

Certificaciones en Seguridad

Autor: Diego Bruno

Edición y Corrección: Lic. Cristian Borghello, MVP - CISSP

Fecha Publicación: 25 de abril de 2010

Publicado en [Segu-Info](http://www.segu-info.com.ar)

INTRODUCCIÓN

Muy a menudo veo que en muchísimos foros, se realizan una gran cantidad de preguntas, orientadas a que se debería estudiar o no en materia de seguridad informática y *Penetration Test*.

Cuando pienso en una “posible” respuesta a esas pregunta, en principio, tan simple cómo “Que tengo que leer y estudiar para ser un profesional exitoso en seguridad?” no se me ocurre una sólo sino muchas respuestas lógicas.

El primer camino lógico, si una persona joven recién salida del secundario, fuera quien nos formula dicha pregunta sería decirle que siga una carrera universitaria y luego se especialice con diferentes cursos y certificaciones.

Pero cuando uno piensa en la respuesta, se da cuenta que no es del todo satisfactoria ni siquiera para uno mismo, ya que no existe una carrera universitaria formal en seguridad informática. Si existen posgrados y cursos de extensión universitaria pero no una carrera integral en la materia.

De todas maneras una carrera de grado en conjunto con un posgrado siempre es una excelente opción en cuanto a formación general se refiere.

Obviamente que está totalmente fuera de toda discusión si una carrera universitaria es útil o no, ya que siempre es una excelente base de conocimientos sobre los que después se puede profundizar.

Pero ¿qué pasa en el mundo de las certificaciones de hoy? Existen realmente tantas? Bueno la realidad es que sí.

Hecha esta pequeña introducción, cabe aclarar, antes de pasar a hablar de los diferentes tipos de certificación, que con esta nota no se busca entrar en debate sobre si el tener o no tener certificaciones o título de grado es igual a la experiencia de campo que pueda tener un determinado individuo.

Lo normal no sólo en nuestro ámbito, sino también a nivel internacional es que las certificaciones tienen peso por un sinfín de factores, pero es importante aclarar algunos puntos importantes sobre las mismas y el porqué sirven o no tomarlas:

- Las certificaciones y los títulos de grado “No prueban absolutamente nada” salvo el hecho en sí de que uno puede ser un muy buen estudiante y un buen pasador de exámenes.
- Las certificaciones y los títulos de grado son a menudo necesarios para acceder a una entrevista de recursos humanos.
- En muchos países, las agencias gubernamentales requieren ciertas certificaciones para ciertos profesionales o ciertos trabajos.

- Muchas empresas o consultoras que intentan acceder a un pliego de trabajo para agencias gubernamentales, deben tener personal certificado, de lo contrario ni siquiera pueden participar.
- Muchas de las grandes empresas fabricantes de productos como Microsoft, Sun Microsystems y Cisco, suelen tener políticas muy restrictivas sobre las empresas que pueden ser o no Partners de sus canales de negocios. Para ellos las empresas deben tener a su personal de staff certificado.
- Las certificaciones lo posicionan a uno de otra manera en el mercado como especialista.
- Por último, tener algún tipo de certificación o título de grado o ambos es siempre un diferencial cuando muchas veces una empresa tiene que tomar la decisión de un aumento, una promoción o sencillamente decidir, ante un recorte presupuestario, quien se queda y quien se va.

En entrevistas que se le han hechos a muchos CEOs y CIOs sobre la decisión de tomar o no a una persona con o sin determinadas certificaciones, de la mayoría de las respuestas las que más primaron fueron:

- Que el individuo es prácticamente egoísta y tiene una imagen tan alta de sí misma como para estar con sus pares en un grupo de trabajo.
- Que es un individuo demasiado perezoso si ni siquiera puede sentarse por un par de horas a rendir un examen.
- Que no se preocupa demasiado de su propia carrera por lo cual no es un profesional confiable.

Se podrá estar o no estar de acuerdo con todas estas afirmaciones pero la realidad es que si uno lo piensa bien, no existen “buenos” argumentos por lo cual no alcanzar una determinada certificación.

Entonces... que certificaciones o cursos tomar para dedicarse a la seguridad? Bueno tendré que darles la respuesta universal sabia del “depende”. Porque realmente depende de lo que uno quiera o no ser y hacer en el mundo de la seguridad, el cual les aseguro es muy vasto.

