Solicitud de la certificación CISA

Solicitantes que han aprobado el examen CISA en 2016 y años posteriores

Utilice Adobe Reader para cumplimentar la solicitud electrónica.

INFORMACIÓN SOBRE EL SOLICITANTE

NOMBRE DEL SOLICITANTE: _____ N°. DE ID DE ISACA: _____

CORREO ELECTRÓNICO: _____ N°. DE TELÉFONO: _____

PASO 1. APROBACIÓN DEL EXAMEN

Los solicitantes de la acreditación CISA deben haber aprobado el examen CISA en los últimos cinco años.
Si usted todavía no ha aprobado el examen CISA, puede inscribirse en línea en www.isaca.org/examreg

AÑO DE APROBACIÓN DEL EXAMEN: _____

PASO 2. INFORMES DE LA EXPERIENCIA LABORAL

Para ser acreditable como CISA, usted debe contar con 5 años de experiencia laboral en auditorías de Sistemas de Información, control, aseguramiento o seguridad, dentro de los 10 años anteriores a la fecha de entrega de la solicitud. Esta experiencia debe estar relacionada con, al menos, una de las áreas / dominios de práctica laboral de CISA, disponibles en la página V-2. Si usted no cumple con los requisitos sobre los 5 años de experiencia dentro de la Sección 2A, puede optar por solicitar convalidaciones de experiencia en la Sección 2B o 2C (hasta un máximo de 3 años).

Sección A: Experiencia laboral en auditorías de Sistemas de Información, control, aseguramiento o seguridad *(requisito obligatorio)*

Enumere su experiencia laboral, relacionada con las materias indicadas. Comience por el puesto actual o más reciente.
No deje fechas en blanco. Si usted está trabajando en la actualidad, escriba la fecha de hoy en Fecha de Finalización.

		Fechas de empleo *(MM/AA)*		Duración de la experiencia en tareas de CISA		Áreas de práctica laboral CISA *(marque las correctas)*				
#	Nombre de la empresa	Inicio	Fin	Años	Meses	1	2	3	4	5
1										
2										
3										
4										

(requisito mínimo de dos años) **SECCIÓN A EXPERIENCIA TOTAL:** _____

Sección B: Convalidación por experiencia laboral general *(opcional)*

Para solicitar una convalidación por experiencia laboral en base a trabajos de auditoría o sobre Sistemas de Información en general, complete los siguientes detalles.
Esta experiencia no puede haber sido obtenida durante las fechas ya declaradas en la Sección A, relacionadas con empleos. La convalidación será de un año.

Convalidación por experiencia *(seleccione)* ☐ Auditoría en general ☐ Sistemas de Información en general

Nombre de la empresa: _____ Fecha de inicio *(MM/AA)*:_____ Fecha de finalización *(MM/AA)*:

(máximo 1 año) **SECCIÓN B EXPERIENCIA TOTAL:** _____

Sección C: Convalidaciones de experiencia en base a formación *(opcional)*

Para solicitar una convalidación de experiencia en base a formación, marque las casillas correspondientes e ingrese la información de la institución educativa, según corresponda.
**Adjunte con la solicitud una copia de su título, expediente académico o carta de su Universidad o Facultad.*
***Adjunte con la solicitud una copia de su certificado de CIMA o ACCA,*

- ☐ Convalidación de 1 año por un grado de asociado (estudios de 2 años).
- ☐ Convalidación de 2 años por una licenciatura, grado+master o un doctorado en cualquier campo de estudio.
- ☐ Convalidación de 3 años para un grado+master en Sistemas de Información o un campo relacionado *
- ☐ Convalidación de 2 años para una certificación completa CIMA, Chartered Institute of Management Accountants**
- ☐ Convalidación de 2 años para miembros de ACCA, la Asociación de Contadores Públicos Colegiados **

NOMBRE DE LA INSTITUCIÓN:_____ TIPO DE TÍTULO:_____CAMPO DE ESTUDIO:_____

(máximo 3 años) **SECCIÓN C EXPERIENCIA TOTAL:** _____

Sección D: Experiencia total

La suma de experiencia total de las secciones A, B y C debe ser igual o superior a **5** años para poder solicitar la certificación como CISA.

(Sección A + Sección B + Sección C) **EXPERIENCIA TOTAL:** _____

Solicitud de la certificación CISA

Solicitantes que han aprobado el examen CISA en 2016 y años posteriores

Utilice Adobe Reader para cumplimentar la solicitud electrónica.

