

Certificaciones Profesionales en Seguridad de la Información

Ing. Reynaldo C. de la Fuente



Temario

- Concepto de certificación profesional
- Contexto nacional e internacional.
- ¿Por que certificarme o certificar al personal?
- Las principales instituciones.
- Las principales certificaciones.
- El Caso del CISSP

La Certificación Profesional

- La certificación profesional es un proceso por medio del cual una persona prueba que cuenta con el conocimiento, la experiencia, y las cualidades necesarias para realizar un trabajo específico.
- La prueba es un certificado obtenido luego de aprobar un examen y cumplir con otros requisitos que se acredita por parte de una organización que monitorea y mantiene estándares específicos para la industria involucrada.
- El certificado brinda aseguramiento a los empleadores , clientes, estudiantes y el público en genera que el que lo mantiene es competente y profesional.

Certificaciones en Seguridad

- Una evaluación reciente realizada por CompTIA, reporto que el 37 % de 1500 profesionales de TI, tenían intenciones de obtener una certificación en el área de Seguridad en los próximos dos años.
- Otro 18 % relacionado con Hacking Ético.
- Y un 13% deseaba obtener certificaciones relacionadas con el Informática Forense.

El contexto nacional e internacional

- En los EEUU, dada la importante recesión un número muy importante de personas se está volcando a obtener certificaciones profesionales.
- A nivel internacional, en la India, por ej., donde muchas veces el número de candidatos exceden ampliamente los puestos, se excluyen a los candidatos que carecen de certificaciones.

El contexto nacional e internacional

- La demanda a nivel internacional de profesionales con experiencia en Seguridad de la información no ha disminuido a pesar de la crisis económica.
- El contar con certificaciones profesionales en el área de seguridad es un requisito para diferentes cargos, llamados, licitaciones a nivel nacional e internacional.

El contexto nacional e internacional

- Según lo establecido por el IT skills and Certification pay index, la prima por certificaciones en el área de seguridad se ha incrementado en un 2.4 %, mientras que la prima por otras certificaciones en el área de TI a decrecido en un 6.5 %.

El contexto nacional e internacional

- Algunas de las certificaciones mejores pagas en EUA, en el área de TI, según diferentes sitios, encuestas y evaluaciones son:
 - PMP
 - VMWARE Certified Professionals
 - ITIL Foundations
 - CISSP
 - Microsoft (MCSA)
 - CISCO (CCNA)
- En promedio, entre U\$\$ 90.000 y U\$\$ 110.000 anuales

Certificaciones en Seguridad

- Las principales áreas de interés
 - Arquitectura
 - Informática Forense
 - Gestión y análisis de incidentes.
 - Análisis de intrusiones.
 - Auditoría
 - Hacking Ético
 - Seguridad en Redes
 - Seguridad en el Ciclo de Desarrollo de Software
 - Gestión de la Seguridad.

¿Por qué Certificarse?

- Algunos beneficios.
 - Diferenciador laboral.
 - Confirma la experiencia y el conocimiento en Seguridad, Auditoria, etc..
 - Formar parte de un selecto grupo de profesionales altamente demandado internacionalmente.
 - Contar con acreditaciones reconocidas en todo el mundo.
 - Adherir a buenas practicas reconocidas internacionalmente.
 - Contar con acceso y comunicación con todos los profesionales certificados.
 - Integrarse al sano requerimiento de la capacitación continua.
 - Base para adquirir certificaciones más específicas.

¿Por qué Certificar al Personal?

- Es el recurso más crítico de las organizaciones, y el más propenso a fallas.
- Algunos beneficios.
 - Contar con profesionales para los cuales la seguridad informática es una prioridad.
 - Contar con profesionales comprometidos con un comportamiento ético.
 - La garantía de contar con personal actualizado en la materia.
 - **Es una de las formas más adecuadas de invertir en seguridad informática.**
 - Garantiza el establecimiento de buenas practicas.
 - Acceso a la red mundial de profesionales capacitados..