Una aclaración válida para hacer es que, cuando hablamos de dedicarnos a la seguridad informática, no estamos haciendo, cómo todavía pasa en nuestro mercado, mención a una persona que se dedica a dar alta o baja de usuarios y blanquearles la password. Eso no está ni remotamente cerca de lo que es ser un profesional de la seguridad de la información.

Un profesional de la seguridad es aquél que, más allá de su especialidad elegida, tiene los suficientes conocimientos de normas internacionales o de ámbito local en seguridad, que conoce al menos los principales sistemas operativos y que, sin ser un gurú de redes entiende bien los conceptos y los protocolos de cómo las mismas trabajan y muchas cosas más, porque de lo contrario no podría asegurar un determinado sistema si mínimamente no lo conoce o si mínimamente no conoce los conceptos que manejan dichos sistemas.

Después es uno el que, cómo veremos a continuación, de acuerdo a su perfil y conocimiento decidirá que especialización toma y cómo la toma.

Hay gente que se inclina más hacia el lado de la auditoría y la normativa, hay gente que le gusta más el Management de un área de seguridad, y hay

gente que no concibe que se la saque del frente de una línea de comando personalizada.

Pasemos entonces a mirar los diferentes caminos que se podrían tomar en materia de cursos y certificaciones en el mundo de la seguridad, aclarando primero un concepto fundamental:

Se debe entender que hasta no hace mucho tiempo atrás no existía ninguna certificación que involucrara a temas de seguridad o relacionados a Information Security System (ISS), ya que realmente es una materia prácticamente nueva.

Recién a finales de los 80 el gobierno de los estados unidos lanzó una serie de documentos sobre guías de seguridad en ciertos sistemas llamados "Rainbow Series" entre los cuales se encontraba el NCSC -TG-006, mejor conocido como el *Orange Book*.

Recomiendo al lector que lea a dichos documentos los cuales le darán una buena idea de cómo fue avanzando todo lo relacionado a ISS a través del siguiente enlace: www.fas.org/irp/nsa/rainbow.htm

Certificaciones de Alto Nivel

(ISC)²

Este organismo es probablemente el mejor reconocido en cuanto a su cuerpo de conocimiento y sus respectivas certificaciones.

Acerca de (ISC)²

Con cuarteles en los Estados Unidos y oficinas en Londres, Hong Kong y Tokyo, este organismo es globalmente hablando, el líder en educar y certificar sin fines de lucro a profesionales de la seguridad de la información.

Esta entidad desarrolla y actualiza constantemente una serie de tópicos concernientes a seguridad llamados CBK, por el acrónimo de *Common Body Knowledge*, los cuales definen los estándares de la industria global en materia de seguridad.

El organismo (ISC)² tiene diferentes certificaciones en ISS de acuerdo a diferentes funciones y especializaciones como ingeniería, arquitectura, Management y todo lo relacionado al ciclo de vida del software.

Systems Security Certified Practitioner (SSCP)

Con un poco más de un año de experiencia en el campo de la seguridad de la información, uno se puede convertir en *un Systems Security Certified Practitioner (SSCP)*. Esta certificación es ideal para aquellos que desempeñan funciones de ingenieros de redes con orientación en seguridad, analistas de seguridad o administradores de seguridad.

Los dominios o CBK que comprenden a esta certificación son los siguientes:

- Access Controls
- Analysis and Monitoring
- Cryptography SSCP
- Malicious Code
- Networks and Telecommunications
- Risk, Response, and Recovery
- Security Operations and Administration

Certified Secure Software Lifecycle Professional (CSSLP)

Para todo aquel individuo que trabaje en todo lo relacionado al ciclo de vida del software y que por ende debería entender los conceptos de seguridad que envuelven al mismo. Esta certificación apunta a una persona con al menos 4 años de experiencia en el campo de desarrollo de software y su ciclo de vida y es ideal para desarrolladores, ingenieros y arquitectos, Project managers, analistas de negocio y testers de QA.

Los dominios o CBK que envuelven a esta certificación son:

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design
- Secure Software Implementation/Coding
- Secure Software Testing
- Software Acceptance
- Software Deployment, Operations, Maintenance, and Disposal

CISSP (Certified Information Security System Professional)

Esta certificación fue la primera en el campo de la seguridad de la información, acreditada por el organismo ANSI (American National Standards Institute) e ISO standard 17024:2003 (International Standards Organization). Esta certificación no es sólo un objeto de excelencia por su calidad sino también un estándar globalmente reconocido.

