UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

PROYECTO DE FIN DE CARRERA

INGENIERÍA TÉCNICA EN INFORMÁTICA DE SISTEMAS

ESTUDIO DE LA OFERTA DE CERTIFICACIONES EN SEGURIDAD INFORMÁTICA

AUTORA: Dña. María del Mar Martínez Contreras

Julio de 2016

TUTOR: D. Jorge Ramió Aguirre

DEPARTAMENTO DE SISTEMAS INFORMÁTICOS

BREVE CURRICULUM VITAE DE LA AUTORA

María del Mar Martínez es Ingeniera Técnica en Informática de Sistemas por la Universidad Politécnica de Madrid. Comenzó a trabajar en el año 2003 en la empresa Grupo Delaware como Consultora Junior en un proyecto de Gestión de Configuración de Software para Orange. En el año 2012, ya como Consultora Senior, pasó a ser Jefe de Equipo. En el año 2014 pasó a realizar tareas de gestión de software y pruebas en un proyecto para TGT (Telefónica Global Technology). En la actualidad desarrolla su carrera profesional en la misma empresa realizando tareas de pruebas y calidad de software.

NOTA DEL DIRECTOR DE LA TESIS

El trabajo realizado por María del Mar, consistente en la recopilación de información sobre las más importantes certificaciones de seguridad informática, se encuentra dentro del marco del proyecto MESI, Mapa de Enseñanza de la Seguridad de la Información, dando con ello cumplimiento a una de las 7 fases de dicho proyecto:

1. Enseñanzas básicas en edades tempranas
2. Concienciación y formación a la sociedad
3. Enseñanza universitaria
4. Formación profesional no universitaria
5. Certificaciones profesionales
6. Perfiles profesionales y mercado laboral
7. Investigación, desarrollo e innovación

Han sido muchos meses de intenso y fructífero trabajo, que han dado como fruto este documento que seguro será de gran utilidad para aquellos profesionales de la seguridad que deseen obtener algunas de estas certificaciones, como todos sabemos muy demandadas y reconocidas en el ámbito laboral.

Como toda investigación, es posible que este trabajo no cubra la totalidad del espectro que podría tener. Sin embargo, el objetivo propuesto y alcanzado en este proyecto consistía en abordar los aspectos más importantes de estas certificaciones y dejarlas plasmadas en un único documento, para su libre consulta.

Este trabajo se hace público con el consentimiento de su autora.

Madrid, septiembre de 2016

Dr. Jorge Ramió Aguirre (tutor del Proyecto Fin de Carrera)

IMPORTANTE: Recuerde que la mayoría de los datos y las referencias que aparecen en este documento están actualizados al primer semestre de 2016.

ÍNDICE

1 INTRODUCCIÓN: CERTIFICACIONES DE SEGURIDAD

El mundo de la seguridad informática ha ido creciendo en los últimos años a pasos agigantados, a medida que ha ido creciendo el uso de Internet en la población y las empresas y el número de intercambios de información entre ordenadores a través de dicha red global.

Según el estudio del INE "*Encuesta sobre el Equipamiento y Uso de Tecnologías de la Información y Comunicación en los Hogares y Encuesta de uso de TIC y comercio electrónico en las empresas*" [1], el comercio electrónico en España ha crecido sin descanso en los últimos años. Según este estudio, en 2013 el 68.9 % de los hogares españoles poseen conexión a Internet, y cerca de 11 millones de personas han realizado algún tipo de compra a través de la web durante el mismo año en España. Los servicios más utilizados por particulares en Internet se muestran en la figura 1.1.

Figura 1.1. Servicios de Internet usados por particulares.
Fuente: INE. Encuesta sobre el Equipamiento y Uso de Tecnologías de la Información y Comunicación en los Hogares y Encuesta de uso de TIC y comercio electrónico en las empresas. [1].

A nivel empresarial, el 98.0% de la empresas españolas de 10 o más empleados dispone de conexión a Internet en enero de 2013. Esto supone que el porcentaje de empresas que tienen acceso a Internet ha aumentado en un 8,9% desde el año 2005. De las empresas conectadas a Internet, prácticamente la totalidad de ellas (98,5%) lo hacen mediante banda ancha fija. Por otro lado, aproximadamente el 72% de las empresas dispone de sitio/página web. Dada la transcendencia de las TIC en el desarrollo del ámbito de los negocios, los especialistas en TIC cobran cada vez más peso en el personal de las empresas.

La red Internet es una red pública, por lo que el riesgo de que las amenazas contra la autenticidad, integridad, confidencialidad y el número de transacciones que sobre ella se realicen será mayor. Los mayores problemas de seguridad pueden provenir de virus informáticos, hackers que pueden realizar ataques informáticos, con el objetivo de dejar sin servicio los sistemas de grandes organizaciones o empresas o para el robo de datos personales de clientes o empleados, así como por el robo y usurpación de identidades personales, muchas veces favorecido por el desconocimiento de las normas básicas de seguridad en la red por parte de usuarios sin conocimientos informáticos.

La mayoría de ataques informáticos e infecciones de virus y troyanos que se producen, se realizan a través de vulnerabilidades de seguridad en los sistemas operativos y programas más empleados. Como ejemplo, en la figura 1.2 se muestran las aplicaciones cuyas vulnerabilidades fueron las más utilizadas por los ataques informáticos basados en *exploits* (programas o partes de programas que tratan de forzar deficiencias de los sistemas, normalmente para acceder a ellos de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros), según un estudio realizado por Kaspersky entre los usuarios de sus productos en el año 2012 (*Kaspersky Security Bulletin*) [2].

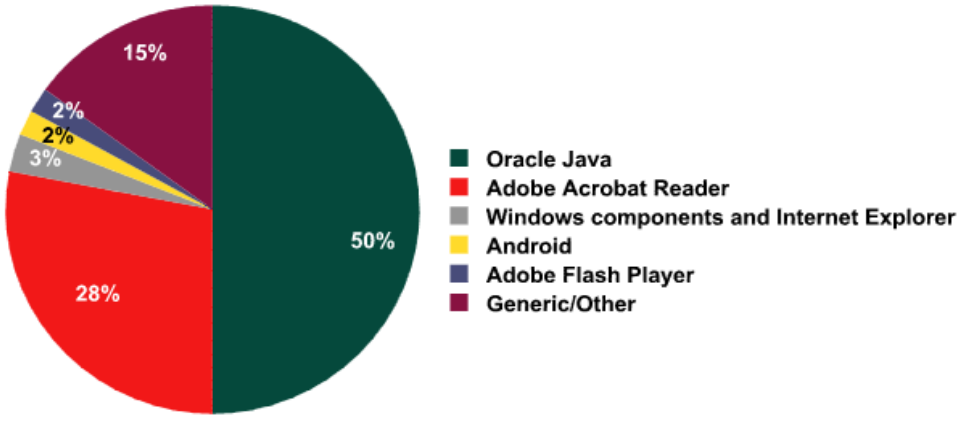

Figura 1.2. Aplicaciones cuyas vulnerabilidades usaron los exploits web.
Fuente: Kaspersky Security Bulletin [2].

En este ámbito, se busca un estándar que establezca las competencias y habilidades requeridas para los profesionales de la seguridad informática. La consultoría en seguridad informática debe mantener un equilibrio entre la experiencia práctica, la innovación y la teoría.

Estos son algunos de los más importantes servicios de seguridad informática:

- Evaluación de riesgos y controles.
- Auditorías de seguridad informática.
- Pruebas de penetración (*hacking* ético).
- Desarrollo de políticas de seguridad informática.
- Informática forense.
- Arquitecturas de seguridad.
- Detección y control de fraude.
- Desarrollo y mantenimiento del software de seguridad.
- Control de acceso.
- Investigación, desarrollo y actualizaciones en seguridad informática.
- Aplicación de las mejores prácticas internacionales en seguridad informática.
- Instalación de productos de seguridad.

En la actualidad, las certificaciones son la mejor manera de demostrar una especificación en determinados campos de las Tecnologías de la Información (TI). Son una estrategia utilizada por la industria para establecer un estándar de formación y habilidades requeridas en seguridad. Todo profesional de seguridad debe recurrir a certificaciones que avalen su conocimiento y experiencia, a nivel nacional e internacional. Las empresas están empezando a solicitar este aval para sus profesionales de cargos gerenciales. Un profesional de seguridad que aspire a altos puestos debe estar capacitado para entender las necesidades del negocio, administrar formas de control y de riesgo, y brindar las mejores alternativas para la continuidad del negocio, protegiendo los activos de la organización. Las certificaciones no reemplazan la formación universitaria, sino que refuerzan habilidades y perfiles según los objetivos y deseos de los candidatos y orientan hacia un desarrollo profesional. Muestran el deseo de los profesionales de mantenerse actualizados.

Posiblemente en la disciplina de la seguridad sea donde nos encontramos el mayor número de certificaciones que regulan el mercado de la TI. Existe gran cantidad de documentación a este respecto en las siguientes referencias [3] [4] [5] [6] [7].

En este estudio se va a realizar la clasificación de dichas certificaciones, acorde con la especialidad en las que son demandadas, datos estadísticos de profesionales certificados, oportunidades de trabajo que se abren con ellas y toda la información necesaria para las personas que deseen certificarse, como empresas y asociaciones que las proporcionan, tipos de exámenes, entre otras.

En cuanto a la clasificación de las certificaciones, el enfoque de unas y otras es completamente distinto y su contenido también. Algunas están centradas en garantizar unos mínimos conocimientos en una tecnología concreta, en cambio otras se centran en metodología y conceptos genéricos de seguridad.

Antes de decidir qué certificado obtener, es imprescindible saber cuál es el objetivo que se persigue, ya que unas están enfocadas a tareas de implantación, configuración o mantenimiento de plataformas, mientras que otras están enfocadas a la consultoría y auditoría en general.

En España, además, también existe el Certificado de Profesionalidad en Seguridad Informática [8]. Se trata de un título oficial, que acredita las competencias profesionales en el ámbito laboral, del mismo modo que los Títulos de Formación Profesional lo hacen en el ámbito educativo. La formación profesional para el empleo tiene como finalidad que los trabajadores ocupados y desempleados adquieran competencias profesionales a lo largo de su vida profesional.

A continuación se enumeran en las siguientes figuras (de la 1.3 a la 1.10), algunas de las certificaciones más conocidas y demandadas en el mercado laboral de la seguridad, ordenadas según las empresas y asociaciones que las proporcionan.

(ISC)^2
CAP: Certified Authorization Professional
CCFP: Certified Cyber Forensics Professional
CISSP: Certified Information Systems Security Professional
CISSP-ISSAP: Information Systems Security Architecture Professional
CISSP- ISSEP: Information Systems Security Engineering Professional
CISSP- ISSMP: Information Systems Security Management Professional
CSSLP: Certified Secure Software Lifecycle Professional
SSCP: Systems Security Certified Practitioner

Figura 1.3. Certificaciones (ISC)^2.
Fuente: (ISC)^2 [9].

ISACA
CISM: Certified Information Security Manager
CISA: Certified Information Systems Auditor
CGEIT: Certified in the Governance of Enterprise IT
CRISC: Certified in Risk and Information Systems Control

Figura 1.4. Certificaciones ISACA.
Fuente: ISACA [10].

GIAC +
GSEC: GIAC Security Essentials (Security Administration)
GCFA: GIAC Certified Forensics Analyst (Forensic)
GSLC: GIAC Security Leadership (Management)
GSNA: GIAC Systems and Network Auditor (Audit)
Software Security GSSP-JAVA: GIAC Secure Software Programmer-Java
GWEB: GIAC Certified Web Application Defender
GSSP-.NET: GIAC Secure Software Programmer- .NET
Legal GLEG: GIAC Law of Data Security & Investigations

Figura 1.5. Certificaciones GIAC.
Fuente: GIAC [11].

EC COUNCIL
CEH: Certified Ethical Hacker
CHFI: Computer Hacking Forensics Investigator
ENSA: EC-Council Network Security Administrator
ECSA: EC-Council Certified Security Analyst
ECSP: EC-Council Certified Secure Programmer
EDRP: EC-Council Disaster Recovery Professional

Figura 1.6. Certificaciones EC Council.
Fuente: EC Council [12].

CompTIA Security +
CompTIA Advanced Security Practitioner (CASP)
CompTIA Mobile App Security+
SMSP Social Media Security Professional
CompTIA Security+

Figura 1.7. Certificaciones CompTIA.
Fuente: CompTIA [13].

ISMS FORUM SPAIN
CDPP: Certified Data Privacy Professional
CCSK: Certificate Of Cloud Security Knowledge

Figura 1.8. Certificaciones ISMS.
Fuente: ISMS [14].

ISECOM
OPST: Professional Security Tester
OPSA: Professional Security Analyst Accredited Certification
OPSE: Professional Security Expert Accredited Certification
OWSE: Wireless Security Expert
CTA: Certified Trust Analyst

Figura 1.9. Certificaciones ISECOM.
Fuente: ISECOM [15].

MILE2
CPTE: Certified Penetration Testing Engineer
CPTC: Certified Penetration Testing Consultant
CCISO: Chief Information Security Officer
CDFE: Certified Digital Forensic Examiner (GESTION)
CNFE: Certified Network Forensic Examiner
CSWAE: Certified Secure Web Application Engineer

Figura 1.10. Certificaciones MILE 2.
Fuente: MILE2 [16].

OTRAS
CPP: Certified Protection Professional
PSP: Physical Security Professional
MCSE: MICROSOFT Security on Windows

Figura 1.11. Otras certificaciones.

El mercado de las certificaciones va avanzando a pasos agigantados. En la actualidad están apareciendo nuevas certificaciones de seguridad. Sólo a modo de ejemplo, citaremos a continuación las certificaciones propuestas por Deloitte [17] y su centro de operaciones de seguridad CyberSOC. Esta multinacional ofrece las siguientes certificaciones a través de los programas de formación de Buguroo [18]:

- B-CEHA, Buguroo Certified Ethical Hacking Associate, basada en las tecnologías y métodos utilizados en el hacking ético para la realización de test de penetración y auditorías de seguridad.
- B-CFIA, Buguroo Certified Forensic Investigator Associate, que proporciona las capacidades necesarias para obtener, mantener y procesar evidencias digitales, a través de herramientas y procedimientos específicos.
- B-CSPA, Buguroo Certified Secure Programmer Associate, orientada al desarrollo de aplicaciones seguras.

En el siguiente apartado se hará una presentación de las empresas y asociaciones que proporcionan cada una de las certificaciones mencionadas.

2 EMPRESAS Y ASOCIACIONES

Hay diferentes empresas y asociaciones que proporcionan las diversas certificaciones de seguridad. Se dedican fundamentalmente a preparar y proporcionar los medios para obtener los requerimientos que se necesitan para certificarse.

La mayoría de estas asociaciones son norteamericanas aunque algunas tienen sedes en España.

2.1 (ISC)²

El Consorcio internacional de Certificación de Seguridad de Sistemas de Información o (ISC)² (del inglés *International Information Systems Security Certification Consortium*), es una organización sin ánimo de lucro con sede en Palm Harbor, Florida, que educa y certifica a los profesionales de la seguridad de la información. (ISC)² fundada en 1989, ha certificado a cerca de 110.000 profesionales de 135 países, y cuenta con oficinas en Londres, Hong Kong y Tokio. La certificación más extendida ofrecida por la organización es la de Profesional Certificado en Sistemas de Seguridad de la Información (CISSP).

Su objetivo es "*hacer del mundo cibernético un lugar de seguridad, a través del apoyo y el desarrollo de la seguridad de información para profesionales alrededor del mundo"*, según indican en su web.

Todas las certificaciones se basan en el (ISC)² CBK (*Common Body of Knowledge*), que es un compendio de temas de interés para los profesionales de seguridad de la información. Establece un marco común de términos y de temas de seguridad de la información que permite a los profesionales discutir, debatir y resolver los asuntos relacionados con la profesión, dentro de un marco de entendimiento global.

Aunque los requisitos varían de certificación a certificación, como por ejemplo, un mínimo número de años de experiencia laboral, todos los candidatos que desean obtener sus certificaciones deben pasar un riguroso examen, deben ser avalados por un miembro actual de la asociación y adherirse al Código de Ética de (ISC)², así como obtener un número determinado de créditos *CPE (Continuing Professional Education*- Educación Profesional Continua*)* para mantener los conocimientos y habilidades adquiridas, relacionadas con la vida profesional, y que se pueden obtener a través de asistencia a congresos, formación o seminarios.

2.2 ISACA

ISACA es el acrónimo de *Information Systems Audit and Control Association*, una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

Tal y como se indica en su web, "con más de 140.000 integrantes (entre miembros de la Asociación y aquellos que no son miembros, pero ostentan una o más certificaciones de ISACA) en 180 países, ISACA (www.isaca.org) ayuda a empresas y líderes de tecnologías de la información a maximizar su potencial, además de gestionar riesgos relacionados con la información y la tecnología".

ISACA fue fundada en el año 1967 cuando un grupo de auditores en sistemas informáticos percibieron la necesidad de centralizar la información y la metodología en el área de la auditoría de las tecnologías de la información. Fue en 1969 que el grupo se formalizó creando originalmente la *EDP Auditors Association*. En 1976 la asociación creó una fundación educativa para expandir el conocimiento y el valor de la gestión de las TIs, conocida como *Information Systems Audit and Control Association* (ISACA), por el que es actualmente conocida, y se estableció la primera certificación profesional de auditoría de sistemas de información, CISA.

Es una organización independiente, sin ánimo de lucro, que representa los intereses de los profesionales relacionados con la seguridad de la información, aseguramiento, gestión de riesgos y mantenimiento de las TIs. Estos profesionales confían en ISACA como fuente de conocimiento sobre la información y la tecnología, los estándares y las certificaciones, según se indica en su página web.

ISACA tiene actualmente asociados en más de 180 países, entre los que se encuentra España. Los cargos de sus miembros son tales como auditor, consultor, educador, profesional de seguridad, regulador, director ejecutivo de información y auditor interno. Trabajan en casi todas las categorías de la industria. Esta diversidad permite a los miembros a aprender unos de otros e intercambiar puntos de vista ampliamente divergentes sobre una gran variedad de temas profesionales.

Cuenta con más de 200 delegaciones establecidas en más de 80 países en todo el mundo, y en dichas sucursales se proporciona la educación, el intercambio de recursos, la promoción y la creación de redes profesionales, entre otros beneficios.

En España existen tres delegaciones de ISACA en tres diferentes ciudades: Madrid, Barcelona y Valencia.

ISACA Internacional otorgó la consideración de Delegación de Madrid (lo que en su web denominan *Chapter* Madrid) a la Asociación de Auditores y Auditoría y Control de Sistemas y Tecnologías de la Información y las Comunicaciones (ASIA), actualmente ISACA Madrid, el día 7 de marzo de 2004.

Nació en abril de 2002, del interés de un nutrido grupo de profesionales, que deseaban contribuir a la calidad y excelencia de la gestión de los sistemas de información y a las tecnologías de la información y las comunicaciones en España. En estos años, ha desarrollado una importante labor de formación y divulgación, así como de desarrollo de aspectos profesionales y de prestación de servicios a sus afiliados. Actualmente ISACA Madrid está compuesta por más de 1000 asociados.

La Delegación de Barcelona se creó el año 2001, con 21 asociados y en la actualidad tiene más de 350 asociados.

En la figura 2.1 se muestran las cuatro certificaciones de ISACA.

Figura 2.1: Certificaciones de ISACA.
Fuente: ISACA [10].

2.3 GIAC - SANS INSTITUTE

GIAC son las siglas de *Global Information Assurance Certification*. Desde el año 2002, ha emitido 76.558 certificaciones, según se indica en su web, y ofrece más de 20 certificaciones especializadas en seguridad, informática forense, pruebas de penetración y la seguridad de aplicaciones web, auditoría y gestión.

Se pueden obtener las certificaciones GIAC a través del Sans Institute.

El *SANS Institute* se fundó en 1989 en EE.UU como una cooperativa de investigación y una organización educativa. Sus programas ahora llegan a más de 165.000 profesionales de la seguridad de todo el mundo. Sus miembros, desde auditores hasta administradores de redes, comparten los conocimientos que aprenden y buscan conjuntamente soluciones a los desafíos a los que se enfrentan.

SANS, con sede en Reino Unido, es una gran fuente de formación en seguridad. También desarrolla, mantiene y pone a disposición de sus miembros, una gran colección de documentos de investigación sobre diversos aspectos de la seguridad de la información.

