



# Certificaciones de Seguridad TI: un valor en alza

EN EL PRESENTE ARTÍCULO SE REVISAN LAS CARACTERÍSTICAS Y BENEFICIOS DE LAS CERTIFICACIONES DE SEGURIDAD TI, ANALIZANDO EN DETALLE LAS TRES MÁS EXTENDIDAS EN EL ÁMBITO ESPAÑOL: CISA Y CISM DE ISACA; Y CISSP DE (ISC)<sup>2</sup>.



**Jesús Romero**

GESTOR DE NEGOCIO  
SEGURIDAD TI  
INDRA

La Seguridad de las Tecnologías de la Información (Seguridad TI) es un área con un grado elevado de cambio y evolución, en la que aparecen cada día nuevas amenazas y vulnerabilidades que transforman los mapas de riesgos. De hecho, el propio proceso global de Gestión de la Seguridad de la Información de las organizaciones es perfilado como un proceso cíclico y de mejora continua en las distintas aproximaciones metodológicas. En este escenario, es importante que los profesionales que trabajan en Seguridad TI no se estancan y mantengan vivo su proceso de adquisición y actualización de conocimientos.

Una de las posibles opciones para verificar si alguien dispone de ese conocimiento actualizado es recurrir a una entidad, preferiblemente de ámbito internacional, que lo certifique. Si

además lo que deseamos es certificar un área de conocimiento, independientemente de tecnologías concretas o de sus productos relacionados, lo más lógico será recurrir a organismos o asociaciones independientes de cualquier fabricante.

Las certificaciones así planteadas aportan algunos beneficios interesantes:

**En el mercado existen diferentes certificaciones, cada una con sus propios requerimientos y áreas de conocimientos**

■ Definen un conjunto de requerimientos mínimos —años de experiencia, conocimientos específicos, horas mínimas anuales de formación continua, etc.— necesarios para el ejercicio de la profesión. En este sentido podríamos decir que las certificaciones son una condición necesaria aunque no suficiente para el profesional de Seguridad TI.

■ Los programas de certificación son un mecanismo interesante para establecer un vocabulario común para los principales conceptos y principios de la profesión, lo cual es importante si tenemos en cuenta el mencionado carácter cambiante y evolutivo de la misma.

■ La profesión de Seguridad TI carece, a diferencia de otras profesiones, de un código ético o deontológico consolidado. Al certificarse, los profesionales aceptan un código ético, pudiéndoles ser revocada la certificación si existieran evidencias de un comportamiento contrario a dicho código.

Es importante volver a incidir en el carácter de condición necesaria y no suficiente de las certificaciones de Seguridad TI. Al igual que sucede en cualquier otra área de TI, el hecho de contar con una certificación no garantiza la excelencia profesional. Lo que se certifica es que dicho profesional cumple una serie de requerimientos mínimos en cuanto a conocimientos, experiencia y formación continua.

Lógicamente en el mercado existen diferentes certificaciones, cada una con sus propios requerimientos y áreas de conocimientos que el aspirante debe dominar para obtener la certificación. En los próximos apartados se analiza-



Habilidades y cualidades necesarias para la certificación.

rán las que en el momento de redacción de este artículo son las tres certificaciones más extendidas dentro del ámbito español: CISA, CISM y CISSP.

### Certified Information Systems Auditor (CISA)

La ISACA (Information Systems Audit and Control Association) otorga dos certificaciones: CISA (Certified Information Systems Auditor) y CISM (Certified Information Security Manager).

Desde su creación en 1978, el objetivo principal del programa CISA es, en palabras de la propia ISACA, certificar el conocimiento y experiencia de los profesionales en las áreas de auditoría, control y seguridad de los sistemas de información.

CISA es la certificación de seguridad TI que más profesionales mantienen en España debido a que aunque en un principio era de dominio exclusivo de auditores de TI, poco a poco se fue extendiendo a otros colectivos. A esta popularización ha contribuido significativamente el hecho de que CISA ha sido hasta hace pocos años la única certificación de seguridad de prestigio con capítulos locales de la asociación promotora y exámenes periódicos en territorio nacional.

ISACA agrupa el cuerpo de conocimientos asociados con esta certificación en siete dominios:

1. Gestión, planificación y organización de los Sistemas de Información
2. Infraestructura técnica y prácticas operacionales

3. Protección de los activos de la información
4. Recuperación de desastres y continuidad del negocio
5. Desarrollo, adquisición, implementación y mantenimiento de los Sistemas de Aplicaciones de Negocio
6. Evaluación del proceso del negocio y gestión del riesgo
7. El proceso de auditoría de los Sistemas de Información.

El examen CISA, del que desde el año pasado existen dos convocatorias anuales en junio y diciembre, se puede realizar en español, tiene cuatro horas de duración y consiste en un test de 200 preguntas en el que hay que elegir una de las cuatro opciones posibles. Para aprobar el examen es necesario obtener como mínimo una nota de 75



puntos sobre 100, según una escala corregida por ISACA para evitar el efecto de posibles enunciados ambiguos o preguntas no del todo claras.

