Marcs de treball de les auditories de seguretat TIC

PID_00239289

Rafael Estevan de Quesada

Temps mínim de dedicació recomanat: 4 hores

Universitat Oberta de Catalunya

Índex

Introducció

A causa de la importància i notorietat recents que han adquirit la seguretat dels sistemes d'informació i la necessitat d'assegurar que s'està gestionant correctament tant organitzativament com tècnica, han sorgit un gran nombre d'iniciatives per a ajudar a comprendre els diferents aspectes que componen una auditoria o fins i tot més ambiciós, un programa d'auditoria completa de la seguretat de la informació. L'ambició i els mitjans de què han disposat les diverses organitzacions que els han promogut varien molt, per la qual cosa tant el detall com l'abast dels aspectes que tracten són molt variats, així com la seva evolució i manteniment al llarg del temps. En aquest apartat, no pretendrem explicar exhaustivament i detalladament tots els marcs de treball en la matèria que s'han publicat i/o estandarditzat. Es pretén donar a conèixer alguns dels més representatius, coneguts i potser amb més projecció ara per ara. Per tant, ens centrarem únicament en un petit conjunt d'aquestes per la gran rellevància que tenen avui dia, i forma part de la professionalitat de cada auditor estar al corrent de les novetats i evolucions dins del seu sector.

L'auditor ha de conèixer els marcs de treball més emprats a cada moment per diversos motius. D'una banda, els clients d'auditoria voldran tenir un punt de referència per a conèixer quins mètodes o quines maneres de treballar té l'auditor i el grau de fiabilitat i el nivell de coneixement de l'evolució de la indústria de la seguretat de la informació. Li proporcionarà aquest suport el fet d'ajustar la manera de treballar, reflectida en un pla d'auditoria, als marcs de treball i a les metodologies (quan aquestes existeixin en aquells marcs de treball que esculli) que més s'adaptin a l'abast i tipus d'auditoria prevista, i és per aquesta raó que és un punt important a incloure en el pla d'auditoria, tal com s'ha comentat en mòduls anteriors. Així mateix, el coneixement dels diferents marcs de treball és una eina que permet a l'auditor mantenir el seu nivell de formació al dia quant a àrees d'interès, nous marcs de control de la seguretat de la informació, i evolució o noves formes de realitzar proves d'auditoria. Aquests marcs de treball que repassarem són revisats i actualitzats periòdicament, per a reflectir l'evolució tant de la tecnologia com dels nous tipus de riscos als quals s'enfronta una infraestructura TIC i la informació manejada per les organitzacions modernes. Un auditor ha d'estar al corrent de la seva evolució i anar adequant els seus procediments de treball propis a aquesta evolució.

D'altra banda, s'ha de tenir molt en compte que no s'ha de donar un crèdit complet a aquests marcs de treball, en el sentit de no pretendre ajustar la forma de treballar completament a les indicacions que s'hi donin. És difícil tant que aquests marcs detallin tots els aspectes a tenir en compte en una auditoria, com que els objectius d'auditoria del client estiguin completament alineats amb els genèrics que poden tenir aquests marcs de treball i que estan fonamentats en models de referència o millors pràctiques. En cada assignació

d'auditoria l'auditor, abans de decidir-se a aplicar-los totalment o parcial en un marc en concret (o diversos combinats), cal examinar detalladament en quines circumstàncies són aplicables, quines en són les característiques i els punts forts que els fan rellevants i útils per a l'assignació. Únicament, ens centrarem en un petit conjunt d'aquestes metodologies, per la gran rellevància que tenen avui dia.

És difícil incloure en aquest mòdul tots els marcs de treball rellevants per a un auditor de seguretat TIC, però sí que hi ha certes iniciatives interessants. La gran majoria posen l'accent en els aspectes més tècnics, i poques fan referència de manera general als aspectes organitzatius de la seguretat de la informació. Les metodologies que examinarem seran:

- Les metodologies i les guies nord-americanes emeses pel NIST relacionades amb la seguretat de la informació (grup de publicacions especials SP 800).

- Les metodologies del moviment de programari lliure fent èmfasi especial al projecte OWASP.