2.4 EC-COUNCIL

El EC-Council (*International Council of Electronic Commerce Consultants*) es un líder global proveedor de formación en seguridad, según se indica en su web. Con más de 500 socios en más de 92 países y unos 60.000 certificados, profesionales y estudiantes por igual pueden tener acceso a la formación necesaria y a los servicios de educación y apoyo que proporciona el EC-Council.

En España se pueden obtener las certificaciones de CEH: *Certified Ethical Hacker* y ENSA: *EC-Council Network Security Administrator* a través del *IT Institute*.

El EC-Council ha sido acreditado por el ANSI (*American National Standards Institute*) por cumplir con los estándares "*ANSI/ISO/IEC 17024 Personnel Certification Accreditation Standard"* por su certificación Certified Ethical Hacker (CEHv8).

ANSI (*American National Standards Institute*) es una organización privada sin ánimo de lucro que administra y coordina la estandarización voluntaria de los Estados Unidos y su sistema de evaluación y conformidad. Es el único representante tanto de la ISO *(International Organization for Standardization*) como de IEC (*International Electro-technical Comission*) y el único organismo de certificación en EEUU ya que sus prácticas son nacionalmente aceptadas por organismos de acreditación (el estándar ANSI/ISO/IEC17024 indica los requerimientos generales para las entidades de certificación).

Para poder conseguir la acreditación, ANSI llevó a cabo un proceso de verificación para asegurar que EC-Council es imparcial y objetivo como una entidad certificadora. También confirmó que los procesos de certificación de EC-Council son realizados en manera consistente, segura y confiable.

2.5 COMPTIA+

La Asociación de la Industria de Tecnología de Computación (*Computing Technology Industry Association* - CompTIA) es una organización sin ánimo de lucro fundada en 1982 en EEUU, y que se dedica a la certificación de profesionales para la industria de tecnologías de información.

La certificación CompTIA+ Security+, es una de las certificaciones de seguridad que proporciona. Su temática está relacionada con criptografía y control de acceso. Actualmente, y de acuerdo a CompTIA, hay más de 23.000 personas en el mundo que se han certificado con esta modalidad.

2.6 ISECOM

ISECOM, *Institute for Security and Open Methodologies*, es una comunidad abierta de investigación y una organización sin ánimo de lucro, creada en enero de 2001, registrada oficialmente en Cataluña, España. ISECOM cuenta con oficinas en Barcelona (España) y en Nueva York (EE.UU). Su objetivo es aportar información en la práctica de la seguridad, para la investigación, la certificación y la integridad de los negocios. ISECOM ofrece programas de formación y estándares.

En enero del 2001, publicó el OSSTMM (*Open Source Security Testing Methodology Manual),* es decir, un manual de metodologías de pruebas para seguridad en código abierto. Fue una manera de mejorar el modo en el que se implementa y se prueba la seguridad.

Ofrece entre otras certificaciones la OPST *Professional Security Tester*.

2.7 MILE 2

Mile2 es un proveedor de certificaciones profesionales de la industria de la seguridad cibernética, cuya sede se encuentra en Tampa, Florida (EEUU)

Sus cursos de certificación enseñan los principios fundamentales de la seguridad cibernética y desarrollan habilidades para la realización de pruebas de penetración, la recuperación de desastres, manejo de incidentes y análisis forense de las redes.

Está avalado por el CNSS (*Committee on National Security Systems*) y por la NSA (*National Security Agency*), cuya misión es proteger los sistemas de seguridad nacional de los Estados Unidos.

Una de sus certificaciones más importantes es CCISO (*Chief Information Security Officer*).

2.8 ISMS

ISMS Forum Spain (Asociación Española para el Fomento de la Seguridad de la Información), es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de toda la comunidad implicada en el sector, tal y como se explica en su web. Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información. Toda su actividad se desarrolla en base a los valores de transparencia, independencia, objetividad y neutralidad, según se indica en su web.

En la actualidad tiene a más de 120 empresas asociadas y más de 800 profesionales asociados. Según su propia definición, "l*a Asociación es ya la mayor red activa de organizaciones y expertos comprometidos con la Seguridad de la Información en España"*.

Sus objetivos son impulsar el conocimiento e implementación de los Sistemas de Gestión de la Seguridad de la Información (SGSI) en España, de acuerdo con los estándares ISO 27000, en instituciones públicas y privadas, nacionales e internacionales, así como colaborar en la resolución de las problemáticas relacionadas con dichas normas ISO 27000. También son interlocutores en España de las diversas asociaciones y foros internacionales relacionados con la seguridad de la información.

Entre las iniciativas del ISMS se encuentra el DPI (*Data Privacy Institute*), que aglutina a personas y organizaciones españolas implicadas en el cumplimiento de normativa sobre Privacidad y Protección de Datos. El DPI organiza foros de debate sobre la privacidad y otras actividades como grupos de trabajo o cursos de formación y ha puesto en marcha la *Certified Data Privacy Professional* (CDPP), la primera certificación española dirigida a los profesionales de la privacidad.

Otro de los socios del ISMS es el *Cloud Security Alliance (*CSA-ES*)* que reúne a miembros representativos de la industria del *cloud computing* en España. Se trata de un foro de debate que promueve el uso de buenas prácticas para garantizar la seguridad y privacidad en el entorno del *cloud computing.*

CSA-ES contribuye al desarrollo de conocimiento en materia de seguridad y cumplimiento en la nube por medio de estudios y eventos propios, a la vez que promueve la guía de las mejores prácticas de seguridad cloud que publica el Cloud Security Alliance Global.

ISMS Forum y CSA-ES han impulsado la primera certificación profesional en castellano sobre Seguridad de la Información en Cloud Computing (*Certificate Of Cloud Security Knowledge (CCSK)).*

El ISMS tiene el Registro de Profesionales Certificados (RPC), que es un servicio público y gratuito dirigido a los profesionales que trabajan en seguridad de la información y a las empresas, organizaciones e instituciones que puedan necesitar de sus servicios.

3 CLASIFICACIÓN DE LAS CERTIFICACIONES DE SEGURIDAD

Podemos clasificar las certificaciones de seguridad según diferentes perfiles, que se muestran en la figura 3.1.

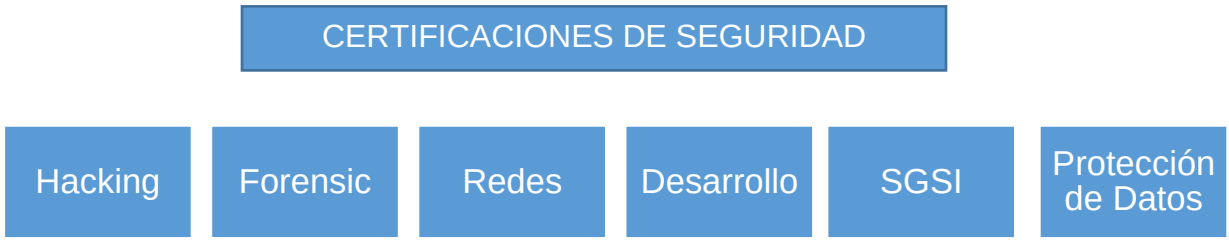

Figura 3.1: Clasificación de las certificaciones de seguridad.

3.1 HACKING

Hacking ético es una forma de referirse al acto de una persona de usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.

La idea es tener el conocimiento de qué elementos dentro de una red son vulnerables y corregirlo antes que ocurra un robo de información, un ataque de un *malware*, etc.

Estas pruebas se llaman "*pen tests"* o "*penetration tests*" en inglés. En español se conocen como "pruebas de penetración". Con ellas se intenta burlar de múltiples formas la seguridad de la red, para luego reportarlo y así mejorar dicha seguridad.

Es recomendable, por tanto, que empresas que vayan a contratar los servicios de un experto en hacking, soliciten personas certificadas, lo que asegura un conocimiento global de la materia y un reconocimiento a nivel mundial.

Las certificaciones de este tipo serían las siguientes:

- CEH, Certified Ethical Hacking (EC-Council).
- ECSA, EC-Council Certified Security Analyst (EC-Council).
- EDRP, EC-Council Disaster Recovery Professional (EC-Council).
- SMSP, Social Media Security Professional (CompTIA)
- OPST, Professional Security Tester (ISECOM).
- CPTE, Certified Penetration Testing Engineer (MILE 2)
- CPTC, Certified Penetration Testing Consultant (MILE 2).

3.2 SGSI (SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN)

El objetivo de un SGSI es proteger la información y para ello lo primero que debe hacer es identificar los 'activos de información' que deben ser protegidos y en qué grado.

Posteriormente debe aplicarse el plan PDCA (*'PLAN – DO – CHECK – ACT'*), es decir:

• Planificar, esto es, establecer el contexto en el que se crean las políticas de seguridad y el análisis de riesgos.

• Hacer, que consiste en implementar un sistema de gestión de seguridad de la información, mediante un plan de riesgos.

• Verificar, mediante la monitorización de las actividades y la realización de auditorías internas.

• Actuar, o lo que es lo mismo, ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y/o correctivas.

Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero sí se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad.

Un SGSI siempre cumple los cuatro niveles repetitivos, indicados anteriormente, y que comienzan por Planificar y terminan en Actuar, consiguiendo así mejorar la seguridad (figura 3.2).

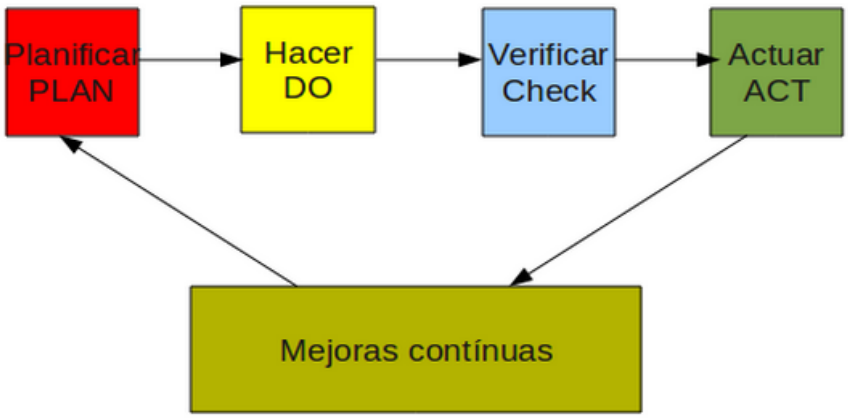

Figura 3.2: Pasos a seguir en un SGSI.
Fuente: http://recursostic.educacion.es/ [19].

El mayor número de certificaciones de seguridad son de gestión, ya que son las más completas y las que engloban mayor cantidad de conocimientos:

- CAP, Certified Authorization Professional ((ISC)^2).
- CISSP, Certified Information Systems Security Professional ((ISC)^2).
- CISSP-ISSMP, Information Systems Security Management Professional ((ISC)^2).
- SSCP, Systems Security Certified Practitioner ((ISC)^2).
- CISM, Certified Information Security Manager (ISACA).
- CISA, Certified Information Systems Auditor (ISACA).
- CRISC, Certified in Risk and Information Systems Control (ISACA).
- CGEIT, Certified in the Governance of Enterprise IT (ISACA).
- GIAC, Global Information Assurance Certification (GIAC).
- GSE GIAC Security Expert (GIAC).
- CompTIA Security+ Professional (CompTIA).
- CPP, Certified Protection Professional.
- OPSE, Professional Security Expert Accredited Certification (ISECOM).
- CTA, Certified Trust Analyst (ISECOM).
- CDFE, Certified Digital Forensic Examiner (MILE2).
- CCISO, Chief Information Security Officer (MILE 2).

3.3 REDES

En la actualidad la mayoría de las empresas dependen de las redes informáticas, y cualquier problema en ellas puede ocasionar grandes pérdidas. Los problemas de redes pueden venir tanto del exterior como del interior.

Las certificaciones relativas a la seguridad en las redes serían las siguientes:

- CISSP-ISSAP, Information Systems Security Architecture Professional ((ISC)^2).
- CISSP-ISSEP, Information Systems Security Engineering Professional ((ISC)^2).
- ENSA, EC-Council Network Security Administrator (EC-Council).
- OWSE, Wireless Security Expert (ISECOM).
- CompTIA Mobile App Security+ (CompTIA).

3.4 FORENSIC (INFORMÁTICA FORENSE)

La informática forense es la aplicación de técnicas científicas y analíticas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Estas técnicas incluyen examinar los datos residuales y autenticar información recabada, y ayudan a detectar pistas sobre ataques informáticos o robos de información.

Esta disciplina hace uso no sólo de tecnología de punta, sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas, para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. El examinador forense debe tener conocimientos, no sólo de software sino también de hardware, redes, seguridad, hacking, cracking, recuperación de información y debe utilizar procedimientos estrictos y rigurosos para la resolución de los delitos. Hay que tener en cuenta que la evidencia digital es muy frágil, con lo cual se necesita personal altamente cualificado, ya que dentro de un proceso legal puede ser necesario llegar a recuperar incluso información borrada de un sistema.

La informática forense está adquiriendo una gran importancia debido al aumento del valor de la información y/o al uso que se le da a ésta.

La informática forense tiene 3 objetivos fundamentales:

1º. La compensación de los daños causados por los criminales o intrusos.
2º. La persecución y procesamiento judicial de los criminales.
3º. La creación y aplicación de medidas para prevenir casos similares.

Las certificaciones de tipo forense son las siguientes:

- CCFP, Certified Cyber Forensics Professional ((ISC)^2).
- CHFI, Certified Hacking Forensic Investigator (EC-Council).
- CNFE, Certified Network Forensics Examiner (MILE 2).

3.5 DESARROLLO

Tiene como objetivo frenar la proliferación de las vulnerabilidades de seguridad que resultan de los procesos de desarrollo, estableciendo mejores prácticas y validando la competencia de un individuo para hacer frente a los problemas de seguridad durante todo el ciclo de vida del software y el desarrollo del mismo.

Las certificaciones de desarrollo son las siguientes:

- CISSLP, Certified Secure Software Lifecycle Professional ((ISC)[2]).
- ECSP, EC-Council Certified Secure Programmer (EC-Council).
- OPSA, Professional Security Analyst Accredited Certification (ISECOM).

3.6 PROTECCIÓN DE DATOS

La protección de datos es una disciplina jurídica de reciente creación que tiene por objeto proteger la intimidad y demás derechos fundamentales de las personas físicas frente al riesgo que para ellos supone la recopilación y el uso indiscriminado de sus datos personales, entendiendo como tales a toda aquella información que forma parte de su esfera privada y que puede ser utilizada para evaluar determinados aspectos de su personalidad (hábitos de compras, creencias, relaciones personales, etc.).

Se pueden considerar certificaciones de protección de datos las siguientes:

- CDPP, Certified Data Privacy Professional (ISMS).
- CCSK, Certificated of Cloud Security Knowledge (ISMS).

Se muestra a continuación, en las figuras 3.3 y 3.4 un resumen gráfico de las certificaciones de seguridad, según la clasificación anterior:

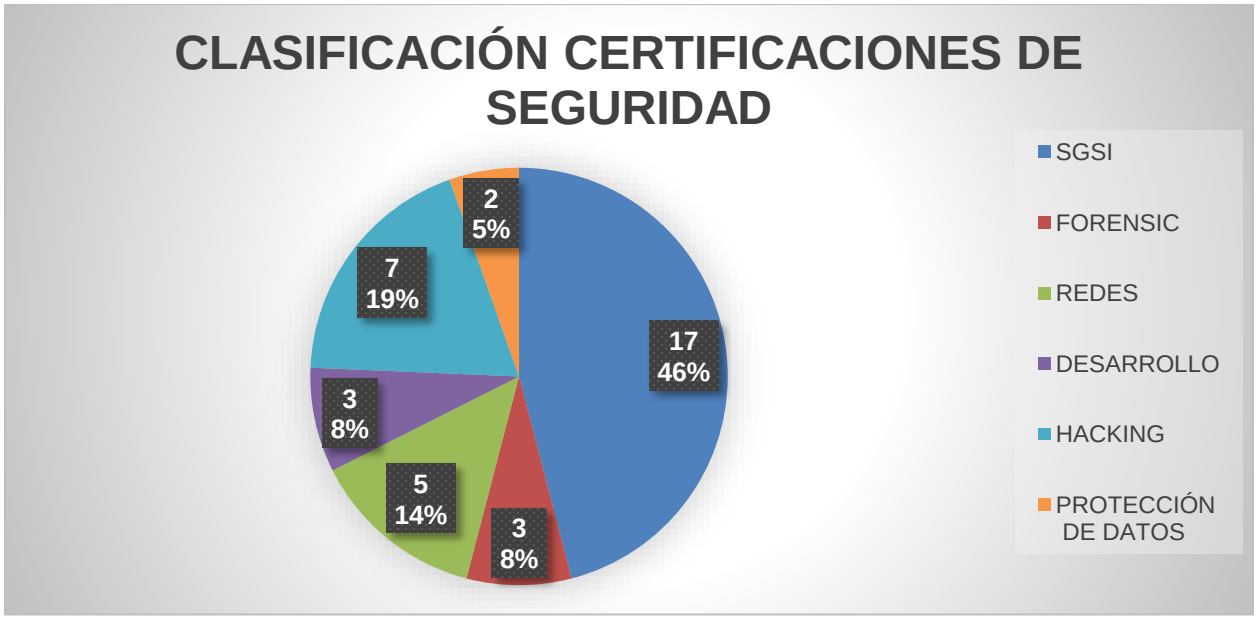

Figura 3.3. Porcentaje según la clasificación.

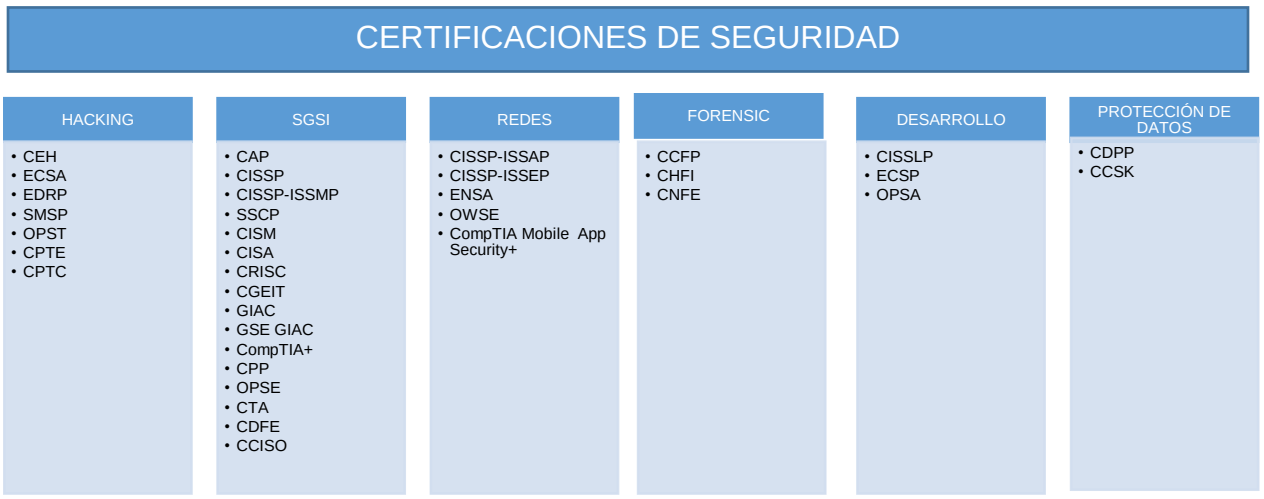

Figura 3.4. Clasificación certificaciones de seguridad.

También mencionar que existen otras certificaciones que no son propiamente de seguridad pero están, en parte, relacionadas con ella como la certificación ITIL (Infraestructura de Tecnologías de la información), que se considera en un estándar de gestión de servicios informáticos, la certificación CCNP (Cisco Certified Network Professional), relacionada con las redes y las comunicaciones; y la MCDBA (Microsoft Certified Database Administrator), y MCITP (Database Administrator), relacionadas con la administración de bases de datos, entre otras.

Es importante mencionar que también existe un estándar para la seguridad de la información que es la norma ISO/IEC 27001 aprobado por la International Organization for Standardization (ISO), que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). Se pueden certificar los SGSI, a través de entidades externas que auditen el cumplimiento e implantación de la norma ISO/IEC 27001 y emitan la correspondiente certificación, pero esto no es aplicable a personas.

4 LISTADO Y DESCRIPCIÓN DE LAS CERTIFICACIONES DE SEGURIDAD

Las certificaciones de seguridad que podemos encontrar en el mercado son muy variadas y se basan en diferentes conceptos de seguridad de las TIs.