Una vez aprobado el examen los aspirantes a CISA deben justificar con al menos cinco años de experiencia profesional (algunos de ellos convalidables por ciertos items, como titulaciones universitarias u otras experiencias en sistemas de información en auditoría, control o seguridad de los sistemas de información. Si el aspirante no dispusiera de dicha experiencia, ISACA da hasta cinco años después de la fecha del examen como plazo para acumularla.

Además para mantener la certificación en el tiempo es necesario justificar un mínimo de 20 horas anuales y 120 horas cada tres años, de formación continua en cursos, seminarios, eventos, charlas, etc. relacionados con la materia.

Al igual que las otras dos certificaciones, la certificación CISA está acreditada por el American National Standards Institute (ANSI) bajo la norma ISO/IEC 17024:2003 (General Requirements for Bodies Operating Certification Systems of Persons).

Para más información sobre la certificación o sobre la propia ISACA, se puede consultar el sitio Web de la asociación: <http://www.isaca.org>

### Certified Information Security Manager (CISM)

La otra certificación de la ISACA, Certified Information Security Manager (CISM) es la más reciente de las tres analizadas y reconoce los conocimientos y experiencia en la gestión («management») de la Seguridad TI.

Debido a lo reciente de su lanzamiento el programa pasó inicialmente por un periodo de «abuelazgo» (grandfathering) en el que para la creación de una masa crítica inicial de

profesionales se le otorgó la certificación CISM a aquellos que demostraron poseer un mínimo de ocho años de experiencia en la gestión de Seguridad TI. Dicho periodo se cerró a finales del 2003, fecha a partir de la cual comenzaron las convocatorias de exámenes.

En la actualidad, la certificación CISM se está consolidando en todo el mundo como la certificación estándar para los profesionales dedicados a gestionar la Seguridad TI para alinearla con los objetivos de negocio de su organización, por lo que es la certificación idónea para directivos y mandos intermedios que trabajan en Seguridad.

**CISM es la más reciente de las tres analizadas y reconoce los conocimientos y experiencia en la gestión [«management»] de la Seguridad TI.**

Los dominios en los que ISACA agrupa el cuerpo de conocimientos asociados con esta certificación son los cinco siguientes (entre paréntesis, una posible traducción del nombre oficial en inglés):

1. *Information Security Governance* (Gobierno de la Seguridad de la Información)
2. *Risk Management* (Gestión del Riesgo)
3. *Information Security Program(me) Management* (Gestión del Plan Director de Seguridad)
4. *Information Security Management* (Gestión de la Seguridad de la Información)

### 5. *Response Management* (Gestión de Respuestas)

Por lo demás, el examen es similar al descrito para la certificación CISA: desde el año pasado existen dos convocatorias anuales en junio y diciembre, tiene cuatro horas de duración, consiste en un test de 200 preguntas en el que es válida una de las cuatro opciones posibles y para aprobarlo es necesario obtener como mínimo una nota de 75 puntos sobre 100, según la escala corregida por ISACA.

Hasta la fecha todas las convocatorias de examen han sido en inglés, aunque a partir de la próxima convocatoria, junio de 2006, los candidatos podrán examinarse en español.

Una vez aprobado el examen los candidatos tienen que justificar un mínimo de cinco años de experiencia profesional en Seguridad TI y un mínimo de tres en gestión de Seguridad TI. Al igual que ocurría para la certificación CISA, alguno de esos años es convalidable por ciertos items. Si el aspirante no dispusiera de dicha experiencia, tiene un plazo de hasta cinco años después de la fecha del examen para acumularla.

Para mantener la certificación en el tiempo es necesario justificar un mínimo de 20 horas anuales y 120 horas cada tres años, de formación continua.

Al igual que las otras dos certificaciones, la certificación CISM está acreditada por el American National Standards Institute (ANSI) bajo la norma ISO/IEC 17024:2003 (General Requirements for Bodies Operating Certification Systems of Persons).

### Certified Information Systems Security Professionals (CISSP)

El consorcio (ISC)<sup>2</sup>, International Information Systems Security Certification Consortium, otorga la certificación CISSP (Certified



Requisitos para la certificación.



Information Systems Security Professionals), que desde 1989 el estándar profesional y la certificación de Seguridad TI más reconocida a nivel internacional.

Aunque CISPP es una de las certificaciones más populares en nuestro país, el programa no ha tenido hasta la fecha una penetración acorde a la del panorama internacional debido sobre todo a la escasez de exámenes locales (por ejemplo, en el momento de redacción de este artículo no hay ningún examen programado en Madrid para el 2006) y a la inexistencia de cursos para la preparación a fondo de los candidatos.

