadas o lista de remitentes seguros.

Los candidatos recibirán un informe de calificaciones que contiene una calificación para cada área de dominio. Los candidatos que tuvieron éxito recibirán, junto con un informe de calificaciones, detalles sobre cómo solicita la certificación CISA.

Las diferentes calificaciones pueden ser útiles para identificar las áreas en las que el candidato reprobado puede necesitar más preparación antes de volver a tomar el examen. Los candidatos reprobados deben tener en cuenta que la calificación total escalada no se puede determinar al calcular un promedio simple o ponderado de las diferentes calificaciones.

Los candidatos que obtengan una calificación reprobatoria en el examen pueden solicitar la calificación manual de sus hojas de respuestas. Este procedimiento garantiza que la calificación computarizada no haya sido alterada por posibles marcas imprecisas, respuestas múltiples u otras condiciones. Sin embargo, los candidatos deben entender que todas las calificaciones son sometidas a varias verificaciones de control de calidad antes de su divulgación; por lo tanto, lo más probable es que las revisiones manuales no produzcan ningún cambio en la calificación. Las solicitudes de calificación manual se deben presentar por escrito al departamento de certificación dentro de los 90 días siguientes a la divulgación de los resultados del examen. Las solicitudes de calificación manual presentadas después de ese plazo no serán procesadas. Todas las solicitudes deben incluir el nombre del candidato, el número de identificación del examen y la dirección de correo. Cada solicitud debe ir acompañada por un pago de US \$75.

## Tipos de preguntas en el examen CISA

Las preguntas del examen CISA se desarrollan con el fin de medir y evaluar conocimiento práctico y la aplicación de normas y conceptos generales. Todas las preguntas se diseñaron de modo que tengan una mejor respuesta.

Todas las preguntas del examen CISA tienen el formato de planteamiento de un problema (pregunta) y cuatro opciones (opciones de respuesta). Se pide al candidato que elija la respuesta correcta o la mejor respuesta entre las opciones. El problema se puede formular como una pregunta o como un enunciado incompleto. En algunas situaciones, pudiera incluirse un escenario. Estas preguntas normalmente incluyen la descripción de una situación y requieren que el candidato responda dos o más preguntas basándose en la información suministrada. Se recuerda al candidato que debe leer cada pregunta cuidadosamente. Algunas preguntas del examen CISA pudieran requerir que el candidato elija la respuesta apropiada con base en un calificativo, como **MÁS** probable o **EL MEJOR**. En cada caso, el candidato debe leer la pregunta cuidadosamente, eliminar las respuestas que sean claramente incorrectas y luego hacer la mejor elección posible. Están disponibles modelos del examen CISA en [www.isaca.org/cisaassessment](http://www.isaca.org/cisaassessment).

# Guía del candidato para el Examen y la Certificación CISA®

## Solicitud para la Certificación CISA

La aprobación del examen no significa que el candidato sea un CISA. Una vez que el candidato aprueba el examen CISA, el/ella tiene cinco años a partir de la fecha del examen para solicitar la certificación. Los candidatos aprobados deben completar la solicitud de certificación y someter a verificación su experiencia laboral utilizando los formularios apropiados incluidos en la solicitud. **Los candidatos no obtienen la certificación, ni pueden utilizar la designación CISA, hasta que no se haya recibido y aprobado la solicitud completa.** Tenga en cuenta que las decisiones sobre las solicitudes no son definitivas, ya que existe un proceso de apelación para el rechazo de las solicitudes de certificación. Las preguntas relativas al rechazo de la certificación se pueden enviar a [certification@isaca.org](mailto:certification@isaca.org). Una vez recibida la certificación, el nuevo CISA recibirá un certificado y un NIP de certificación de CISA. Al momento de la solicitud, los individuos deben manifestar que están de acuerdo con que ISACA se reserve el derecho, sin estar obligado, a publicar o divulgar de cualquier modo el estado de sus CISA. Cada solicitud para la certificación CISA debe ir acompañada por un pago de \$50 dólares en concepto de cuota de tramitación.

## Requisitos para obtener la certificación inicial CISA

En principio, la certificación se otorga a aquellos individuos que hayan completado de manera satisfactoria el examen CISA y cumplan con los siguientes requisitos de experiencia laboral.