En los próximos capítulos se van a describir las características más importantes de cada una de las certificaciones de seguridad, con una introducción preliminar, candidatos, mercado laboral, exámenes, requisitos, número de personas certificadas y si es posible certificarse en España.

En este primer informe, se ha creído oportuno centrarse en las certificaciones proporcionadas por $(ISC)^2$ e ISACA, que son las más importantes y copan el mercado de las certificaciones de seguridad.

Se van a exponer las certificaciones por el orden indicado en las figuras 1.3 y 1.4, del apartado 1.INTRODUCCION: CERTIFICACIONES DE SEGURIDAD (páginas 10 y 11). Es decir, se van a detallar las certificaciones ordenadas por las empresas y asociaciones que las proporcionan.

Se comenzará con las certificaciones de $(ISC)^2$ para continuar con las de ISACA.

5 (ISC)²

A continuación se pasan a describir las diferentes certificaciones emitidas por (ISC)².

5.1 (ISC)²: CAP (CERTIFIED AUTORIZATION PROFESSIONAL)

5.1.1 Introducción

Es una certificación emitida por la empresa (ISC)². Tiene como objetivo medir el conocimiento y las habilidades del personal involucrado en el proceso de autorización y mantenimiento de los sistemas de información. Principalmente esta credencial se aplica a los responsables de la creación de procesos utilizados para la evaluación de riesgos y establecimiento de los requisitos de seguridad. Sus decisiones asegurarán que los sistemas de información posean una seguridad acorde con el nivel de exposición a los riesgos potenciales que existan.

En la actualidad hay 1.933 certificados en CAP, según se indica en la web de (ISC)² [9].

5.1.2 Candidatos

El candidato ideal debe tener experiencia, habilidades o conocimientos en

- Seguridad de TI.
- Seguridad de la información.
- Gestión de información de riesgos.
- Certificación.
- Administración de sistemas.
- Uno - dos años de experiencia técnica general.
- Dos años de experiencia general en sistemas.
- Uno - dos años de base de datos, desarrollo de sistemas o experiencia en redes.
- Conocimientos en políticas de seguridad.
- Experiencia técnica en auditoría de empresas.

• Estar familiarizado con la documentación del NIST (*National Institute of Standards and Technology*). El Instituto Nacional de Normas y Tecnología, es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos, mediante avances en metodología, normas y tecnología para mejorar la estabilidad económica y la calidad de vida.

5.1.3 Mercado laboral

A medida que el paisaje mundial de seguridad de la información evoluciona rápidamente, las empresas y las agencias gubernamentales implementan nuevas tecnologías que muy pocos usuarios comprenden verdaderamente. El nivel de exposición que trae a su empresa implica un riesgo considerable. Un creciente número de clientes, contratistas, socios y empleados acceden a su información y en este nuevo escenario cambian la forma en que las personas protegen los activos de sus organizaciones. Al ser CAP una certificación de gestión, el mercado laboral es muy amplio y abarca desde pequeñas empresas privadas a grandes multinacionales. También en el mundo financiero tienen cabida los certificados en CAP.

5.1.4 Conocimientos

El examen de CAP pone a prueba la amplitud y profundidad de los conocimientos de un candidato, centrándose en los siete dominios de la CAP CBK , que son:

• Marco de gestión de riesgos (RMF: *Risk Management Framework*). La evaluación de los posibles riesgos sirve como base para la implementación de mejores controles de seguridad.

• Clasificación de los sistemas de información, para la realización de un análisis de impacto. Mediante el estudio de los tipos de información permitidos, con sus requisitos de seguridad, se pueden sentar las bases de un plan de seguridad completo.

• Selección de los controles de seguridad, basados en la clasificación de los sistemas de información, para la documentación de un plan de seguridad.

• Implementación del control de seguridad: los controles de seguridad especificados en el plan de seguridad, se implementan teniendo en cuenta los requisitos mínimos que garantizan la seguridad de una organización. En el plan de seguridad se describe cómo se utilizan los controles dentro del sistema de información y su entorno operativo. En el plan de evaluación de la seguridad, se documentan los métodos para probar dichos controles y los resultados esperados a lo largo del ciclo de vida de los sistemas.

• Evaluación del control de seguridad, para determinar su efectividad en el cumplimiento de los requisitos de seguridad del sistema de información. Los resultados están documentados en el Informe de Evaluación de Seguridad

• Monitorización de los controles de seguridad.

5.1.5 Cómo obtener la certificación

Para obtener la certificación CAP hay que cumplir con una serie de requisitos, que son los siguientes:

1º Experiencia. Se necesita como mínimo dos años de experiencia en uno o más de los siete dominios que se han indicado anteriormente (CAP CBK).

2º Exámenes. Es necesario aprobar el examen, obteniendo más de 700 puntos sobre 1.000.

3º Aval. Una vez aprobado el examen se requiere que se complete un formulario de aval, firmado por un profesional de $(ISC)^2$, que sea un miembro activo de la organización y que sea capaz de dar fe de la experiencia profesional del candidato. La propia organización, $(ISC)^2$, también puede actuar de posible aval. Si en los 9 meses posteriores a la aprobación del examen el candidato no ha conseguido dicho aval o no se ha convertido en miembro de la asociación, se deberá repetir el examen.

4º Mantener la certificación. Se requiere la recertificación cada tres años, con los requisitos correspondientes para mantener sus credenciales en regla. Esto se logra principalmente a través de créditos CPE, *Continuing Professional Education* (Educación Profesional Continua) que se pueden obtener a través de asistencias a congresos, formación o seminarios. Este es el medio para que las personas mantengan sus conocimientos y habilidades durante su vida profesional. Se requieren 60 créditos cada tres años. Se deben obtener un mínimo de 10 CPEs cada año dentro del ciclo de certificación de tres años.

La cuota anual de mantenimiento de esta certificación es de 65 $.

5.1.6 Exámenes

Los exámenes contienen 125 preguntas de opción múltiple con 4 opciones en cada una. Para la realización del examen se dispone de 3 horas. Para aprobar hay que obtener más de 700 puntos sobre 1.000.

Los exámenes se realizan en inglés y en España se pueden realizar en Madrid y Barcelona, en las sedes de Pearson Vue [20].

No se dispone información sobre el número de convocatorias anuales para realizar los exámenes. Para más información se puede acudir a la página web oficial de $(ISC)^2$ [9].

Por otro lado, los precios del examen se muestran en la tabla inferior (figura 5.1).

América, Asia, Oriente Medio	Gran Bretaña	Europa
•419 DÓLARES	•290 LIBRAS	•280 EUROS

Figura 5.1: Precios examen certificación CAP.
Fuente: (ISC)² Fecha de consulta Octubre 2015.

Existe también una herramienta para la autoevaluación: (ISC)² *Official Self Assessment*. Esta herramienta además de evaluar las respuestas de los exámenes, analiza los resultados para elaborar un plan de estudios, determinando las áreas en la que el candidato está bien preparado e identifica los temas en los que se necesita adquirir más conocimientos.

5.2 (ISC)²: CCFP CERTIFIED CYBER FORENSICS PROFESSIONAL

5.2.1 Introducción

El objetivo de la informática forense es examinar los medios digitales de manera válida a efectos legales con el objetivo de identificar, preservar, recuperar, analizar y presentar hechos y opiniones acerca de la información

Tiene como misión mucho más que analizar discos duros e investigar intrusos. Certifica a profesionales que sean capaces de tener y adquirir todos los conocimientos y habilidades de la informática forense. En este aspecto, es importante tener en cuenta que hay que saber enfrentarse a los retos más recientes como el ataque a móviles o el ataque a nubes entre otros.

El CCFP es la primera certificación disponible dentro de la disciplina forense, que aglutina prácticas internacionalmente aceptadas, a la vez que adapta el conocimiento específico requerido por los profesionales forenses a nivel nacional.

En la actualidad hay 168 certificados en CCFP, según se indica en la web de (ISC)² [9].

5.2.2 Candidatos

Dadas las posibles aplicaciones de la ciencia forense informática, los profesionales certificados CCFP pueden provenir de una gran variedad de clientes corporativos, legales, policiales, gubernamentales, incluyendo:

- Examinadores forenses digitales, que aplican la ley para apoyar las investigaciones penales

• Profesionales de la ciberdelincuencia y ciberseguridad, que trabajan en los sectores público o privado.

• Ingenieros y gerentes, que trabajan en seguridad de la información de la informática forense.

• Consultores forenses para temas legales.

• Analistas de inteligencia cibernética, que trabajan para agencias de inteligencia.

• Consultores forenses informáticos que trabajan para empresas de gestión o consultoría especializadas.

5.2.3 Mercado laboral

El mercado laboral de los profesionales certificados en CCFP (figura 5.2), es muy amplio, ya que abarca desde organismos oficiales como policía, servicios de inteligencia de los gobiernos para la investigación de delitos, hasta las empresas privadas que necesitan un personal certificado para protegerse o para investigar los posibles ataques de hackers.

Figura 5.2: Mercado Laboral para certificados en CCFP.
Fuente: (ISC)[2].

5.2.4 Conocimientos

El examen CCFP pondrá a prueba la competencia del candidato en los seis dominios CCFP de (ISC)[2] CBK, que son:

• Principios éticos y legales. Directrices de comportamiento ético y marcos de cumplimiento regulatorio:

- La naturaleza de la evidencia.
- Cadena de custodia.
- Reglas de procedimiento.
- El papel de testigo experto.
- Códigos de ética.

• Investigaciones, que abarcan las medidas y técnicas de investigación necesarias para obtener evidencia digital:

- Proceso de investigación.
- Gestión de pruebas.
- Investigaciones criminales.
- Investigaciones civiles.
- Investigaciones administrativas.

• Respuesta a incidentes de seguridad:

- Propiedad intelectual.

• Ciencias forenses, que conllevan la aplicación de un amplio espectro de las ciencias y tecnologías para investigar y aclarar los hechos en relación con el derecho penal o civil:

- Métodos forenses.
- Planificación y análisis forense.
- Redacción de informes y presentación de pruebas.
- Control de calidad y control de gestión.
- Análisis de las evidencias.

• *Digital Forensics*, que se refiere a la recolección de evidencias digitales, que pueden ser desde datos almacenados hasta datos transmitidos a través de medios electrónicos:

- Sistemas operativos.
- Redes.
- Dispositivos móviles.
- Contenidos multimedia.
- Sistemas virtuales.

- Técnicas y herramientas forenses.

• Aplicaciones forenses, que aborda la complejidad de las aplicaciones que se pueden encontrar en una investigación forense:

- Software forense.
- Web, email, mensajería.
- Bases de datos.
- Malware o software malintencionado.

• Tecnologías emergentes, que contiene las tecnologías en constante evolución que se espera que un candidato debe conocer:

- Nubes (Clouds).
- Redes sociales.
- Paradigma big data (hace referencia a los sistemas que manipulan grandes conjuntos de datos, con las dificultades de captura, almacenamiento y análisis que ello conlleva).
- Sistemas de control.
- Infraestructura crítica.
- Realidad virtual.

5.2.5 Cómo obtener la certificación

Para obtener esta certificación son necesarios ciertos requisitos, que son los siguientes:

1º Experiencia: Los candidatos deben tener un título universitario de cuatro años, además de tres años de análisis forense digital a tiempo completo o experiencia en seguridad de TI en tres de los seis dominios de la credencial (CCFP de (ISC)^2 CBK), que se han indicado anteriormente.

Los candidatos sin la experiencia necesaria, pueden recibir una exención de un año. Es posible presentar el examen y convertirse en un Asociado de (ISC)^2 hasta que haya adquirido la experiencia necesaria.

2º Examen, en el que hay que superar 700 puntos sobre los 1.000 posibles.

3º Completar el proceso de aprobación. Una vez que se le notifique que ha pasado con éxito el examen, se dispondrá de nueve meses a partir de la fecha en la que se realizó el examen para completar un proceso de aprobación, que consta de la cumplimentación de un Formulario de Solicitud de Aval, respaldado por un miembro de (ISC)^2 y suscribirse al Código de Ética de (ISC)^2.

4º Mantener la certificación: Se requiere una recertificación cada tres años. Esto se logra consiguiendo 90 CPE cada tres años, con un mínimo de 15 CPEs ganados cada año después de la certificación. Si estos requisitos no se cumplen, se debe repetir el examen para mantener la certificación.

También hay que pagar una cuota de mantenimiento anual (AMF: *Annual Manteinance Fee*) de $ 100.

5.2.6 Exámenes

Los exámenes contienen 125 preguntas de opción múltiple con 4 opciones en cada una. Se dispone de tres horas para realizar dicho examen y hay que superar los 700 puntos sobre los 1.000 posibles.

Los exámenes se realizan en inglés, alemán y coreano y en España se pueden realizar en Madrid y Barcelona, en las sedes de Pearson Vue [20].

No se dispone información sobre el número de convocatorias anuales para realizar los exámenes. Para más información se puede acudir a la página web oficial de (ISC)² [9].

Actualmente el examen CCFP está disponible en los EE.UU, la Unión Europea, India y Corea del Sur. Con el tiempo, se están agregando exámenes específicos de otros países y regiones. Reconocidos expertos de todo el mundo se están asociando con (ISC)² para personalizar el examen con las leyes correspondientes, reglamentos y léxico de cada país.

Por otro lado, los precios del examen se muestran en la tabla inferior (figura 5.3).

América, Asia, Oriente Medio	Gran Bretaña	Europa
•549 DÓLARES	•380 LIBRAS	•480 EUROS

Figura 5.3: Precios examen certificación CCFP.
Fuente: (ISC)² Fecha de consulta Octubre 2015.

Para realizar el examen hay que registrarse previamente aquí:

www.isc2.org/certificationregister-now

5.3 (ISC)²: CISSP CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

5.3.1 Introducción

La certificación CISSP es un estándar reconocido a nivel mundial que confirma el conocimiento de un individuo en el campo de la seguridad de la información. Los certificados en CISSP son profesionales de la seguridad de la información, que tienen conocimientos para definir la arquitectura, el diseño, la gestión y/o los controles que garantizan la seguridad de los entornos empresariales. Fue la primera certificación en el ámbito de la seguridad de la información para cumplir con los estrictos requisitos de la norma ISO/IEC 17024.

En la actualidad hay 105.705 certificados en CISSP, según se indica en la web de (ISC)² [9].

5.3.2 Candidatos

La certificación tiene el objetivo de ayudar a las empresas a reconocer a los profesionales con formación en el área de seguridad de la información. Su experiencia juega un papel crítico para ayudar a las organizaciones a integrar los protocolos de seguridad más fuertes y proteger contra amenazas en un cada vez más complejo panorama de la seguridad cibernética.

5.3.3 Mercado laboral

La certificación CISSP ayuda a los empleados a aumentar la credibilidad de la organización, con la utilización de un lenguaje universal, evitando la ambigüedad de los términos y aumentando su confianza, proporcionándoles conocimiento y experiencia. Las profesiones a las que se puede acceder con la certificación CISSP se representan en la figura 5.4.

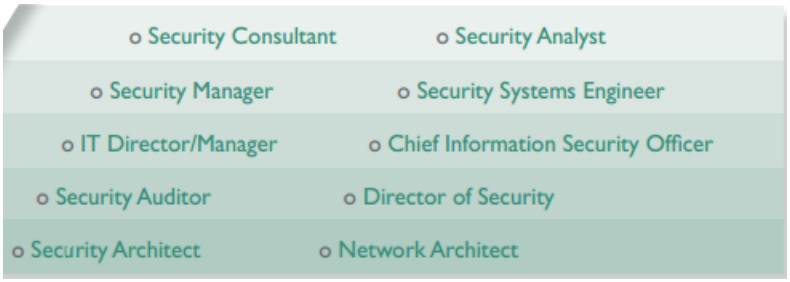

Figura 5.4: Mercado Laboral para certificados en CISSP.
Fuente: (ISC)².

5.3.4 Conocimientos

Para obtener la certificación se pondrá a prueba el conocimiento del candidato en los dominios (ISC)² CISSP CBK :

• Control de acceso, se define un conjunto de mecanismos para crear una arquitectura de seguridad para proteger los sistemas de información:

- Conceptos/Metodologías/Técnicas.
- Efectividad.
- Ataques.

• Telecomunicaciones y seguridad de redes, que analiza las estructuras de redes, los métodos de transmisión, los formatos de transporte y las medidas de seguridad que se utilizan para proporcionar disponibilidad, integridad y confidencialidad de los datos:

- Arquitectura de red y diseño.
- Canales de comunicación.
- Componentes de red.
- Ataques de red.

• Políticas de seguridad y gestión de riesgos, con la implementación de normas, procedimientos y directrices:

- Conceptos de gestión de riesgos.
- Políticas de seguridad.
- Seguridad del personal.

• Seguridad en el desarrollo del software:

- Ciclo de vida de desarrollo de sistemas.
- Controles y seguridad de entornos de las aplicaciones.
- Eficacia de la seguridad de las aplicaciones.

• Criptografía, y los principios, medios y métodos de manipular información para asegurar su integridad, confidencialidad y autenticidad:

- Conceptos de cifrados.
- Las firmas digitales.
- Alternativas para ocultar la información.
- Ataques cripto-analíticos.
- Infraestructura de clave pública (PKI).

• Arquitectura de seguridad y diseño, que contiene los conceptos, estructuras y estándares utilizados para diseñar e implementar los sistemas operativos, equipos, redes, aplicaciones y los controles que se utilizan para hacer cumplir los diversos niveles de confidencialidad, integridad y disponibilidad:

- Conceptos fundamentales de los modelos de seguridad.
- Capacidades de los sistemas de información.
- Principios y medidas de prevención.
- Vulnerabilidades y amenazas.

• Operaciones de seguridad que se utilizan para identificar los controles sobre el hardware, los medios de comunicación y los operadores, con permisos de acceso a cualquiera de estos recursos.

• Continuidad del negocio y planificación de recuperación de desastres, que se dirige a la defensa de la empresa de cara a grandes trastornos en las operaciones normales del negocio:

- Análisis del impacto comercial.
- Proceso de recuperación de desastres.
- Proporcionar capacitación a los empleados.

• Legalidad y reglamentos, que son las directrices de leyes y reglamentos sobre la ciber-delincuencia; las medidas de investigación y las técnicas que se pueden utilizar para determinar si un delito ha sido cometido y los métodos para reunir pruebas:

- Procedimientos forenses.
- Cuestiones jurídicas.
- Investigaciones.

• Seguridad física, aborda las amenazas, vulnerabilidades y contra-medidas que pueden ser utilizadas para proteger físicamente los recursos e informaciones sensibles de una empresa:

- Instalaciones de seguridad.
- Consideraciones de diseño de las instalaciones.
- Seguridad interna y perímetro de seguridad.

5.3.5 Cómo obtener la certificación

Para obtener la certificación hay que cumplir con los siguientes requisitos:

1º Experiencia. Los candidatos deben tener título universitario y cinco años de experiencia profesional en seguridad en dos o más de los diez dominios del $(ISC)^2$ CISSP CBK, o cuatro años de experiencia laboral profesional en dos o más de dichos dominios. Si no se tiene la experiencia necesaria, es posible hacer el examen y convertirse en un Asociado de $(ISC)^2$ hasta que se haya adquirido.

2º Examen. El examen consta de 250 preguntas de opción múltiple con 4 opciones en cada una. Es necesario obtener más de 700 puntos sobre los 1000 posibles para aprobar.

3º Completar el proceso de ratificación. Al igual que en el resto de certificaciones de $(ISC)^2$ es necesario un aval durante los nueve meses posteriores a la aprobación del examen, mediante un formulario de aval, para que un miembro de $(ISC)^2$ la ratifique. También es necesaria la suscripción al Código de Ética de la asociación.

4º Mantener la certificación. Se requiere la recertificación cada tres años. Esto se logra principalmente consiguiendo 120 CPEs cada tres años, con un mínimo de 20 CPEs obtenidos cada año después de la certificación. Si no se cumplen los requerimientos de CPE, habría que volver a realizar el examen para mantener la certificación.

La cuota anual de mantenimiento anual es de $85.

5.3.6 Exámenes

Como ya se ha indicado anteriormente, el examen consta de 250 preguntas de opción múltiple con 4 opciones en cada una. Es necesario obtener más de 700 puntos sobre los 1.000 posibles para aprobar.

