



CERTIFIED INFORMATION SECURITY MANAGER®

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

Exámenes CISM 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 CISM® 2012
Impreso en los Estados Unidos de América

Tabla de Contenido

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

Acerca de ISACA®

Con más de 95,000 miembros en 160 países, ISACA (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, administración de TI así como riesgos y cumplimiento relacionados con TI. Fundada en 1969, ISACA es una organización no lucrativa e independiente, 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 a prestar un servicio a la empresa.

Cláusula de exención de responsabilidad

ISACA y el Comité de certificación CISM han diseñado la *Guía del candidato para el examen y la certificación CISM® 2012* como guía para quienes aspiran a la certificación CISM. 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 CISM.

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
Página Internet: www.isaca.org

Guía del candidato para el examen y la certificación CISM®

Introducción

El programa de certificación Certified Information Security Manager (CISM, o Gerente Certificado en Seguridad de la Información) está desarrollado en forma específica para los gerentes experimentados en seguridad de la información y aquellas personas que tengan responsabilidades en la gerencia de seguridad de la información.

La certificación CISM es para la persona que gerencia, diseña y supervisa la seguridad de la información de una empresa. Aunque se concentra en la gerencia de seguridad, la credencial CISM también será valiosa para todos aquellos profesionales de SI con experiencia en seguridad. La certificación CISM promueve prácticas internacionales y brinda a la gerencia ejecutiva la seguridad de que las personas que obtienen la designación tienen la experiencia y el conocimiento necesarios para brindar servicios de consultoría y gerencia de seguridad efectivos. Las personas que obtienen la certificación CISM se convierten en parte de una red selecta de profesionales, logrando una credencial única.

Acreditación del programa CISM renovada bajo ISO/IEC 17024:2003

El Instituto Nacional de Normalización Estadounidense (ANSI, por sus siglas en inglés) ha acreditado la certificación CISM 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 los medios de desplazamiento 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 brindadas por certificaciones de 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 CISM en todo el mundo.

El examen CISM

Desarrollo/Descripción del Examen CISM

El Comité de certificación CISM supervisa el desarrollo del examen y garantiza la vigencia del contenido. Las preguntas del examen CISM 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 CISM para su revisión.

La práctica laboral sirve de base para el examen y los requisitos de experiencia para obtener la certificación CISM. Esta práctica de trabajo ha sido actualizado recientemente, es efectivo para el examen de junio de 2012 y consta de cuatro áreas de dominio. 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 CISM 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 de prácticas de trabajo vigente actualizado contiene los siguientes dominios y porcentajes:

- **Gobierno de seguridad de la información (24%)**
- **Gestión de riesgos de información y cumplimiento (33%)**
- **Desarrollo y gestión del programa de seguridad de la información (25%)**
- **Gestión de incidentes de Seguridad de la Información (18%)**

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 diversos idiomas. Si desea una lista actualizada de idiomas, visite www.isaca.org/cismterminology.

Guía del candidato para el examen y la certificación CISM®

Preparación para el examen CISM

Se puede lograr la aprobación del examen CISM 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/cismguide para conocer las guías de estudio de ISACA que pueden ayudarle 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.

En el *Manual de preparación al examen CISM 2012* se ofrece una lista completa de referencias recomendadas para el estudio señalado a la preparación del examen.

ISACA posee un glosario de términos, así como glosarios específicos de cada certificación. Estos glosarios están disponibles en www.isaca.org/glossary.

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

Administración del examen CISM

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

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 Contactarse con la sede internacional de ISACA mediante correo postal o electrónico (exam@isaca.org). Estos 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 primeras 2 semanas posteriores al examen.

Boleto de admisión:

Aproximadamente de dos a tres semanas antes de la fecha del examen CISM, los candidatos recibirán de ISACA un boleto físico de admisión y un boleto electrónico. Los candidatos al examen pueden descargar una copia del boleto de admisión en la página www.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 CISM. 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 cambia la dirección de correo postal o la dirección de correo electrónico del candidato, éste deberá actualizar su perfil en el sitio web de ISACA (www.isaca.org) o ponerse en contacto con exam@isaca.org.

Es imperativo que los candidatos anoten las horas específicas de registro y del examen en su boleto de admisión. NO SE PERMITIRÁ A NINGÚN CANDIDATO INGRESAR AL CENTRO DE PRUEBA UNA VEZ QUE EL JEFE EXAMINADOR HAYA COMENZADO A DAR LAS INSTRUCCIONES ORALES, APROXIMADAMENTE 30 MINUTOS ANTES DE 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

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.