Para obtener la certificación, se requiere un período mínimo de cinco años de experiencia laboral profesional en auditoría, control, aseguramiento o seguridad de SI. Se puede obtener sustituciones o excepciones a la experiencia de la siguiente manera:

- Un máximo de un año en sistemas de información o un año de experiencia en auditoría no relacionada con SI puede sustituir un año de experiencia.
- Se puede sustituir de 60 a 120 horas completas de crédito universitario semestral (el equivalente a un título universitario de dos o cuatro años), no limitado por la restricción de 10 años detallada posteriormente, por uno o dos años, respectivamente, de experiencia. Incluso si se han obtenido múltiples títulos, sólo se puede cambiar por un máximo de dos años.
- Se puede sustituir un título de licenciatura o master de una universidad que apoye el Currículum Modelo patrocinado por ISACA por un año de experiencia. Para ver una lista de estas escuelas, por favor dirigirse a [www.isaca.org/modeluniversities](http://www.isaca.org/modeluniversities). No se puede usar esta opción si ya se han reclamado tres años de sustitución de experiencia y excepción educativa.
- Un título de master en seguridad de información o tecnología de la información de una universidad reconocida se puede sustituir por un año de experiencia.

Excepción: Se pueden sustituir dos años de experiencia como instructor universitario de tiempo completo en un campo relacionado (por ejemplo: ciencias de la computación, contabilidad, o auditoría de sistemas de información) por cada año de experiencia.

La experiencia se debe haber obtenido dentro del período de 10 años que precede a la fecha de solicitud de certificación CISA o dentro de los cinco años posteriores a la fecha de haber aprobado el examen inicialmente. Si no se envía una solicitud completa para la certificación CISA dentro de los cinco años posteriores a la fecha de aprobación del examen, será necesario volver a tomar y aprobar el examen.

Es importante resaltar que muchas personas deciden tomar el examen CISA antes de cumplir con los requisitos de experiencia. Esta práctica es aceptable y recomendada, aunque la designación CISA no se concederá hasta que se haya cumplido con todos los requisitos.

## Requisitos para mantener la certificación CISA

Los CISA deben cumplir con los siguientes requisitos para mantener su certificación:

- Acumular y reportar un mínimo de 20 horas anuales de formación profesional continua (CPE, Continuing Professional Education), y acumular y reportar un mínimo de 120 horas CPE para un período de notificación de tres años. Para obtener más detalles vea la política CPE de CISA en [www.isaca.org/cisacpepolicy](http://www.isaca.org/cisacpepolicy).
- Entregar la totalidad de las cuotas anuales de mantenimiento de CPE a ISACA International Headquarters.
- Responder y entregar la documentación requerida de actividades de CPE como respaldo de las horas reportadas si fue seleccionado para una auditoría anual.
- Cumplir con el Código de Ética Profesional de ISACA.

**El incumplimiento de estos requisitos generales ocasionará la revocación de la designación CISA de la persona. Todos los certificados son propiedad de ISACA. Si una persona ha sido aprobada para la certificación y posteriormente ésta es revocada, dicha persona debe destruir el certificado.**

## Código de Ética Profesional de ISACA

ISACA establece un Código de Ética Profesional para guiar la conducta profesional y personal de los miembros de la asociación y/o de los poseedores de la certificación. El incumplimiento de este Código de Ética Profesional puede acarrear una investigación de la conducta de un miembro y/o titular de la certificación y, en última instancia, medidas disciplinarias. El Código de Ética Profesional de ISACA puede consultarse en línea en [www.isaca.org/ethics](http://www.isaca.org/ethics).

## Revocación de la certificación CISA

El Comité de certificación CISA puede, a su juicio y después de la debida consideración exhaustiva, revocar la certificación CISA de una persona por cualquiera de las siguientes razones:

- Incumplimiento de la norma de CPE de CISA
- Quebrantamiento de cualquier disposición del Código de Ética Profesional de ISACA
- Falsificación o retención deliberada de información relevante
- Distorsión intencional de un hecho importante
- Tener o ayudar a otras personas a tener un comportamiento deshonesto, no autorizado o inapropiado en cualquier momento en relación con un examen CISA o con el proceso de certificación