Antes de la realización del examen se puede preparar mediante una serie de herramientas educativas como un esquema de exámenes para comprobar la preparación (www.isc2.org/exam-outline), Webcast de los dominios CBK (www.isc2.org/previews), el libro de texto oficial (www.isc2.org/store), la herramienta de autoevaluación studISCope (www.isc2.org/studiscope) y un Seminario de Capacitación Oficial presencial o mediante e-learning (www.isc2.org/self-paced).

Desde el 15 de enero del 2014 se han incluido una serie de preguntas Drag & Drop (Arrastrar & Soltar) y Hotspot que son tipos de preguntas innovadoras y proporcionan varias ventajas sobre las preguntas tradicionales de cuatro opciones (figuras 5.5 y 5.6).

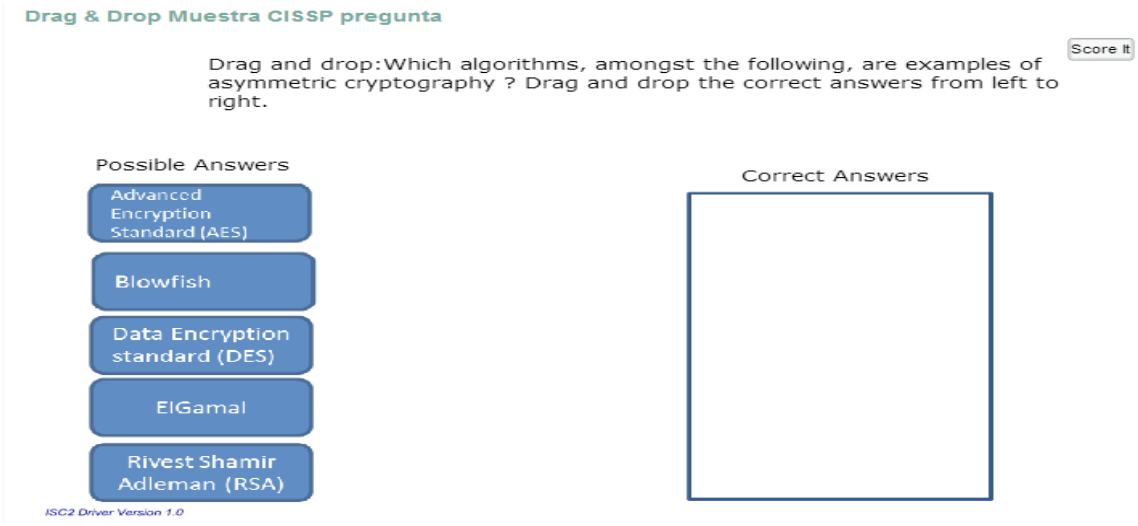

Figura 5.5: Preguntas Drag & Drop.
Fuente: (ISC)²

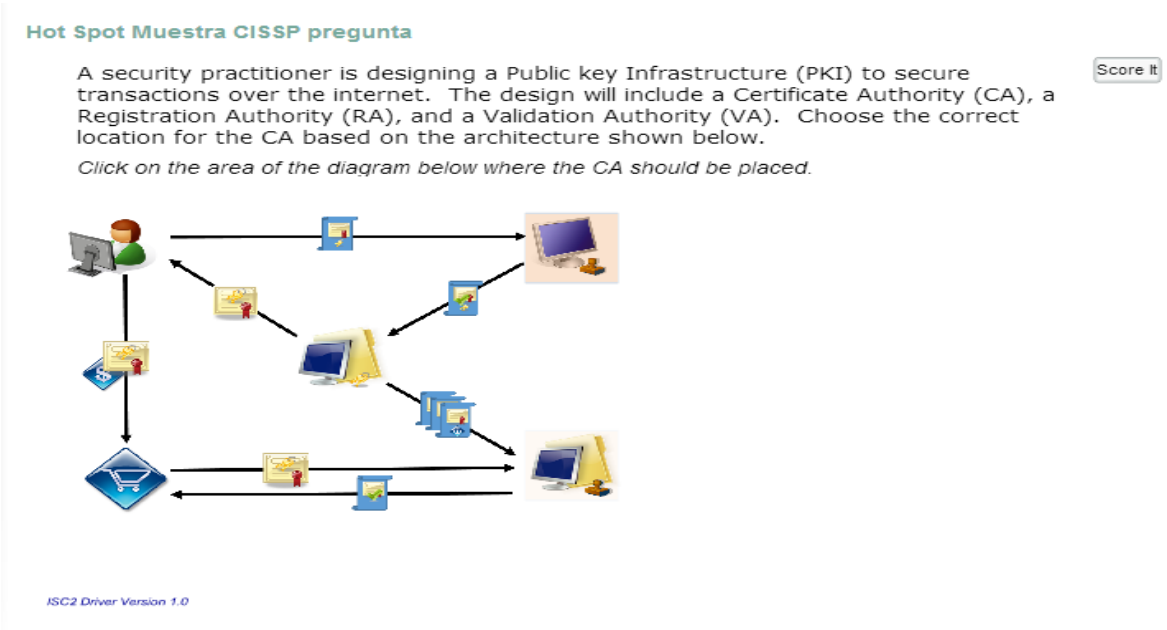

Figura 5.6: Preguntas HotsPot.
Fuente: (ISC)²

Los exámenes se realizan en inglés, francés, alemán, portugués, español, japonés, chino y coreano, y en España se pueden realizar en Madrid y Barcelona, en las sedes de Pearson Vue [20].

No se dispone información sobre el número de convocatorias anuales para realizar los exámenes. Para más información se puede acudir a la página web oficial de (ISC)² [9].

Por otro lado, los precios del examen se muestran en la tabla inferior (figura 5.7).

América, Asia, Oriente Medio	Gran Bretaña	Europa
•599 DÓLARES	•415 LIBRAS	•520 EUROS

Figura 5.7: Precios examen certificación CISSP.
Fuente: (ISC)² Fecha de consulta Octubre 2015.

5.4 (ISC)²: CISSP-ISSAP CERTIFIED INFORMATION SYSTEMS SECURITY ARCHITECTURE PROFESSIONAL

5.4.1 Introducción

CISSP-ISSAP, certifica Profesionales en Arquitectura en Seguridad de los Sistemas de Información.

Después de la concepción original de CISSP y la evolución continua de la seguridad de la información, $(ISC)^2$ descubrió la necesidad de desarrollar credenciales que cubrieran las necesidades específicas de sus miembros. Estas credenciales permiten el desarrollo de funciones más demandadas por las empresas de mayor tamaño y una especialización más concreta en las áreas funcionales de Arquitectura (ISAAP), Ingeniería (ISSEP) y Gestión de la Seguridad (ISSMP) de la Información. Para tener derecho a esta certificación, se debe mantener la validez de la certificación CISSP obtenida con anterioridad y aprobar el examen de la certificación correspondiente. Cada especialidad de CISSP tiene sus propios dominios CBK.

En la actualidad hay 1.731 certificados en CISSP-ISSAP, según se indica en la web de $(ISC)^2$ [9].

5.4.2 Candidatos

Es una certificación adecuada para jefes en arquitectura de seguridad y analistas que suelen trabajar como consultores independientes o en un puesto similar dentro de las empresas. El arquitecto desempeña una función clave dentro del departamento de seguridad de la información con responsabilidades que encajan funcionalmente entre el nivel de alta dirección y el de gestión superior e implementación del programa de seguridad, ya que su función normalmente sería la de desarrollar, diseñar o analizar un plan completo de seguridad. Aunque esta función puede parecer que está estrechamente vinculada a la tecnología, no es así necesariamente, sino que consiste fundamentalmente en el proceso de consulta y análisis en la seguridad de la información.

5.4.3 Mercado laboral

En la figura 5.8 se muestra gráficamente el mercado de trabajo posible para los certificados en CISSP-ISSAP.

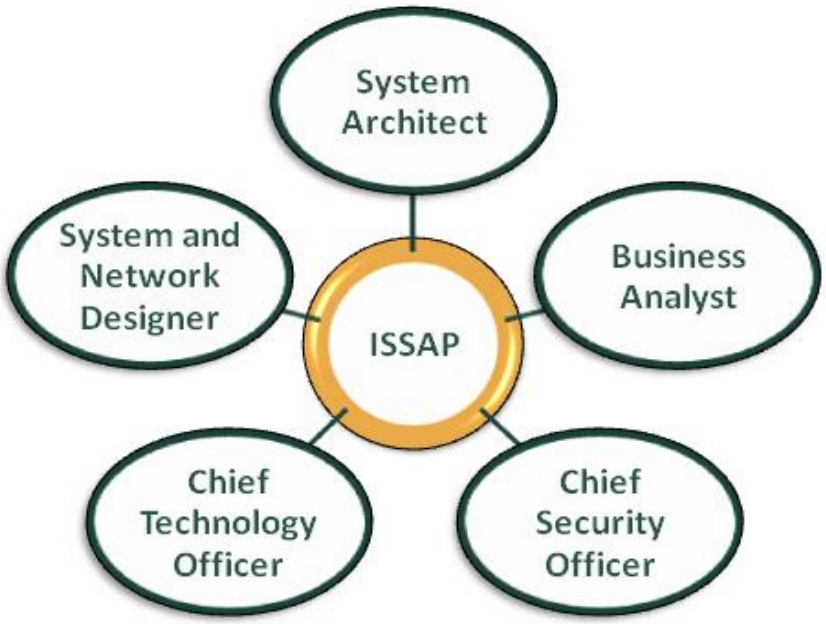

Figura 5.8: Mercado de trabajo para certificados en CISSP-ISSAP.
Fuente: (ISC)[2].

5.4.4 Conocimientos

Para obtener la certificación CISSP-ISSAP, el candidato debe mostrar sus conocimientos en los seis dominios CBK de ésta, que son:

- Metodología y sistemas de control de acceso.
- Criptografía.
- Integración de la seguridad física.
- Análisis de requisitos y estándares, directrices y criterios de seguridad.
- Planificación de recuperación de desastres y continuidad del negocio relacionada con la tecnología.
- Seguridad de redes y telecomunicaciones.

5.4.5 Cómo obtener la certificación

Para obtener la certificación CISSP-ISSAP, al ser una especialización de la certificación CISSP, tiene que estar certificado en ésta previamente. Además hay que tener como mínimo 2 años de experiencia laboral en el área de la arquitectura y realizar el examen correspondiente.

Se requiere la recertificación con 120 CPEs cada 3 años con un mínimo de 20 en la especialización ISSAP y el pago de una cuota anual de 85$.

5.4.6 Exámenes

Los exámenes ISSAP contienen 125 preguntas de opción múltiple, con 4 opciones en cada una, y se disponen 3 horas para completarlo. Cada uno de estos exámenes contiene 25 preguntas que se incluyen solamente con fines de investigación. Las preguntas de la investigación no se identifican. Para aprobar hay que superar los 700 puntos de un máximo de 1.000 posibles.

Los exámenes se realizan en inglés y en España se pueden realizar en Madrid y Barcelona, en las sedes de Pearson Vue [20].

No se dispone información sobre el número de convocatorias anuales para realizar los exámenes. Para más información se puede acudir a la página web oficial de (ISC)² [9].

Por otro lado, los precios del examen se muestran en la tabla inferior (figura 5.9).

América, Asia, Oriente Medio	Gran Bretaña	Europa
•399 DÓLARES	•280 LIBRAS	•350 EUROS

Figura 5.9: Precios examen certificación CISSP-ISSAP.
Fuente: (ISC)² Fecha de consulta Octubre 2015.

5.5 (ISC)²: CISSP-ISSEP CERTIFIED INFORMATION SYSTEMS SECURITY ENGINEERING PROFESSIONAL

5.5.1 Introducción

CISSP-ISSEP (Profesional en Ingeniería en Seguridad de los Sistemas de Información) ha sido desarrollado conjuntamente con la Agencia de Seguridad Nacional de Estados Unidos proporcionando una importante herramienta para los profesionales de ingeniería de seguridad de los sistemas.

En la actualidad hay 3.862 certificados en CISSP-ISSEP, según se indica en la web de (ISC)² [9].

5.5.2 Candidatos

La certificación es una guía para incorporar la seguridad a los proyectos, aplicaciones, procesos del negocio y todos los sistemas de información. Proporciona al candidato prácticas y metodologías estándar en el mundo actual para la gestión de riesgos, la ingeniería en seguridad de sistemas, y la certificación y acreditación. Los profesionales de la seguridad buscan metodologías factibles y buenas prácticas con las que puedan trabajar para integrar la seguridad en todos los aspectos operativos del negocio.

5.5.3 Mercado de laboral

La certificación es adecuada para ingenieros de Sistemas de Información y analistas. En la figura 5.10, se muestra gráficamente el mercado de trabajo.

Figura 5.10: Mercado de trabajo para certificados en CISSP-ISSEP.
Fuente: (ISC)².

5.5.4 Conocimientos

Los candidatos deben demostrar sus conocimientos en los cuatro dominios del CISSP-ISSEP CBK, que son:

- Certificación y acreditación.
- Ingeniería de seguridad en sistemas.
- Gestión técnica.
- Normativas estadounidenses sobre seguridad de la información.

5.5.5 Cómo obtener la certificación

Para obtener la certificación CISSP-ISSEP, al ser una especialización de la certificación CISSP, tiene que estar certificado en ésta previamente. Además hay que tener como mínimo 2 años de experiencia laboral en el área de la ingeniería y realizar el examen correspondiente.

Se requiere la recertificación con 120 CPEs cada 3 años con un mínimo de 20 en la especialización ISSEP y el pago de una cuota anual de 85$.

5.5.6 Exámenes

Los exámenes ISSEP contienen 150 preguntas de opción múltiple, con 4 opciones en cada una, y se disponen 3 horas para completarlo. Cada uno de estos exámenes contiene 25 preguntas que se incluyen solamente con fines de investigación. Las preguntas de la investigación no se identifican. Para aprobar, hay que superar los 700 puntos de un máximo de 1.000 en la escala de calificaciones.

Los exámenes se realizan en inglés y en España se pueden realizar en Madrid y Barcelona, en las sedes de Pearson Vue [20].

No se dispone información sobre el número de convocatorias anuales para realizar los exámenes. Para más información se puede acudir a la página web oficial de (ISC)² [9].

Por otro lado, los precios del examen se muestran en la tabla inferior (figura 5.11).

América, Asia, Oriente Medio	Gran Bretaña	Europa
• 399 DÓLARES	• 280 LIBRAS	• 350 EUROS

Figura 5.11: Precios examen certificación CISSP-ISSEP.
Fuente: (ISC)² Fecha de consulta Octubre 2015.

5.6 (ISC)²: CISSP-ISSMP CERTIFIED INFORMATION SYSTEMS SECURITY MANAGEMENT PROFESSIONAL

5.6.1 Introducción

CISSP-ISSMP (Profesional en Administración en Seguridad de los Sistemas de Información) proporciona elementos de gestión en mayor profundidad, como la gestión de proyectos, la gestión de riesgos, la preparación y el establecimiento de un programa de conocimiento de la seguridad y la gestión de un programa de planificación de la continuidad del negocio (*Business Continuity Planning Program*).

En la actualidad hay 1.111 certificados en CISSP-ISSMP, según se indica en la web de (ISC)^2 [9].

5.6.2 Candidatos

Un CISSP-ISSMP establece, presenta y gestiona las políticas y procedimientos de seguridad de la información con el fin de apoyar los objetivos globales del negocio y no agotar los recursos. Normalmente, el candidato o titular de la certificación tendrá la responsabilidad de crear la estructura del departamento de seguridad de la información y definir los medios para apoyar al grupo internamente.

5.6.3 Mercado laboral

Las diferentes áreas de trabajo de los certificados se muestran en la figura 5.12.

Figura 5.12: Mercado de trabajo para certificados en CISSP-ISSMP. Fuente: (ISC)^2.

5.6.4 Conocimientos

Los profesionales de CISSP-ISSMP disponen de un conocimiento más completo y global sobre la seguridad de la información. Los cinco dominios CISSP -ISSMP CBK cambiaron a partir del 1 de abril del 2013, y son los que se describen a continuación:

- Planificación de continuidad del negocio, en la recuperación de desastres y en la continuidad de las operaciones.
- Prácticas de gestión de la seguridad en la empresa.
- Seguridad del desarrollo de sistemas.
- Leyes e investigaciones forenses, para la gestión de incidentes.
- Supervisión del cumplimiento en la seguridad de las operaciones

5.6.5 Cómo obtener la certificación

Al igual que las dos anteriores especificaciones, es necesario estar certificado en CISSP y además tener dos años de experiencia profesional en el área de gestión.

Se requiere la recertificación con 120 CPEs cada 3 años con un mínimo de 20 en la especialización ISSMP y el pago de una cuota anual de 85$.

5.6.6 Exámenes

Para aprobar el examen correspondiente, hay que superar los 700 puntos sobre un total de 1.000 posibles. El examen consta de 125 preguntas, de tipo test, con 4 opciones en cada una y hay que realizarlo en un máximo de 3 horas.

Los exámenes se realizan en inglés y en España se pueden realizar en Madrid y Barcelona, en las sedes de Pearson Vue [20].

No se dispone información sobre el número de convocatorias anuales para realizar los exámenes. Para más información se puede acudir a la página web oficial de (ISC)² [9].

Por otro lado, los precios del examen se muestran en la tabla inferior (figura 5.13).

América, Asia, Oriente Medio	Gran Bretaña	Europa
• 399 DÓLARES	• 280 LIBRAS	• 350 EUROS

Figura 5.13: Precios examen certificación CISSP-ISSMP.
Fuente: (ISC)² Fecha de consulta Octubre 2015.

5.7 (ISC)²: CSSLP CERTIFIED SECURE SOFTWARE LIFECYCLE

5.7.1 Introducción

La CSSLP, Certificación en Seguridad del Ciclo de Vida del Software, valida que los profesionales de software tienen la experiencia para incorporar prácticas de seguridad - la autenticación, autorización y auditoría - en cada fase del ciclo de vida de desarrollo de software, desde el diseño e implementación de software de prueba y hasta su despliegue.

En la actualidad hay 1.611 certificados en CSSLP, según se indica en la web de (ISC)² [9].

5.7.2 Candidatos

Los candidatos son todos aquellos involucrados en ciclo de vida del SW. La certificación ayuda a validar la experiencia de los candidatos en la seguridad de las aplicaciones, a determinar las vulnerabilidades de los sistemas y a demostrar un conocimiento práctico en la seguridad de las aplicaciones.

En cuanto a las empresas, mejora la credibilidad de los equipos de desarrollo, proporciona una reducción de costos en la producción, así como de la pérdida de ingresos por el desarrollo de un software inseguro. También asegura el cumplimiento de las regulaciones del gobierno o de la industria.

5.7.3 Mercado laboral

La certificación no sólo está indicada para desarrolladores de software seguro, sino también para analistas y certificadores (*testers*). En la figura 5.14 se muestra el mercado de trabajo.

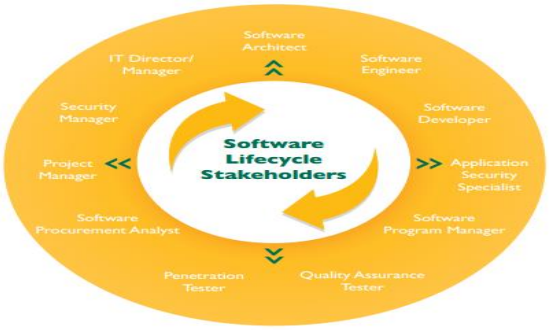

Figura 5.14: Mercado de trabajo para certificados CSSLP.
Fuente: (ISC)[2].

5.7.4 Conocimientos

El candidato debe demostrar sus conocimientos en los siguientes dominios:

- Asegurar los requisitos del software seguro, con los principios básicos del diseño, basándose en metodologías seguras.
- Diseño seguro del SW.
- Implementación segura del SW.
- Certificación segura del SW (*testing*).
- Puesta en marcha del SW.
- Instalación e implementación del SW, con sus correspondientes acciones de mantenimiento.

• Cadena de suministro y adquisición del SW.

5.7.5 Cómo obtener la certificación

Para obtener la certificación se necesitan al menos 4 años de experiencia en alguno de los 8 dominios indicados anteriormente y aprobar el examen correspondiente.

Se requiere la recertificación con 90 CPEs cada 3 años con un mínimo de 30 al año y el pago de una cuota anual de 100$.

5.7.6 Exámenes

Para aprobar el examen correspondiente, hay que superar los 700 puntos sobre un total de 1.000 posibles. El examen consta de 175 preguntas, de tipo test, con 4 opciones en cada una y hay que realizarlo en un máximo de 4 horas.

Los exámenes se realizan en inglés y en España se pueden realizar en Madrid y Barcelona, en las sedes de Pearson Vue [20].