PASO 3. VERIFICACIÓN DE LA EXPERIENCIA LABORAL

Solicite de su/s empleador/es la verificación de la experiencia laboral declarada por usted en el Paso 2, utilizando el formulario de verificación de la experiencia (páginas V-1 y V-2 de la solicitud). Si es necesario que actúe más de un verificador, puede obtener formularios adicionales de verificación de la experiencia aquí: *www.isaca.org/cisaapp*. Para los certificados o títulos declarados en la Sección C, remita una copia de la certificación, el título o expediente académico.

PASO 4. PAGO DEL PROCESAMIENTO DE LA SOLICITUD

Todos los solicitantes deben pagar una tarifa de procesamiento de solicitud de USD 50.00 antes de que su solicitud pueda ser procesada. Puede realizar el pago en: *www.isaca.org/cisapay*

PASO 5. REVISIÓN Y FIRMA DEL ACUERDO DE TÉRMINOS Y CONDICIONES

Política de Educación Profesional Continua (CPE)
Por medio del presente documento solicito a ISACA mi Certificación como Auditor de Sistemas de Información (CISA), en conformidad con los procedimientos y las políticas de ISACA, y sujeta a los mismos. He leído y acepto las condiciones establecidas en la Solicitud para la Certificación y la Política de Educación Profesional Continua (CPE) vigentes en el momento de mi solicitud, las cuales incluyen el proceso de certificación y la política CPE.

Código de Ética
Acepto: presentar pruebas de que cumplo con los requisitos de elegibilidad; permitir que ISACA solicite clarificación o verificación adicional de toda la información remitida relacionada con la solicitud, incluidos, entre otros, el contacto con los profesionales verificadores para confirmar la información remitida; cumplir con los requisitos para obtener y mantener la certificación, incluyendo requisitos de elegibilidad por desempeño de tareas de un CISA; cumplir con el Código de Ética, los estándares y las políticas de ISACA; cumplir con los requisitos de renovación; notificar inmediatamente al departamento de certificación de ISACA en caso de no poder cumplir con los requisitos de certificación; desempeñar las tareas de un CISA; solicitar reconocimientos o derechos respecto a la certificación solo para el alcance para el cual se ha otorgado la certificación; y no utilizar la certificación CISA o los logos o marcas de manera engañosa o contradictoria con las pautas de ISACA.

Información verídica
Entiendo y acepto que se me negará la solicitud de la certificación y que se revocarán y perderé todas las credenciales que me haya otorgado ISACA si alguna de las declaraciones o respuestas que he proporcionado en la solicitud son falsas o si he violado alguna de las reglas del examen o de los requisitos de certificación. Entiendo que todos los certificados son propiedad de ISACA y que, si se me otorga el certificado y luego se revoca, destruiré el certificado, suspenderé su uso y retiraré todas mis solicitudes de reconocimiento o derechos asociadas a dicha certificación. Autorizo a ISACA a realizar todas las consultas e investigaciones que considere necesarias para verificar mis credenciales y mi situación profesional.

Divulgación de información a terceros
Reconozco que, si se me otorga la certificación, mi estado de certificación será público y podrá ser divulgado a terceras partes que pudieran solicitarlo. Si mi solicitud de certificación no es aprobada, entiendo que puedo apelar la decisión contactando con ISACA. Las apelaciones emprendidas por una persona que ha realizado el examen de certificación, un/a candidato/a a la certificación o una persona ya certificada son realizadas a criterio y coste de la persona que realiza la apelación. Con mi firma al pie de esta página, autorizo a ISACA a divulgar mi estado de certificación. Esta información de contacto se utilizará para las consultas y solicitudes de mi certificación.

Política de contacto
Con mi firma al pie de esta página, autorizo a ISACA a comunicarse conmigo a la dirección y los números proporcionados. Esta información que he proporcionado es mía y es verdadera y vigente. Autorizo a ISACA a divulgar información confidencial sobre la solicitud de la certificación y la certificación si así lo exige la ley o en conformidad con la Política de Privacidad de ISACA. Para conocer más sobre cómo utilizamos la información que ha proporcionado en este formulario, por favor lea nuestra Política de Privacidad, disponible en www.isaca.org/privacy.