# Guía del candidato para el Examen y la Certificación CISA®

## Descripción de las áreas de práctica laboral del CISA Enunciados de tareas y conocimientos del CISA

<b>ÁREA DE CONTENIDO (Dominio)</b>
<b>Dominio 1 Proceso de auditoría de sistemas de información</b> —Proporcionar servicios de auditoría de acuerdo con los estándares de auditoría de TI para ayudar a la organización a proteger y controlar los sistemas de información.
<b>Dominio 1 Enunciado de tarea</b>
T1.1 Desarrollar e implementar una estrategia de auditoría de TI basada en riesgos de conformidad con los estándares de auditoría de TI para garantizar que se han incluido las áreas clave.
T1.2 Planificar auditorías específicas para determinar si los sistemas de información están protegidos y controlados, y si proporcionan valor a la organización.
T1.3 Realizar auditorías de conformidad con los estándares de auditoría de TI para lograr los objetivos de auditoría planificados.
T1.4 Reportar los hallazgos de auditoría y hacer recomendaciones a las partes interesadas clave para comunicar los resultados y efectuar cambios cuando sea necesario.
T1.5 Realizar seguimientos o preparar informes de estado para garantizar que la Gerencia ha llevado a cabo las acciones apropiadas de forma oportuna.
<b>Dominio 1 Conocimientos Relacionados</b>
KS1.1 Conocimiento de estándares, directrices, y herramientas y técnicas de aseguramiento y auditoría de TI de ISACA; código de ética profesional; y otros estándares aplicables
KS1.2 Conocimiento de los conceptos de valoración de riesgos, las herramientas y las técnicas en un contexto de auditoría
KS1.3 Conocimiento de los objetivos de control y los controles relacionados con los sistemas de información
KS1.4 Conocimiento de técnicas de planificación de la auditoría y de gestión de proyectos de auditoría, incluido el seguimiento
KS1.5 Conocimiento de procesos del negocio fundamentales (por ejemplo, compras, nómina, cuentas por pagar, cuentas por cobrar), incluyendo TI relevante
KS1.6 Conocimiento de las leyes y regulaciones aplicables que afectan al alcance, a la recopilación y el mantenimiento de evidencias, y a la frecuencia de las auditorías
KS1.7 Conocimiento de técnicas de recopilación de evidencia (por ejemplo, observación, consulta, inspección, entrevista, análisis de datos) usadas para reunir, proteger y mantener las evidencias de auditoría
KS1.8 Conocimiento de distintas metodologías de muestreo
KS1.9 Conocimiento de técnicas de reporte y comunicación (por ejemplo, facilitación, negociación, resolución de conflictos y estructura de informes de auditoría)
KS1.10 Conocimiento de sistemas y marcos de aseguramiento de la calidad de la auditoría
<b>Dominio 2 Gobierno y gestión de TI</b> —Garantizar la operatividad de las estructuras organizativas y de liderazgo necesarias para conseguir los objetivos y apoyar la estrategias de la organización.
<b>Dominio 2 Enunciado de tarea</b>
T2.1 Evaluar la efectividad de la estructura de gobierno de TI para determinar si las decisiones, las direcciones y el desempeño de TI respaldan las estrategias y los objetivos de la organización.
T2.2 Evaluar la estructura organizativa de TI y la gestión de recursos humanos (personal) para determinar si respaldan las estrategias y los objetivos de la organización.
T2.3 Evaluar la estrategia de TI, incluyendo la dirección de TI, y los procesos para el desarrollo, la aprobación, la implementación y el mantenimiento de la estrategia para que esté alineada con las estrategias y los objetivos de la organización.
T2.4 Evaluar las políticas, los estándares y los procedimientos de TI de la organización y los procesos para su desarrollo, aprobación, implementación, mantenimiento y monitoreo a fin de determinar si respaldan la estrategia de TI y cumplen con los requerimientos legales y regulatorios.
T2.5 Evaluar la adecuación del sistema de gestión de la calidad para determinar si respalda las estrategias y los objetivos de la organización de forma rentable.
T2.6 Evaluar la gestión de TI y el monitoreo de controles (por ejemplo, monitoreo continuo, aseguramiento de la calidad [QA]) para determinar si cumplen con las políticas, los estándares y los procedimientos de la organización.
T2.7 Evaluar las prácticas de inversión, uso y asignación de recursos de TI, incluyendo criterios de priorización, para determinar si están alineados con las estrategias y los objetivos de la organización.
T2.8 Evaluar las estrategias y las políticas de contratación de TI y las prácticas de gestión de contratos para determinar si respaldan las estrategias y los objetivos de la organización.
T2.9 Evaluar las prácticas de gestión de riesgos para determinar si los riesgos de la organización relacionados con TI se gestionan adecuadamente.
T2.10 Evaluar las prácticas de monitoreo y aseguramiento para determinar si el consejo de dirección y la alta dirección reciben información suficiente y oportuna sobre el desempeño de TI.
T2.11 Evaluar el plan de continuidad del negocio de la organización para determinar la capacidad de la organización de continuar con las operaciones del negocio esenciales durante el período de una interrupción de TI.