Los dominios o CBK que componen a esta certificación son los siguientes:

- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance, and Investigations
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security

El organismo (ISC)2 tiene además también algunas certificaciones concentradas que se desprenden del CISSP y que por ende el candidato para poder acceder a ellas debe haber primero adquirido el CISSP. Estas concentraciones están referidas al campo de la arquitectura, la ingeniería y el Management. Cada una de estas concentraciones utiliza un subconjunto de información de los 10 dominios del CISSP lo cual requiere por parte del participante un alto nivel de conocimiento de dichos dominios.

Para una persona relacionada al campo de la ingeniería y arquitectura, las certificaciones de Information Systems Security Architecture Professional (ISSAP) e Information Systems Security

Engineering Professional (ISSEP) son ideales, mientras que la certificación CISSP-ISSMP está más orientada a los individuos relacionados al Management y a los Project managers.

CISSP-ISSAP

Esta certificación de concentración de conocimiento requiere del candidato al menos dos años de experiencia real comprobable en el área de arquitectura y es apropiada para profesionales que trabajen como consultores o similares.

Los dominios o CBK que contienen a esta certificación son:

- Access Control Systems and Methodology
- Cryptography
- Physical Security Integration

- Requirements Analysis and Security Standards, Guidelines and Criteria
- Technology-Related Business Continuity and Disaster Recovery Planning
- Telecommunications and Network Security

CISSP-ISSEP

Esta certificación fue desarrollada en conjunto con la NSA (National Security Agency) de los Estados Unidos, y la misma es una herramienta invaluable para cualquier ingeniero de sistemas en seguridad.

Los dominios o CBK que comprenden a esta certificación son:

- Certification and Accreditation
- Systems Security Engineering
- Technical Management
- U.S. Government Information Assurance Regulations

CISSP-ISSMP

Esta certificación de concentración requiere que el candidato pueda demostrar al menos dos años de experiencia profesional en el área de Management. Esta certificación contiene información muy profunda sobre Project Management, risk Management, security awareness program y manejo de un Business continuity plan.

Los dominios o CBK que la componen son los siguientes:

- Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) and Continuity of Operations Planning (COOP)
- Enterprise Security Management Practices
- Enterprise-wide System Development Security
- Law, Investigations, Forensics, and Ethics
- Overseeing Compliance of Operations Security

Information Systems Audit and Control Association (ISACA)

Esta entidad tiene un par de certificaciones que se mapean al campo de la seguridad de la información y las mismas gozan de muy buena reputación aunque tienen focos diferentes una de otra.

Históricamente esta asociación, creada en 1967, tuvo siempre el foco en los auditores de sistemas.

De las dos certificaciones que dijimos que se pueden mapear al campo de la seguridad tenemos la Certified Information Systems Auditor (CISA) y la Certified Information Security Manager (CISM).

La primera es netamente útil y diseñada para auditores de sistemas y la misma puede ser muy útil para aquellos ingenieros de infraestructura que tengan que trabajar en procesos de relevamiento y auditoría, mientras que la segunda si está más netamente orientada a la seguridad pero con un alto foco en el Management.

CISA

Los dominios para esta certificación son:

- IS Audit Process
- IT Governance
- Systems and Infrastructure Lifecycle Management
- IT Service Delivery and Support
- Protection of Information Assets
- Business Continuity and Disaster Recovery

CISM

Los dominios de esta certificación son los siguientes:

- Information Security Governance
- Information Risk Management
- Information Security Program Development
- Information Security Program Management
- Incident Management & Response

Comparado con la certificación de CISSP y sus concentraciones estas dos no parecerían tener demasiada demanda, pero como dijimos al principio, hay diferentes caminos en la carrera a la seguridad de la información con lo cual se requieren diferentes tipos de certificaciones.

Estas dos certificaciones de ISACA están dentro del documento “Directiva 8750” del departamento de defensa de los Estados Unidos.

Recomiendo leer el documento DoD Directive 8750 el cual puede ser consultado en el siguiente enlace:

www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

A continuación en el siguiente cuadro se muestran algunas posiciones laborales dentro del campo de la seguridad de la información que se encuentran dentro de dicha directiva:

IAT Level I		IAT Level II		IAT Level III	
A+ Network+ SSCP		GSEC Security+ SCNP SSCP		CISA CISSP (or Associate) GSE SCNA	
IAM Level I		IAM Level II		IAM Level III	
GISF GSLC Security+		GSLC CISM CISSP (or Associate)		GSLC CISM CISSP (or Associate)	
CND Analyst		CND Infrastructure Support	CND Incident Responder	CND Auditor	CND-SP Manager
GCIA		SSCP	GCIH CSIH	CISA GSNA	CISSP-ISSMP CISM
IASAE I		IASAE II		IASAE III	
CISSP (or Associate)		CISSP (or Associate)		ISSEP ISSAP	

Global Information Assurance Certification (GIAC)

El GIAC es otro cuerpo de certificación que tiene varias certificaciones relacionadas a la seguridad de la información que cumplen con los requerimientos de la directiva 8570 del departamento de defensa de los estados unidos.

