Auditoria tècnica i de certificació

PID_00239284

Rafael Estevan de Quesada

Material docent de la UOC

Universitat Oberta de Catalunya

Rafael Estevan de Quesada

Enginyer superior de Telecomunicacions per la Universitat Politècnica de València. Consultor en seguretat de la informació certificat en Auditoria de Sistemes d'Informació (CISA®) per la ISACA, amb formació en enginyeria de telecomunicació i quinze anys d'experiència en empreses multinacionals del sector de les telecomunicacions i empreses consultores especialitzades en seguretat de la informació.

La revisió d'aquest material docent ha estat coordinada pel professor: Carles Garrigues Olivella (2017)

Segona edició: febrer 2017

Av. Tibidabo, 39-43, 08035 Barcelona
Disseny: Manel Andreu
Realització editorial: Oberta UOC Publishing, SL
Dipòsit legal: B-685-2017

Introducció

Amb l'objectiu de reduir els incidents de seguretat, les organitzacions tenen implantades una sèrie de mesures amb la idea que, si s'esdevenen, les conseqüències que provoquin siguin mínimes. La selecció de les mesures més idònies estarà basada en un procés d'anàlisi del risc al qual està sotmesa la informació i, en certs casos, aquestes mesures hauran estat escollides d'un catàleg de bones pràctiques reconegut per la indústria, per exemple en la Norma ISO/IEC 27002:2013 (anteriorment es denominava *17799* i ha sofert diverses modificacions i actualitzacions des de la seva creació) o en la COBIT (última versió, 5 de 2012).

D'altra banda, les organitzacions més preocupades per la protecció de la seva informació són conscients que la seguretat total no s'aconseguirà mai; per això, per a tractar d'aconseguir aquesta seguretat global en una organització, també es requereixen uns plans de continuïtat de negoci.

Totes aquestes mesures de seguretat i els mecanismes per a gestionar-les formen el que es denomina un *sistema de gestió de la seguretat de la informació* (SGSI), un sistema que té per objectiu tractar d'evitar els incidents de seguretat; però, si s'arriben a esdevenir, que es puguin gestionar de la millor manera possible i, finalment, que al llarg del temps es pugui aprendre de les conclusions obtingudes i millorar els mecanismes de seguretat.

No obstant això, cal recordar que la seguretat és un procés viu, que no és una meta que s'aconsegueix, que ha d'estar en revisió constant i que és fonamental que en tot moment les mesures de seguretat de què disposa l'organització reflecteixin la situació actual i s'adeqüin a l'entorn en què aquesta es troba.

Per aquesta raó es produeixen canvis constants tant en la configuració dels sistemes d'informació com en el mateix entorn en què es troben. Per tant, és recomanable disposar d'algun tipus de mecanisme de revisió, preferiblement independent, amb l'objectiu que es detectin els aspectes que puguin ser més vulnerables o que no estan correctament configurats.

Aquestes revisions de la seguretat d'una organització es denominen *auditories de seguretat*. Formen part d'aquest cicle viu de la seguretat i permeten assegurar que els controls de seguretat implantats són els més adequats i estan configurats correctament.

Quan les auditories de seguretat es basen en la revisió del conjunt de mesures i del seu procés de gestió davant normatives vigents i concretament davant l'ISO/IEC 27001, ens trobem amb processos que pretenen comprovar que es

gestiona la seguretat d'acord amb uns paràmetres reconeguts per la indústria i això dóna com a resultat les denominades ***certificacions de seguretat del sistema de gestió de la seguretat de la informació***.

D'altra banda, també és interessant destacar que actualment ens trobem davant l'obligació legal de comprovar periòdicament les mesures de seguretat implantades per a reduir els riscos que amenacen la informació. Tant en el marc de la legislació en matèria de protecció de dades (a Espanya, Llei orgànica 15/1999, de protecció de dades de caràcter personal, i la seva legislació d'acompanyament, més concretament el Reial decret 1720/2007, del Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal), com en el marc financer (en l'àmbit europeu, els acords Basilea III (actualització respecte a II el 2010), i per a totes les empreses cotitzades als Estats Units, la Llei Sarbanes-Oxley), s'exigeix fer periòdicament revisions del risc operacional i, per tant, se'n deriva la necessitat de fer auditories de seguretat dels sistemes d'informació. En aquest sentit, és interessant destacar un resum de la secció 404 de la Llei Sarbanes-Oxley disponible en el lloc web de l'AICPA, que expressa clarament aquesta necessitat:

> "Section 404: Management Assessment of Internal Controls
>
> Requires each annual report of an issuer to contain an "internal control report", which shall:
>
> 1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
>
> 2) contain an assessment, as of the end of the issuer's fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting."

La citació indica que la direcció de les empreses cotitzades en els mercats de valors americans ha d'establir i mantenir estructures internes per al control financer i que anualment s'ha de revisar que aquests controls interns siguin efectius. Com que actualment la gestió i el control de les finances recauen íntegrament en sistemes d'informació, tant els controls com les auditories exigides per la Llei Sarbanes-Oxley són extensibles als sistemes d'informació.

