# Formulario de verificación de la experiencia para CISM

Solicitantes que han aprobado el examen CISM entre 2013 y 2016

*Utilice Adobe Reader para cumplimentar 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 CISM 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 CISM y en las 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 experiencia laboral en Gestión de Seguridad de la Información que aparece a continuación, 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 por experiencia global en Seguridad de la Información, tal como se indica en la página A-1, sección B (*marque todas las opciones que correspondan*):

☐ Sección B: Empresa 1 ☐ Sección B: Empresa 2

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

FECHA DE INICIO: _____ FECHA DE FINALIZACIÓN: _____

4. He desempeñado las siguientes funciones en relación con el solicitante:

☐ Supervisor ☐ Gerente ☐ Colega ☐ Cliente

5. Al dar fe de la experiencia obtenida en la Sección A, también puedo dar fe de que las tareas realizadas por el solicitante, tal como se enumeran 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 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 Gerente de Seguridad de la Información. También estoy dispuesto a responder preguntas de ISACA sobre la información proporcionada, en caso de ser requerido para ello.

FIRMA DEL VERIFICADOR: _____ FECHA: _____

# Formulario de verificación de la experiencia para CISM

Solicitantes que han aprobado el examen CISM entre 2013 y 2016

*Utilice Adobe Reader para cumplimentar esta solicitud electrónicamente.*

## INSTRUCCIONES DE LOS 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—Gobierno de la Seguridad de la Información

Establecer y mantener un marco de Gobierno de la Seguridad de la Información y procesos de apoyo, para garantizar que la estrategia de Seguridad de la Información esté alineada con las metas y objetivos de la Organización, que el riesgo de la información se gestione adecuadamente y que los recursos del programa se gestionen de forma responsable.

***Declaraciones de tarea:***

- Establecer y mantener un marco de Gobierno de la Seguridad de la Información y sus procesos de apoyo, en línea con los objetivos y las metas organizacionales, para guiar el establecimiento y la gestión continua del programa de Seguridad de la Información.
- Establecer y mantener un marco de Gobierno de la Seguridad de la Información para guiar las actividades que respaldan la estrategia de Seguridad de la Información.
- Integrar el Gobierno de la Seguridad de la Información en la gobernanza corporativa, para garantizar que los objetivos y las metas organizacionales estén respaldadas por el programa de Seguridad de la Información.
- Establecer y mantener políticas de Seguridad de la Información para comunicar las directivas de la Gerencia y guiar el desarrollo de estándares, procedimientos y directrices.
- Desarrollar casos de negocio para respaldar las inversiones en Seguridad de la Información.
- Identificar las influencias internas y externas de la Organización (por ejemplo, la tecnología, el entorno de negocio, la tolerancia al riesgo, la ubicación geográfica y los requisitos legales y reglamentarios) para garantizar que estos factores se abordan en la estrategia de Seguridad de la Información.
- Obtener el compromiso de la Alta Dirección y el apoyo de otras partes interesadas para maximizar la probabilidad de implementación exitosa de la estrategia de Seguridad de la Información.
- Definir y comunicar las funciones y responsabilidades de la Seguridad de la Información en toda la organización, para establecer responsabilizaciones (accountability) y líneas jerárquicas claras.
- Establecer, monitorear, evaluar y reportar métricas (por ejemplo, indicadores clave de metas [KGIs], indicadores clave de desempeño [KPIs], indicadores clave de riesgo [KRIs]) para proporcionar a la Gerencia información precisa sobre la efectividad de la estrategia de Seguridad de la Información.

### ☐ DOMINIO 2— Gestión de riesgos de la información y cumplimiento normativo

Gestionar los riesgos de información y reducirlos a un nivel aceptable, para cumplir los requisitos de negocio y de cumplimiento normativo de la Organización.

***Declaraciones de tarea:***

- Establecer y mantener un proceso para la clasificación de activos de información para garantizar que las medidas tomadas para proteger a los activos sean proporcionales a su valor para el negocio.
- Identificar los requisitos legales, reglamentarios, organizativos y otros requisitos aplicables para gestionar el riesgo de incumplimiento y reducirlo a niveles aceptables.
- Garantizar que las evaluaciones de riesgos, las evaluaciones de vulnerabilidades y los análisis de amenazas se lleven a cabo de forma periódica y coherente, con el fin de identificar los riesgos para la información de la Organización.
- Determinar las opciones de tratamiento de riesgos apropiadas para gestionar los riesgos y reducirlos a niveles aceptables.
- Evaluar los controles de Seguridad de la Información para determinar si son apropiados y mitigan eficazmente el riesgo hasta un nivel aceptable.
- Identificar la brecha entre los niveles de riesgo actuales y los deseados, para gestionar los riesgos y reducirlos a un nivel aceptable.
- Integrar la gestión de riesgos de la información en los procesos de negocio y de TI (por ejemplo, desarrollo, adquisiciones, gestión de proyectos, fusiones y adquisiciones) para promover un proceso de gestión del riesgo de la información coherente y completo en toda la Organización.
- Monitorear el riesgo existente para asegurar que los cambios sean identificados y gestionados adecuadamente.
- Reportar incumplimientos y otros cambios en los riesgos de la información a la Gerencia competente, para ayudar en el proceso de toma de decisiones sobre la gestión de riesgos.