Cómo se puede observar en el cuadro del DoD, la certificaciones son:

GIAC Security Essentials Certification (GSEC), GIAC Information Security Fundamentals (GISF), GIAC Security Leadership Certification (GSLC) y GIAC Security Expert (GSE).

Las que están reconocidas por el GIAC cómo las de alto nivel son las GSE y GSLC.

GSLC

Esta certificación, según el GIAC, está orientada a profesionales de la seguridad que realicen un Management o supervisión de un área de seguridad.

Los contenidos de esta certificación no llegan a un contenido tan profundo en cuanto a los aspectos técnicos y cubre de manera similar los contenidos de ISACA e (ISC)².

A continuación se muestran los tópicos que incluye:

Table 3.1 GSLC Topics		
Exam Certification Objectives		
■ 802.11	■ Fraud Management	■ Managing Technical People
■ Access Control and Password Management	■ General Types of Cryptosystems	■ Managing the Mission
■ Advanced Reconnaissance and Vulnerability Scanning	■ Honeypots and Honeynets	■ Managing the Procurement Process
■ Building a Security Awareness Program	■ Incident Handling and the Legal System	■ Managing the Total Cost of Ownership
■ Business Situational Awareness	■ Incident Handling Foundations	■ Methods of Attack
■ Change Management and Security	■ Information Warfare	■ Mitnick-Shimomura
■ Computer and Network Addressing	■ IP Terminology and Concepts	■ Offensive OPSEC
■ Cryptography Algorithms and Concepts	■ Malicious Software	■ Offensive Vulnerability Scanning
■ Cryptography Applications, VPNs and IPSec	■ Managerial Wisdom	■ PGP and PKI
■ Cryptography Fundamentals	■ Managing Ethics	■ Project Management for Security Leaders
■ Defense-in-Depth	■ Managing Globally	■ Risk Management and Auditing
■ Defensive OPSEC	■ Managing Intellectual Property	■ Security and Organizational Structure
■ Disaster Recovery/Contingency Planning	■ Managing IT Business and Program Growth	■ Steganography
■ DNS	■ Managing Legal Liability	■ The Intelligent Network
■ Facilities, Safety, and Physical Security	■ Managing Negotiations	■ The Network Infrastructure
	■ Managing Privacy	■ Web and Communications Security
	■ Managing Security Policy	■ Wireless Advantages and Bluetooth
	■ Managing Software Security	

GSE

La certificación GSE es un poco diferente de otras certificaciones del GIAC, ya que requiere conocimientos en múltiples certificaciones de alto nivel.

Las certificaciones necesarias que se deben tener sólo para poder rendir el GSE son:

GSEC, GIAC Certified Intrusion Analyst (GCIA) y GIAC Certified Incident Handler (GCIH), las cuales son certificaciones que están dentro de los tracks de certificaciones técnicas de administración.

La certificación GSE está inclusive dividida en dos especializaciones posteriores las cuales son GSE - Malware y GSE - Compliance.

Los dominios necesarios para la certificación GSE son los siguientes:

- **IDS and Traffic Analysis Domain**

Capture Traffic

Analyze Traffic

Interpret Traffic

IDS Tools

- **Incident Handling Domain**

IH Process

Common Attacks

Malware

Preserving Evidence

- **ITSEC Domain**

Windows Security

UNIX Security

Secure Communications

Protocols

Security Principles

- **Security Technologies Domain**

Firewalls

Vulnerability Scanners and Port Scanners

Sniffers and Analyzers

Common Tools

- **Soft Skills Domain**

Security Policy and Business Issues

Information Warfare and Social Engineering

Ability to Write

Ability to Present

Ability to Analyze

Teamwork

La certificación GSE requiere dos exámenes escritos que se deberán pasar exitosamente junto a un laboratorio que dura 2 días y que requiere que la persona aplicante presente un reporte escrito y oral que cumpla con los estándares del GIAC en cuanto a demostrar conocimiento en manejo de incidentes y detección de intrusiones.}

Para saber más sobre esta certificación se puede chequear el siguiente enlace: www.giac.org/certifications/gse.php

CompTIA

CompTia es una compañía ya muy reconocida en el mercado mundial, la cual se identifica así misma como “La mayor compañía desarrolladora de certificaciones neutrales en la industria IT”.