Guía del candidato para el examen y la certificación CISM®

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 CISM de ISACA.

La Política completa de Pertenencias Personales está disponible en www.isaca.org/cismbelongings. 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 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 CISM 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 CISM los registros correspondientes a tales irregularidades para su revisión y adopción de decisiones.

Razones para la expulsión o descalificación

El supervisor puede expulsar a un candidato por alguna de las siguientes razones:

- Admisión desautorizada al centro de prueba.
- El candidato perturba o da o recibe ayuda.
- El candidato intenta sacar materiales o notas de la prueba fuera del centro de prueba.
- El candidato finge ser 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.

Guía del candidato para el examen y la certificación CISM®

Calificación del examen CISM

El examen CISM consta de 200 ítems 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. Un candidato deberá recibir una calificación de 450 o mayor para aprobar el examen. Por ejemplo, la calificación escalada de 800 representa una calificación perfecta, ya que se respondió correctamente a todas las preguntas; una calificación escalada de 200 es la calificación más baja posible y significa que sólo se respondió un número muy bajo de preguntas correctamente. Una calificación de 450 representa una norma consistente mínima de conocimiento de acuerdo a lo establecido por el Comité de Certificación CISM. El candidato que recibe una clasificación aprobatoria, puede entonces solicitar certificación si cumple con el resto de los requisitos.

El examen CISM 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 solicitar la certificación CISM.

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 CISM

Las preguntas del examen CISM se desarrollan con el fin de medir y evaluar conocimiento práctico y la aplicación de normas y conceptos generales. Todas las preguntas son de selección múltiple y tienen una mejor respuesta.

Todas las preguntas del examen CISM 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 o una descripción del problema. 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 CISM pudieran requerir que el candidato elija la respuesta apropiada con base en un calificativo, como **LA MÁS** probable o **LA 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 de preguntas del examen CISM en www.isaca.org/cismassessment.

Solicitud para la Certificación CISM

La aprobación del examen no significa que el candidato sea un CISM. Una vez que el candidato aprueba el examen CISM, 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 CISM, 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. Una vez recibida la certificación, el nuevo CISM recibirá un certificado y un NIP de certificación de CISM. 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 CISM. Cada solicitud para la certificación CISM debe ir acompañada por un pago de \$50 dólares para el pago de la cuota de tramitación.

Requisitos para obtener la certificación CISM inicial

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

Cinco o más años de experiencia laboral en seguridad de la información, con un mínimo de tres años de experiencia laboral en gerencia de seguridad de la información en tres o más de las áreas de práctica laboral. Pudiera utilizarse sustitutos para la experiencia en seguridad de la información. Sin embargo, la experiencia en gerencia de seguridad de la información no tiene sustitutos.

Guía del candidato para el examen y la certificación CISM®

Sustitutos de experiencia

Se puede utilizar otros certificados de seguridad y experiencia en gerencia de sistemas de información para satisfacer hasta dos años de experiencia laboral en gerencia de seguridad de la información.

Se puede sustituir dos años de información de experiencia laboral en gerencia de seguridad de la información por uno de los siguientes logros:

- Certified Information Systems Auditor (CISA) en vigencia
- Certified Information Systems Security Professional (CISSP) en vigencia
- Título de postgrado en seguridad de la información o campo relacionado (por ejemplo: administración de empresas, sistemas de información o aseguramiento de la información) **0**

Se puede sustituir un año por uno de los siguientes logros:

- Un año completo de experiencia en gerencia de sistemas de información
- Un año completo de experiencia en gerencia de seguridad general
- Certificación de seguridad basada en conocimientos [por ejemplo, SANS' Global Information Assurance Certification (GIAC), Microsoft Certified Systems Engineer (MCSE), CompTIA Security+, Disaster Recovery Institute Certified Business Continuity Professional (CBCP) o ESL IT Security Manager]

Por ejemplo, el candidato que sea titular de la certificación CISA o CISSP tendrá derecho a la sustitución máxima de dos años de experiencia. Sin embargo, el candidato deberá poseer también un mínimo de 3 años de experiencia laboral en gerencia de seguridad de la información en tres de las cuatro áreas de práctica laboral.