Acuerdo de uso
Por la presente, acepto exonerar a ISACA y a sus ejecutivos, directores, examinadores, miembros, empleados y agentes, así como a los de las organizaciones que colaboran con ISACA, ante cualquier queja, reclamación o daño producido por cualquier acción u omisión de alguno de ellos en relación con la presente solicitud; el proceso de solicitud; fallos a la hora de emitir un certificado; o cualquier demanda sobre retirada o reemisión de dicho certificado. Sin embargo, entiendo y convengo en que, si surgiera algún litigio como consecuencia o relacionado con esta solicitud, éste se presentará en el Tribunal de Circuito del Condado de Cook, estado de Illinois, EE. UU., y se regirá por las leyes del Estado de Illinois, EE. UU.

Entiendo que la decisión sobre mi estatus de cumplimiento con los requisitos para la certificación recae única y exclusivamente en ISACA, y que la decisión de ISACA es definitiva.

He leído y entiendo estas declaraciones y acepto quedar obligado legalmente por las mismas.

FIRMA DEL SOLICITANTE:_____ FECHA: _____

PASO 6. ENTREGA DE LA SOLICITUD

Envíe su solicitud en línea, junto con el/los formulario/s de verificación, accediendo a: *https://support.isaca.org*

Seleccione **Certifications & Certificate Programs** (Certificaciones y Programas de Certificación) y **Submit an Application** (Enviar una Solicitud).

El procesamiento de las solicitudes remitidas tarda alrededor de dos a tres semanas. En caso de aprobación, se le notificará por correo electrónico. Se le enviará un “paquete de certificación” con una carta de aprobación, un Certificado CISA y un prendedor de metal como CISA, por correo postal, a la dirección principal de su perfil de ISACA. El tiempo estimado de entrega de este paquete se sitúa entre 4 y 8 semanas.

Formulario de verificación de la experiencia de CISA

Solicitantes que han aprobado el examen CISA en 2016 y años posteriores

Utilice Adobe Reader para llenar la solicitud electrónica.

DETALLES DEL SOLICITANTE

NOMBRE DEL SOLICITANTE: _____ N°. DE ID DE ISACA: _____

INSTRUCCIONES DEL FORMULARIO

El solicitante (mencionado arriba) realiza la solicitud de la certificación CISA a través de ISACA. ISACA requiere que la experiencia laboral del solicitante sea verificada en forma independiente por parte de un supervisor o gerente con quien haya trabajado. Los verificadores no pueden ser familia inmediata o lejana, ni pueden trabajar en el Departamento de Recursos Humanos.

Usted debe avalar la experiencia laboral del solicitante en base a lo que éste indica en su formulario de solicitud adjunto (página A-1) y tal como se describe en los Dominios de Práctica Laboral de CISA y en las declaraciones de tarea (página V-2).

Por favor, devuelva el presente formulario de verificación al solicitante, para su remisión a ISACA por parte de éste. Si tiene alguna pregunta, contacte con ISACA en https://support.isaca.org o +1.847.660.5505.

INFORMACIÓN SOBRE EL VERIFICADOR

NOMBRE DEL VERIFICADOR: _____

NOMBRE DE LA EMPRESA: _____ CARGO: _____

CORREO ELECTRÓNICO: _____ N°. DE TELÉFONO: _____

PREGUNTAS DEL VERIFICADOR

1. Avalo la siguiente experiencia laboral obtenida por el solicitante, como se indica en la página A-1 (*marque todas las opciones que correspondan*):

☐ Sección A: Empresa 1 ☐ Sección A: Empresa 3

☐ Sección A: Empresa 2 ☐ Sección A: Empresa 4

2. Avalo las siguientes convalidaciones, como se indica en la página A-1, secciones B y C (*marque todas las opciones que correspondan*):

☐ Sección B: Convalidaciones por experiencia laboral ☐ Sección C: Título educativo

3. Avalo la experiencia laboral del solicitante durante el siguiente período de tiempo:

FECHA DE INICIO: _____ FECHA DE FINALIZACIÓN: _____

4. He trabajado en los siguientes cargos con el solicitante:

☐ Supervisor ☐ Gerente ☐ Colega ☐ Cliente

5. Avalo toda la experiencia obtenida en la Sección A, y también puedo avalar que las tareas realizadas por el solicitante, como se indica en la página V-2 del presente formulario, son correctas a mi leal saber y entender.