Instituciones Certificadoras

- **ISACA**
 - Fundada en el 1969, con mas 86.000 miembros a nivel mundial y capítulos en 75 países.
- **(ISC)²**
 - International Information Systems Security Certification Consortium
- **SANS Institute**
 - El SANS (SysAdmin, Audit, Network, Security) Institute fue establecido en 1989 como una organización de educación e investigación.

Certificaciones de la ISACA

- **CISA**
 - Certified Information Systems Auditor
 - El programa CISA está diseñado para evaluar y certificar a los individuos en la profesión de auditoría, control, aseguramiento o seguridad de SI
- **CISM**
 - Certified Information Security Manager
 - El programa CISM esta diseñado para evaluar y certificar a los individuos en la profesión de gestión de seguridad de la información
- **CGEIT**
 - Certified in the Governance of Enterprise IT
- **CRISC**
 - Certified in Risk and Information Systems Control
 - Actualmente en proceso de Gandfathering.
- **Primer examen en junio de 2011**
- **Examen**
 - Proxima Fecha: 11 de diciembre de 2010
- **Costo:**
 - Hasta el 18 de agosto - miembros US \$415 - No miembros US \$545
 - Hasta el 6 de octubre - miembros US \$465 - No miembros US \$595

Certificaciones de la (ISC)²

- **SSCP**
 - Systems Security Certified Practitioner

- **CISSP**
 - Certified Information Systems Security Professional.

 - Analizado en detalle.

- **CSSLP**
 - Certified Secure Software Lifecycle Professional

 - Dominios considerados:
 - Secure Software Concepts
 - Secure Software Requirements
 - Secure Software Design
 - Secure Software Implementation/Coding
 - Secure Software Testing – testing for security
 - Software Acceptance
 - Software Deployment, Operations, Maintenance and Disposal

- **Concentraciones CISSP**

Certificaciones del SANS

- **Certificaciones GIAC (Global Information Assurance Certification)**
 - GIAC Certified ISO-17799 Specialist (G7799), GIAC Systems and Network Auditor (GSNA), GIAC Legal Issues (GLEG), GIAC Information Security Professional (GISP), GIAC Security Leadership Certification (GSLC), GIAC Certified Project Manager Certification (GCPM)
 - GIAC Information Security Fundamentals (GISF), GIAC Security Essentials Certification (GSEC), GIAC Web Application Penetration Tester (GWAPT), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Enterprise Defender (GCED), GIAC Certified Firewall Analyst (GCFW), GIAC Certified Intrusion Analyst (GCIA)
 - GIAC Certified Incident Handler (GCIH), GIAC Certified Windows Security Administrator (GCWN), GIAC Certified UNIX Security Administrator (GCUX), GIAC Certified Penetration Tester (GPEN), GIAC Reverse Engineering Malware (GREM), GIAC Assessing Wireless Networks (GAWN), GIAC Secure Software Programmer - .NET (GSSP-NET), GIAC Secure Software Programmer - Java (GSSP-JAVA)
- **Costo : U\$S 899 – U\$S 499 junto con Curso.**
- **El examen es tomado en sitios Autorizados, Online. (No esta disponible en Uruguay)**
- **Tiene un perfil más técnico que otras certificaciones, validando la experiencia práctica de los candidatos.**
- **Requiere repetir el examen cada 4 años.**

Obtención de la certificación.

- Para obtener la certificación se debe:
 - Pagar el costo del examen.
 - Aprobar el examen correspondiente.
 - Acreditar los años de experiencia requeridos (4 – 5 años).
 - Pueden ser sustituidos según el caso por Título Universitario y contar con otra certificación en el área específica (1-2 años).
 - Adherir al código de ética de la institución y aprobar los requisitos formales.
 - Superar auditorías en el caso que sea seleccionado.

Mantenimiento de la Certificación

- Períodos de 3 o 4 años.
- Costo de Mantenimiento anual (U\$S 80 – U\$S 120).

- Opciones:
 - Tomar el examen nuevamente.