No se dispone información sobre el número de convocatorias anuales para realizar los exámenes. Para más información se puede acudir a la página web oficial de (ISC)² [9].

Por otro lado, los precios del examen se muestran en la tabla inferior (figura 5.15).

América, Asia, Oriente Medio	Gran Bretaña	Europa
•549 DÓLARES	•380 LIBRAS	•480 EUROS

Figura 5.15: Precios examen certificación CSSLP.
Fuente: (ISC)² Fecha de consulta Octubre 2015.

5.8 (ISC)²: SSCP SYSTEMS SECURITY CERTIFIED PRACTITIONER

5.8.1 Introducción

La certificación SSCP está abierta a todos los candidatos con apenas un año de experiencia, convirtiéndose en el punto de inicio ideal para una nueva carrera en seguridad de la información.

En la actualidad hay 2.545 certificados en SSCP, según se indica en la web de (ISC)² [9].

5.8.2 Candidatos

El SSCP es ideal para aquellos que trabajan en posiciones tales como los que muestra la figura 5.16.

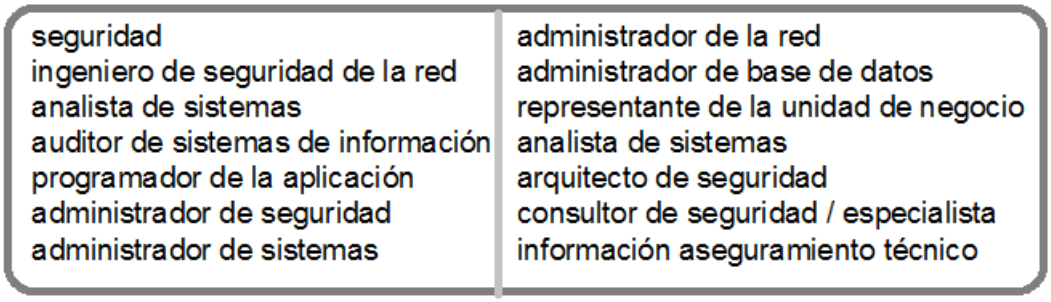

Figura 5.16: Mercado de trabajo para certificados SSCP.
Fuente: (ISC)^2.

5.8.3 Mercado laboral

La certificación SSCP está destinada a personas que pueden tener puestos técnicos o de ingeniería en seguridad de la información tales como ingenieros en seguridad de redes, analistas en seguridad de redes, administradores de seguridad y puestos en tecnología de la información no específicamente relacionados con la seguridad que requieren una comprensión de los conceptos de seguridad y las mejores prácticas de seguridad que incluyen a administradores de sistemas, programadores de aplicaciones, administradores de bases de datos y analistas de sistemas. El enfoque de la certificación SSCP radica en los aspectos técnicos de la seguridad de la información y en el diseño, implementación y administración de los sistemas de información en cumplimiento de las políticas establecidas

5.8.4 Conocimientos

La credencial SSCP demuestra competencia en los siguientes dominios CBK :

- Controles de acceso.
- Criptografía.
- Código malicioso.
- Análisis de código.
- Redes y comunicaciones.
- Riesgo, respuesta y recuperación de datos.

• Operaciones de seguridad y administración.

5.8.5 Cómo obtener la certificación

Para obtener la certificación se requiere un año de experiencia de trabajo a tiempo completo en uno de los 7 dominios indicados anteriormente. Si no se dispone de la experiencia necesaria, la entidad certificadora permite realizar el examen y convertirse, tras aprobarlo, en asociado de $(ISC)^2$ hasta obtener la experiencia requerida, tras lo cual se obtendrá la certificación.

Para mantener la certificación se requiere la obtención de 60 CPEs cada 3 años con un mínimo de 20 al año y el pago de una cuota anual de 65$.

5.8.6 Exámenes

Para aprobar el examen correspondiente, hay que superar los 700 puntos sobre un total de 1.000 posibles. El examen consta de 125 preguntas, de tipo test, con 4 opciones en cada una y hay que realizarlo en un máximo de 3 horas.

Los exámenes se realizan en inglés, japonés y portugués, y en España se pueden realizar en Madrid y Barcelona, en las sedes de Pearson Vue [20].

No se dispone información sobre el número de convocatorias anuales para realizar los exámenes. Para más información se puede acudir a la página web oficial de $(ISC)^2$ [9].

Por otro lado, los precios del examen se muestran en la tabla inferior (figura 5.17).

América, Asia, Oriente Medio	Gran Bretaña	Europa
•250 DÓLARES	•175 LIBRAS	•215 EUROS

Figura 5.17: Precios examen certificación SSCP.
Fuente: $(ISC)^2$ Fecha de consulta Octubre 2015.

5.9 $(ISC)^2$: RESUMEN

5.9.1 Relación entre certificaciones $(ISC)^2$

En la figura 5.18 se muestra una posible proyección entre las diferentes certificaciones de $(ISC)^2$.

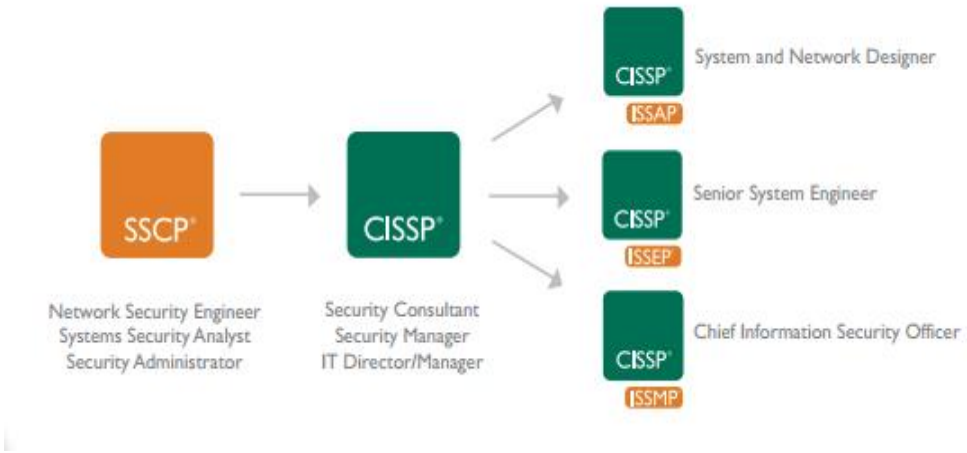

Figura 5.18: Posible evolución entre las diferentes certificaciones. Fuente: (ISC)².

5.9.2 Preguntas de exámenes

Cada uno de estos exámenes contiene 25 preguntas que se incluyen solamente con fines de investigación. Las preguntas de la investigación no se identifican. Cada pregunta es de opción múltiple con 4 posibles opciones de respuesta. La calificación aprobatoria requerida es una puntuación en la escala de 700 de un máximo de 1.000 puntos en la escala de calificaciones. El número de preguntas dependiendo de la certificación puede ser de 250, 175, 150 o 125.

Se muestra a continuación, en la figura 5.19, la información sobre el número de preguntas y la duración de cada uno de los exámenes de las certificaciones de (ISC)², así como los idiomas y las sedes en las que se puede realizar. No se ha encontrado información sobre el número de convocatorias para la realización de los exámenes.

CERTIFICACIÓN	PREGUNTAS	DURACIÓN	IDIOMAS	ESPAÑA	CONVOCATORIAS
CISSP	250 preguntas de opción múltiple	6 horas	Inglés, francés, alemán, portugués, español, japonés, chino coreano	Madrid y Barcelona Sedes de Pearson Vue	N/A
CSSLP	175 preguntas de opción múltiple	4 horas	Inglés		
HCISPP	125 preguntas de opción múltiple	3 horas	Inglés		
CCFP	125 preguntas de opción múltiple	3 horas	Inglés, alemán, coreano		
SSCP	125 preguntas de opción múltiple	3 horas	Inglés, japonés, portugués		
ISSAP	125 preguntas de opción múltiple	3 horas	Inglés		
ISSEP	150 preguntas de opción múltiple	3 horas	Inglés		
ISSMP	125 preguntas de opción múltiple	3 horas	Inglés		
CAP	125 preguntas de opción múltiple	3 horas	Inglés		

Figura 5.19: Resumen exámenes de certificaciones de (ISC)^2.
Fuente: (ISC)^2 Fecha de consulta Octubre 2015.

5.9.3 Créditos CPE

Los créditos CPE (*Continuing Professional Education*-Educación Profesional Continua) según (ISC)[2] se categorizan como créditos del Grupo A o créditos del Grupo B, según la relación de las actividades asociadas con el dominio para cada certificación. Los créditos del Grupo A son para actividades directamente relacionadas con el dominio. Los créditos del Grupo B son para actividades que están fuera del dominio, pero que mejoran las destrezas y competencias profesionales generales del miembro (ver figura 5.20).

Credencial	Mínimo anual (Obligatorio) Sólo Grupo A	Período de certificación de 3 años: Grupo A (Mínimo por período de certificación de 3 años)	Grupo B Opcional (Máximo ver a continuación)	Total requerido (Por período de certificación de 3 años)
SSCP	10	40	20	60
CAP	10	40	20	60
CSSLP	15	60	30	90
CISSP	20	80	40	120
ISSAP ISSEP ISSMP	Durante los períodos siguientes de certificación de 3 años para estas concentraciones, 20 de los 120 CPE ya requeridos para el certificado previo CISSP deben relacionarse con el área específica de concentración. Por ejemplo, si un CISSP tomó el examen de la concentración ISSEP y aprobó, debe presentar al menos 20 de las 120 horas totales requeridas para el certificado CISSP en el área específica de ingeniería.			

Figura 5.20: Mantenimiento de las certificaciones a través de CPEs.
Fuente: (ISC)[2] Fecha de consulta Octubre 2015.

5.9.4 Precios de exámenes

Los precios que hay que pagar para presentarse a los exámenes son diferentes dependiendo del continente desde donde se realicen. Estos precios se muestran en la figura 5.21.

(ISC)[2]

2015 Examination Pricing

	CISSP Exam (6 Hours)*	CISSP-ISSAP/ISSEP/ISSMP Exam (3 Hours)*	CSSLP Exam (4 Hours)*	CCFP Exam** (4 Hours)*	CAP Exam (3 Hours)*	HCISPP Exam (3 Hours)*	SSCP Exam (3 Hours)*	CCSP Exam (4 Hours)*
Americas and all other regions not listed below								
Standard Registration	USD 599	USD 399	USD 549	USD 549	USD 419	USD 349	USD 250	USD 549
Asia Pacific								
Standard Registration	USD 599	USD 399	USD 549	USD 549	USD 419	USD 349	USD 250	USD 549
EMEA (Europe, Middle East and Africa)								
Standard Registration	EUR 520	EUR 350	EUR 480	EUR 480	EUR 360	EUR 280	EUR 215	EUR 480
United Kingdom: Standard Registration	GBP 415	GBP 280	GBP 380	GBP 380	GBP 290	GBP 240	GBP 175	GBP 380
Middle East: Standard Registration	USD 599	USD 399	USD 549	USD 549	USD 419	USD 349	USD 250	USD 549
Africa: Standard Registration	USD 599	USD 399	USD 549	USD 549	USD 419	USD 349	USD 250	USD 549

*Pricing and taxes based on location of exam.
**Applies to all regional versions of the exam.

Figura 5.21: Precio de los exámenes.
Fuente: (ISC)[2] Fecha de consulta Octubre 2015.

5.9.5 Sedes para la realización de exámenes en España

Para la realización de los exámenes se utilizan las sedes de Pearson Vue [20].

Pearson VUE es una empresa multinacional dedicada a la educación y certificación de recursos a nivel mundial para empresas de diferentes industrias.

Al contar con una red mundial de Centros Autorizados para la realización de exámenes, provee a las empresas la capacidad de certificar sus recursos independientemente de la ubicación geográfica.

En la figura 5.22 se muestran las sedes de examen en España.

Figura 5.22: Sedes de examen en España.
Fuente: Pearson Vue [20] Fecha de consulta Octubre 2015.

6 ISACA

A continuación se pasan a describir las diferentes certificaciones emitidas por ISACA.

6.1 ISACA: CISA CERTIFIED INFORMATION SYSTEMS AUDITOR

6.1.1 Introducción

CISA (Certified Information Systems Auditor), cuyas siglas se traducen como Certificación de Auditor de Sistemas de Información, es una certificación para auditores respaldada por la Asociación de Control y Auditoría de Sistemas de Información (ISACA).

En la actualidad hay 109.000 certificados en CISA, según se indica en la web de ISACA [10].

6.1.2 Candidatos

Los candidatos deben cumplir con los requisitos establecidos por ISACA que se describen más adelante.

6.1.3 Mercado laboral

CISA es una certificación reconocida globalmente para profesionales en auditoría, control, aseguramiento y seguridad de SI.

Las empresas demandan auditores profesionales que posean el conocimiento y la experiencia necesaria para ayudar a identificar problemas críticos y personalizar prácticas para apoyar la confianza y el valor de los sistemas de información. Fundamentalmente, sus servicios son requeridos por empresas del mundo financiero.

6.1.4 Conocimientos

Las áreas de práctica son la base para el examen y los requisitos de experiencia para lograr la certificación CISA. Estas áreas de práctica consisten en tareas y declaraciones de conocimiento organizados en dominios, cuyas definiciones y el porcentaje de preguntas que les corresponde en el examen son brevemente descritas a continuación. Para mayor información se puede consultar la Guía de candidatos al examen CISA [21].

• Dominio 1: Proceso de auditoría de sistemas de información (14%). Para brindar servicios de auditoría de sistemas acorde a las normas, guías, estándares y mejores prácticas para apoyar a la organización a asegurar que sus sistemas y la tecnología de información están protegidos y controlados.

• Dominio 2: Gobierno y gestión de TI (14%). Para proporcionar aseguramiento de que la organización tiene la estructura, las políticas, los mecanismos de control y supervisión necesarias para cumplir los requisitos del gobierno corporativo y la gestión de las TI.

• Dominio 3: Adquisición, desarrollo e implementación de sistemas de información (19%). Para proporcionar aseguramiento de que las prácticas de gestión para el desarrollo, adquisición, testing e implementación de los sistemas de información satisfacen los objetivos y la estrategia de la organización.

• Dominio 4: Operaciones, mantenimiento y soporte de sistemas de información (23%). Para proporcionar aseguramiento de que las prácticas de gestión para la operación, mantenimiento y soporte de los sistemas de información satisfacen los objetivos y la estrategia de la organización.

• Dominio 5: Protección de los activos de información (30%). Para proporcionar aseguramiento de que la arquitectura de seguridad (políticas, estándares, procedimientos y controles) aseguran la confidencialidad, integridad y disponibilidad de los activos de información.

En la figura 6.3 se muestran gráficamente dichos dominios y su porcentaje.

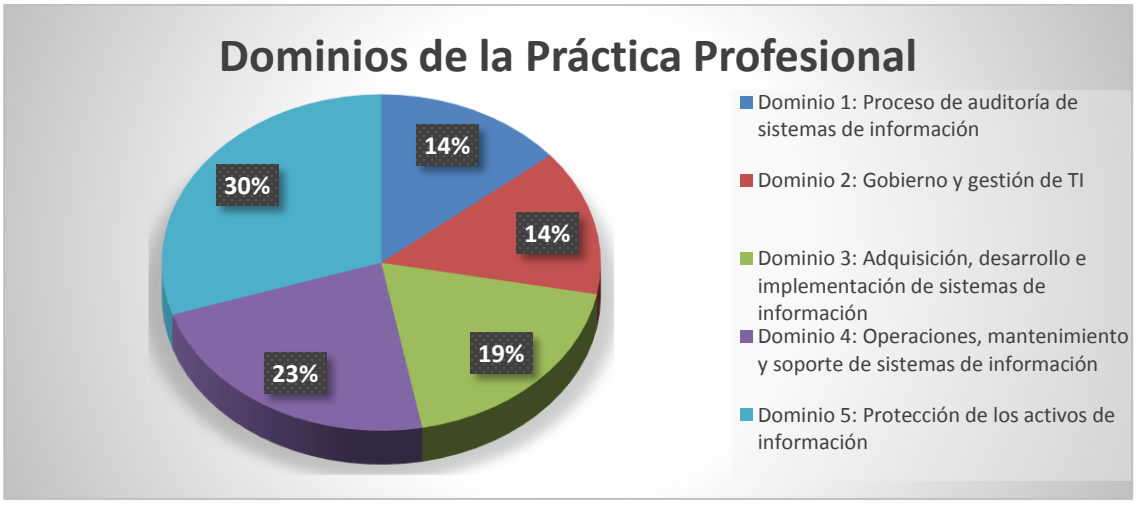

Figura 6.3: Dominios y porcentajes de Experiencia para CISA.
Fuente: ISACA.

6.1.5 Cómo obtener la certificación

Uno de los requisitos que tienen que tener los candidatos es una experiencia previa de 5 o más años en auditoría, control o seguridad de SI. Si no se dispone de la experiencia requerida, están disponibles convalidaciones de hasta un máximo de tres años de la experiencia requerida, que se pueden obtener de la siguiente forma manera:

- Un año puede ser convalidado por un año de experiencia en sistemas de información o un año de experiencia en auditorías de otro tipo de sistemas que no sean SI.
- Entre 60 y 120 horas de créditos de estudios universitarios (equivalente a un grado de 2 o 4 años respectivamente) puede sustituir 1 o 2 años de la experiencia requerida.
- Una licenciatura o máster en una universidad que incluya en su currículum formación de ISACA (ver listado de universidades en www.isaca.org/modeluniversities) sustituye un año de la experiencia requerida. Esta opción no puede ser utilizada si ya se han convalidado 3 años de experiencia debida a estudios realizados.
- Un máster en seguridad de la información o en tecnología de la información proporcionado por una universidad acreditada, sustituye 1 año de la experiencia requerida.
- Dos años de experiencia como profesor a tiempo completo de informática, contabilidad o auditoría de sistemas de información, sustituye a un 1 año de la experiencia requerida.

Para mantener la certificación es necesaria la obtención de 120 CPEs en ciclos de 3 años con un mínimo de 20 CPEs anuales y el pago de una cuota anual de 45 $ para miembros de ISACA y 85$ para el resto.

6.1.6 Exámenes

Los exámenes para acceder a las certificaciones de ISACA se realizan en 3 convocatorias anuales: Junio, Septiembre y Diciembre.

En España, se realizan en Diciembre y Junio en las ciudades de Madrid, Barcelona, Valencia, Logroño. La convocatoria en Septiembre sólo se realiza en Madrid.

Los idiomas oficiales de los exámenes son chino mandarín simplificado, inglés, francés, japonés, coreano, español, turco. En la convocatoria de Junio, además se pueden realizar en chino mandarín tradicional, alemán, hebreo e italiano.

En la siguiente tabla (figura 6.4) se muestran los precios de inscripción para el examen del 13 de junio de 2015. Hay que tener en cuenta que las fechas y los precios pueden variar cada año, por lo que se recomienda visitar la web de ISACA [10] para más información.

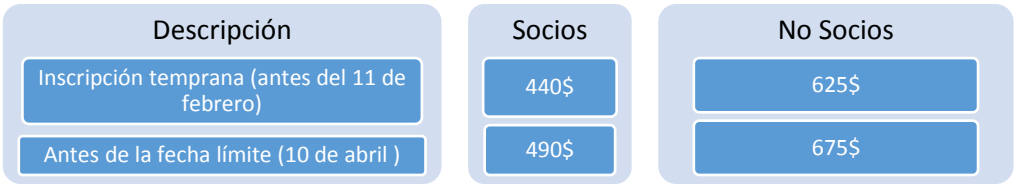

Figura 6.4: Fechas y precios de inscripción al examen de CISA.
Fuente: ISACA. Fecha de consulta Octubre-2015.

Los manuales disponibles en español son: “Manual de Preguntas y Explicaciones de Preparación al Examen CISA 2014”, “Manual de Preguntas y Explicaciones de Preparación al Examen CISA Suplemento 2014”, “Manual de Preguntas y Explicaciones de Preparación al Examen CISA Suplemento 2015” y “Manual de Preparación al Examen CISA 2015”.