Excepción: Dos años como instructor de tiempo completo de enseñanza de gerencia de seguridad de la información se pueden sustituir por cada año de experiencia laboral en gerencia de seguridad de la información.

La experiencia se debe haber obtenido dentro del período de 10 años que precede a la fecha de solicitud de certificación CISM 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 CISM 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 puede tomar el examen CISM antes de cumplir con los requisitos de experiencia. Esta práctica es aceptable y recomendada, aunque la designación CISM no se concederá hasta que se hayan cumplido con todos los requisitos.

Requisitos para mantener la certificación CISM

Los CISM 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 CISM en www.isaca.org/cismcpepolicy.
- Entregar la totalidad de las cuotas anuales de mantenimiento de CPE a ISACA Internacional.
- Responder y entregar la documentación de actividades de CPE requerida 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 CISM de la persona. Todos los certificados son propiedad de ISACA. Si una persona ha sido aprobada para la certificación y posteriormente es revocada, la 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.

Revocación de la certificación CISM

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

- Incumplimiento de la norma de CPE de CISM
- 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 CISM o con el proceso de certificación

Guía del candidato para el examen y la certificación CISM®

Descripción de las áreas de práctica laboral del CISM Enunciados de tareas y conocimientos de CISM

ÁREA DE CONTENIDO (Dominio)
Dominio 1—Gobierno de seguridad de la información (24%) —Establecer y mantener un marco de referencia del gobierno de la seguridad de la información y dar apoyo a los procesos para asegurar que la estrategia de seguridad de la información esté alineada con las metas y los objetivos de la organización, que los riesgos de la información se administren de manera adecuada y que los recursos del programa se administren de forma responsable.
Enunciados de tareas
1.1 Establecer y mantener una estrategia de seguridad de la información alineada con las metas y objetivos de la organización para orientar el establecimiento y la administración continua del programa de seguridad de la información.
1.2 Establecer y mantener un marco de referencia del gobierno de la seguridad de la información para orientar las actividades que den apoyo a la estrategia de seguridad de la información.
1.3 Integrar el gobierno de la seguridad de la información dentro del gobierno corporativo para asegurar que las metas y objetivos organizacionales sean respaldados por el programa de seguridad de la información.
1.4 Establecer y mantener políticas de seguridad de la información para comunicar las directrices a los gerentes y orientar el desarrollo de normas, procedimientos y pautas.
1.5 Desarrollar casos de negocio para apoyar la inversión en seguridad de la información.
1.6 Identificar las influencias internas y externas a la organización (por ejemplo, la tecnología, el entorno empresarial, la tolerancia al riesgo, la ubicación geográfica, los requisitos legales y reglamentarios) para asegurarse de que estos factores son abordados por la estrategia de seguridad de la información.
1.7 Obtener el compromiso de la alta dirección y el apoyo de otras partes interesadas para maximizar la probabilidad de una implementación exitosa de la estrategia de seguridad de la información.
1.8 Definir y comunicar las funciones y responsabilidades de seguridad de la información en toda la organización para establecer claramente las responsabilidades y las líneas de autoridad.
1.9 Establecer, supervisar, evaluar y reportar mediciones (por ejemplo, indicadores clave de objetivos [KGIs], indicadores clave de desempeño [KPIs], indicadores clave de riesgo [KRIs]) para proporcionar una administración con información precisa en cuanto a la efectividad de la estrategia de seguridad de la información.
Enunciados de conocimientos
KS1.1 Conocimiento de los métodos para desarrollar una estrategia de seguridad de la información
KS1.2 Conocimiento de la relación entre la seguridad de la información y los objetivos, funciones, procesos y prácticas de la empresa.
KS1.3 Conocimiento de los métodos para implementar un marco de referencia del gobierno de la seguridad de la información
KS1.4 Conocimiento de los conceptos fundamentales de gobierno y cómo se relacionan con la seguridad de la información
KS1.5 Conocimiento de los métodos para integrar el gobierno de la seguridad de la información dentro del gobierno corporativo
KS1.6 Conocimiento de las normas, los marcos de referencia y las mejores prácticas reconocidas internacionalmente relacionadas con el gobierno de la seguridad de la información y el desarrollo de estrategias
KS1.7 Conocimiento de los métodos para desarrollar políticas de seguridad de la información
KS1.8 Conocimiento de los métodos para desarrollar casos de negocio
KS1.9 Conocimiento de la planificación estratégica presupuestaria y de los métodos para la elaboración de informes
KS1.10 Conocimiento de las influencias internas y externas a la organización (por ejemplo, la tecnología, el entorno empresarial, la tolerancia al riesgo, la ubicación geográfica, los requisitos legales y reglamentarios) y cómo impactan a la estrategia de seguridad de la información
KS1.11 Conocimiento de los métodos para obtener el compromiso de la alta dirección y el apoyo de otros grupos de interés para la seguridad de la información
KS1.12 Conocimiento de las funciones y responsabilidades de la administración de seguridad de la información
KS1.13 Conocimiento de las estructuras organizacionales y de las líneas de autoridad
KS1.14 Conocimiento de los métodos para establecer informes y canales de comunicación nuevos, o utilizar los existentes en toda la organización
KS1.15 Conocimiento de los métodos para seleccionar, implementar e interpretar mediciones (por ejemplo, indicadores clave de objetivos [KGIs], indicadores clave de desempeño [KPIs], indicadores clave de riesgo [KRIs])