- Les metodologies publicades per les principals entitats emissores de targetes de crèdit i aplicables a les organitzacions involucrades en les transaccions de pagament i que, per tant, emmagatzemen, processen o transmeten dades de targetes de crèdit: *payment card industry* (PCI), *data security standard*, *security audit procedures*.

- Els estàndards i les guies de bones pràctiques publicades per la ISACA (Information Systems Audit and Control Association).

Insistim finalment una altra vegada que és important que un equip auditor conegui els marcs de treball ja publicats per anar formant la seva pròpia metodologia, i així dissenyar la més apropiada a l'abast i l'enfocament de cada auditoria concreta, per a poder formalitzar-la en el document de pla d'auditoria.

1. Metodologies i guies del NIST

Per a entendre el context en què s'aplica aquesta guia, s'ha de comprendre l'entorn en què s'aplica a les agències federals nord-americanes. Com en altres països desenvolupats, l'Administració nord-americana ha comprès que és necessari garantir la seguretat de la informació manejada pels serveis públics per a donar un servei correcte i segur als ciutadans en tractar la seva informació i en general la del govern del país. Per a això, l'any 2002, es va aprovar als Estats Units la Federal Information Security Management Act (FISMA), que reconeix la importància de la seguretat de la informació per a la seguretat econòmica i nacional del país.

Aquesta llei obliga totes les agències federals a desenvolupar un sistema de gestió de la seguretat de la informació, basat en una gestió del risc i un procés de millora contínua, fonamentat en revisions anuals de la seguretat. És a dir, obligava totes les agències (excepte les encarregades de la seguretat nacional) a gestionar la seguretat de la informació segons els paràmetres i el mecanisme que hem estat repassant en aquest curs. En aquest context, la FISMA atorga al NIST un paper important. El NIST és una agència federal nord-americana de caràcter públic l'objectiu del qual és la divulgació, innovació i competitivitat industrial mitjançant la promoció de la investigació, per a l'establiment de patrons de mesura (per exemple operen el rellotge atòmic NIST-F1 que estableix l'hora oficial al país) i el desenvolupament d'estàndards, guies i metodologies en gairebé tots els àmbits de la ciència. Per tant, el NIST està encarregat de desenvolupar estàndards, guies, directrius, mètodes i tècniques, i fins i tot requisits mínims aplicables a un gran nombre de diferents tipus de sistemes, inclosos els sistemes d'informació i la seva seguretat.

Emmarcades en el NIST existeixen múltiples suborganitzacions dedicades cadascuna d'elles a diferents àrees del coneixement. Entre elles, pel que fa a seguretat de la informació (o també anomenada *ciberseguretat*), hi ha un centre específic per a aquesta temàtica, el Computer Security Resource Center (CSRC).

El CSRC facilita l'intercanvi i la divulgació d'eines i bones pràctiques de seguretat de la informació, proporciona recursos sobre estàndards de seguretat de la informació i directrius, i identifica els principals recursos de seguretat a la xarxa per recolzar els usuaris en la indústria, el govern i el món acadèmic.

Algunes de les seves conclusions i els seus treballs són elevats més endavant a estàndards federals (dins de la família de normes FIPS [*federal information processing standard*]) que són d'aplicació obligada en l'àmbit de l'Administració nord-americana. Però també hi ha els seus treballs més generals de bones pràctiques (denominats SP-800 *special publications serie 800*) que estan disponibles per al públic en general, i són una font molt completa i fiable sobre diferents

temes relacionats amb la seguretat de la informació (reflecteixen els resultats de les seves recerques i guies sobre criptografia, infraestructures de clau pública, sistemes d'identificació i autenticació, seguretat de xarxes de dades, seguretat en sistemes de control industrial i també en gestió de la seguretat de la TIC). Per tant, és interessant que els auditors de sistemes d'informació els coneguin per aplicar-los en la mesura que hi sigui aplicable.

1.1. Marc de referència de la FISMA (*Federal Information Security Management Act*)

El NIST ha desenvolupat tot un conjunt de documents SP-800 per tal de donar un marc de referència complet a la gestió de la seguretat de la informació, que ha de ser aplicat per les agències nord-americanes a causa de la llei FISMA (*Federal Information Security Management Act*).