Los exámenes de ISACA constan de ítems de selección múltiple. Las calificaciones de los candidatos se reportan como calificaciones escaladas. La calificación escalada es la conversión de la calificación bruta del candidato en un examen a una escala común. ISACA utiliza y reporta las calificaciones en una escala común de 200 a 800. Por ejemplo, una calificación de 800 en esta escala representa una puntuación perfecta, ya que se respondieron todas las preguntas correctamente; una calificación de 200 en esta escala constituye la calificación más baja posible y significa que sólo se respondió correctamente un número muy bajo de respuestas. Un candidato deberá recibir una calificación de 450 o mayor para aprobar el examen. La calificación de 450 representa un estándar consistente mínimo de conocimiento. El candidato que recibe una calificación aprobatoria, puede entonces solicitar la certificación si cumple con el resto de los requisitos.

Los exámenes contienen algunas preguntas que se incluyen solamente con propósitos de investigación y análisis. Estas preguntas no están identificadas ni separadas, tampoco se utilizan para calcular su calificación final.

El examen consta de 150 preguntas a responder en un tiempo de 4 horas.

6.2 ISACA: CISM CERTIFIED INFORMATION SECURITY MANAGER

6.2.1 Introducción

La certificación CISM está respaldada por ISACA. Es una certificación para administradores de seguridad de la información. Es una de las certificaciones más solicitadas en el mercado laboral de las TIs y la principal certificación para administradores de seguridad.

Está enfocada fundamentalmente a la administración de seguridad de la información y a la gerencia. A diferencia de otras certificaciones de seguridad, CISM define los principales estándares de competencias y desarrollo profesionales que un director de seguridad de la información debe poseer, competencias necesarias para dirigir, diseñar, revisar y asesorar un programa de seguridad de la información.

El CISM es el estándar aceptado globalmente para las personas que diseñan, construyen y gestionan los programas de seguridad de la información empresarial.

En la actualidad hay 25.000 certificados en CISM, según se indica en la web de ISACA [10].

6.2.2 Candidatos

CISM es la principal certificación para administradores de seguridad de la información. El último índice trimestral de valoración de Habilidades y Certificaciones IT (ITSCPI) de Foote Partners clasificó a CISM como la más codiciada y la que más se paga de las certificaciones de seguridad.

6.2.3 Mercado laboral

En el mercado de la seguridad de la información, CISM está diseñada específicamente y exclusivamente para personas que tienen experiencia en el manejo de programas de seguridad. La formación necesaria para obtener la certificación, así como los exámenes, están orientados, sobre todo a los gerentes, administradores y directores de seguridad.

La certificación CISM está orientada a la gerencia de riesgos y gestión de seguridad de la información.

Se centra exclusivamente en la administración de la seguridad de la información.

6.2.4 Conocimientos

Los dominios sobre los que hay que demostrar conocimientos para obtener la certificación se muestran en la figura 6.1, en la que se indica también el porcentaje de preguntas que les corresponde en el examen.

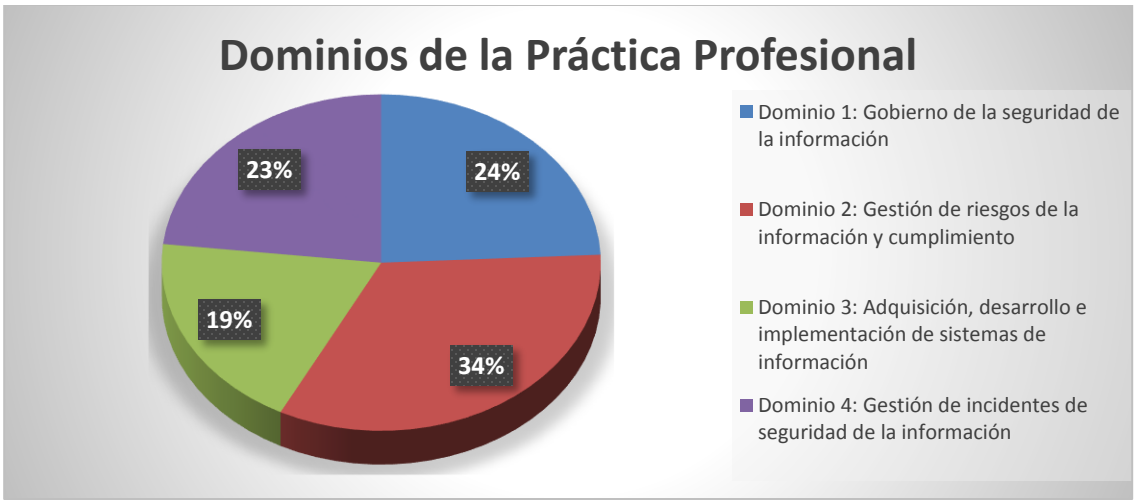

Figura 6.1: Dominios y porcentajes de Experiencia para CISM.
Fuente: ISACA.

6.2.5 Cómo obtener la certificación

La clasificación para CISM requiere una combinación de experiencia, ética, educación y además superar un examen. En concreto, los requisitos son:

1º Aprobar el examen CISM.

2º Cumplir con el código de ética profesional de ISACA.

3º Comprometerse a cumplir con la política de educación profesional continua (CPE).

4º Demostrar un mínimo de cinco años de experiencia laboral en seguridad de la información, con un mínimo de tres años de experiencia laboral en gerencia de seguridad de la información en tres o más de las áreas de práctica laboral de la seguridad. Hay ciertas exenciones si se cumplen ciertos requisitos de educación o certificación.

Una vez que el candidato haya superado el examen de certificación CISM y ha cumplido con los requisitos de experiencia laboral, el último paso es completar una solicitud para recibir la certificación. Las solicitudes se realizarán en inglés y los candidatos deben indicar lo siguiente:

- Experiencia en gestión de seguridad de la información (3 o más años).
- Experiencia general en seguridad de la información.
- Sustitución de experiencia general en seguridad de la información. En caso de no tener experiencia laboral, se puede justificar con títulos académicos. No puede ser mayor que dos años, que es el máximo permitido de sustitución de experiencia general en seguridad de la información.

En total, la experiencia para optar a esta certificación tiene que ser superior a 5 años en seguridad de la información, de los cuales, tres o más años deben ser de experiencia en la gestión de la seguridad.

Para mantener la certificación es necesario seguir una política continuada de educación profesional. Cada persona certificada debe obtener un mínimo de 20 horas anuales de CPEs y 120 horas en total para cada ciclo de tres años.

El objetivo de la política de educación profesional continua es asegurar que todos los certificados de ISACA mantengan un nivel adecuado de conocimientos actuales y pericia en el campo de la auditoría, control y seguridad de sistemas de información.

Además se requiere una cuota anual de mantenimiento de 45$ para los miembros de ISACA y 80$ para el resto.

6.2.6 Exámenes

Los exámenes para acceder a las certificaciones de ISACA se realizan en 3 convocatorias anuales: Junio, Septiembre y Diciembre.

En España, se realizan en Diciembre y Junio en las ciudades de Madrid, Barcelona, Valencia, Logroño. La convocatoria en Septiembre sólo se realiza en Madrid.

Los idiomas oficiales de los exámenes son inglés, español, coreano y japonés (éstos dos últimos solo para el examen de Junio).

En la siguiente tabla (figura 6.2) se muestran los precios de inscripción para el examen del 13 de junio de 2015. Hay que tener en cuenta que las fechas y los precios pueden variar cada año, por lo que se recomienda visitar la web de ISACA [10] para más información.

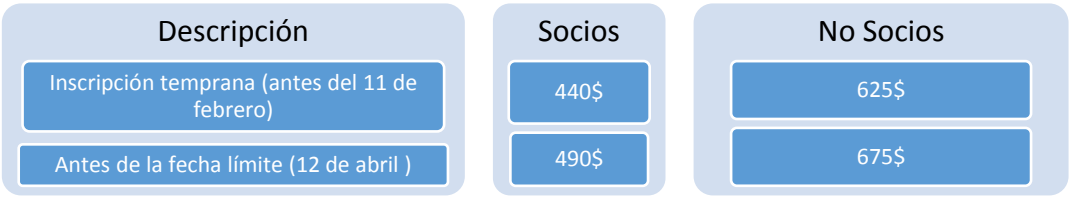

Figura 6.2: Fechas y precios de inscripción al examen de CISM.
Fuente: ISACA. Fecha de consulta Octubre-2015.

Para la preparación de los exámenes ISACA, se dispone de manuales en diferentes idiomas. En el año 2014, se han publicado en inglés, español y japonés.

Los manuales disponibles en español son: “Manual de Preguntas y Explicaciones de Preparación al Examen CISM 2014”, “Manual de Preguntas y Explicaciones de Preparación al Examen CISM

Suplemento 2014", "Manual de Preguntas y Explicaciones de Preparación al Examen CISM Suplemento 2015" y "Manual de Preparación al Examen CISM 2015", que se pueden adquirir en su página web (https://www.isaca.org/bookstore/Pages/CISM-Exam-Resources.aspx). En estos manuales, se detallan, entre otros temas, 100 nuevas preguntas de ejemplo, sus respuestas y explicaciones para ayudar a los candidatos a prepararse eficazmente para el examen CISM. Estas nuevas preguntas están diseñadas para ser similares a los exámenes reales y se presentan de dos formas:

- Ordenadas por área de práctica de trabajo, lo cual permite a los candidatos CISM concentrarse en ciertos temas en particular.
- Mezcladas, simulando un ejemplo de examen de 100 preguntas, lo cual permite a los candidatos identificar, de manera eficaz, sus fortalezas y debilidades, así como simular un examen real.

ISACA utiliza una escala de 200 a 800 puntos, siendo 450 el aprobado para los exámenes. La puntuación de examen no se basa en una media aritmética. Una calificación de 450 representa un estándar consistente mínimo de conocimiento a lo establecido para el examen por el respectivo Comité de Certificación de ISACA.

El examen consta de 200 preguntas de opción múltiple y su duración es de 4 horas.

Las certificaciones CISM y CISA son diferentes aunque hay cierta tendencia a confundirlas. CISA, es más antigua está orientada a la auditoría mientras que CISM se centra exclusivamente en la administración y la gestión de la seguridad de la información.

En cuanto al número de certificados, es mayor el número de certificados es CISA (109.000) que el de certificados es CISM (25.000) pero está ultima es una de las certificaciones más solicitadas y mejor pagadas.

Para conseguir la certificación CISM se necesitan 5 años de experiencia en seguridad con un mínimo de 3 en gerencia de seguridad mientras que para CISA se necesitan 5 años de experiencia en auditoria de seguridad de la información. El coste de ambas certificaciones es el mismo.

6.3 ISACA: CRISC CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL

6.3.1 Introducción

El CRISC es un Certificado en Sistemas de Información de Riesgos y Control. Es una nueva certificación del 2010 de ISACA. La certificación ha sido diseñada para profesionales de TI y de negocios

que identifiquen y gestionen los riesgos mediante la elaboración, implementación y mantenimiento de sistemas adecuados de información de los controles.

En la actualidad hay 17.000 certificados en CRISC, según se indica en la web de ISACA [10].

6.3.2 Candidatos

CRISC está diseñado exclusivamente para Profesionales de Riesgo y Control de Información que:

- Identifican, valoran y analizan los riesgos.
- Diseñan, implantan y mantienen controles para gestionar los riesgos.
- Responden a eventos de riesgo.

6.3.3 Mercado laboral

Según las estadísticas publicadas en ISACA, los certificados en CRISC trabajan en puestos de director ejecutivo dentro de sus organizaciones, como responsables o directores de áreas de auditoría, como directores de seguridad de la información (CISO: *Chief Information Security Officer*), como directores, gestores, consultores en áreas de seguridad o de auditoría.

6.3.4 Conocimientos

Los cinco dominios de la práctica profesional son los siguientes.

- Dominio1. Identificación valoración y evaluación de riesgos (31%): identificar, valorar evaluar el riesgo y para habilitar la ejecución de la estrategia de gestión de riesgos de la empresa.
- Dominio 2. Respuesta ante riesgos (17%): desarrollar e implementar las respuestas ante riesgos para garantizar qué cuestiones, oportunidades e incidencias de riesgos se atiendan de manera efectiva en términos de coste y de acuerdo con los objetivos del negocio.
- Dominio 3. Monitorización de riesgos (17%): monitorizar los riesgos y comunicar información a las áreas interesadas relevantes para garantizar la efectividad de la estrategia de gestión de riesgos de la empresa.
- Dominio 4. Diseño e implantación de mecanismos de control de SI (17%): diseñar e implementar controles de SI de acuerdo con los niveles de necesidad y tolerancia para apoyar los objetivos del negocio.
- Dominio 5. Monitorización y mantenimiento de SI (18%): monitorizar y mantener los controles de SI para asegurar su funcionamiento efectivo y eficiente.

En la figura 6.5 se muestran gráficamente dichos dominios y su porcentaje.

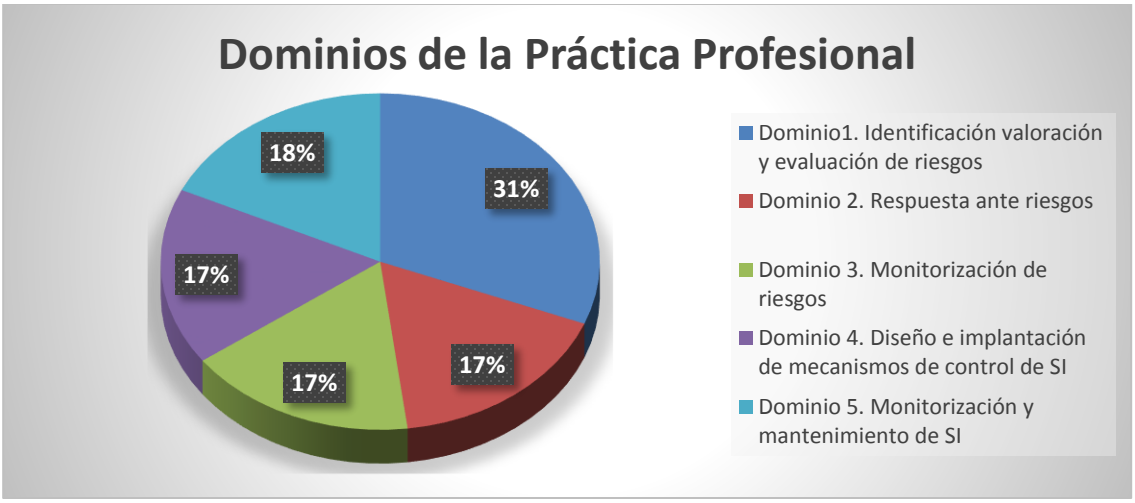

Figura 6.5: Dominios y porcentajes de Experiencia para CRISC.
Fuente: ISACA.

6.3.5 Cómo obtener la certificación

Para acceder a la certificación se deben cumplir los siguientes requisitos:

1º Aprobar el examen.

2º Aportar evidencias verificables de una experiencia laboral de al menos 3 años en el ámbito de riesgos y control de sistemas de SI, cubriendo 3 de los 5 dominios de práctica profesional indicados en el apartado anterior.

3º Enviar la solicitud cumplimentada dentro de los 5 años posteriores a la aprobación del examen.

4º Adherirse al código de ética profesional de ISACA.

5º Cumplir con la política de educación profesional continuada (CPE) de CRISC. Los requisitos de dicha política son los siguientes:

- Obtener un mínimo de 20 horas de CPE al año.
- Obtener un mínimo de 120 horas por ciclos de 3 años.
- Pagar la cuota de mantenimiento anual.
- Presentar la documentación requerida de actividades de educación continuada en caso de ser seleccionado por una auditoría anual.

Para solicitar la certificación se ha de hacer directamente a ISACA internacional. La solicitud está disponible en la Web. Dicha solicitud contiene al detalle los requisitos necesarios para obtener la certificación, el código de ética profesional, las instrucciones para cumplimentar el formulario, la verificación

de la experiencia laboral. Desde el 1 de junio de 2012 se aplica una tarifa de 50$ para solicitar la certificación.

Hasta que una solicitud no sea recibida y aprobada, los candidatos no son certificados CRISC, y por tanto no pueden utilizar este título. Los candidatos disponen de 5 años desde la fecha de aprobación del examen para solicitar la aprobación. Posteriormente el examen se anulará.

Para mantener la certificación es necesaria la obtención de 120 CPEs en ciclos de 3 años con un mínimo de 20 CPEs anuales y el pago de una cuota anual de 45 $ para miembros de ISACA y 85$ para el resto.

6.3.6 Exámenes

Los exámenes para acceder a las certificaciones de ISACA se realizan en 2 convocatorias anuales: Junio y Diciembre.

El examen, que es en inglés, aunque a partir de junio del 2015 se podrá realizar en español, se ofrece en más de 240 lugares del mundo, lugares en los que hay una delegación de ISACA, o donde haya un grupo de individuos interesados en examinarse. En España, se realizan en las ciudades de Madrid, Barcelona, Valencia y Logroño.

En la siguiente tabla (figura 6.6) se muestran los precios de inscripción para el examen del 13 de junio de 2015. Hay que tener en cuenta que las fechas y los precios pueden variar cada año, por lo que se recomienda visitar la web de ISACA [10] para más información.

Figura 6.6: Fechas y precios de inscripción al examen de CRISC.
Fuente: ISACA. Fecha de consulta Octubre-2015.

Los manuales disponibles en español son: “Manual de Preguntas y Explicaciones de Preparación al Examen CRISC 2015”, “Manual de Preguntas y Explicaciones de Preparación al Examen CRISC Suplemento 2015”, “Manual de Preparación al Examen CRISC 2015”.

El examen consta de 150 preguntas a responder en un tiempo de 4 horas.

6.4 ISACA: CGEIT CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT

6.4.1 Introducción

ISACA ha desarrollado una nueva certificación denominada CGEIT (Certified in the Governance of Enterprise IT) Certificado en Gestión TI de Empresas, que permite a las empresas disponer de profesionales capaces de aplicar las mejores prácticas y obtener los mejores resultados en la gestión de los Sistemas de Información y Comunicaciones.

La ANSI (American National Standards Institute) ha acreditado la certificación CGEIT bajo la ISO/IEC 17024:2013. Esta acreditación significa que los procedimientos de ISACA cumplen los principales requisitos sobre procesos de desarrollo accesibles, consensuados y estandarizados.

En la actualidad hay 6.000 certificados en CGEIT, según se indica en la web de ISACA [10].

6.4.2 Candidatos

El certificado está orientado a profesionales de las áreas de gestión, asesoramiento y auditoría de las tecnologías de la información.

6.4.3 Mercado laboral

El proceso de certificación ha sido específicamente desarrollado para profesionales que tienen un significativo rol de gestión, asesoría o aseguramiento relacionado al gobierno de TI. La certificación promueve el avance de profesionales que desean ser reconocidos por su conocimiento y experiencia relacionados con el gobierno de las tecnologías de la información (TI).

La certificación también está orientada a:

- Apoyar las crecientes demandas de negocios relacionadas con el gobierno de TI.
- Incrementar la sensibilidad y la importancia de las buenas prácticas y los aspectos del gobierno de TI.
- Definir los roles y responsabilidades de los profesionales que realizan trabajos de gobierno de TI.

6.4.4 Conocimientos

Los dominios de la práctica profesional se muestran en la figura 6.7:

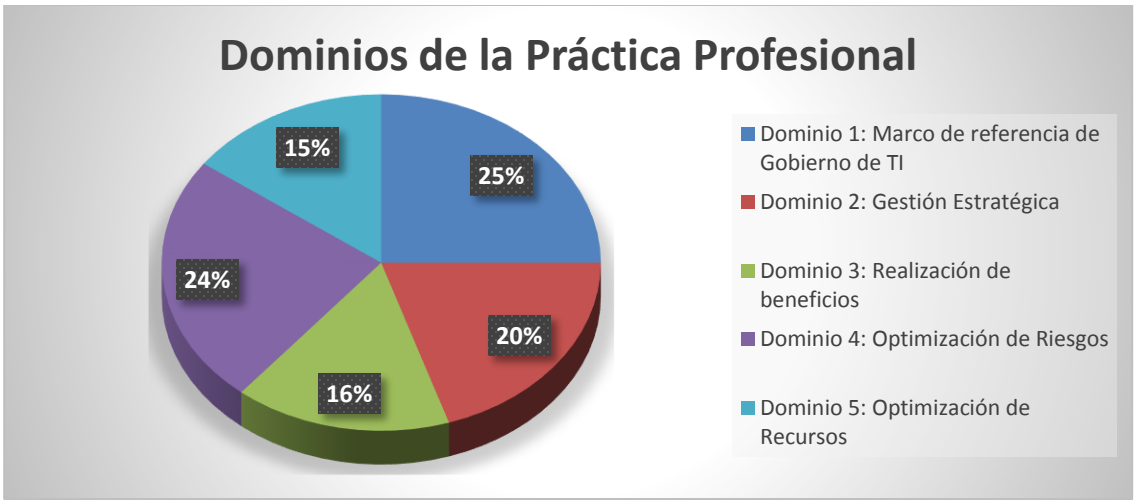

Figura 6.7: Dominios y porcentajes de Experiencia para CGEIT.
Fuente: ISACA.