☐ Sí ☐ No

ACUERDO DEL VERIFICADOR

Por la presente confirmo que la información de la página V-1 y V-2 es correcta a mi leal saber y entender y que no hay motivo por el cual el solicitante no debería estar certificado como un Auditor de Sistemas de Información. También estoy dispuesto a responder preguntas de ISACA sobre la información proporcionada, en caso de ser requerido a ello.

FIRMA DEL VERIFICADOR: _____ FECHA: _____

Formulario de verificación de la experiencia de CISA

Solicitantes que han aprobado el examen CISA en 2016 y años posteriores

Utilice Adobe Reader para llenar la solicitud electrónica.

INSTRUCCIONES SOBRE LAS ÁREAS / DOMINIOS DE PRÁCTICA LABORAL

Es obligatorio que el solicitante marque todos los dominios en los que ha completado tareas, a confirmar por parte del verificador.

☐ DOMINIO 1 - El proceso de Auditoría de Sistemas de Información

Proporcionar servicios de auditoría de acuerdo con las normas de auditoría de SI para ayudar a la Organización a proteger y controlar los Sistemas de Información.

Declaraciones de tarea:

- Ejecutar una estrategia de auditoría de SI basada en riesgos, en cumplimiento con los estándares de auditoría de SI, para garantizar que las áreas clave son auditadas.
- Planificar auditorías específicas para determinar si los Sistemas de Información están protegidos, controlados y proporcionan valor a la Organización.
- Realizar auditorías de acuerdo con las normas de auditoría de SI para alcanzar los objetivos de auditoría previstos.
- Comunicar los resultados de la auditoría y hacer recomendaciones a las partes interesadas clave a través de reuniones e informes de auditoría, para promover cambios cuando sea necesario.
- Realizar seguimientos de la auditoría para determinar si la dirección ha tomado las medidas apropiadas en el momento oportuno.

☐ Dominio 2 - Gobierno y gestión de TI

Asegurar que se cuenta con las estructuras y procesos organizacionales y de liderazgo necesarios para lograr los objetivos y apoyar la estrategia de la Organización.

Declaraciones de tarea:

- 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, respecto a su alineamiento con las estrategias y los objetivos de la Organización.
- Evaluar la efectividad de la estructura de Gobierno de TI para determinar si las decisiones, direcciones y desempeño de TI apoyan las estrategias y objetivos de la Organización.
- Evaluar la estructura organizacional de TI y la gestión de recursos humanos (personal) para determinar si apoyan las estrategias y objetivos de la Organización.
- Evaluar las políticas, estándares y procedimientos de TI de la Organización, así como los procesos para su desarrollo, aprobación, publicación, implementación y mantenimiento, para determinar si son compatibles con la estrategia de TI y cumplen con los requisitos legales y reglamentarios.
- Evaluar la gestión de los recursos de TI, incluyendo la inversión, priorización, asignación y uso, respecto a su alineamiento con las estrategias y objetivos de la Organización.
- Evaluar la gestión de la cartera (portfolio) de TI, incluyendo la inversión, priorización y asignación, respecto a su alineamiento con las estrategias y objetivos de la Organización.
- Evaluar las prácticas de gestión de riesgos para determinar si los riesgos de la Organización relacionados con TI se identifican, evalúan, supervisan, informan y gestionan.
- Evaluar la gestión de TI y el monitoreo de los controles (por ejemplo, monitoreo continuo, aseguramiento de la calidad (QA)) para verificar el cumplimiento de las políticas, estándares y procedimientos de la Organización.
- Evaluar la supervisión y la presentación de informes sobre indicadores clave de desempeño (KPI) de TI, para determinar si la Dirección recibe la información necesaria a su debido tiempo.
- Evaluar el plan de continuidad de negocios (BCP), incluido el alineamiento con el plan de recuperación de desastres de TI (DRP), para determinar la capacidad de la Organización para continuar con las operaciones esenciales de negocios durante el período de una interrupción de TI.

☐ DOMINIO 3 - Adquisición, desarrollo e implementación de Sistemas de Información

Asegurar que las prácticas para la adquisición, desarrollo, prueba e implementación de Sistemas de Información cumplan con las estrategias y objetivos de la Organización.