És interessant conèixer-lo, ja que és molt complet i ha passat pel filtre d'una institució de prestigi reconegut i que dedica esforços a mantenir actualitzades les seves guies i directrius. A més, tracta àmpliament de les fases de revisió de la seguretat de la informació, que és l'objecte que ens ocupa.

El marc que s'ha creat es pot resumir en les grans directrius següents:

- **Categorització dels sistemes d'informació** (SP 800-60 *Guide for Mapping Types of Information and Information Systems to Security Categories* i FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*). Es defineixen diferents categories de sistemes TIC d'acord amb els diferents nivells de riscos per a la confidencialitat, disponibilitat i integritat. Proporciona eines per a categoritzar i mapar diferents tipus d'informació a aquestes categories.

- **Gestió de riscos** (SP 800-30 *Risk Management Guide for Information Technology Systems*). S'ofereix una guia per a implantar un procés complet de gestió dels riscos per a assegurar la confidencialitat, disponibilitat o integritat pel seu impacte en les operacions de l'organització. Per tant, ofereix una metodologia per a dur a terme l'anàlisi de riscos (anàlisi de les amenaces, vulnerabilitats sobre els sistemes TIC i els impactes o danys potencials), i les subsegüents fases de la gestió de la mitigació del risc basant-se en l'avaluació de cost-benefici i, posteriorment, la revisió de l'anàlisi.

- **Catàleg de controls de seguretat** (SP 800-53 *Recommended Security Controls for Federal Information Systems* i FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems*). Aquest catàleg proporciona directrius per a assegurar els sistemes d'informació dins del Govern federal mitjançant la selecció i especificació dels controls de seguretat. Aquestes directrius de la NIST SP 800-53 són adequades per a tots els sistemes d'informació federals, a excepció dels sistemes nacionals, com els sistemes de seguretat, per la qual cosa també es poden considerar vàlids per a un

Antecedent SP 800-53A

Antigament, existia el document NIST-SP 800-26 *Guide for Information Security Program Assessments and System Reporting Form*, que incloïa un annex amb un qüestionari detallat que havia de completar l'auditat (o amb l'ajuda d'un assessor o, en el nostre cas, l'equip auditor), indicant el nivell d'implantació aconseguit de cadascun dels aspectes del marc definit pel NIST-SP 800-53. No obstant això, aquest document va ser retirat pel NIST i substituït pel document NIST-SP 800-53A.

altre tipus d'organitzacions, encara que no siguin part de l'Administració pública nord-americana.

– Descriu el procés de selecció i especificació dels controls de seguretat d'un sistema d'informació, i de definició de l'organització general de l'enfocament de la gestió del risc de l'organització.

– Descriu el procés de selecció del conjunt inicial dels controls de seguretat millorat, partint dels resultats de l'avaluació de riscos.

– Defineix el conjunt mínim de controls de seguretat que s'hi han d'aplicar per a crear un programa de seguretat de la informació eficaç.

– Proporciona directrius sobre l'actualització dels controls, com a part d'un procés de supervisió continu i exhaustiu.

– Aporta aclariments sobre com la utilització de controls de seguretat ajuda a la implantació d'un programa de seguretat de la informació.

És important entendre l'amplitud d'aquesta guia. La FISMA obliga les agències federals a implantar els controls del FIPS 200, que deriven del NIST SP 800-53. Primerament, han de categoritzar, mitjançant el FIPS 199 (derivat del NIST SP 800-60), els diferents tipus de sistemes d'informació que tinguin i, posteriorment, aplicar-hi els controls mínims (es denomina *baseline*) que es reflecteixin en el FIPS 200 per al nivell determinat d'acord amb les guies i les directrius del NIST SP 800-53. Per tant, aquest document és detallat quant a donar una guia per a la implantació, però no deixa de ser un catàleg de controls similar, encara que més exhaustiu, a l'ISO/IEC 27002.