La compañía desarrolló una certificación de seguridad de la información “vendor-neutral” llamada Security + que tiene los siguientes tópicos:

SECURITY +

Systems Security

Saber entender y explicar los riesgos de seguridad pertenecientes a los sistemas de hardware y periféricos.

Saber implementar prácticas de hardening de diferentes sistemas operativos tanto para servidores como workstations.

Saber implementar seguridad en las aplicaciones.

Saber entender y explicar el propósito de la tecnología de virtualización.

Network Infrastructure

Saber diferenciar los distintos puertos y sus protocolos, cómo sus respectivos riesgos asociados.

Saber distinguir entre los diferentes elementos de red y sus componentes.

Saber utilizar diferentes herramientas de seguridad.

Saber sobre vulnerabilidades y sus mitigaciones en los dispositivos de red, seguridad en wireless y seguridad física.

Access Control

Saber identificar y aplicar las mejores prácticas de la industria para el control de acceso.

Saber explicar los diferentes modelos existentes de control de acceso.

Saber organizar usuarios y equipos en grupos de dominio o no y acceder acceso por grupos.

Saber identificar y aplicar la diferencia entre identificación y autorización.

Assessments and Audits

Saber conducir asesorías de análisis de riesgo y saber mitigar las mismas.

Manejo de vulnerability assessment y las herramientas más comunes.

Cryptography

Saber los conceptos básicos de la criptografía.

Saber explicar los conceptos básicos de hashing y saber mapear diferentes algoritmos a diferentes aplicaciones.

Entender el funcionamiento de PKI

Saber implementar PKI y manejo de certificados.

Organizational Security

Saber explicar y aplicar planeamiento de redundancia y sus componentes.

Saber implementar procedimientos de disaster recovery.

Saber identificar y explicar las diferentes políticas y legislaciones que existen.

Nota: De los principales puntos mencionados sólo se remarcaron los más importantes a modo de acortar un poco el listado. Para más información chequear la página oficial de ComTIA.

CERTIFICACIONES ORIENTADAS AL SKILL Y AL VENDOR

Tener una certificación de alto nivel es siempre una excelente opción por el reconocimiento en si que tienen las mismas ya mencionadas. Normalmente tener una de estas certificaciones es suficiente para quien realiza una administración de un área de seguridad ya que no sería necesario que la persona que administra el área tenga que entender las implicancias de cómo cambia un bit en un flag de TCP-IP o exactamente que botón apretar en una determinada herramienta para capturar el hash de una password.

Pero si la persona va a ser el que esté del lado de la implementación de un Pentest o hardening de un determinado sistema y/o aplicación entonces el panorama cambiar y ahí es dónde entran las certificaciones técnicas.

Depende del foco que se le quiera dar, se puede obtener certificaciones específicas al área de system o al área de network. Algunas certificaciones son vendor-neutral, sobre todo las del GIAC, pero la mayoría de ellas están directamente relacionadas a un vendor

CISCO

Si bien Cisco tiene una gran cantidad de tracks de carreras de networking, lo cual obviamente siempre fue su especialidad, en los últimos años ha desarrollado un track orientado al network security, el cual está compuesto de las siguientes tres certificaciones:

Cisco Certified Network Associate (CCNA) Security, Cisco Certified Security Professional (CCSP), and Cisco Certified Internetwork Expert (CCIE) Security.

Estas tres certificaciones tienen mucho prestigio dentro de la especialidad de seguridad redes ya que no se las puede render a menos que no se tenga ya la certificación de administración correspondiente (CCNA, CCNP y CCIE correspondientemente), además de tener que tener una vasta experiencia en la configuración de los diferentes appliances de la compañía.

Los cuerpos de conocimiento que tienen estas tres certificaciones son:

CCNA Security:

- Secure Cisco routers.
- Implement AAA on Cisco routers using local router database and external ACS.
- Mitigate threats to Cisco routers and networks using ACLs.
- Implement secure network management and reporting.
- Mitigate common Layer 2 attacks.
- Implement the Cisco IOS firewall feature set using SDM.
- Implement the Cisco IOS IPS feature set using SDM.
- Implement site-to-site VPNs on Cisco Routers using SDM.