Tota aquesta situació que hem comentat ha comportat l'auge de la disciplina de l'auditoria de sistemes d'informació com un derivat inicial de les auditories de comptes. Aquest protagonisme està reforçat per l'entorn actual en què els sistemes d'informació participen cada dia més en tots els processos productius i no solament en els de control financer de les institucions. Per tant, aquest curs té per objecte presentar els conceptes fonamentals que defineixen les auditories de sistemes d'informació i molt especialment centrat en l'auditoria de la seguretat de la informació i mostrar a l'alumnat l'ampli camp que hi ha en aquesta àrea per al seu propi desenvolupament professional.

El material del curs està organitzat en diversos mòduls que van aprofundint en la labor de l'auditor i estan orientats a cobrir un objectiu concret.

El mòdul I presenta a l'estudiant la labor d'auditoria, des d'un punt de vista general i ampli, com una tasca de control en un procés de gestió en una organització. Es presenten els diferents tipus d'auditoria genèrics segons el client, l'auditor i l'auditat, així com el procés que se segueix de manera general i els aspectes pràctics que són comuns a tots els tipus d'auditoria. Igualment, s'introdueix el concepte de programa d'auditoria com la funció de govern d'aquesta àrea dins d'una organització, i el paper de determinades organitzacions que vetllen per estandarditzar la labor d'auditoria.

El mòdul II se centra en l'auditoria emmarcada en la seguretat de la informació, ofereix una introducció a la norma ISO/IEC 27001, explica el procés d'auditoria de certificació i les característiques d'aquest procés.

Així com el mòdul II està centrat en un procés molt ben definit i controlat en l'àmbit de la gestió de la seguretat (la certificació), el mòdul III presenta com el procés d'auditoria intervé en el govern de la seguretat de la informació i explica les característiques comunes als diferents tipus o formes d'afrontar una auditoria sobre algun aspecte de la gestió de la seguretat de la informació.

En el mòdul IV s'explica com, quan s'avalua concretament el nivell de seguretat d'una infraestructura TIC, hi ha diferents iniciatives i estàndards que poden ajudar l'auditor de seguretat TIC a preparar el seu pla d'auditoria. En aquest mòdul se'n presenten unes quantes d'existents i àmpliament conegudes, incloent-hi una introducció a la norma PCI-DSS i els diferents tipus de formes d'avaluació del seu compliment.

Finalment, el mòdul V introdueix l'alumne en diferents tècniques d'auditoria i presenta també diverses eines encara que, per l'extensió d'aquest curs, s'ha de considerar com una mera una introducció per tal que l'alumne tingui coneixement dels diferents tipus i tècniques, i pugui ampliar el seu coneixement, en la mesura que l'aplicació dels coneixements adquirits en aquest curs ho requereixi per a la seva pràctica professional diària.

Continguts

Bibliografia

Champlain, Jack J. (2003). *Auditing Information Systems* (2a. ed.). John Wiley and Sons.

Davis, Chris; Schiller, Mike. (2011). *IT Auditing, Using controls to protect Information Assets* (2a. ed.). McGraw Hill.

Deraison, Renaud; Meer, Haroon; Temmingh, Roelof; van der Walt, Charl; Alder, Raven; Alderson, Jimmy; Johnston, Andy; Theall, George A. (2004). *Nessus Network Auditing*. Syngress Publishing.

Diversos autors. *OWASP – Guide to building Secure Web Applications and Web Services* [en línea]. <http://www.owasp.org/index.php/Guide>. OWASP.

Diversos autors. *OWASP – Testing Guide* [en línea]. <http://www.owasp.org/index.php/OWASP_Testing_Project>. OWASP.

Herzog, Pete (dir.) i altres *Open-Source Security Testing Methodology Manual*. ISECOM.

ISACA. *COBIT© 3rd Edition, 4th Edition, 5th Edition*. Information Systems Audit and Control Foundation (ISACF) / Information Technology Governance Institute.

ISACA. *COBIT© 5 for Assurance*. Information Systems Audit and Control Foundation (ISACF) / Information Technology Governance Institute.

ISACA. *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*. Information Systems Audit and Control Foundation (ISACF) / Information Technology Governance Institute.

McNab, Chris (2004). *Network Security Assessment*. O'Reilly.

Moeller, Robert R. (2010). *IT Audit, Control and Security*. John Willey & Sons.

NIST. *NIST SP 800 53 rev .4: Security and Privacy Controls for Federal Information Systems and Organizations*. U. S. Government Printing Office.

NIST. *NIST SP 800 115 Technical Guide to Information Security Testing and Assessment*. U. S. Government Printing Office.

PCI Security Standard Council. *Payment Card Industry (PCI) Data Security Standard: version 3.2*. PCI Security Standard Council.

PCI Security Standard Council. *Payment Card Industry (PCI) Data Security Standard: Security Audit Procedures*. PCI Security Standard Council.

Peltier, Thomas R.; Peltier, Justin; Blackley, John A. (2003). *Managing a Network Vulnerability Assessment*. Auerbach Publications.

Rogers, Russ; Miles, Greg; Fuller, Ed; Dykstra, Ted; Hoagberg, Matthew (2004). *Security Assessment: Case Studies for Implementing the NSA IAM*. Syngress Publishing.