- **Pla de seguretat dels sistemes TIC** (SP 800-18 *Guide for Developing Security Plans for Federal Information Systems*). S'hi introdueix un pla de seguretat dels sistemes TIC que documenti els requisits de seguretat i els controls de seguretat implantats, o en previsió de ser-ho, per a la protecció de la informació i els sistemes d'informació. També es reconeix que aquest tipus de documents han de ser vius i que requereixen una revisió periòdica, una modificació, i plans d'acció i de fites per a l'aplicació de controls de seguretat. Hi ha d'haver procediments d'avaluació que s'esbossin en els plans, s'ha de mantenir el pla actual i donar seguiment als controls de seguretat previstos.

- **Certificació i posterior verificació i revisió contínua** (SP800-53A *Guide for Assessing the Security Controls in Federal Information Systems*). Una vegada implantats els controls, s'han d'avaluar per a comprovar que funcionen correctament. Aquest procés s'ha de fer abans de la posada en producció (es denomina *certificació*), però també, després, durant el seu cicle de vida. Per tant, el NIST SP 800-53A és un document per a orientar l'avaluació d'una organització i compleix el NIST SP 800-53. Un dels principals objectius de disseny és proporcionar un marc d'avaluació inicial i un punt de

partida per als procediments d'avaluació contínua, que són essencials per a aconseguir la coherència de les avaluacions.

– Proporciona directrius per a la construcció de plans eficaços d'auditoria de la seguretat i procediments que permetin l'avaluació dels controls de seguretat utilitzats.

– Descriu el marc conceptual per a la creació de procediments específics per a l'auditoria dels controls de seguretat del NIST SP 800-53.

– Il·lustra els components d'un marc d'auditoria de la seguretat.

– Amplia i explica el procés de derivar procediments d'auditoria a partir del marc d'auditoria.

– Descriu el procés d'auditoria dels controls de seguretat en l'organització de sistemes d'informació, incloent-hi la creació de proves d'auditoria.

– Analitza les accions necessàries per a preparar una auditoria de seguretat.

– Descriu el procés d'anàlisi, documentació, informes i resultats de l'auditoria de la seguretat.

– Comunica la importància de la continuïtat de les auditories de seguretat per a la protecció a llarg termini.

És interessant destacar que el NIST SP 800-53A proporciona un conjunt de procediments d'auditoria per als diferents controls del NIST SP 800-53, però constitueix en realitat un punt de partida perquè els auditors desenvolupin els seus propis procediments i plans d'auditoria basant-se en aquesta metodologia. Addicionalment a aquest marc, i partint del grau d'oficialitat que dóna un document SP, el NIST també facilita un conjunt de cas d'avaluació molt més concret i detallat per a diferents tipus d'auditoria o, com ells en diuen, *assessment cases*.

- **Acreditació** (SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*). El procés d'acreditació de la seguretat d'un sistema TIC és el procés pel qual un responsable d'una agència federal pren la decisió d'autoritzar el funcionament d'un sistema d'informació i, explícitament, acceptar el risc per al funcionament de les agències d'acord amb l'aplicació d'un conjunt acordat de controls de seguretat. Mitjançant l'acreditació d'un sistema d'informació, es responsabilitza plenament de qualsevol impacte advers en cas d'una violació de la seguretat. Per tant, la responsabilitat i la rendició de comptes són principis fonamentals que caracteritzen l'acreditació de seguretat. És essencial que els funcionaris que han de prendre aquesta decisió tinguin la informació més completa, precisa i fiable possible sobre l'estat de seguretat dels seus sistemes d'informació,

amb la finalitat de fer-la oportuna i creïble, a partir del risc i de les decisions sobre la possibilitat d'autoritzar el funcionament dels sistemes. Aquesta guia ofereix detalladament com ha de ser tant el procés de certificació com el d'acreditació.

A l'auditor de seguretat li resultarà especialment interessant conèixer el catàleg de controls del NIST SP 800-53, i la seva relació amb altres tipus de catàlegs, com l'ISO/IEC 27002. Aquest coneixement i comparació li permetrà aplicar les recomanacions que dóna el NIST SP 800-53A i els diferents casos d'auditoria (*assessment case*) que contenen informacions i ajudes valuoses. Tanmateix, serà necessària la seva perícia per a adaptar-les als seus propis interessos.