El (ISC)<sup>2</sup> estructura los conocimientos asociados a la certificación en lo

que denomina el «Cuerpo Común de Conocimiento» (Common Body of Knowledge, CBK) que abarca los diez

**Una vez aprobado el examen los aspirantes a CISA deben justificar con al menos cinco años de experiencia profesional**

dominios siguientes (entre paréntesis, una posible traducción del nombre oficial en inglés):

1. *Access Control Systems and Methodology* (Sistemas de Control de Acceso y Metodología)
2. *Applications and Systems Development Security* (Seguridad en el Desarrollo de Sistemas y Aplicaciones)
3. *Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)*. (Planes de Continuidad del Negocio y de Recuperación ante Desastres).
4. *Cryptography* (Criptografía)
5. *Law, Investigation and Ethics* (Normativa, investigación y ética)
6. *Operations Security* (Seguridad de Operaciones)
7. *Physical Security* (Seguridad Física)
8. *Security Architecture and Models* (Arquitectura y modelos de Seguridad)



**9. Security Management Practices**  
(Prácticas de Gestión de la Seguridad de la Información)

**10. Telecommunications and Network Security** (Seguridad en redes y Telecomunicaciones)

Como se puede comprobar, el programa CISSP es el de contenidos más amplios de los tres analizados, cubriendo desde temas muy técnicos hasta aspectos de la gestión de la Seguridad; y pasando por aspectos tan específicos como la Seguridad Física. De hecho, los contenidos de los

**Desde 1989 la certificación CISSP es el estándar profesional y la certificación de Seguridad TI más reconocida a nivel internacional.**

programas CISA y CISM tienen algunos solapamientos con los de CISSP, aunque ambos se focalizan mucho más en la perspectiva del negocio que en las tecnologías de seguridad.

#### Para más información:

- **Fundación DINTEL**  
<http://www.dintel.org>
- **Certificaciones CISA y CISM**  
<http://www.isaca.org>
- **Certificación CISSP**  
<http://www.isc2.org>

**JESÚS ROMERO, es**  
Director del Área CISM de ÉTICA

Como diferencia fundamental entre las tres certificaciones se puede destacar que CISSP es una certificación generalista, de «espectro amplio», mientras que CISA y CISM están enfocadas a la Auditoría y la Gestión de Seguridad respectivamente.

A diferencia de las certificaciones de ISACA, la experiencia es requisito previo para acceder al examen CISSP. En concreto es necesario disponer de un mínimo de cuatro años de experiencia (alguno de ellos convalidables por ciertos items) en tareas relacionadas con uno o más de los diez dominios del CBK.

El examen CISSP se realiza en inglés, tiene seis horas de duración y consiste en un test de 250 preguntas. Para aprobar el examen es necesario obtener como mínimo una nota de 700 puntos sobre 1000, según escala corregida por (ISC)<sup>2</sup>.

Como curiosidad y a diferencia de lo que ocurre en los exámenes en inglés de las certificaciones de ISACA, con objeto de facilitar la traducción se permite el uso de diccionarios en papel (no se permite ningún tipo de diccionario electrónico).

Una vez aprobado el examen, un profesional certificado CISSP deberá corroborar la experiencia profesional el candidato. Al igual que en las certificaciones de la ISACA para mantener la certificación se exige justificar la formación continua, en este caso cada profesional tiene que conseguir 120 créditos de «formación profesional continua» (CPE) cada tres años, conseguibles mediante cursos, seminarios, eventos, charlas, etc. relacionados con la materia.

Al igual que las dos certificaciones de ISACA, la certificación CISSP está acreditada por el American National Standards Institute (ANSI) bajo la norma ISO/IEC 17024:2003 (General Requirements for Bodies Operating Certification Systems of Persons). ♦

## CONCLUSIONES

**A** la hora de acreditar conocimientos y experiencia en el área de Seguridad TI, es recomendable recurrir a las certificaciones de entidades independientes y de ámbito internacional. Dichas certificaciones, cada vez de mayor utilidad para los distintos actores de nuestra industria, definen los conjuntos de requerimientos profesionales mínimos, establecen un lenguaje común para la profesión y fijan códigos éticos de comportamiento.

En el mercado existen diferentes certificaciones, siendo las más extendidas dentro del ámbito español CISA y CISM de ISACA; y CISSP de (ISC)<sup>2</sup>. Como diferencia fundamental entre las tres certificaciones se puede destacar que CISSP es una certificación generalista, de «espectro amplio», mientras que CISA y CISM están enfocadas en la Auditoría y al «Management» de Seguridad, respectivamente.

No quiero concluir este artículo sin incidir una vez más en el carácter de condición necesaria pero no suficiente de las certificaciones. El hecho de certificar el conocimiento y la experiencia es importante, pero no garantiza la excelencia profesional.

En definitiva, no es recomendable considerar las certificaciones como factor único a la hora de evaluar a un profesional, ya que éstas nunca podrán reemplazar el valor aportado por una titulación universitaria de carácter técnico, o el conocimiento acumulado por la propia experiencia profesional.