# Guía del candidato para el Examen y la Certificación CISA®

<b>ÁREA DE CONTENIDO (Dominio)</b>	
<b>Dominio 2 Conocimientos Relacionados</b>	
KS2.1	Conocimiento del gobierno, la gestión, la seguridad y los marcos de control de TI, así como los estándares, las directrices y las prácticas relacionados
KS2.2	Conocimiento del propósito de la estrategia, las políticas, los estándares y los procedimientos de TI para una organización y los elementos esenciales de cada uno de ellos
KS2.3	Conocimiento de la estructura organizacional, los roles y las responsabilidades relacionados con TI
KS2.4	Conocimiento de los procesos para el desarrollo, la implementación y el mantenimiento de la estrategia, las políticas, los estándares y los procedimientos de TI
KS2.5	Conocimiento de la dirección de la tecnología y la arquitectura de TI de la organización y sus implicaciones para establecer direcciones estratégicas a largo plazo
KS2.6	Conocimiento de leyes, regulaciones y estándares de la industria relevantes que afecten a la organización
KS2.7	Conocimiento de sistemas de gestión de la calidad
KS2.8	Conocimiento del uso de modelos de madurez
KS2.9	Conocimiento de las técnicas de optimización de procesos
KS2.10	Conocimiento de las prácticas de inversión y asignación de recursos de TI, incluyendo criterios de priorización (por ejemplo, gestión de portafolios, gestión del valor, gestión de proyectos)
KS2.11	Conocimiento de procesos de selección proveedores de TI, gestión de contratos, gestión de relaciones y monitoreo del desempeño, incluyendo relaciones de externalización (outsourcing) de terceros
KS2.12	Conocimiento de la gestión de riesgos de la empresa
KS2.13	Conocimiento de las prácticas para monitorear y reportar el desempeño de TI (por ejemplo, cuadros de mando (balanced scorecards), indicadores clave de desempeño [KPI]).
KS2.14	Conocimiento de las prácticas de gestión de recursos humanos (personal) de TI utilizadas para invocar el plan de continuidad del negocio
KS2.15	Conocimiento del análisis del impacto en el negocio (BIA) relacionado con el plan de continuidad del negocio (BCP)
KS2.16	Conocimiento de los estándares y procedimientos para el desarrollo y el mantenimiento del plan de continuidad del negocio (BCP) y métodos de prueba
<b>Dominio 3 Adquisición, desarrollo e implementación de sistemas de información—Garantizar que las prácticas para adquirir, desarrollar, probar e implementar los sistemas de información cumplan las estrategias y los objetivos de la organización.</b>	
<b>Dominio 3 Enunciado de tarea</b>	
T3.1	Evaluar el caso de negocio para las inversiones propuestas en la adquisición, el desarrollo, el mantenimiento o el requerimiento subsiguiente de sistemas de información para determinar si cumple los objetivos del negocio.
T3.2	Evaluar las prácticas y controles de gestión de proyectos para determinar si los requerimientos del negocio se logran de forma rentable a la vez que se gestionan los riesgos para la organización.
T3.3	Realizar revisiones para determinar si un proyecto está progresando de acuerdo con los planes del proyecto, está soportado de manera adecuada por documentación y el informe de avance es correcto.
T3.4	Evaluar los controles para sistemas de la información durante las fases de requerimiento, adquisición, desarrollo y pruebas para cumplir con las políticas, los estándares, los procedimientos y los requerimientos externos aplicables de la organización.
T3.5	Evaluar la preparación de los sistemas de información para su implementación y migración a producción para determinar si se cumplen los entregables del proyecto, controles y requerimientos de la organización.
T3.6	Realizar revisiones posteriores a la implementación de los sistemas para determinar si se cumplen los entregables del proyecto, controles y requerimientos de la información.
<b>Dominio 3 Conocimientos Relacionados</b>	
KS3.1	Conocimiento de los beneficios de las prácticas de realización (por ejemplo, estudios de viabilidad, casos de negocio, costo total de propiedad [TCO], ROI)
KS3.2	Conocimiento de los mecanismos de gobierno de proyectos (por ejemplo, comité de dirección, junta de supervisión de proyectos, oficina de gestión de proyectos)
KS3.3	Conocimiento de las prácticas, herramientas y marcos de control de la gestión de proyectos
KS3.4	Conocimiento de las prácticas de gestión de riesgos aplicadas a proyectos
KS3.5	Conocimiento de la arquitectura de TI en relación con los datos, las aplicaciones y la tecnología (por ejemplo, aplicaciones distribuidas, aplicaciones basadas en la web, servicios web, aplicaciones de n-capas)
KS3.6	Conocimiento de prácticas de adquisición (por ejemplo, evaluación de los proveedores, gestión de proveedores, depósito de fuentes [escrow])
KS3.7	Conocimiento de análisis de requerimientos y prácticas de gestión (por ejemplo, verificación de requerimientos, trazabilidad, análisis de brechas [gap analysis], gestión de vulnerabilidades, requerimientos de seguridad)
KS3.8	Conocimiento de los criterios de éxito y riesgos de un proyecto