 - Acumular “créditos” de educación continua.
 - **Asistencia a cursos de entrenamiento o seminarios.**
 - **Asistencia a conferencias de seguridad.**
 - **Miembro de asociaciones y asistencia a eventos.**
 - **Asistencia a presentaciones de Proveedores.**
 - **Publicación de artículos o libros.**
 - **Brindar entrenamiento en seguridad.**
 - **Auto-estudio.**
 - **Trabajo voluntario.**

¿Cual debo elegir?

- Algunos de los aspectos a considerar a la hora de seleccionar la certificación a obtener son:
 - El rumbo profesional que deseamos emprender.
 - La experiencia que hemos adquirido.
 - El reconocimiento local e internacional con el que cuenta.
 - La estructura de la organización en la cual me desempeño o deseo desempeñarme.

EL CASO DE LA CERTIFICACIÓN CISSP[®]



Datasec
seguridad·informática

International Information Systems Security Certification Consortium

- **Organización global sin fines de lucro fundada en 1989 por miembros de las siguientes organizaciones:**
 - ISSA (Information Systems Security Association)
 - CSI (Computer Security Institute)
 - CIPS (Canadian Information Processing Society)
 - IFIP (International Federation for Information Processing)
 - DPMA (Data Processing Management Association)
 - ISU (Idaho State University)



International Information Systems Security Certification Consortium

- **Dedicada a:**
 - Mantener una Base de Conocimiento para los Profesionales dedicados a la seguridad de los sistemas de información.
 - Certificar profesionales sobre una consensuada base de conocimientos profesionales.
 - Administrar los exámenes de la certificación.
 - Asegurar el mantenimiento de las credenciales, por medio de la educación continua.

- **Fondos obtenidos.**
 - Costos del Examen.
 - Costos de las Conferencias.
 - Mantenimiento anual de la certificación.

- **No esta asociada a proveedor alguno.**

International Information Systems Security Certification Consortium

- **Certificaciones Otorgadas.**
 - Systems Security Certified Practitioner (SSCP®).
 - Certified Information Systems Security Professional (CISSP®)
 - ISSAP® (Arquitectura)
 - ISSEP® (Ingeniería)
 - ISSMP® (Gestión)
 - Certified Secure Software Lifecycle Professional (CSSLP)

CISSP®

Certified Information Systems Security Professional.

Certified Information Systems Security Professional

- **Descripción:**

- Certificación creada a partir de la base de conocimiento en seguridad de los sistemas de información mantenida por la (ISC)².
- No asociada a ninguna tecnología ni proveedor.
- Certificada ISO/IEC 17024.

- **Reconocimiento:**

- La más antigua certificación profesional enfocada exclusivamente a la seguridad informática.
- Una de las certificaciones más deseadas.
- La 2da certificación mejor paga durante varios años en los EUA.
- Indispensable para desempeñar distintos puestos en los EUA y el Reino Unido.

Certified Information Systems Security Professional

- **Crecimiento:**
 - En 1997 – 700 CISSP.
 - En 2002 – 15.000 CISSP.
 - En 2006 – 29.000 CISSP.
 - En 2009 – 64.000 CISSP

- **Distribución:**
 - Existen CISSP en 134 Países.
 - Norteamérica
 - EUA – 39.000.
 - Canadá – 3.300
 - Latinoamérica
 - México – 245
 - Brasil - 249
 - Argentina – 86
 - Chile - 69
 - Uruguay – 25

Certified Information Systems Security Professional

- **Requerimientos:**

- Aprobar el examen con un puntaje de 700/1000 puntos o superior.
- Contar con al menos cinco años de experiencia en algunos de los 10 dominios de la base común de conocimiento CISSP, o cuatro años de experiencia y contar con un título universitario.
- Enviar el formulario de consentimiento adecuadamente completado, firmado por un CISSP o supervisor.
- Dar respuesta adecuada a la auditoria que se efectúe, en el caso de ser seleccionado para la misma.
- Suscribir al código de ética de la (ISC)²

Certified Information Systems Security Professional

- **Código de Ética:**
 - Proteger a la sociedad, al bien común y a la infraestructura tecnológica.
 - Actuar en forma honorable, justa, responsable y legal.
 - Brindar servicios competentes y atentos.
 - Fomentar y proteger la profesión.
- **Costos del Mantenimiento Anual**
 - U\$S 85 (dólares americanos, ochenta y cinco).

