# Formulario de verificación de la experiencia para CISM

Solicitantes que han aprobado el examen CISM de 2017 y posteriores

*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 de 2017 y posteriores

*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 o mantener un marco de Gobierno de la Seguridad de la Información y sus procesos de soporte, para garantizar que la estrategia de Seguridad de la Información está en línea con los objetivos y las metas organizacionales.

***Declaraciones de tarea:***

- Establecer o mantener un marco de Gobierno de la Seguridad de la Información y los procesos de apoyo, en línea con los objetivos y las metas organizacionales, para guiar el establecimiento y la gestión continuos del programa de Seguridad de la Información.
- Establecer y/o 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 guiar el desarrollo de estándares, procedimientos y pautas, alineadas con las metas y los objetivos corporativos.
- Desarrollar casos de negocio para respaldar las inversiones en Seguridad de la Información.
- Identificar influencias internas y externas de la Organización (p. ej., tecnologías emergentes, medios sociales, entorno de negocio, tolerancia al riesgo, requisitos normativos, consideraciones de terceros, panoramas de amenazas) para garantizar que esos factores sean abordados de forma continua por la estrategia de Seguridad de la Información.
- Obtener el compromiso continuo de la Alta Dirección y de otras partes interesadas para respaldar la implementación exitosa de la estrategia de Seguridad de la Información.
- Definir, comunicar y monitorear las responsabilidades en materia de Seguridad de la Información a lo largo de la Organización (p. ej., propietarios de datos, custodios de datos, usuarios finales, usuarios privilegiados o de alto riesgo) así como las líneas jerárquicas.
- Establecer, monitorear, evaluar e informar sobre los parámetros clave de Seguridad de la Información, para proporcionar a la Gerencia información precisa y significativa sobre la eficacia de la estrategia de Seguridad de la Información.

### ☐ DOMINIO 2 - Gestión de riesgos de la información

Gestionar el riesgo de la información hasta reducirlo a un nivel aceptable, basado en el apetito de riesgo, con el fin de cumplir con los objetivos y las metas organizacionales.

***Declaraciones de tarea:***

- Establecer y/o mantener un proceso para la clasificación de activos de información, para garantizar que las medidas tomadas para proteger los activos sean proporcionales a su valor para el negocio.
- Identificar requisitos legales, normativos, organizacionales y otros requisitos aplicables, con el fin de gestionar el riesgo relacionado con sus incumplimientos y conseguir niveles de riesgo aceptables.
- Garantizar que las evaluaciones de riesgos, las evaluaciones de vulnerabilidades y los análisis de amenazas se lleven a cabo de forma coherente, en los momentos adecuados, para identificar y evaluar los riesgos sobre la información de la Organización.
- Identificar, recomendar o implementar opciones apropiadas de tratamiento/respuesta al riesgo, para gestionar los riesgos y reducirlos a niveles aceptables, basados en el apetito de riesgo de la Organización.
- Determinar si los controles de Seguridad de la Información son apropiados y eficaces para gestionar los riesgos y reducirlos a niveles aceptables.
- Facilitar la integración de la gestión de riesgos de la información con los procesos de negocio y de TI (por ejemplo, desarrollo de sistemas, adquisiciones, gestión de proyectos) para permitir un programa de gestión de riesgos de la información coherente y completo en toda la organización.
- Monitorear los factores internos y externos (p. ej., indicadores clave de riesgo [KRIs], panorama de amenazas, cambios normativos, geopolítica) que puedan requerir la reevaluación del riesgo para garantizar que los cambios en los escenarios de riesgos, nuevos o ya existentes, se identifiquen y gestionen de manera adecuada.
- Informar sobre incumplimientos y otros cambios en los riesgos de la información, para facilitar el proceso de toma de decisiones en la gestión de riesgos.
- Garantizar que los riesgos de Seguridad de la Información se informen a la Alta Dirección, con el fin de apoyar la comprensión de su impacto potencial en los objetivos y las metas organizacionales.

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

Desarrollar y mantener un programa de Seguridad de la Información que identifique, gestione y proteja los activos de la Organización, en conformidad con la estrategia de Seguridad de la Información y los objetivos de negocio, respaldando así una posición eficaz en materia de seguridad.

***Declaraciones de tarea:***

- Establecer y mantener un programa de Seguridad de la Información en línea con la estrategia de Seguridad de la Información.
- Alinear el programa de Seguridad de la Información con los objetivos operativos de otras funciones de negocio (por ejemplo, Recursos Humanos [RRHH], Contabilidad, Compras y TI) para garantizar que el programa de Seguridad de la Información añada valor al negocio y lo proteja.
- Identificar, adquirir y gestionar los recursos internos y externos requeridos para ejecutar el programa de Seguridad de la Información.
- Establecer y mantener procesos y recursos de Seguridad de la Información (incluidas personas y tecnologías) para ejecutar el programa de Seguridad de la Información, en línea con los objetivos de negocio de la Organización.
- Establecer, comunicar y mantener estándares, pautas, procedimientos y otra documentación organizacional sobre Seguridad de la Información, para guiar y reforzar el cumplimiento de las políticas de Seguridad de la Información.
- Establecer, promover y mantener un programa para la concienciación y formación sobre Seguridad de la Información, para promover una cultura eficaz en materia de seguridad.
- Integrar requisitos de Seguridad de la Información en los procesos organizacionales (p. ej., control de cambios, fusiones y adquisiciones, desarrollo de sistemas, continuidad de negocio, recuperación de desastres) para mantener la estrategia de seguridad de la Organización.
- Integrar requisitos de Seguridad de la Información en los contratos y las actividades de terceros (p. ej. empresas conjuntas, proveedores externos, socios, clientes) y supervisar el cumplimiento de los requisitos establecidos para mantener la estrategia de seguridad de la Organización.
- Establecer, supervisar y analizar la gestión de programas y parámetros operacionales para evaluar la eficacia y la eficiencia del programa de Seguridad de la Información.
- Compilar y presentar informes a las partes interesadas clave sobre actividades, tendencias y la eficacia general del programa de Seguridad de la Información y los procesos de negocio subyacentes, con el fin de comunicar a dichas partes el desempeño en materia de seguridad.

### ☐ 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 garantizar una respuesta oportuna a incidentes de Seguridad de la Información.
- Desarrollar e implementar procesos para garantizar la identificación temprana de incidentes de Seguridad de la Información que podrían impactar sobre el negocio.
- Establecer y mantener procesos para investigar y documentar los incidentes de Seguridad de la Información para determinar la respuesta apropiada y sus causas, manteniendo el alineamiento con los requisitos organizacionales, legales y normativos.
- Establecer y mantener procesos de notificación y escalado, para garantizar que las partes interesadas correspondientes estén involucradas en la gestión de la respuesta ante incidentes.
- Organizar, formar y dotar de recursos a equipos de respuesta ante incidentes, para responder a incidentes de Seguridad de la Información de manera oportuna y eficaz.
- Probar, revisar y adaptar (si procede) periódicamente el plan de respuesta a incidentes, para garantizar 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 eficacia de la respuesta y tomar las acciones correctivas apropiadas.
- Establecer y mantener la integración entre el plan de respuesta ante incidentes, el plan de continuidad de negocio y los planes de recuperación de desastres.