

Solicitud de la certificación CRISC

Solicitantes que han aprobado el examen CRISC de 2015 y posteriores

Por favor use Adobe Reader cuando cumplimente esta solicitud electrónicamente.

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 CRISC deben haber aprobado el examen CRISC en los últimos cinco años.
Si usted aún no ha aprobado el examen CRISC, puede inscribirse en línea en www.isaca.org/examreg

AÑO DE APROBACIÓN DEL EXAMEN: _____

PASO 2. REMISIÓN DE LA EXPERIENCIA LABORAL PARA CRISC

Para ser acreditable como CRISC, usted debe contar con 3 años de experiencia en administración de riesgos y control de Sistemas de Información dentro de los 10 años anteriores a la fecha de entrega de la solicitud.

Esta experiencia debe ser adquirida en un mínimo de dos Dominios de Práctica Laboral de CRISC, y una de ellas debe ser el dominio 1 o 2. Puede encontrar los Dominios de Práctica Laboral de CRISC en www.isaca.org/criscjobpractice

Sección A: Experiencia en control de riesgos y Sistemas de Información

Declare a continuación la experiencia laboral para la que solicita reconocimiento, 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.

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

(se requiere un mínimo de 3 años) **EXPERIENCIA DE LA SECCIÓN TOTAL:** _____

Solicitud de la certificación CRISC

Solicitantes que han aprobado el examen CRISC de 2015 y posteriores

Por favor use Adobe Reader cuando cumplimente esta solicitud electrónicamente.

PASO 3. VERIFICACIÓN DE LA EXPERIENCIA LABORAL PARA CRISC

Utilizando el Formulario de Verificación de Experiencia disponible en las páginas V-1 y V-2 de esta solicitud, por favor pídale a el/los empleador/es la verificación de toda la experiencia declarada en el Paso 2. Si su experiencia incluye a más de un empleador, puede obtener formularios de verificación adicionales en: www.isaca.org/criscapp

PASO 4. REMISIÓN DEL PAGO DE LA SOLICITUD

Todos los solicitantes deben pagar una Cuota por Procesamiento de Solicitud de US \$50.00 antes de que la solicitud pueda ser procesada completamente. Envíe su pago a: www.isaca.org/criscpay

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

Política de Educación Profesional Continua (CPE)

Por la presente solicito a Information Systems Audit and Control Association, Inc. (ISACA), la certificación Certified in Risk and Information Systems Control (CRISC) 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 que abarcan el proceso de certificación y la política CPE.

Código Ético

Acepto: presentar pruebas de que cumpla 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 verificados 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 CRISC, cumplimiento con el Código de Ética, los estándares y las políticas de ISACA; cumplimiento con los requisitos de renovación; notificar al departamento de certificación de ISACA en caso de no poder cumplir con los requisitos de certificación; desempeñar todas las tareas de un CRISC; 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 CRISC o los logos o marcas de manera engañosa o contradictoria con las directrices de ISACA.

Veracidad de la información

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 reconocimientos 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.

Intercambio de información con 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, verdadera y actual. 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, este 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. PRESENTACIÓN 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 CRISC y un prendedor de metal como CRISC, por correo postal, a la dirección principal de su Perfil MyISACA en: www.isaca.org/myisaca. El tiempo estimado de entrega de este paquete se sitúa entre 4 y 8 semanas.

Formulario de Verificación de Experiencia para CRISC

Solicitantes que aprobaron el examen CRISC de 2015 y posteriores

Por favor use Adobe Reader cuando cumplimente esta solicitud electrónicamente.

DETALLES DEL SOLICITANTE

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

INSTRUCCIONES DEL FORMULARIO PARA EL VERIFICADOR

El solicitante (mencionado arriba) realiza la solicitud de la certificación CRISC a través de ISACA. ISACA requiere que la experiencia laboral del solicitante sea verificada de 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.

Al completar el formulario, usted avala la experiencia laboral del solicitante, tal como éste declara en su solicitud adjunta (página A-1), en conformidad con las áreas de dominio de práctica laboral de CRISC y sus declaraciones de tareas (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, comuníquese 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. He desempeñado las siguientes funciones en relación con el solicitante:

Supervisor

Gerente

Colega

Cliente

3. Avalo también que las tareas realizadas por el aspirante, según lo declarado en la página V-2 de este formulario, son correctas a mi leal saber y entender.

Sí

No

ACUERDO DEL VERIFICADOR:

Por la presente confirmo que la información en la página V-1 y V-2 es correcta a mi leal saber y entender y no hay razón para que este solicitante no esté certificado en Control de Riesgos y 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: _____

Por favor use Adobe Reader cuando cumplimente esta solicitud electrónicamente.

INSTRUCCIONES PARA EL DOMINIO 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 - Identificación de riesgos de TI

Identificar el universo de riesgos de TI para contribuir a la ejecución de la estrategia de gestión de riesgos de TI y respaldar los objetivos de negocio y mantenerse alineado con la estrategia de gestión de riesgo empresarial (ERM).