Guía del candidato para el examen y la certificación CISM®


ÁREA DE CONTENIDO (Dominio)
Dominio 2—Gestión de riesgos de la información y cumplimiento (33%) —Gestionar los riesgos de información a un nivel aceptable para cumplir con los requerimientos de negocio y cumplimiento de la organización.
Enunciados de tareas
Dominio 2—Gestión de riesgos de la información y cumplimiento (cont.)
2.1 Establecer y mantener un proceso de clasificación de los activos de información para asegurar que las medidas adoptadas para proteger los activos sean proporcionales a su valor para el negocio.
2.2 Identificar los requisitos legales, reglamentarios, organizativos y otros aplicables para gestionar el riesgo de incumplimiento a niveles aceptables.
2.3 Asegurar que las evaluaciones de riesgos, las evaluaciones de vulnerabilidad y los análisis de amenazas se lleven a cabo periódicamente y de manera consistente para identificar los riesgos a la información de la organización.
2.4 Determinar las opciones adecuadas de tratamiento del riesgo para gestionar el riesgo a niveles aceptables.
2.5 Evaluar los controles de seguridad de la información para determinar si son apropiados y en efecto mitigan el riesgo a un nivel aceptable.
2.6 Identificar las diferencias entre los niveles actuales de riesgo y los deseados para gestionar el riesgo a un nivel aceptable.
2.7 Integrar la gestión de riesgos de la información en las empresas y en los procesos de TI (por ejemplo, en el desarrollo, las compras, la gestión de proyectos, las fusiones y las adquisiciones) para promover un proceso de gestión de riesgo de la información consistente e integral en toda la organización.
2.8 Supervisar el riesgo existente para asegurar que los cambios sean identificados y manejados apropiadamente.
2.9 Informar el incumplimiento y otros cambios en el riesgo de la información para manejar adecuadamente la asistencia en el proceso de toma de decisiones en la gestión del riesgo.
Enunciados de conocimientos
KS2.1 Conocimiento de los métodos para establecer un modelo de clasificación de los activos de información coherente con los objetivos de negocio
KS2.2 Conocimiento de los métodos utilizados para asignar las responsabilidades y propiedad de los activos de información así como el riesgo
KS2.3 Conocimiento de los métodos para evaluar el impacto de eventos adversos en el negocio
KS2.4 Conocimiento de metodologías de valoración de activos de información
KS2.5 Conocimiento de los requisitos legales, reglamentarios, organizativos y otros, relacionados con la seguridad de la información
KS2.6 Conocimiento de fuentes de información fidedignas, confiables y oportunas concernientes a las nuevas amenazas a la seguridad y vulnerabilidad de la información
KS2.7 Conocimiento de los eventos que pueden requerir reevaluaciones de riesgos y cambios a los elementos del programa de seguridad de la información
KS2.8 Conocimiento de las amenazas a la información, las vulnerabilidades y las exposiciones y su naturaleza cambiante
KS2.9 Conocimiento de las metodologías de evaluación y análisis de riesgos
KS2.10 Conocimiento de los métodos utilizados para priorizar los riesgos
KS2.11 Conocimiento de los requisitos para la presentación de informes de riesgos (por ejemplo, frecuencia, audiencia, componentes)
KS2.12 Conocimiento de los métodos utilizados para monitorear los riesgos
KS2.13 Conocimiento de los métodos y estrategias para tratamiento de riesgos y métodos para aplicarlos
KS2.14 Conocimiento de modelado de línea base y su relación con el análisis basado en riesgos
KS2.15 Conocimiento de los controles de seguridad de la información y de las contramedidas y los métodos para analizar su efectividad y su eficiencia
KS2.16 Conocimiento de las técnicas de análisis de desvíos relativos a la seguridad de la información
KS2.17 Conocimiento de las técnicas para la integración de la gestión de riesgos en el negocio y en los procesos de TI
KS2.18 Conocimiento de los procesos y los requisitos de presentación de informes de cumplimiento
KS2.19 Conocimiento del análisis de costo-beneficio para evaluar las opciones de tratamiento de riesgos
Dominio 3—Desarrollo y gestión del programa de seguridad de la información (25%) —Establecer y gestionar el programa de seguridad de la información alineado con la estrategia de seguridad de la información.
Enunciados de tareas
3.1 Establecer y mantener el programa de seguridad de la información alineado con la estrategia de seguridad de la información.
3.2 Asegurar la alineación entre el programa de seguridad de la información y otras funciones empresariales (por ejemplo, recursos humanos [RH], contabilidad, compras y TI) para apoyar la integración con los procesos de negocio.
3.3 Identificar, adquirir, administrar y definir los requisitos de recursos internos y externos para ejecutar el programa de seguridad de la información.