Dominios del CISSP CBK

- **CISSP CBK**

- El Common Body of Knowledge del CISSP, es la base de conocimiento utilizada para la certificación. La misma se encuentra separada en áreas temáticas, denominadas dominios. Los mismos son los siguiente:

1. Prácticas de administración de la seguridad.
2. Metodologías y sistemas de control de acceso.
3. Seguridad en redes y telecomunicaciones.
4. Criptografía.
5. Modelos y arquitecturas de seguridad.

Dominios del CISSP CBK

- **CISSP CBK**

- 6. Seguridad de las operaciones.
 - 7. Seguridad en el desarrollo de aplicaciones y sistemas.
 - 8. Planeamiento de la continuidad del negocio y recuperación de desastres.
 - 9. Legislación, investigación y ética.
 - 10. Seguridad Física.
- Vinculación con los dominios de la norma ISO/IEC 17799
 - Descargar la guía de estudio del CISSP CBK
https://www.isc2.org/cgi-bi/request_studyguide.cgi

Prácticas de administración de la seguridad.

- Alcance
 - Este dominio examina:
 - la identificación y valoración de los activos de la compañía,
 - el desarrollo, documentación e implementación de políticas, estándares, procedimientos y guías para asegurar la confidencialidad, integridad y disponibilidad.
 - Muy asociado a los aspectos requeridos por las normas ISO/IEC 27001 e ISO/IEC 17799

Prácticas de administración de la seguridad.

- Algunos de los temas cubiertos son:
 - Principios y conceptos de Administración de la Seguridad.
 - Administración y control de cambios.
 - Clasificación de datos.

 - Administración y análisis del riesgo.

 - Políticas y procedimientos.
 - Estándares y guías.
 - Roles y Responsabilidades.
 - Concientización, entrenamiento y seguridad del personal.

Metodología y Sistemas de Control de Acceso

- Alcance.
 - Este dominio examina los mecanismos y métodos utilizados para brindarle a los administradores y gerentes el control sobre:
 - lo que corresponda que los usuarios puedan o no acceder,
 - la posibilidad de extender sus capacidades luego de la adecuada autenticación y autorización, y la auditoria y monitoreo de estas actividades.

Metodología y Sistemas de Control de Acceso

- Algunos de los temas cubiertos son:
 - Responsabilidad. 'Obligación de rendir Cuentas'
 - Técnicas de Control de Acceso.
 - Administración del Control de Acceso.
 - Modelos de Control de Acceso.
 - Técnicas de Autenticación e identificación.
 - Metodologías e implementaciones de control de acceso.
 - Custodia y propiedad de los datos.
 - Métodos de Ataque.
 - Monitoreo.
 - Testeo de Penetración.

Seguridad en redes y telecomunicaciones.

- El dominio más extenso.

- Alcance
 - Este dominio examina:
 - los sistemas de comunicaciones internos, externos, públicos y privados,
 - y las medidas de seguridad utilizadas para brindarle integridad, confidencialidad y disponibilidad a las transmisiones.
 - Analizando la estructura de redes, tipos de dispositivos, protocolos, métodos de acceso y su administración.

Seguridad en redes y telecomunicaciones.

- Algunos de los temas cubiertos son:
 - Modelos ISO/OSI
 - Seguridad en redes y comunicaciones.
 - Internet/Intranet/Extranet.
 - Protocolos de Seguridad.
 - Seguridad en el Comercio/E-mail/ etc.
 - Comunicaciones de voz seguras.
 - Ataques y medidas correctivas.

Criptografía.

- Uno de los dominios más complejos.
- Alcance
 - Este dominio examina los métodos y técnicas para cifrar y descifrar información con el propósito de mantener su integridad, confidencialidad y autenticidad. Esto involucra diferentes técnicas criptográficas, enfoques y tecnologías.