CCSP

- Securing Networks with Cisco Routers and Switches.
- Securing Networks with Adaptive Security Appliance (ASA) Foundation.
- Implementing Cisco Intrusion Prevention System.

Y además uno de los siguientes temas:

1. Implementing Cisco Network Admission Control (NAC) Appliance.
2. Implementing Cisco Security Monitoring, Analysis and Response System.
3. Networks with ASA Advanced.

CCIE Security

Realmente cuesta imaginarse a un individuo con esta certificación manejando proyectos de pentest, normalmente una persona con este nivel de certificación está orientado a grandes proyectos de infraestructura de redes, y que obviamente contemplen la seguridad desde el diseño, pero los contenidos obviamente son de un altísimo nivel.

Los tópicos que engloban a esta certificación son varios, veámoslos en detalle:

Table 3.2 CCIE Security Topics

Topic Area	Specific Topics
General Networking	Networking Basics OSI Layers TCP/IP Protocols Switching (VTP, VLANs, Spanning Tree, Trunking, etc.) Routing Protocols (RIP, EIGRP, OSPF, and BGP) Multicast
Security Protocols, Ciphers, and Hash Algorithms	RADIUS TACACS+ Ciphers RSA, DSS, RC4 Message Digest 5 (MD5) Hash Algorithm (SHA) EAP PEAP TKIP TLS Data Encryption Standard (DES) Triple DES (3DES) Advanced Encryption Standard (AES) IP Security (IPSec) Authentication Header (AH) Encapsulating Security Payload (ESP) Internet Key Exchange (IKE) Certificate Enrollment Protocol (CEP) Transport Layer Security (TLS) Socket Layer (SSL) Point to Point Protocol (PPTP) Layer 2 Tunneling Protocol (L2TP) Generic Route Encapsulation (GRE) Shell (SSH) Pretty Good Privacy (PGP)
Application Protocols	Hypertext Transfer Protocol (HTTP) Simple Mail Transfer Protocol (SMTP) File Transfer Protocol (FTP) Domain Name System (DNS) Trivial File Transfer Protocol (TFTP) Network Time Protocol (NTP) Lightweight Directory Access Protocol (LDAP) Syslog
Security Technologies	Packet Filtering Content Filtering URL Filtering

Table 3.2 CCIE Security Topics—cont'd

Topic Area	Specific Topics
	Authentication Technologies Authorization technologies Proxy Authentication Public Key Infrastructure (PKI) IPSec VPN SSL VPN Network Intrusion Prevention Systems Host Intrusion Prevention Systems Event Correlation Adaptive Threat Defense (ATD) Network Admission Control (NAC) 802.1x Endpoint Security Network Address Translation
Cisco Security Appliances and Applications	Cisco Secure PIX Firewall Cisco Intrusion Prevention System (IPS) Cisco VPN 3000 Series Concentrators Cisco EzVPN Software and Hardware Clients Cisco Adaptive Security Appliance (ASA) Firewall Cisco Security Monitoring, Analysis and Response System (MARS) Cisco IOS Firewall Cisco IOS Intrusion Prevention System Cisco IOS IPSec VPN Cisco IOS Trust and Identity Cisco Secure ACS for Windows Cisco Secure ACS Solution Engine Cisco Traffic Anomaly Detectors Cisco Guard DDoS Mitigation Appliance Cisco Catalyst 6500 Series Security Modules (FWSM, IDSM, VPNSM, WebVPN, SSL modules) Cisco Traffic Anomaly Detector Module & Cisco Guard Service Module
Cisco Security Management	Cisco Adaptive Security Device Manager (ASDM) Cisco Router & Security Device Manager (SDM) Cisco Security Manager (CSM)
Cisco Security General	IOS Specifics Routing and Switching Security Features: IP & MAC Spoofing, MAC Address Controls, Port Security, DHCP Snoop, DNS Spoof NetFlow

(Continued)

Table 3.2 CCIE Security Topics—cont'd

Topic Area	Specific Topics
	Layer 2 Security Features Layer 3 Security Features Wireless Security IPv6 Security
Security Solutions	Network Attack Mitigation Virus and Worms Outbreaks Theft of Information DoS/DDoS Attacks Web Server & Web Application Security
Security General	Policies – Security Policy Best Practices Information Security Standards (ISO 17799, ISO 27001, BS7799) Standards Bodies Common RFCs (e.g. RFC1918, RFC2827, RFC2401) BCP 38 Attacks, Vulnerabilities and Common Exploits – recon, scan, priv escalation, penetration, cleanup, backdoor Security Audit & Validation Risk Assessment Change Management Process Incident Response Framework Computer Security Forensics

Global Information Assurance Certification (GIAC)

Si se decide ir por el lado de las certificaciones del GIAC, las mejores que se adecuan para los ingenieros de pen testing, son aquellas que están dentro del track de security administrator, el cual comienza con la certificación GISF seguida por la GSEC. Una vez que tiene estas dos certificaciones se puede ahondar de especialización incluyéndolas relativas al campo del pentesting.