Guía del candidato para el examen y la certificación CISM®

ÁREA DE CONTENIDO (Dominio)
Domain 3—Desarrollo y gestión del programa de seguridad de la información (cont.)
3.4 Establecer y mantener arquitecturas de seguridad de la información (personas, procesos, tecnología) para ejecutar el programa de seguridad de la información.
3.5 Establecer, comunicar y mantener los estándares, procedimientos, guías y otros documentos de seguridad de la información de la organización para apoyar y guiar el cumplimiento de las políticas de seguridad de la información.
3.6 Establecer y mantener un programa de concientización y capacitación de seguridad de la información para promover un entorno seguro y una cultura de seguridad eficaz.
3.7 Integrar los requisitos de seguridad de la información en los procesos de la organización (por ejemplo, control de cambios, fusiones y adquisiciones, desarrollo, continuidad del negocio, recuperación en caso de desastres) para mantener la línea base de la seguridad de la organización.
3.8 Integrar los requisitos de seguridad de la información en los contratos y en las actividades de terceros (por ejemplo, empresas conjuntas, proveedores externos, socios comerciales, clientes) para mantener la línea base de la seguridad de la organización.
3.9 Establecer, supervisar e informar periódicamente de la gestión del programa y de las métricas operacionales para evaluar la eficacia y la eficiencia del programa de seguridad de la información.
Enunciados de conocimientos
KS3.1 Conocimiento de los métodos para alinear los requisitos del programa de seguridad de la información con los de otras funciones del negocio
KS3.2 Conocimiento de los métodos para identificar, adquirir, administrar y definir los requerimientos de recursos internos y externos
KS3.3 Conocimiento de las tecnologías de seguridad de la información, las tendencias emergentes, (por ejemplo, computación en la nube, computación móvil) y los conceptos subyacentes
KS3.4 Conocimiento de los métodos para diseñar controles de seguridad de la información
KS3.5 Conocimiento de las arquitecturas de seguridad de la información (por ejemplo, personas, procesos, tecnología) y los métodos para aplicarlas
KS3.6 Conocimiento de los métodos para desarrollar normas, procedimientos y directrices de seguridad de información
KS3.7 Conocimiento de los métodos para implementar y comunicar políticas, normas, procedimientos y directrices de seguridad de la información
KS3.8 Conocimiento de los métodos para establecer y mantener un conocimiento efectivo de seguridad de la información y programas de capacitación
KS3.9 Conocimiento de los métodos para integrar los requisitos de seguridad de la información en los procesos de la organización
KS3.10 Conocimiento de los métodos para incorporar los requisitos de seguridad de la información en los contratos y en los procesos de gestión de terceros
KS3.11 Conocimiento de los métodos para diseñar, implementar y reportar las métricas operacionales de la seguridad de la información
KS3.12 Conocimiento de los métodos para probar la eficacia y aplicabilidad de los controles de seguridad de la información
Dominio 4—Gestión de Incidentes de Seguridad de la Información (18%)—Planificar, establecer y administrar la capacidad de detectar, investigar, responder y recuperarse de incidentes de seguridad de la información para minimizar el impacto en el negocio.
Enunciados de tareas
4.1 Establecer y mantener una definición de la organización y de jerarquía de gravedad de los incidentes de seguridad de la información que permita identificar y responder con precisión a los incidentes.
4.2 Establecer y mantener un plan de respuesta a incidentes para asegurar una respuesta eficaz y oportuna a los incidentes de seguridad de la información.
4.3 Desarrollar e implementar procesos para garantizar la identificación oportuna de los incidentes de seguridad de la información.
4.4 Establecer y mantener procesos para investigar y documentar los incidentes de seguridad de la información para poder responder adecuadamente y determinar sus causas, adhiriéndose a los requisitos legales, reglamentarios y de la organización.
4.5 Establecer y mantener el escalamiento de incidentes y los procesos de notificación para garantizar que las partes interesadas correspondientes estén involucradas en la gestión de respuesta a incidentes.
4.6 Organizar, capacitar y equipar a los equipos para responder eficazmente a los incidentes de seguridad de la información de manera oportuna.
4.7 Probar y revisar periódicamente el plan de respuesta a incidentes para garantizar una respuesta eficaz a los incidentes de seguridad de la información y mejorar la capacidad de respuesta.
4.8 Establecer y mantener los planes y procesos de comunicación para gestionar la comunicación con entidades internas y externas.
4.9 Realizar revisiones posteriores al incidente para determinar el origen de los incidentes de seguridad de la información, desarrollar acciones correctivas, reevaluar riesgos, evaluar la efectividad de la respuesta y tomar las medidas correctivas adecuadas.
4.10 Establecer y mantener la integración entre el plan de respuesta a incidentes, el plan de recuperación de desastres y el plan de continuidad del negocio.