Criptografía.

- Algunos de los temas cubiertos son:
 - Usos de la criptografía.
 - Conceptos, metodologías y practicas criptográficas.
 - Algoritmos simétricos y asimétricos.
 - Infraestructura de clave publica (PKI).
 - Arquitecturas para la implementación de funciones criptográficas.
 - Métodos de ataque.

Modelos y arquitecturas de seguridad.

- Alcance
 - Este dominio examina los conceptos, principios, y estándares para el diseño, implementación, monitoreo y protección de aplicaciones y sistemas operativos.
 - Esto cubre estándares internacionales de evaluación y su significado para distintos tipos de plataformas.

Modelos y arquitecturas de seguridad.

- Algunos de los temas cubiertos son:
 - Organización de redes y computadores, arquitecturas y diseños.
 - Modelos de seguridad, arquitecturas y criterios de evaluación.
 - **TCSEC**
 - **Common Criteria**
 - Fallas más comunes y aspectos de seguridad en las arquitecturas de sistemas y diseños.

Seguridad en las Operaciones.

- Alcance
 - Este dominio examina los distintos controles sobre el hardware, los sistemas, los datos, y el personal con derecho de acceso sobre ellos.
 - Se analizan las técnicas de auditoría y monitoreo, cubriendo los posibles medios para perpetuar abuso y como reconocerlos y enfrentarlos.

Seguridad en las Operaciones.

- Algunos de los temas cubiertos son:
 - Responsabilidades administrativas pertenecientes al personal y sus funciones de trabajo.
 - Tipos de controles
 - Controles sobre las operaciones.
 - Protección de recursos.
 - **Auditoría.**
 - **Monitoreo**
 - **Detección de intrusos.**

Seguridad en el desarrollo de aplicaciones y sistemas.

- Alcance
 - Este dominio examina los controles incorporados en los sistemas operativos y las aplicaciones, y los pasos involucrados en su desarrollo.
 - Se analiza al ciclo de vida del software, control de cambios, controles, y seguridad de las aplicaciones.

Seguridad en el desarrollo de aplicaciones y sistemas.

- Algunos de los temas cubiertos son:
 - Conceptos de aplicaciones.
 - Conceptos de bases de datos.
 - Componentes de almacenamiento y procesamiento.
 - Sistemas basados en el conocimiento.
 - **Controles en el desarrollo de sistemas**
 - **Amenazas en código.**
 - **Métodos de ataque.**

Planeamiento de la continuidad del negocio y recuperación de desastres.

- Alcance
 - Este dominio examina la preservación de las actividades del negocio cuando se enfrenta a una interrupción o desastre.
 - Esto involucra la identificación de riesgos reales, una adecuada evaluación de riesgos e implementación de medidas correctivas.

Planeamiento de la continuidad del negocio y recuperación de desastres.

- Algunos de los temas cubiertos son:
 - Identificación de los activos del negocio y la asignación de valor.
 - Análisis de impacto sobre el negocio y la predicción de posibles pérdidas.
 - Determinación de áreas prioritarias.
 - Administración de la crisis.
 - Desarrollo, implementación, testeo y mantenimiento del plan.

Legislación, investigación y ética.

- Alcance
 - Este dominio examina los distintos tipos de delitos, legislaciones y reglamentaciones. A su vez, se analizan técnicas en la investigación de delitos, la obtención de evidencias, y el manejo de procedimientos.
 - También cubre como desarrollar e implementar un programa de manejo de incidentes.

Legislación, investigación y ética.

- Algunos de los temas cubiertos son:
 - Legislaciones, reglamentaciones y delitos.
 - Licenciamiento y piratería de software.
 - Temas y leyes de importación y exportación de software.
 - Tipos de evidencias y la admisión de las mismas en caso de juicio.
 - Manejo de incidentes.
 - Ética

Seguridad Física.