# Guía del candidato para el Examen y la Certificación CISA®

<b>ÁREA DE CONTENIDO (Dominio)</b>	
<b><i>Dominio 3 Conocimientos Relacionados (continuación)</i></b>	
KS3.9	Conocimiento de los objetivos y técnicas de control que aseguran la completitud, precisión, validez y autorización de transacciones y datos
KS3.10	Conocimiento de las metodologías y herramientas de desarrollo de sistemas, incluidas sus fortalezas y debilidades (por ejemplo, prácticas de desarrollo ágil, desarrollo de prototipos, desarrollo rápido de aplicaciones [RAD] y técnicas de diseño orientado a objetos)
KS3.11	Conocimiento de metodologías y prácticas de pruebas relacionadas con el desarrollo de sistemas de información
KS3.12	Conocimiento de gestión de la configuración y de versiones en relación con el desarrollo de sistemas de información
KS3.13	Conocimiento de prácticas de migración de sistemas y despliegue de infraestructuras, así como de herramientas, técnicas y procedimientos de conversión de datos
KS3.14	Conocimiento de objetivos y prácticas de revisión posterior a implementación (por ejemplo, cierre de proyectos, implementación de controles, realización de beneficios, medición del desempeño)
<b>Dominio 4 Operaciones, mantenimiento y soporte de sistemas de información</b> —Garantizar que las operaciones, el mantenimiento y el soporte de los sistemas de información cumplan las estrategias y los objetivos de la organización.	
<b><i>Dominio 4 Enunciado de tarea</i></b>	
T4.1	Realizar revisiones periódicas de los sistemas de información para determinar si siguen cumpliendo los objetivos de la organización.
T4.2	Evaluar las prácticas de gestión de nivel de servicio para determinar si el nivel de servicio de los proveedores internos y externos está definido y gestionado.
T4.3	Evaluar las prácticas de gestión de terceros para determinar si el proveedor acata los niveles de control esperados por la organización.
T4.4	Evaluar las operaciones y los procedimientos de usuario final para determinar si los procesos programados y los no programados se gestionan hasta su finalización.
T4.5	Evaluar el proceso de mantenimiento de los sistemas de información para determinar si están controlados de forma efectiva y continúan soportando los objetivos de la organización.
T4.6	Evaluar las prácticas de administración de datos para determinar la integridad y optimización de las bases de datos.
T4.7	Evaluar el uso de herramientas y técnicas de monitoreo de desempeño y capacidad para determinar si los servicios de TI cumplen con los objetivos de la organización.
T4.8	Evaluar las prácticas de gestión de problemas e incidentes para determinar si los incidentes, problemas o errores son registrados, analizados y resueltos a su debido tiempo.
T4.9	Evaluar las prácticas de gestión de cambios, configuración y versiones para determinar si los cambios programados y los no programados hechos en el entorno de producción de la organización están controlados y documentados adecuadamente.
T4.10	Evaluar la adecuación de las provisiones de respaldo y de recuperación para determinar la disponibilidad de la información requerida para reanudar el procesamiento.
T4.11	Evaluar el plan de recuperación en caso de desastre de la organización para determinar si permite la recuperación de las capacidades de procesamiento de TI en caso de un desastre.
<b><i>Dominio 4 Conocimientos Relacionados</i></b>	
KS4.1	Conocimiento de las prácticas de gestión del nivel de servicio y de los componentes de un acuerdo de nivel de servicio
KS4.2	Conocimiento de técnicas para monitorear el cumplimiento por parte de terceros de los controles internos de la organización
KS4.3	Conocimiento de operaciones y procedimientos de usuario final para gestionar procesos programados y no programados
KS4.4	Conocimiento de los conceptos de tecnología relacionados con componentes de hardware y de red, software del sistema y sistemas de gestión de bases de datos
KS4.5	Conocimiento de técnicas de control que garanticen la integridad de las interfaces de sistema
KS4.6	Conocimiento de las prácticas de inventario y licenciamiento de software
KS4.7	Conocimiento de técnicas y herramientas de resiliencia (capacidad para retornar al estado inicial de operación) del sistema (por ejemplo, hardware tolerante a fallas, eliminación de un punto único de falla, clustering)
KS4.8	Conocimiento de prácticas de administración de bases de datos
KS4.9	Conocimiento de planificación de la capacidad y de herramientas y técnicas de monitoreo relacionadas
KS4.10	Conocimiento de procesos, herramientas y técnicas de monitoreo del desempeño de los sistemas (por ejemplo, analizadores de red, reportes de utilización de sistemas, balanceo de carga)
KS4.11	Conocimiento de las prácticas gerenciales de problemas e incidentes (por ejemplo, help desk, procedimientos de escalado, trazabilidad)
KS4.12	Conocimiento de procesos para gestionar los cambios programados y no programados en los sistemas y/o la infraestructura de producción, incluyendo las prácticas gerenciales de cambios, configuración, incorporación y parches
KS4.13	Conocimiento de prácticas de respaldo, almacenamiento, mantenimiento, retención y restauración de datos
KS4.14	Conocimiento de asuntos regulatorios, legales, contractuales y de seguros relacionados con la recuperación en caso de desastre
KS4.15	Conocimiento del análisis del impacto en el negocio (BIA) relacionado con el plan de recuperación en caso de desastre