6.4.5 Cómo obtener la certificación

Para obtener la certificación hay que cumplir con los siguientes requisitos:

1º Aprobar el examen.

2º Aportar evidencias verificables de una experiencia laboral de al menos 5 años en los ámbitos definidos en los dominios de práctica profesional CGEIT (indicados en el apartado anterior).

3º Enviar la solicitud en los 5 años siguientes de aprobar el examen.

4º Adherirse al código de ética profesional de ISACA.

5º Cumplir con la política de educación profesional continuada.

Una vez aprobado el examen, se solicita la certificación a través de ISACA internacional, cuyo coste es de 50$. Dicha solicitud se encuentra disponible en su página web y contiene lo siguiente:

- Formulario de solicitud CGEITT
- Detalle de los requisitos necesarios para obtener la certificación y que han sido indicados con anterioridad.
- Código de ética profesional.
- Instrucciones para cumplimentar el formulario.
- Verificación de la experiencia laboral para el formulario de solicitud.

Una vez obtenida la certificación, esta debe renovarse anualmente. Para ello se debe obtener un mínimo de 20 horas de educación profesional al año y de 120 horas por ciclos de tres años. Además es necesario presentar la documentación requerida de estas actividades en caso de ser seleccionado en una auditoría anual. También hay una cuota de mantenimiento anual (45 $ para miembros de ISACA y 85 $ para el resto) y cumplir con el código de ética profesional de ISACA. Actualmente, se ofrece un curso oficial en ISACA Madrid de preparación para la certificación.

6.4.6 Exámenes

Los exámenes para acceder a las certificaciones de ISACA se realizan en 2 convocatorias anuales: Junio y Diciembre.

El examen es en inglés. En España, se realizan en Diciembre y Junio en las ciudades de Madrid, Barcelona, Valencia y Logroño.

En la siguiente tabla (figura 6.8) se muestran los precios de inscripción para el examen del 13 de junio de 2015. Hay que tener en cuenta que las fechas y los precios pueden variar cada año, por lo que se recomienda visitar la web de ISACA [10] para más información.

Figura 6.8: Fechas y precios de inscripción al examen de CGEIT.
Fuente: ISACA. Fecha de consulta Octubre-2015.

Los manuales disponibles en español son: “Manual de Preguntas y Explicaciones de Preparación al Examen CGEIT 2015”, “Manual de Preguntas y Explicaciones de Preparación al Examen CGEIT Suplemento 2015”, “Manual de Preparación al Examen CGEIT 2015”.

El examen consta de 150 preguntas a responder en un tiempo de 4 horas.

6.5 ISACA: RESUMEN

6.5.1 Código ética ISACA

Para obtener cada una de las certificaciones hay que adherirse al código de ética de ISACA cuyos principios se muestra en la figura 6.9:

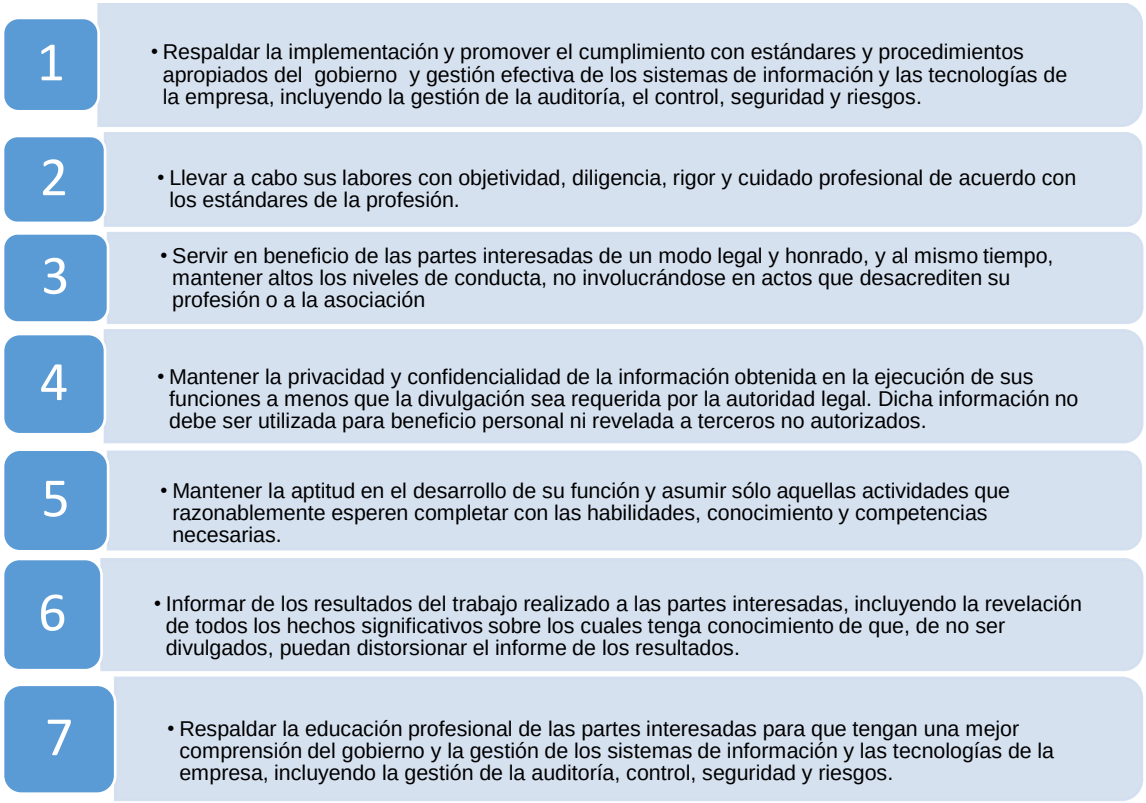

Figura 6.9: Código ética ISACA.
Fuente: ISACA.

6.5.2 Preguntas de exámenes

ISACA realiza dos convocatorias anuales de sus cuatro certificaciones: una en Junio, y una en Diciembre. Adicionalmente, sólo para CISA y CISM existe una tercera fecha, en Septiembre.

Se muestra a continuación, en la figura 6.10, la información sobre el número de preguntas y la duración de cada uno de los exámenes de las certificaciones de ISACA, así como los idiomas en los que se puede realizar.

CERTIFICACIÓN	PREGUNTAS	DURACIÓN	IDIOMAS	ESPAÑA	CONVOCATORIAS
CISA	200 preguntas de opción múltiple	4 horas	Chino mandarín simplificado, inglés, francés, japonés, coreano, español y turco. Chino mandarín, alemán, hebreo, e italiano (sólo convocatoria Junio).	Madrid	Junio, Septiembre, Diciembre
CISM	200 preguntas de opción múltiple	4 horas	Inglés y español. Japonés y coreano (sólo convocatoria Junio).	Madrid	
CGEIT	150 preguntas de opción múltiple	4 horas	Inglés.	Madrid	Junio, Diciembre
CRISC	150 preguntas de opción múltiple	4 horas	Inglés y español.	Madrid	

Figura 6.10: Código ética ISACA.
Fuente: ISACA. Fecha de Consulta: Octubre 2015.

6.5.3 Precios de exámenes

La inscripción en el examen, así como la compra del material de estudio se realiza directamente a través de ISACA Internacional.

A continuación, en la figura 6.11 se muestran los importes de inscripción a los exámenes en UDS

CERTIFICACIÓN	SOCIOS	NO SOCIOS	DESCRIPCIÓN
CGEIT/CRISC	440	625	Online inscripción temprana
CGEIT/CRISC	515	700	Por correo/ fax, inscripción temprana
CGEIT/CRISC	490	675	Online antes de la fecha límite
CGEIT/CRISC	565	750	Por correo/ fax, antes de la fecha límite
CISM/CISA	440	625	Inscripción temprana online
CISM/CISA	490	675	Antes de la fecha límite online

Figura 6.11: Importe inscripción exámenes certificaciones ISACA.
Fuente: ISACA. Fecha Consulta Octubre 2015.

7 CONCLUSIONES

Las certificaciones de seguridad que existen actualmente son muy diversas y aportan a los candidatos nuevas capacidades para encontrar trabajo o mejorar el actual. En un mundo globalizado y con un mercado de trabajo donde cada vez más se necesitan profesionales en IT especializados en algún campo en particular, las certificaciones en seguridad informática otorgan unos conocimientos y habilidades cada vez más demandadas por las empresas. Cada una de las certificaciones posee unos requisitos y aporta unos conocimientos distintos que deben ser valorados por los candidatos para elegir la que más se adecue a sus necesidades.

Si realizamos una comparativa en cuanto al número de personas certificadas en alguno de los certificados disponibles en el mercado, vemos que las entidades ISACA e (ISC)^2 destacan claramente sobre el resto, habiendo aportado al mercado, entre las dos, casi la mitad del total de profesionales certificados, como podemos ver en la figura 8.2. De éstas dos, los certificados de ISACA son algo más demandados que los de (ISC)^2.

En la figura 8.3 podemos ver que la demanda por tipo de certificado dentro de ISACA no es nada uniforme. De hecho, en torno al 70% de los profesionales certificados por esta entidad eligió la certificación CISA. Este dato no puede tomarse como concluyente, ya que esta certificación fue la primera que ofreció ISACA y, por tanto, la que más tiempo ha estado disponible en el mercado, pero da una idea de cuál es el perfil en seguridad más demandado por las empresas en general.

En la figura 8.4 se puede observar que la certificación más solicitada de (ISC)^2 es CISSP, elegida por más del 90% de las personas certificadas por esta entidad.

Por otro lado, en cuanto a cuotas de examen se refiere, las certificaciones de ISACA tienen todas el mismo precio mientras que el coste de las de (ISC)^2 varía bastante dependiendo de la certificación elegida. En cuanto al precio por certificación, la de menor coste de inscripción es SSCP, estando en el lado opuesto CISSP, ambas de (ISC)^2, que es la más cara.

En el caso del coste de mantenimiento anual, las certificaciones de ISACA conllevan un menor coste si se es socio de la misma y si se hace la inscripción de manera temprana. En caso contrario son más caras, en general, que las de (ISC)^2. Concretando un poco más, las más caras son CCFP y CSSLP, ambas con un coste de mantenimiento de 100$ y ambas de (ISC)^2. Las más baratas serían CAP y SSCP, ambas con un precio de 65$ y también de (ISC)^2. Las de ISACA serían las más baratas de mantener en caso de ser socio (45$).

La duración de los exámenes de ISACA es, en todos los casos, de 4 horas. Todos constan de 150 preguntas, excepto el de CISM, que tiene 200. En el caso de (ISC)^2 los exámenes duran 3 o 4 horas y el número de preguntas varía entre 125, 175 y 250, dependiendo de la certificación.

Es destacable que todos los exámenes se pueden realizar en España, casi siempre en Madrid y Barcelona, excepto las certificaciones de ISACA, cuyos exámenes también se pueden realizar, en Valencia y Logroño en determinadas convocatorias (además de en Madrid y Barcelona). La mayor facilidad que ofrece ISACA para realizar los exámenes puede ser uno de los motivos por los que es la entidad certificadora más demandada, como se dijo anteriormente. En cuanto al idioma, todos los exámenes de ISACA, menos el de CRISC, se pueden realizar en español. Sin embargo, de $(ISC)^2$ sólo se puede realizar en español el de CISSP.

Como trabajo futuro o mejoras a incluir, el presente trabajo se podría ampliar con la creación de una web de consulta. Dado que gran parte de la información que aquí se presenta, como fechas y lugares de los exámenes o temario, van variando con el tiempo, en una web esta información se podría mantener actualizada, de manera que resulte útil para todo aquel profesional interesado en obtener alguna de las certificaciones en seguridad informática que aquí se presentan.

8 ANEXO A

En el ANEXO A se muestran tablas resumen del contenido de este informe y la representación gráfica de algunos datos.

8.1 TABLA 1: REQUISITOS PARA OBTENER LAS CERTIFICACIONES DE (ISC)² E ISACA

Requisitos para obtener las certificaciones

EMPRESA ASOCIACION	(ISC)²								ISACA			
CERTIFICACIÓN	**CAP**	**CCFP**	**CISSP**	**CISSP-ISSAP**	**CISSP-ISSEP**	**CISSP-ISSMP**	**CSSLP**	**SSCP**	**CISA**	**CISM**	**CGEIT**	**CRISC**
EXPERIENCIA PREVIA	MÍNIMO 2 AÑOS DE EXPERIENCIA EN UNO O MÁS DE LOS 7 DOMINIOS DE CAP (ISC)²	TÍTULO UNIVERSITARIO, 3 AÑOS DE ANÁLISIS FORENSE Y MÍNIMO DE 3 AÑOS DE EXPERIENCIA EN 3 DE LOS 6 DOMINIOS DE CCFP (ISC)²	TÍTULO UNIVERSITARIO Y 5 AÑOS DE EXPERIENCIA EN 2 O MÁS DE LOS 10 DOMINIOS CISSP (ISC)²	CERTIFICADO EN CISSP Y 2 AÑOS DE EXPERIENCIA EN ARQUITECTURA	CERTIFICADO EN CISSP Y 2 AÑOS DE EXPERIENCIA EN INGERNIERÍA	CERTIFICADO EN CISSP Y 2 AÑOS DE EXPERIENCIA EN GESTIÓN	MÍNIMO 4 AÑOS DE EXPERIENCIA EN ALGUNO DE LOS 8 DOMINIOS DE CSSLP (ISC)²	MÍNIMO 1 AÑO DE EXPERIENCIA EN ALGUNO DE LOS 7 DOMINIOS DE SSCP (ISC)²	MÍNIMO 5 DE EXPERIENCIA EN AUDITORÍA , CONTROL O SEGURIDAD DE LA INFORMACIÓN	MÍNIMO 5 AÑOS DE EXPERIENCIA LABORAL EN SEGURIDAD CON UN MÍNIMO DE 3 EN GERENCIA DE SEGURIDAD EN 3 O MÁS ÁREAS DE LA PRÁCTICA LABORAL DE LA SEGURIDAD	MÍNIMO 3 AÑOS DE EXPERIENCIA EN RIESGOS Y CONTROL DE SI, CUBRIENDO 3 DE LOS 5 DOMINIOS DE LA PRÁCTICA PROFESIONAL DE ISACA	MÍNIMO 5 DE EXPERIENCIA CUBRIENDO LOS DOMINIOS DE PRÁCTICA PROFESIONAL DE ISACA
EXAMEN	APROBAR EL EXAMEN OBTENIENDO 700 PUNTOS SOBRE 1000.	APROBAR EL EXAMEN OBTENIENDO 700 PUNTOS SOBRE 1000.	APROBAR EL EXAMEN OBTENIENDO 700 PUNTOS SOBRE 1000.	APROBAR EL EXAMEN OBTENIENDO 700 PUNTOS SOBRE 1000.	APROBAR EL EXAMEN OBTENIENDO 700 PUNTOS SOBRE 1000.	APROBAR EL EXAMEN OBTENIENDO 700 PUNTOS SOBRE 1000.	APROBAR EL EXAMEN OBTENIENDO 700 PUNTOS SOBRE 1000.	APROBAR EL EXAMEN OBTENIENDO 700 PUNTOS SOBRE 1000.	APROBAR EL EXAMEN SUPERANDO LOS 450 PUNTOS SOBRE 800	APROBAR EL EXAMEN SUPERANDO LOS 450 PUNTOS SOBRE 800	APROBAR EL EXAMEN SUPERANDO LOS 450 PUNTOS SOBRE 800	APROBAR EL EXAMEN SUPERANDO LOS 450 PUNTOS SOBRE 800
OTROS REQUISITOS	AVAL POR UN MIEMBRO DE LA ASOCIACIÓN (EN LOS 9 MESES POSTERIORES A APROBAR EL EXAMEN) Y SUSBCRIPCION CÓDIGO ÉTICA (ISC)²	AVAL POR UN MIEMBRO DE LA ASOCIACIÓN (EN LOS 9 MESES POSTERIORES A APROBAR EL EXAMEN) Y SUSBCRIPCION CÓDIGO ÉTICA (ISC)²	AVAL POR UN MIEMBRO DE LA ASOCIACIÓN (EN LOS 9 MESES POSTERIORES A APROBAR EL EXAMEN) Y SUSBCRIPCION CÓDIGO ÉTICA (ISC)²	AVAL POR UN MIEMBRO DE LA ASOCIACIÓN (EN LOS 9 MESES POSTERIORES A APROBAR EL EXAMEN) Y SUSBCRIPCION CÓDIGO ÉTICA (ISC)²	AVAL POR UN MIEMBRO DE LA ASOCIACIÓN (EN LOS 9 MESES POSTERIORES A APROBAR EL EXAMEN) Y SUSBCRIPCION CÓDIGO ÉTICA (ISC)²	AVAL POR UN MIEMBRO DE LA ASOCIACIÓN (EN LOS 9 MESES POSTERIORES A APROBAR EL EXAMEN) Y SUSBCRIPCION CÓDIGO ÉTICA (ISC)²	AVAL POR UN MIEMBRO DE LA ASOCIACIÓN (EN LOS 9 MESES POSTERIORES A APROBAR EL EXAMEN) Y SUSBCRIPCION CÓDIGO ÉTICA (ISC)²	AVAL POR UN MIEMBRO DE LA ASOCIACIÓN (EN LOS 9 MESES POSTERIORES A APROBAR EL EXAMEN) Y SUSBCRIPCION CÓDIGO ÉTICA(ISC)²	ENVIAR SOLICITUD EN LOS 5 AÑOS POSTERIORES A LA APROBACIÓN DE EXAMEN Y ADHERIRSE AL CÓDIGO DE ÉTICA DE ISACA	ENVIAR SOLICITUD EN LOS 5 AÑOS POSTERIORES A LA APROBACIÓN DE EXAMEN Y ADHERIRSE AL CÓDIGO DE ÉTICA DE ISACA	ENVIAR SOLICITUD EN LOS 5 AÑOS POSTERIORES A LA APROBACIÓN DE EXAMEN Y ADHERIRSE AL CÓDIGO DE ÉTICA DE ISACA	ENVIAR SOLICITUD EN LOS 5 AÑOS POSTERIORES A LA APROBACIÓN DE EXAMEN Y ADHERIRSE AL CÓDIGO DE ÉTICA DE ISACA