- Alcance
 - Este dominio examina las amenazas, riesgos, y medidas correctivas para proteger físicamente los establecimientos, el hardware, los datos, y al personal.
 - Esto incluye la elección del establecimiento, los métodos de autorización de acceso, y los procedimientos de seguridad física y ambiental.

Seguridad Física.

- Algunos de los temas cubiertos son:
 - Áreas restringidas, métodos y controles de autorización.
 - Controles técnicos.
 - Elementos de seguridad ambiental.
 - Amenazas a la seguridad física.
 - Elementos de seguridad física.

Examen CISSP

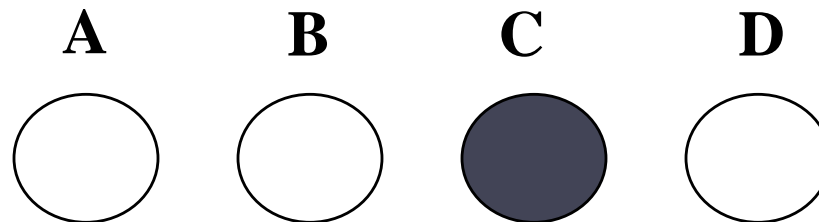
- **Descripción:**
 - Cubre los diez dominios del CISSP CBK.
 - 250 Preguntas Múltiple-Opción, con cuatro opciones.
 - Papel y lápiz.
 - ***Desde 2005 - con traducción en español.***
- **Duración:**
 - 6 Horas.
 - Normalmente, de 8:30 a 15:00.

Examen CISSP

- **Costo:**
 - U\$S 549 (dólares americanos, quinientos cuarenta y nueve).
 - Mismo precio en todo el mundo.
 - Se abona directamente a la (ISC)²
- **Preguntas:**
 - Normalmente no muy extensas.
 - Ejemplo:
 - Un propósito de los programas de concientización en seguridad es el modificar
 - a. **Comportamientos y actitudes del personal.**
 - b. Gestión de la Dirección.
 - c. Actitudes de empleados con información sensible.
 - d. Actitudes corporativas acerca del cuidado de la información.

Examen CISSP

- **Formato:**
 - 250 preguntas, en ingles, de múltiple opción, con cuatro opciones.
 - 25 preguntas no puntúan.
 - No hay puntos negativos.
 - Solamente una opción es correcta.
 - Estilo examen First Certificate.



Información Adicional

- **Sitios de Interés:**
 - <http://www.isc2.org>
 - <http://www.cccure.org>
 - <http://www.sans.org>
 - <http://http://csrc.nist.gov/>
- **Mailing lists:**
 - CISSP-Discuss
 - CISSPStudy_1
 - CISSP_BOSON
 - <http://groups.yahoo.com>
- **Software.**
 - <http://www.boson.com>
 - <http://www.bfq.com/>
 - <http://www.srvbooks.com/>
 - <http://www.lostclusterz.com/quiz/quiz.php>
- **Libros**
 - The CISSP Prep Guide - Krutz
 - All In One CISSP Certification - Harris
 - The CISSP Official Guide.

(ISC)² SECURITY TRANSCENDS TECHNOLOGY™

LOG IN User ID Password [Forgot your password?](#)

Education Examinations Credential Offerings Member Benefits News & Information Post-Certification

Support for Every Step of Your Information Security Career

Concentrations

SSCP®

TACTICIANS

Associate of (ISC)²

STRATEGISTS

CISSP®

Search

About (ISC)²

Contact (ISC)²

(ISC)² Policies

(ISC)² Japan

Stop & shop at (ISC)² STORE

(ISC)² ALERTS

Constituent Book Reviews Available

Constituent book reviews are now available on the secure side of the (ISC)² Website. Click [here](#) to look for book reviews via search criteria or click the submit button at the bottom right-hand corner to view all of them. You can also find a link to the book reviews on the services page under CISSP Resources (left-hand navigation). By the way, MANY THANKS to our test group of constituents who helped us develop and pre-test the search/results

Links de Interés

- www.isaca.org
- www.isc2.org
- www.giac.org

Consultas

- reynaldo@datasec-soft.com
- **Gracias..**