# Guía del candidato para el Examen y la Certificación CISA®

<b>ÁREA DE CONTENIDO (Dominio)</b>
<b><i>Dominio 4 Conocimientos Relacionados (continuación)</i></b>
KS4.16 Conocimiento del desarrollo y mantenimiento de planes de recuperación en caso de desastres
KS4.17 Conocimiento de tipos de sitios y métodos de procesamiento alternativo para monitorear los acuerdos contractuales (por ejemplo, hot sites, warm sites, cold sites)
KS4.18 Conocimiento de procesos utilizados para invocar planes de recuperación en caso de desastre
KS4.19 Conocimiento de métodos de prueba de recuperación en caso de desastre
<b>Dominio 5 Protección de los activos de información</b> —Garantizar que las políticas de seguridad, las normas, los procedimientos y los controles de la organización aseguren la confidencialidad, la integridad y la disponibilidad de los activos de información.
<b><i>Dominio 5 Enunciado de tarea</i></b>
T5.1 Evaluar las políticas, los estándares y los procedimientos de seguridad de la información para determinar su integridad y alineación con las prácticas generalmente aceptadas.
T5.2 Evaluar el diseño, la implementación y el monitoreo de los controles de seguridad lógicos y del sistema para verificar la confidencialidad, la integridad y la disponibilidad de la información.
T5.3 Evaluar el diseño, la implementación y el monitoreo de los procesos y procedimientos de clasificación de datos para determinar si están alineados con las políticas, los estándares, los procedimientos y los requerimientos externos aplicables de la organización.
T5.4 Evaluar el diseño, la implementación y el monitoreo de los controles de acceso físico y del entorno para determinar si los activos de información están adecuadamente protegidos.
T5.5 Evaluar los procesos y los procedimientos utilizados para almacenar, recuperar, transportar y desechar activos de información (por ejemplo, soportes de respaldo, almacenamiento externo, copia impresa, y soportes de copia electrónica) para determinar si los activos de información están adecuadamente protegidos.
<b><i>Dominio 5 Conocimientos Relacionados</i></b>
KS5.1 Conocimiento de técnicas para el diseño, la implementación y el monitoreo de controles de seguridad, incluyendo programas de concienciación de la seguridad
KS5.2 Conocimiento de procesos relacionados con el monitoreo y la respuesta a incidentes de seguridad (por ejemplo, procedimientos de escalamiento, equipo de respuesta a incidentes de emergencia)
KS5.3 Conocimiento de los controles de acceso lógico para la identificación, autenticación y restricción de usuarios a funciones y datos autorizados
KS5.4 Conocimiento de controles de seguridad relacionados con hardware, software del sistema (por ejemplo, aplicaciones, sistemas operativos) y sistemas de gestión de bases de datos
KS5.5 Conocimiento de los riesgos y controles asociados con la virtualización de sistemas
KS5.6 Conocimiento de la configuración, la implementación, las operaciones y el mantenimiento de los controles de seguridad de la red