Declaraciones de tarea:

- Evaluar los casos de negocio para las inversiones propuestas sobre adquisición, desarrollo, mantenimiento y posterior retirada de Sistemas de Información, para determinar si los casos de negocio cumplen con los objetivos de negocio.
- Evaluar la selección de proveedores de TI y los procesos de gestión de contratos para garantizar que se cumplan los niveles de servicio de la Organización y los controles sobre los requisitos.
- Evaluar el marco de gestión de proyectos y sus controles para determinar si los requisitos de negocio se logran de forma efectiva en relación con sus costes, gestionándose paralelamente los riesgos para la Organización.
- Realizar revisiones de los sistemas después de su implementación para determinar si los entregables y controles del proyecto han sido obtenidos y se han cumplido los requerimientos de la Organización.
- Llevar a cabo revisiones para determinar si un proyecto está progresando de acuerdo con los planes del proyecto, si cuenta con soporte documental adecuado y si dispone de informes de estado oportunos y precisos.
- Evaluar los controles sobre los Sistemas de Información durante las fases de requisitos, adquisición, desarrollo y pruebas para verificar el cumplimiento de las políticas, normas, procedimientos y requisitos externos aplicables en la Organización.
- Evaluar el grado de preparación de los Sistemas de Información para su implementación y migración a producción, determinando si los entregables y controles del proyecto han sido obtenidos y se han cumplido los requerimientos de la Organización.

☐ DOMINIO 4 - Gestión de servicios, mantenimiento y operaciones de Sistemas de Información

Asegurar que los procesos de operación, mantenimiento y soporte de los Sistemas de Información cumplan con las estrategias y objetivos de la Organización.

Declaraciones de tarea:

- Evaluar el marco y las prácticas de gestión de servicios de TI (internos o de terceros) para determinar si se cumplen los controles y los niveles de servicio esperados por la Organización y si se cumplen los objetivos estratégicos.
- Realizar revisiones periódicas de los Sistemas de Información para determinar si continúan cumpliendo los objetivos de la Organización dentro de la arquitectura empresarial (EA).
- Evaluar las operaciones de TI (por ejemplo, la programación de tareas, la gestión de la configuración, la gestión de la capacidad y el rendimiento) para determinar si se controlan de manera eficaz y si continúan respaldando los objetivos de la Organización.
- Evaluar el mantenimiento de TI (parches, actualizaciones) para determinar si se controlan de manera efectiva y si continúan respaldando los objetivos de la Organización.
- Evaluar las prácticas de gestión de las bases de datos para determinar la integridad y optimización de las bases de datos.
- Evaluar la calidad de los datos y la gestión de su ciclo de vida para determinar si continúan cumpliendo los objetivos estratégicos.
- Evaluar las prácticas de gestión de problemas e incidentes para determinar si los problemas e incidentes son prevenidos, detectados, analizados, reportados y resueltos de manera oportuna para respaldar los objetivos de la Organización.
- Evaluar las prácticas de gestión de cambios y liberación de actualizaciones, para determinar si los cambios realizados en los sistemas y aplicaciones están adecuadamente controlados y documentados.
- Evaluar la computación de usuario final para determinar si los procesos se controlan de forma eficaz y respaldan los objetivos de la Organización.
- Evaluar la continuidad y resiliencia de TI (copias de seguridad y restauración, planes de recuperación ante desastres [DRP]) para determinar si se controlan de forma eficaz y siguen respaldando los objetivos de la Organización.

☐ DOMINIO 5 - Protección de los activos de información

Asegurar que las políticas, estándares, procedimientos y controles de la Organización aseguren la confidencialidad, integridad y disponibilidad de los activos de información.

Declaraciones de tarea:

- Evaluar las políticas, estándares y procedimientos de Seguridad de la Información y privacidad, para determinar si están completos, si están alineados con las prácticas generalmente aceptadas y si cumplen con los requisitos externos aplicables.
- Evaluar el diseño, la implementación, el mantenimiento, el monitoreo y la presentación de informes de los controles físicos y ambientales para determinar si los activos de información están adecuadamente protegidos.
- Evaluar el programa de Seguridad de la Información para determinar su eficacia y su alineamiento con las estrategias y los objetivos de la Organización.
- Evaluar el diseño, la implementación, el mantenimiento, el monitoreo y la presentación de informes de los controles de seguridad lógicos y del sistema para verificar la confidencialidad, la integridad y la disponibilidad de la información.
- Evaluar el diseño, la implementación y la supervisión de los procesos y procedimientos de clasificación de datos respecto a su alineamiento con las políticas, los estándares, los procedimientos de la Organización y los requisitos externos aplicables.
- Evaluar los procedimientos y procesos utilizados para almacenar, recuperar, transferir y retirar activos, para determinar si los activos de información están adecuadamente protegidos.