Aquests documents són mantinguts, per la qual cosa es recomana acudir al lloc web esmentat per a obtenir-ne l'última versió i altres documents que puguin haver estat publicats com a annexos.

1.2. NIST SP 800-115 - *Technical guide to Information Security testing and assessment*

Fora del marc desenvolupat pel NIST descrit anteriorment, també desenvolupa altres tipus de documents de tipus més pràctic. Quant a això, destacarem el NIST SP 800-115 - *Technical guide to Information Security testing and assessment*.

Nota

Aquest document substitueix l'*SP800-42 Guideline on Network Security Testing*, què tenia un abast més limitat.

Aquest document és una guia que complementa el document SP800-53A, el qual és més oficial i està integrat en els mecanismes de control de la informació que ha dissenyat el NIST per a les organitzacions federals nord-americanes. No obstant això, aquesta guia és més generalista, descriu aspectes tècnics bàsics a tenir en compte en la realització d'avaluacions de seguretat de la informació i és un material utilitzable de manera més general per part de la comunitat de Seguretat. Presenta mètodes tècnics de proves, exàmens, tècniques i aspectes de planificació i organització que una organització podria utilitzar com a part d'una avaluació, a més d'informacions per als auditors sobre la seva execució i l'impacte potencial que poden tenir en els sistemes i xarxes. D'altra banda, s'ha de ser conscient que, a més de l'execució de les proves tècniques, hi ha altres factors ja comentats que donen suport per garantir l'èxit del procés d'avaluació i, en general, aportar valor per millorar la posició de seguretat d'un sistema (i en última instància, de tota l'organització). Alguns d'aquests altres factors també es presentan en aquesta guia, com ara un procés de planificació robusta, una anàlisi de resultats i detecció de les causes arran dels problemes identificats i una correcta presentació de resultats.

Aquest document facilita a l'auditor indicacions sobre 2 vessants molt diferenciades: d'una banda, com organitzar l'activitat d'auditoria i, de l'altra, facilitar informació sobre el tipus d'accions tècniques que pot desenvolupar un auditor

per realitzar les seves proves d'auditoria. En termes generals, aquesta guia facilita tant a les organitzacions auditores com a les auditades indicacions sobre els següents aspectes:

- Desenvolupar una política en l'organització referent a l'avaluació de la seguretat, la metodologia a emprar i els rols i responsabilitats individuals relacionades amb els aspectes tècnics de l'avaluació.

- Planificar amb precisió per a una avaluació tècnica de seguretat d'informació, proporcionant una guia per a determinar quins sistemes s'utilitzen per a avaluar i quin enfocament. Fer front a les consideracions logístiques que puguin ser d'aplicació. Desenvolupar un pla d'auditoria i donar garanties que s'han pres en consideració els aspectes legals i de compliment d'altres polítiques o normatives aplicables.

- Executar de forma segura i amb eficàcia una avaluació tècnica de seguretat d'informació utilitzant els mètodes i les tècniques que es presenten, i respondre a qualsevol incident que pugui ocórrer durant l'avaluació.

- Manejar adequadament les dades tècniques (recollida, emmagatzematge, transmissió i destrucció) en tot el procés d'avaluació.

- Realitzar l'anàlisi de resultats i elaborar els informes tècnics, així com traduir les troballes en accions de mitigació de riscos que millorin la situació de seguretat de l'organització.

Aquest document no dóna una metodologia concreta per realitzar les avaluacions, però determina que qualsevol persona que engegui una organització ha de comptar amb un mínim de fases i facilita informació per definir-les:

1) Planificació:

- Desenvolupament d'una política d'avaluació de la seguretat que sigui conforme a les necessitats de l'organització i estigui degudament recolzada per la direcció per poder establir rols, responsabilitats, periodicitats, lliurables a realitzar, etc.

- Planificació i priorització d'assignacions d'acord amb la importància dels actius a analitzar, segons el seu nivell crític (per la missió que compleix un determinat sistema o per la tipologia de la informació que tracti, per exemple, podria tractar-se de dades personals molt sensibles com ara la salut, dades de targetes de crèdit o informació crítica per al negoci). Es poden establir diferents requeriments tant quant als tipus d'avaluacions com a les freqüències, de manera que s'optimitzin els recursos disponibles per realitzar les avaluacions.