Declaraciones de tareas:

- Recopilar y revisar información, incluyendo la documentación existente sobre los entornos de TI y los negocios internos y externos de la organización para identificar los impactos potenciales de los riesgos de TI en los objetivos y las operaciones de la organización.
- Identifique amenazas y vulnerabilidades potenciales relativas al personal, los procesos y la tecnología de la organización para permitir el análisis de riesgo de TI.
- Desarrollar un conjunto integral de escenarios de riesgo de TI con base en la información disponible para determinar el impacto potencial a las operaciones y los objetivos del negocio.
- Identificar a las partes interesadas clave en los escenarios de riesgo de TI para ayudar a establecer las responsabilidades.
- Establecer un registro de riesgo de TI para ayudar a garantizar que los escenarios de riesgo de TI identificados se tengan en cuenta y se incorporen al perfil de riesgo de toda la organización.
- Identificar el apetito y la tolerancia al riesgo definidos por la alta Dirección y las partes interesadas claves para garantizar la alineación con los objetivos de negocio.
- Colaborar en el desarrollo del programa de concienciación de riesgos y llevar a cabo capacitaciones con el fin de garantizar que las partes interesadas comprendan los riesgos y fomenten una cultura de conciencia de riesgos.

DOMINIO 2 - Evaluación de riesgos de TI

Analizar y evaluar los riesgos de TI para determinar la probabilidad y el impacto en los objetivos de negocio para que se tomen decisiones basadas en el riesgo.

Declaraciones de tareas:

- Analizar los escenarios de riesgo de acuerdo con los criterios organizacionales (p. ej., estructura organizacional, políticas, estándares, tecnología, arquitectura, controles) para determinar la probabilidad y el impacto de un riesgo identificado.
- Identificar el estado actual de los controles existentes y evaluar su eficacia para la mitigación de riesgos de TI.
- Revisar los resultados del análisis de riesgo y controles para evaluar las brechas que existan entre los estados actual y deseado del entorno de riesgo de TI.
- Garantizar que se asigne la propiedad de riesgos en el nivel correspondiente para establecer líneas claras de responsabilidad.
- Comunicar los resultados de evaluaciones de riesgo a la alta gerencia y a las partes interesadas correspondientes para permitir la toma de decisiones en función de los riesgos.
- Actualizar el registro de riesgos con los resultados de la evaluación del riesgo.

DOMINIO 3 - Mitigación y respuesta al riesgo

Determinar las opciones de respuesta al riesgo, y evaluar su eficiencia y eficacia al momento de gestionar el riesgo de manera alineada con los objetivos del negocio.

Declaraciones de tareas:

- Consultar con los propietarios del riesgo para seleccionar y alinear las respuestas ante riesgos recomendadas con los objetivos del negocio y permitir decisiones informadas sobre el riesgo.
- Consultar con los propietarios del riesgo, o asistirlos, al momento del desarrollo de planes de acción ante riesgos para garantizar que los planes incluyan elementos clave (por ejemplo, respuesta, coste, fecha prevista).
- Consultar sobre el diseño y la implementación de ajustes de los controles de mitigación para garantizar que el riesgo se gestione a un nivel aceptable.
- Garantizar que la propiedad del control es asignada para establecer líneas claras de responsabilidad.
- Asistir a los propietarios de control para desarrollar documentación y procedimientos de desarrollo de controles, a fin de permitir la ejecución eficaz y efectiva del control.
- Actualizar el registro de riesgos a fin de reflejar los cambios en el riesgo y la correspondiente respuesta por parte de la gerencia.
- Validar que las respuestas al riesgo se hayan ejecutado de acuerdo con los planes de acción ante riesgos.

DOMINIO 4 - Monitoreo y Reporte de Riesgos y Controles

Monitorear continuamente el riesgo y los controles de TI, e informar sobre estos a las partes interesadas pertinentes para garantizar la eficiencia y la eficacia constantes de la estrategia de gestión del riesgo de TI y su adecuación a los objetivos de negocio.

Declaraciones de tareas:

- Definir y establecer indicadores clave de riesgo (KRI) y umbrales sobre la base de los datos disponibles para permitir el monitoreo de los cambios en los riesgos.
- Monitorear y analizar los indicadores clave de riesgo (KRI) para identificar cambios o tendencias en el perfil de riesgos de TI.
- Informar sobre cambios o tendencias relacionadas con el perfil de riesgos de TI para asistir a la gerencia y a las partes interesadas pertinentes en la toma de decisiones.
- Facilitar la identificación de métricas y de indicadores clave de desempeño (KPI) que permitan medir el desempeño de los controles.
- Monitorear y analizar los indicadores clave de desempeño (KPI) para identificar cambios o tendencias relacionadas con el ambiente de control y determinar la eficiencia y la eficacia de los controles.
- Revisar los resultados de evaluación de control para determinar la eficacia del ambiente de control.
- Informar sobre el desempeño o los cambios o tendencias en el perfil de riesgo general y el ambiente de control para partes interesadas pertinentes que permitan la toma de decisiones.