### ☐ DOMINIO 3 - Desarrollo y gestión del programa de Seguridad de la Información

Establecer y gestionar el programa de Seguridad de la Información en línea con la estrategia de Seguridad de la Información.

***Declaraciones de tarea:***

- Establecer y mantener un programa de Seguridad de la Información en línea con la estrategia de Seguridad de la Información.
- Garantizar la alineación entre el programa de Seguridad de la Información y otras funciones de negocio (por ejemplo, Recursos Humanos [RRHH], Contabilidad, Compras y TI) para apoyar la integración con los procesos de negocio.
- Identificar, adquirir, administrar y definir los recursos internos y externos requeridos para ejecutar el programa de Seguridad de la Información.
- Establecer y mantener arquitecturas de Seguridad de la Información (personas, procesos, tecnología) para ejecutar el programa de Seguridad de la Información.
- Establecer, comunicar y mantener normas, procedimientos, directrices y otra documentación sobre Seguridad de la Información de la Organización, para apoyar y guiar el cumplimiento de las políticas de Seguridad de la Información.
- Establecer y mantener un programa de concienciación y formación sobre Seguridad de la Información, a fin de promover un entorno seguro y una cultura eficaz en materia de seguridad.
- Integrar los requisitos de Seguridad de la Información en los procesos de la Organización (por ejemplo, control de cambios, fusiones y adquisiciones, desarrollo, continuidad de negocio, recuperación de desastres) para mantener las referencias en materia de seguridad de la Organización.
- Integrar los requisitos de Seguridad de la Información en los contratos y actividades de terceros (por ejemplo, empresas conjuntas, proveedores subcontratados, socios comerciales, clientes) para mantener las referencias de seguridad de la Organización.
- Establecer, monitorear y reportar periódicamente métricas operativas y de gestión del programa, para evaluar la efectividad y eficiencia del programa de Seguridad de la Información.

### ☐ DOMINIO 4 – Gestión de incidentes de Seguridad de la Información

Planificar, establecer y gestionar la capacidad de detección, investigación, respuesta y recuperación ante incidentes de Seguridad de la Información, para minimizar su impacto en el negocio.

***Declaraciones de tarea:***

- Establecer y mantener una definición organizacional de los incidentes de Seguridad de la Información, y su escala de gravedad, con el fin de permitir una clasificación y categorización precisas para una adecuada respuesta a los incidentes.
- Establecer y mantener un plan de respuesta ante incidentes para asegurar una respuesta efectiva y oportuna a los incidentes de Seguridad de la Información.
- Desarrollar e implementar procesos para asegurar la identificación temprana de incidentes de Seguridad de la Información.
- Establecer y mantener procesos de investigación y documentación de incidentes de Seguridad de la Información para poder responder adecuadamente y determinar sus causas, cumpliendo al mismo tiempo los requisitos legales, reglamentarios y organizativos.
- Establecer y mantener procesos de notificación y escalado de incidentes, para garantizar que las partes interesadas pertinentes participen en la gestión de las respuestas a los incidentes.
- Organizar y formar equipos, dotándoles de recursos, para responder de forma eficaz y oportuna a los incidentes de Seguridad de la Información.
- Probar y revisar periódicamente el plan de respuesta ante incidentes, para asegurar una respuesta eficaz a los incidentes de Seguridad de la Información y mejorar las capacidades de respuesta.
- Establecer y mantener planes y procesos de comunicación para gestionar la comunicación con entidades internas y externas.
- Realizar revisiones post-incidente para determinar la causa raíz de los incidentes de Seguridad de la Información, desarrollar acciones correctivas, reevaluar el riesgo, evaluar la efectividad de la respuesta y tomar las acciones correctivas apropiadas.
- Establecer y mantener la integración entre el plan de respuesta a incidentes, el plan de recuperación de desastres y el plan de continuidad de negocio.