GISF

Cómo dijimos antes, dentro del track de security administrator, existen una gran cantidad de certificaciones incluyéndolas relativas a Windows, unix, Linux, etc.

GISF es la primera del track la cual cubre los siguientes aspectos técnicos:

Table 3.3 GISF Topics

GISF Topic Areas

■ Access Control & Hardening	■ Defense In Depth (Site Network)	■ Overview of Security Principles
■ Applying OODA Loops	■ Exploiting Data Management & Malware	■ Personnel Screening & Terms of Employment
■ Attack Theory & Layer 3 Attacks	■ Exploiting Software Use & Web Applications	■ Practical Networking Fundamentals
■ Auditing, Physical Security, Detection & Response	■ Fundamentals of Hashing & Digital Signatures	■ Public Key Infrastructure (PKI)
■ Building a Security Policy	■ Human Attacks	■ Real World Perimeter Policy Assessment
■ Configuration Management & Backups	■ Implementing & Assessing Security Policy	■ Risk & Vulnerability Management
■ Cryptographic Algorithms	■ Implementing Security Principles	■ Security Awareness
■ Cryptosystems	■ Information Assurance Pillars and Enablers	■ Security in the Enterprise
■ Defense In Depth (Applications)	■ Introduction to Network Communications	■ Security Perspectives
■ Defense In Depth (Border)	■ Introduction to Security Policy	■ Security Process & Incident Detection & Response
■ Defense In Depth (Computers)	■ Network Management & Design	■ Security Process & Risk Analysis
■ Defense In Depth (DMZ)	■ OSI Network Layer	■ Understanding Security Concepts
■ Defense In Depth (Firewalls)		■ Wireless Technology Overview
■ Defense In Depth (Incident Handling)		
■ Defense In Depth (Measuring Progress)		

GSEC

Esta certificación fue creada para certificar que un individuo cuenta con el conocimiento apropiado y habilidad necesaria para manejar responsabilidades técnicas de un área de seguridad. Los tópicos de la misma son:

Table 3.4 GSEC Topics

GSEC Topic Areas

■ 802.11	■ Mitnick-Shimomura	■ UNIX Logging and Monitoring
■ Access Control Theory	■ Network Addressing	■ UNIX OS Security
■ Alternate Network Mapping Techniques	■ Network Design	■ Unix Password System and Root Access
■ Best Practice Approach to Risk Management	■ Network Hardware	■ Unix Patch Management and Maintenance
■ Bluetooth	■ Network Mapping Tools	■ Unix Processes and Minimizing System Services
■ Common Types of Attacks	■ Network Plumbing	■ Unix Security Tools
■ Contingency Planning	■ Network Protocol	■ Virtual Machines
■ Crypto Attacks	■ Network Scanning	■ Virtual Private Networks VPNs
■ Crypto Concepts	■ NIDS Overview	■ Viruses and Malicious Code
■ Crypto Fundamentals	■ NIPS Overview	■ VoIP Functionality & Architecture
■ Defense-in-Depth	■ Password Management	■ Vulnerability Management Overview
■ DNS	■ Physical Security	■ Vulnerability Scanning
■ Firewall Subversion	■ Policy Framework	■ Web Application Security
■ Firewalls	■ Pretty Good Privacy (PGP)	■ Web State
■ General Types of Cryptosystems	■ Public Key Infrastructure (PKI)	■ Windows Active Directory & Group Policy
■ General Types of Stego	■ Reading Packets	■ Windows Automation and Auditing
■ HIDS Examples	■ Real-World Crypto Implementations	■ Windows Backup & Restore
■ HIDS Overview	■ Risk Management Overview	■ Windows Family of Products
■ HIPS Overview	■ Routing Fundamentals	■ Windows IIS Security
■ Honeypots	■ Safety Threats	■ Windows Network Security Overview
■ ICMP	■ Snort as a NIDS	■ Windows Patches & Hotfixes
■ IDS Overview	■ Steganography Overview	■ Windows Permissions & User Rights
■ Incident Handling Fundamentals	■ Symmetric & Asymmetric Cryptosystems	■ Windows Security Templates & Group Policy
■ Information Warfare Examples	■ TCP	■ Windows Workgroups & Accounts
■ Information Warfare Theory	■ TCP Concepts	■ Wireless Overview
■ Introduction to OPSEC	■ tcpdump/windump	■ Wireless Security
■ IP Packets	■ Threat Assessment, Analysis & Report to Management	
■ IPS Examples	■ Traceroute	
■ IPS Overview	■ UDP	
■ IPv6	■ UNIX Backups & Archiving	
■ Legal Aspects of Incident Handling	■ UNIX Command Line and OS Tools	
■ Mitnick Attack Defensive Strategies	■ UNIX Cron Security and Process Scheduling	
	■ UNIX Landscape	