8.2 TABLA 2: EXÁMENES DE (ISC)² E ISACA

EXÁMENES												
EMPRESA ASOCIACION	(ISC)²								ISACA			
CERTIFICACIÓN	CAP	CCFP	CISSP	CISSP-ISSAP	CISSP-ISSEP	CISSP-ISSMP	CSSLP	SSCP	CISA	CISM	CGEIT	CRISC
PREGUNTAS	125 PREGUNTAS DE OPCIÓN MÚLTIPLE CON 4 OPCIONES CADA UNA	125 PREGUNTAS DE OPCIÓN MÚLTIPLE CON 4 OPCIONES CADA UNA	250 PREGUNTAS DE OPCIÓN MÚLTIPLE CON 4 OPCIONES CADA UNA	125 PREGUNTAS DE OPCIÓN MÚLTIPLE CON 4 OPCIONES CADA UNA	150 PREGUNTAS DE OPCIÓN MÚLTIPLE CON 4 OPCIONES CADA UNA	125 PREGUNTAS DE OPCIÓN MÚLTIPLE CON 4 OPCIONES CADA UNA	175 PREGUNTAS DE OPCIÓN MÚLTIPLE CON 4 OPCIONES CADA UNA	125 PREGUNTAS DE OPCIÓN MÚLTIPLE CON 4 OPCIONES CADA UNA	150 PREGUNTAS DE OPCIÓN MÚLTIPLE CON 4 OPCIONES CADA UNA	200 PREGUNTAS DE OPCIÓN MÚLTIPLE CON 4 OPCIONES CADA UNA	150 PREGUNTAS DE OPCIÓN MÚLTIPLE CON 4 OPCIONES CADA UNA	150 PREGUNTAS DE OPCIÓN MÚLTIPLE CON 4 OPCIONES CADA UNA
DURACION	3 HORAS	3 HORAS	3 HORAS	3 HORAS	3 HORAS	3 HORAS	4 HORAS	3 HORAS	4 HORAS	4 HORAS	4 HORAS	4 HORAS
COSTE	ASIA, AMERICA 419$ GRAN BRETAÑA 290 LIBRAS EUROPA 280 EUROS	ASIA, AMERICA 549$ GRAN BRETAÑA 380 LIBRAS EUROPA 480 EUROS	ASIA, AMERICA 599$ GRAN BRETAÑA 415 LIBRAS EUROPA 520 EUROS	ASIA, AMERICA 399$ GRAN BRETAÑA 280 LIBRAS EUROPA 350 EUROS	ASIA, AMERICA 399$ GRAN BRETAÑA 280 LIBRAS EUROPA 350 EUROS	ASIA, AMERICA 399$ GRAN BRETAÑA 280 LIBRAS EUROPA 350 EUROS	ASIA, AMERICA 549$ GRAN BRETAÑA 380 LIBRAS EUROPA 480 EUROS	ASIA, AMERICA 250$ GRAN BRETAÑA 175 LIBRAS EUROPA 215 EUROS	INSCRIPCION TEMPRANA 440$(SOCIOS)-625$(NO SOCIOS) ANTES FECHA LIMITE 490$(SOCIOS) - 675$(NO SOCIOS)	INSCRIPCION TEMPRANA 440$(SOCIOS)-625$(NO SOCIOS) ANTES FECHA LIMITE 490$(SOCIOS) - 675$(NO SOCIOS)	INSCRIPCION TEMPRANA 440-515(SOCIOS)-625-700(NO SOCIOS) ANTES FECHA LIMITE 490-565(SOCIOS) - 675-750(NO SOCIOS)	INSCRIPCION TEMPRANA 440-515(SOCIOS)-625-700(NO SOCIOS) ANTES FECHA LIMITE 490-565(SOCIOS) - 675-750(NO SOCIOS)
APROBAR	700 PUNTOS SOBRE 1000	700 PUNTOS SOBRE 1000	700 PUNTOS SOBRE 1000	700 PUNTOS SOBRE 1000	700 PUNTOS SOBRE 1000	700 PUNTOS SOBRE 1000	700 PUNTOS SOBRE 1000	700 PUNTOS SOBRE 1000	450 PUNTOS SOBRE 800	450 PUNTOS SOBRE 800	450 PUNTOS SOBRE 800	450 PUNTOS SOBRE 800
CONVOCATORIAS	NO SE DISPONE DE INFORMACION	NO SE DISPONE DE INFORMACION	NO SE DISPONE DE INFORMACION	NO SE DISPONE DE INFORMACION	NO SE DISPONE DE INFORMACION	NO SE DISPONE DE INFORMACION	NO SE DISPONE DE INFORMACION	NO SE DISPONE DE INFORMACION	JUNIO, SEPTIEMBRE Y DICIEMBRE	JUNIO, SEPTIEMBRE Y DICIEMBRE	JUNIO Y DICIEMBRE	JUNIO Y DICIEMBRE
ESPAÑA	MADRID y BARCELONA (PEARSON VUE)	MADRID y BARCELONA (PEARSON VUE)	MADRID y BARCELONA (PEARSON VUE)	MADRID y BARCELONA (PEARSON VUE)	MADRID y BARCELONA (PEARSON VUE)	MADRID y BARCELONA (PEARSON VUE)	MADRID y BARCELONA (PEARSON VUE)	MADRID y BARCELONA (PEARSON VUE)	DICIEMBRE Y JUNIO: MADRID, BARCELONA, VALENCIA Y LOGROÑO SEPTIEMBRE: MADRID	DICIEMBRE Y JUNIO: MADRID, BARCELONA, VALENCIA Y LOGROÑO SEPTIEMBRE: MADRID	MADRID, BARCELONA, VALENCIA Y LOGROÑO	MADRID, BARCELONA, VALENCIA Y LOGROÑO
IDIOMA	INGLÉS	INGLÉS, ALEMÁN Y COREANO	INGLÉS, FRANCÉS, ALEMÁN, PORTUGUÉS, ESPAÑOL, JAPONÉS, CHINO Y COREANO	INGLÉS	INGLES	INGLES	INGLES	INGLÉS, JAPONÉS Y PORTUGUÉS	CHINO MANDARÍN SIMPLIFICADO, INGLÉS, FRANCÉS, JAPONÉS, COREANO, ESPAÑOL, TURCO, CHINO MANDARÍN TRADICIONAL, ALEMÁN, HEBREO E ITALIANO(JUNIO ESTOS 4 ÚLTIMOS)	INGLÉS, ESPAÑOL, COREANO Y JAPONÉS (ÉSTOS 2 ÚLTIMOS SÓLO PARA EL EXAMEN DE JUNIO)	INGLÉS Y ESPAÑOL	INGLÉS

8.3 TABLA 3: MANTENIMIENTO DE LAS CERTIFICACIONES DE (ISC)² E ISACA

MANTENIMIENTO DE LA CERTIFICACIÓN

EMPRESA ASOCIACION	(ISC)²								ISACA			
CERTIFICACIÓN	CAP	CCFP	CISSP	CISSP-ISSAP	CISSP-ISSEP	CISSP-ISSMP	CSSLP	SSCP	CISA	CISM	CGEIT	CRISC
CPE	RECERTIFICACIÓN CON 60 CRÉDITOS CADA 3 AÑOS CON UN MÍNIMO DE 10 CADA AÑO	RECERTIFICACIÓN CON 90 CRÉDITOS CADA 3 AÑOS CON UN MÍNIMO DE 15 CADA AÑO	RECERTIFICACIÓN CON 120 CRÉDITOS CADA 3 AÑOS CON UN MÍNIMO DE 20 CADA AÑO	RECERTIFICACIÓN CON 120 CRÉDITOS CADA 3 AÑOS CON UN MÍNIMO DE 20 CADA AÑO EN LA ESPECIALIZACIÓN ISSAP	RECERTIFICACIÓN CON 120 CRÉDITOS CADA 3 AÑOS CON UN MÍNIMO DE 20 CADA AÑO EN LA ESPECIALIZACIÓN ISSEP	RECERTIFICACIÓN CON 120 CRÉDITOS CADA 3 AÑOS CON UN MÍNIMO DE 20 CADA AÑO EN LA ESPECIALIZACIÓN ISSMP	RECERTIFICACIÓN CON 90 CRÉDITOS CADA 3 AÑOS CON UN MÍNIMO DE 30 CADA AÑO	RECERTIFICACIÓN CON 60 CRÉDITOS CADA 3 AÑOS CON UN MÍNIMO DE 20 CADA AÑO	RECERTIFICACIÓN CON 120 CRÉDITOS CADA 3 AÑOS CON UN MÍNIMO DE 20 CADA AÑO	RECERTIFICACIÓN CON 120 CRÉDITOS CADA 3 AÑOS CON UN MÍNIMO DE 20 CADA AÑO	RECERTIFICACIÓN CON 120 CRÉDITOS CADA 3 AÑOS CON UN MÍNIMO DE 20 CADA AÑO.	RECERTIFICACIÓN CON 120 CRÉDITOS CADA 3 AÑOS CON UN MÍNIMO DE 20 CADA AÑO
COSTE	CUOTA ANUAL 65$	CUOTA ANUAL 100$	CUOTA ANUAL 85$	CUOTA ANUAL 85$	CUOTA ANUAL 85$	CUOTA ANUAL 85$	CUOTA ANUAL 100$	CUOTA ANUAL 65$	45$ MIEMBROS ISACA Y 80$ RESTO	45$ MIEMBROS ISACA Y 85$ RESTO	45$ MIEMBROS ISACA Y 85$ RESTO	45$ MIEMBROS ISACA Y 85$ RESTO

8.4 GRÁFICO: CUOTA ANUAL DE MANTENIMIENTO DE LA CERTIFICACIONES DE (ISC)² E ISACA

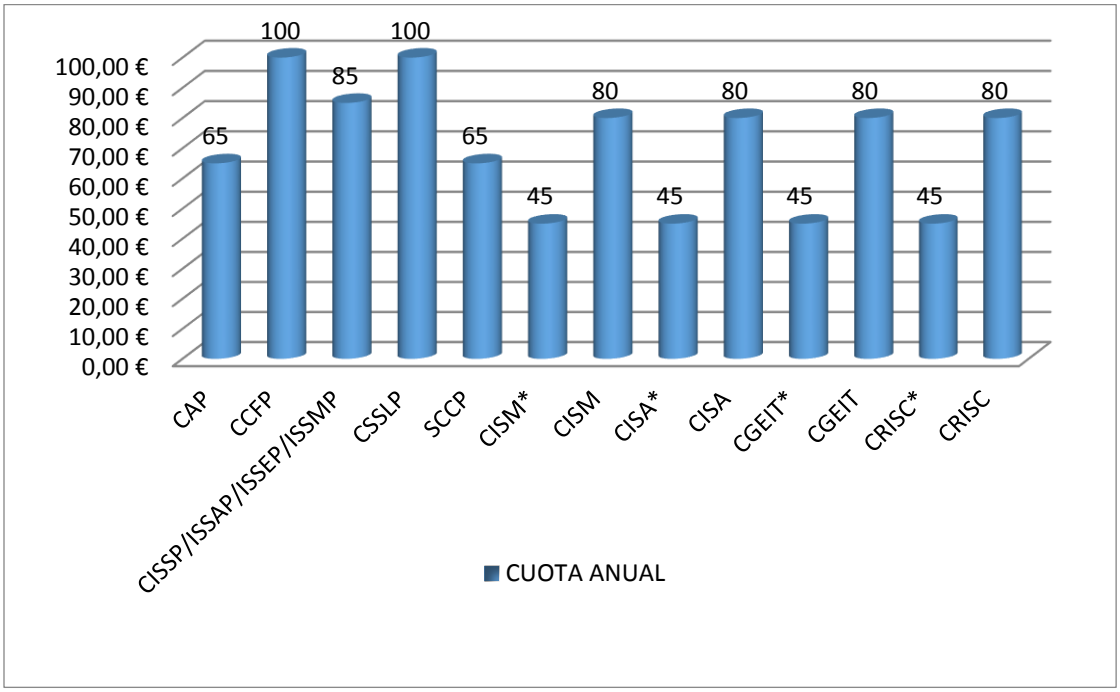

Figura 8.1: Cuota anual de mantenimiento de la certificación.
Las certificaciones marcadas con * indican el coste para miembros de ISACA.

8.5 GRÁFICO: NÚMERO DE CERTIFICADOS POR ENTIDAD

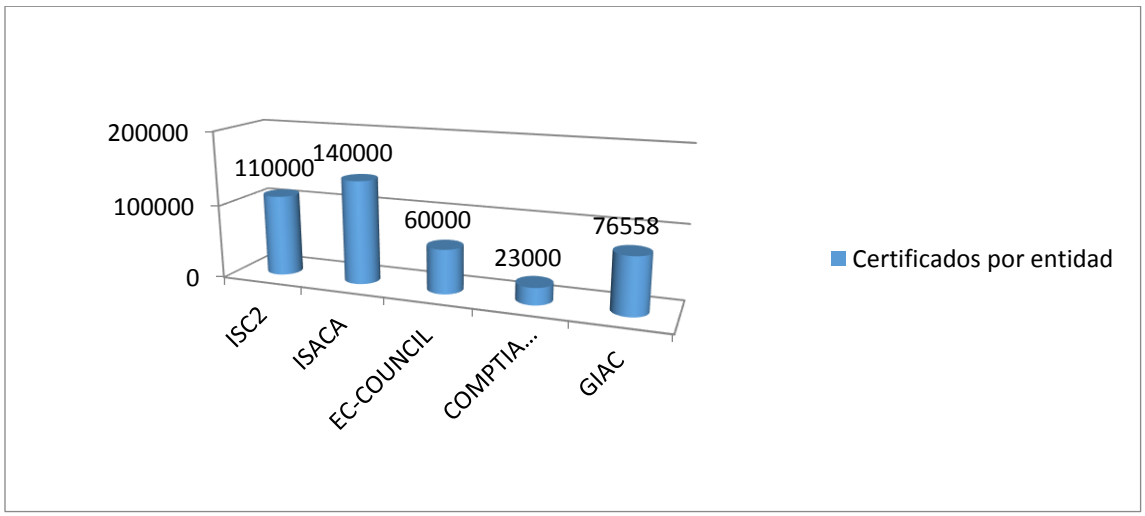

Figura 8.2: Número de certificados por entidad.
Se muestran únicamente las entidades de las que se han encontrado datos.

8.6 GRÁFICO: NÚMERO DE CERTIFICADOS POR (ISC)²

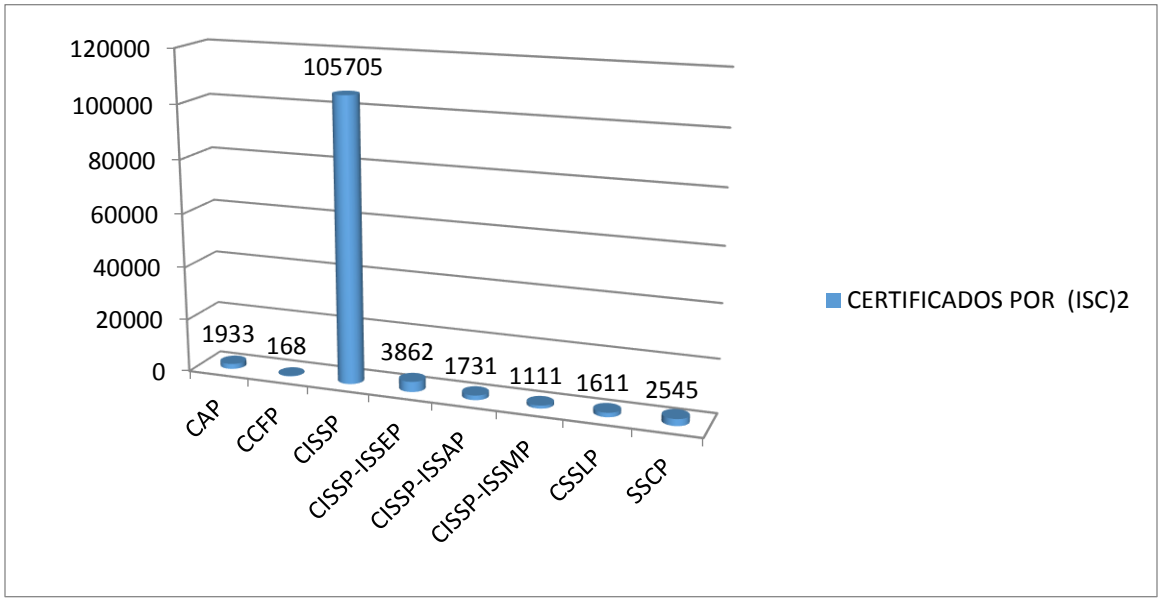

Figura 8.3: Número de certificados por (ISC)².
Fuente (ISC)². Fecha de consulta Marzo 2016.

8.7 GRÁFICO: NÚMERO DE CERTIFICADOS POR ISACA

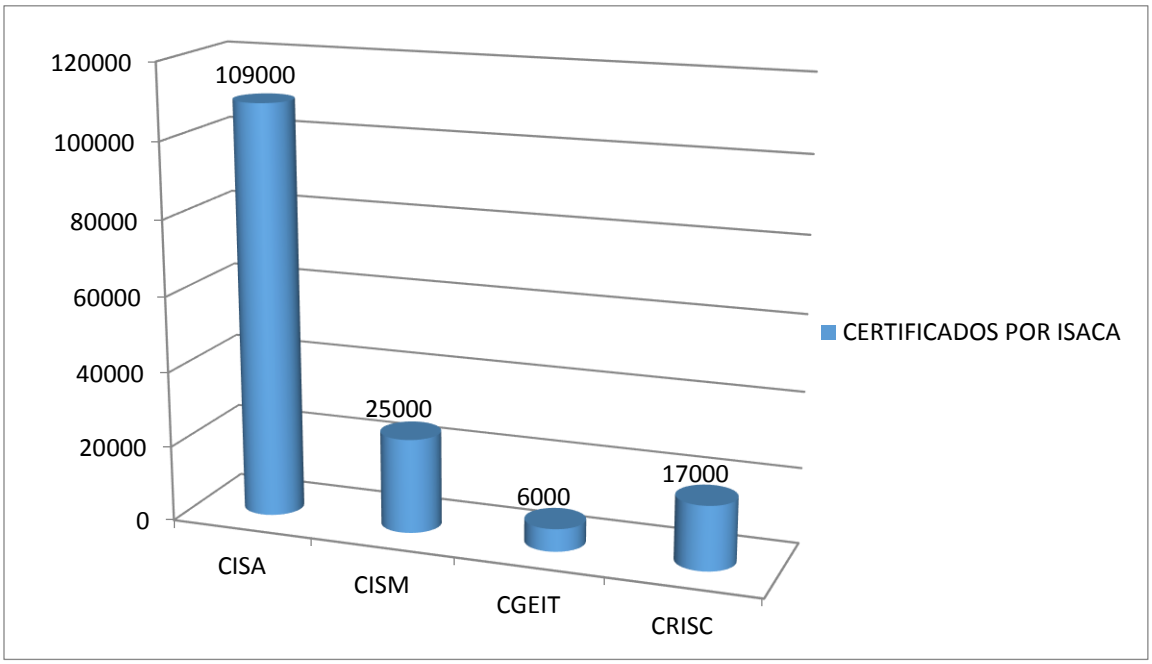

Figura 8.4: Número de certificados por cada certificación de ISACA.
Fuente ISACA. Fecha Consulta Diciembre 2015.

9 REFERENCIAS

[1] Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares 2013.INE. Fecha de consulta Mayo-2014.
http://www.ine.es/jaxi/menu.do?type=pcaxis&path=/t25/p450/base_2011/a2013&file=pcaxis

[2] Kaspersky Security Bulletin 2012. The overall statistics for 2012. Fecha de consulta Mayo-2014
https://securelist.com/analysis/kaspersky-security-bulletin/36703/kaspersky-security-bulletin-2012-the-overall-statistics-for-2012/

[3] CANO, Jeimy. Certificaciones en Seguridad Informática. Conceptos y Reflexiones, marzo 2003. Fecha de consulta: 30/09/2013.
http://www.criptored.upm.es/guiateoria/gt_m142i.htm

[4] GÓMEZ, Roberto. Certificaciones en Seguridad Informática, agosto 2005. Fecha de consulta: 30/09/2013.
http://www.criptored.upm.es/guiateoria/gt_m626a.htm

[5] RAMOS, Alejandro. Certificaciones de seguridad, Security By Default, Mayo 2009. Fecha de consulta: 30/09/2013.
http://www.securitybydefault.com/2009/05/certificaciones-de-seguridad.html

[6] MARTINEZ, Lorenzo. ¿Qué buscamos en una certificación de seguridad?
Security By Default, febrero 2011. Fecha de consulta: 30/09/2013.
http://www.securitybydefault.com/2011/02/que-buscamos-en-una-certificacion-de.html

[7] D'ANTUONO, María, Certificaciones de Seguridad Informática, junio
2007, actualizado 2007 BORGHELLO Cristian. Fecha de consulta: 30/09/2013.
http://www.segu-info.com.ar/articulos/39-certificaciones-en-seguridad.htm

[8] Certificado de profesionalidad en Seguridad Informática. Fecha de consulta Mayo-2015
http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-10055

[9] $(ISC)^2$.
https://www.isc2.org/

[10] ISACA.
https://www.isaca.org/Pages/default.aspx

[11] GIAC.
http://www.giac.org/

[12] EC Council.
http://www.eccouncil.org/

[13] CompTIA Security+.
http://certification.comptia.org/getCertified/certifications/security.aspx

[14] ISMS
https://www.ismsforum.es/

[15] ISECOM
http://www.isecom.es/

[16] MILE2
http://www.mile2.com/

[17] Deloitte. Fecha de consulta Octubre-2015
http://cyberacademy.deloitte.es/

[18] Buguroo. Fecha de consulta Octubre-2015
https://buguroo.com/

[19] Información de SGSI, fecha consulta Mayo-2014
http://recursostic.educacion.es/

[20] Pearson Vue
http://home.pearsonvue.com/

[21] Sedes de exámenes Pearson Vue
https://wsr.pearsonvue.com/testtaker/registration/SelectTestCenterProximity/ISC2/466177

[22] Guía del candidato de ISACA
http://www.isaca.org/Certification/Documents/2015-ISACA-Exam-Candidate-Information-Guide_exp_Spa_1114.pdf

[23] Internet Security Auditors
http://www.isecauditors.com/

[24] Prometric
https://www.prometric.com/en-us/Pages/home.aspx