KS5.7 Conocimiento de dispositivos, protocolos y técnicas de seguridad de la red y de Internet
KS5.8 Conocimiento de métodos y técnicas de ataques a los sistemas de información
KS5.9 Conocimiento de herramientas de detección y técnicas de control (por ejemplo, software malintencionado [malware], detección de virus, software espía [spyware])
KS5.10 Conocimiento de técnicas de pruebas de seguridad (por ejemplo, pruebas de intrusión, exploración de vulnerabilidades)
KS5.11 Conocimiento de riesgos y controles asociados con la fuga de datos
KS5.12 Conocimiento de técnicas relacionadas con la encriptación
KS5.13 Conocimiento de componentes de infraestructura de clave pública (PKI) y técnicas de firma digital
KS5.14 Conocimiento de riesgos y controles asociados con computación peer-to-peer, mensajería instantánea y tecnologías basadas en web (por ejemplo, redes sociales, tableros de mensajes, blogs)
KS5.15 Conocimiento de controles y riesgos asociados con el uso de dispositivos móviles e inalámbricos
KS5.16 Conocimiento de seguridad en comunicaciones de voz (por ejemplo, PBX, VoIP)
KS5.17 Conocimiento de técnicas y procesos de preservación de evidencias seguidos en investigaciones forenses (por ejemplo, TI, proceso, cadena de custodia)
KS5.18 Conocimiento de estándares de clasificación de datos y procedimientos de soporte
KS5.19 Conocimiento de los controles de acceso físico para la identificación, autenticación y restricción de usuarios a instalaciones autorizadas
KS5.20 Conocimiento de dispositivos de protección del entorno y prácticas de soporte
KS5.21 Conocimiento de los procesos y procedimientos utilizados para almacenar, recuperar, transportar y desechar los activos de información confidencial



# Prepárese para los exámenes CISA 2012

## Recursos de Revisión de Preparación para el Examen y Desarrollo Profesional CISA 2012

---

Los candidatos que hayan pasado el examen Certified Information Systems Auditor® (CISA®) tienen un plan de estudio organizado. A fin de brindar apoyo a las personas con el desarrollo de un plan de estudio exitoso, ISACA® ofrece varias guías de estudio y cursos de repaso para los candidatos al examen. Éstas incluyen:

### Materiales de estudio

- *Manual de Preparación al Examen CISA® 2012*
- *Manual de Preguntas, Respuestas y Explicaciones de Preparación al Examen CISA® 2011*
- *Manual de Preguntas, Respuestas y Explicaciones de Preparación al Examen CISA® Suplemento 2011*
- *Manual de Preguntas, Respuestas y Explicaciones de Preparación al Examen CISA® Suplemento 2012*
- Base de Datos de Preguntas de Práctica v12 CISA®

Para efectuar el pedido, visite [www.isaca.org/cisabooks](http://www.isaca.org/cisabooks).

### Cursos de Preparación al Examen

- Cursos de preparación al examen patrocinados por el capítulo ([www.isaca.org/cisareview](http://www.isaca.org/cisareview))
- Cursos de preparación al examen en línea CISA ([www.isaca.org/elearning](http://www.isaca.org/elearning))