Recordar que estas certificaciones que estamos mencionando son netamente técnicas y están entre las primeras a tomar dentro del track del administrador de seguridad propuesto por el GIAC.

Las otras certificaciones técnicas que se podrían tomar para todo lo relacionado al pentesting y análisis de seguridad de aplicaciones son las siguientes:

- GIAC Web Application Penetration Tester (GWAPT)
- 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 Forensics Analyst (GCFA)
- GIAC Securing Oracle Certification (GSOC)
- GIAC Certified Penetration Tester (GPEN)

Hasta aquí hemos hecho una descripción bastante extensa de las principales certificaciones del Mercado mundial en material de seguridad de la información, tanto las de alto nivel cómo las específicamente técnicas.

Sería imposible, a menos que escribiera un libro sobre la material, seguir mencionando la gran cantidad de certificaciones que existen a nivel de vendor ya que realmente son muchísimas, pero al menos sin describirlas en detalle ni mencionar sus tópicos, tratemos de mencionar al menos a las principales, de acuerdo a si son de networking o de sistema:

CHECKPOINT

- Check Point Certified Security Administrator (CCSA)
- Check Point Certified Security Expert (CCSE)
- Check Point Certified Security Expert Plus (CCSE Plus)
- Check Point Certified Managed Security Expert (CCMSE)
- Check Point Certified Managed Security Expert Plus VSX (CCMSE Plus VSX)
- Check Point Certified Master Architect (CCMA)

JUNIPER

JNCIA-ER (Juniper Networks tracks)

MICROSOFT

- Designing Security for a Windows Server 2003 Network
- Implementing and Administering Security in a Microsoft Windows Server 2003 Network.
- Implementing Microsoft Internet Security and Acceleration (ISA) Server 2004.
- Configuring Microsoft Internet Security and Acceleration (ISA) Server 2006.

SUN Microsystems

- SCSECA

CONCLUSIONES FINALES

Cómo hemos observado con mucho detenimiento y detalle, el mercado de las certificaciones es muy vasto y no menor en cuanto a sus implicancias y contenidos.

Lo mejor para seguir el camino correcto es posicionarse dentro del contexto real del mercado en el que uno se mueve y por sobre todo de acuerdo al rol y tarea que realiza.

Si me dedico a la infraestructura y quiero además participar en proyectos de seguridad dentro de la infraestructura puedo tomar algunas de las certificaciones de alto nivel o alguna relacionada a un vendor con la cual uno trabaje en forma diaria.

Si lo que quiero es dedicarme a realizar todo tipo de tests de intrusión lo ideal sería que tome algunas de las certificaciones del GIAC relativas a la material o inclusive la del E-Council llamada Certified Ethical Hacker, la cual también cuenta con contenido técnico orientado al penetration test.

Si soy un administrador de seguridad, puedo tomar algunas relacionadas a la tecnología/s que administre (Cisco, Checkpoint, Juniper, RedHat, Microsoft, etc.)

Sea cual sea el camino que tomemos siempre hay que tomar en cuenta que las certificaciones son una herramienta, al igual que un título universitario, que nos proveen de una formación base (De la que después tendremos que profundizar por cuenta propia) la cuales nos diferencian dentro del mercado y la comunidad de Infosec.

Bibliografía Utilizada:

Infosec Career Hawking (Sell your skillz, not your Soul) (Editorial Syngress)

Professional Penetration Testing de Thomas Wilhelm (Editorial Syngress)

<http://www.giac.org/>

www.cisco.com/certifications

www.microsoft.com