Guía del candidato para el examen y la certificación CISM®

ÁREA DE CONTENIDO (Dominio)
<i>Enunciados de conocimientos</i>
Dominio 4—Gestión de Incidentes de Seguridad de la Información(cont.)
KS4.1 Conocimiento de los componentes de un plan de respuesta a incidentes
KS4.2 Conocimiento de los conceptos y las prácticas de gestión de incidentes
KS4.3 Conocimiento de planificación de la continuidad del negocio (BCP, por sus siglas en inglés) y de la planificación de recuperación ante desastres (DRP, por sus siglas en inglés) y su relación con el plan de respuesta a incidentes
KS4.4 Conocimiento de los métodos de clasificación de incidentes
KS4.5 Conocimiento de los métodos de contención de daños
KS4.6 Conocimiento de los procesos de notificación y escalamiento
KS4.7 Conocimiento de las funciones y responsabilidades en la identificación y gestión de incidentes de seguridad de la información
KS4.8 Conocimiento de los tipos y las fuentes de herramientas y equipamiento requeridos para equipar adecuadamente a los equipos de respuesta a incidentes
KS4.9 Conocimiento de los requisitos y capacidades forenses para recoger, preservar y presentar evidencia (por ejemplo, admisibilidad, calidad e integridad de la evidencia, cadena de custodia)
KS4.10 Conocimiento de los requisitos y procedimientos de reportes internos y externos de incidentes
KS4.11 Conocimiento de las prácticas de revisión posteriores al incidente y los métodos de investigación para identificar el origen y determinar las acciones correctivas
KS4.12 Conocimiento de las técnicas para cuantificar daños, costos y otros impactos empresariales ocasionados por incidentes de seguridad de la información
KS4.13 Conocimiento de tecnologías y procesos que detecten, registren y analicen eventos de seguridad de la información
KS4.14 Conocimiento de los recursos internos y externos disponibles para investigar incidentes de seguridad de la información



Prepárese para los exámenes CISM 2012

Recursos de Revisión de Preparación para el Examen y Desarrollo Profesional CISM 2012

Los candidatos que hayan pasado el examen Certified Information Security Manager® (CISM®) 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 CISM® 2012*
- *Manual de Preguntas, Respuestas y Explicaciones de Preparación al Examen CISM® 2012*
- *Manual de Preguntas, Respuestas y Explicaciones de Preparación al Examen CISM® Suplemento 2012*
- *CISM® Practice Question Database v12*

Para efectuar el pedido, visite www.isaca.org/cismbooks.

Cursos de Preparación al Examen

- Cursos de Preparación al Examen patrocinados por el capítulo

Para buscar o registrarse en un curso en su localidad, visite www.isaca.org/cismreview.