- Determinació dels tipus de tècniques d'avaluació de seguretat a emprar segons els requeriments que s'han establert en la planificació i prioritització. Com veurem més endavant, algunes tècniques poden implicar certs riscos a l'hora d'executar-les i això ha de tenir-se en compte en la planificació.

- Resolució dels aspectes logístics de les avaluacions, des de l'assignació de persones, desplaçaments, possible maquinari que sigui necessari, llicències d'eines, etc.

- Desenvolupament i comunicació per a cada assignació del corresponent pla d'auditoria que detalli les activitats que s'hagin de realitzar.

2) Execució de l'avaluació d'acord amb la política establerta mitjançant la realització de les diferents assignacions d'avaluació conformement al seu corresponent pla d'auditoria previ. Durant l'execució, és important tenir en compte aspectes com la comunicació amb les parts interessades, l'escalat en cas d'incidències o el descobriment de problemes greus. D'altra banda, aquesta fase comporta en si mateixa la realització de les proves i la seva posterior anàlisi.De vegades, segons el tipus de tècnica emprada, això pot produir-se de manera iterativa, ja que l'anàlisi de certs resultats pot determinar la necessitat o conveniència de realitzar noves proves fins a aconseguir els objectius generals de l'avaluació. Aquest seria el cas, per exemple, en el qual es realitza un test d'intrusió. Així mateix, també s'ha de tenir especial cura amb la manera en què es tracta la informació recollida durant l'execució de proves i hi ha d'haver un protocol adequat per al seu tractament, que cobreixi les diferents fases (recollida, emmagatzematge, comunicació i destrucció), ja que la informació recollida durant aquest tipus de proves pot ser especialment sensible.

3) Postexecució. La guia preveu que, amb posterioritat a l'execució i a l'anàlisi de la informació, hi ha una fase pròpia destinada a transmetre a les parts interessades els resultats mitjançant l'elaboració d'un informe que tingui en compte les troballes i també faciliti recomanacions per a la seva mitigació.

La implementació en una organització d'una metodologia que contingui aquestes fases que preveu la guia ajudarà a poder gestionar correctament els recursos necessaris (persones, eines, maquinari, terminis de temps, freqüències, etc.) i, en general els costos, així com a obtenir els objectius de les esmentades avaluacions de seguretat.

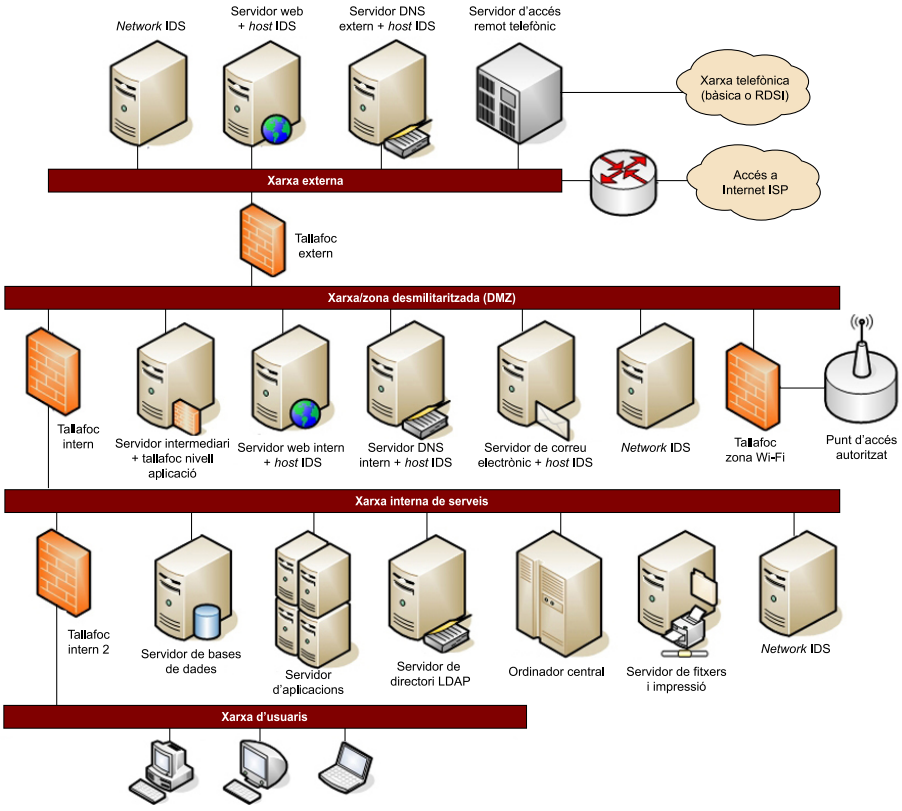
Un aspecte important a tenir en compte és que el document està orientat únicament a l'avaluació de la seguretat de sistemes d'informació i xarxes de comunicació i no a altres aspectes organitzatius de la seguretat de la informació (aquest és el punt que ho fa clarament diferent de l'SP800-53A). És purament tècnic i per tant aplicable a sistemes com els següents:

- Elements d'interconnexió. Per exemple, encaminadors, interruptors (gestionables o no).

- Elements de seguretat perimetral, com ara tallafocs (tant interns com externs), sistemes de detecció o prevenció d'intrusos (IDS/IPS).

- Serveis típics de xarxa. Per exemple, servidors de noms (DNS), servidors de directoris (LDAP, Activedirectory, etc.), servidors de fitxers, servidors web, servidors de correu electrònic (tant servidors SMTP com IMAP o POP3) i, en general, servidors d'aplicacions.

Una arquitectura típica que seria analitzable, mitjançant les tècniques i proves descrites en aquesta metodologia, seria el diagrama que apareix en el següent exemple de referència d'una arquitectura de xarxa a auditar:



Aquesta guia planteja diferents tipus de tècniques de proves a realitzar per avaluar la manera en què una infraestructura compleix amb els requeriments de seguretat. Aquestes tècniques poden ser tant proves com exàmens i la matisació que introdueix aquesta guia entre aquests dos tipus és que les proves solen comportar una interacció amb els sistemes d'informació, mentre que els exàmens acostumen a relacionar-se amb la verificació del nivell d'implementació d'un control de seguretat tècnic d'una manera indirecta mitjançant observa-

ció, per exemple de la documentació, de fitxers de configuració, de conjunts de regles, etc. Tenint això en compte, de manera general la guia agrupa les diferents tècniques en les següents tres grans categories:

1) Tècniques de revisió

- Revisió de documentació que descrigui arquitectures de sistemes d'informació i d'altres sistemes específics de seguretat.
- Revisió de registres d'activitat.
- Revisió de conjunts de regles (de tallafocs, d'IDS, d'antivirus, en general de qualsevol sistema de seguretat que estigui basat en regles).
- Revisions de configuracions.
- Recollida i anàlisi de trànsit de xarxa.
- Verificació d'integritat de fitxers crítics.

2) Tècniques d'identificació i anàlisi d'objectius

- Descobriment de sistemes connectats a la xarxa.
- Identificació de ports i serveis disponibles en els sistemes connectats a la xarxa.
- Escaneig de vulnerabilitats.
- Escaneig en xarxes sense fils.

3) Tècnica de verificació de vulnerabilitats

- Atacs contra contrasenyes (per força bruta o més convenient per diccionari).
- Test d'intrusió.
- Enginyeria social (que es pot combinar amb el test d'intrusió per tenir una visió més realista de la posició general de seguretat d'una organització).

Per a cadascuna d'aquestes categories, la guia facilita informació i suggeriments sobre els aspectes que s'hauran de tenir en compte a l'hora de realitzar-les. És important tenir present que la guia no facilita informació concreta sobre la manera explícita en què es realitzen les proves, però sí que facilita informació molt interessant per tal que l'auditor pugui elaborar correctament un pla

d'auditoria i dissenyar les seves proves sense obviar tots els aspectes pràctics que cadascun d'aquests tipus de proves pot comportar, des de logístics fins a de coordinació amb l'auditat.

2. Metodologies del moviment de programari lliure

Una altra font d'informació i referència que cada dia està rebent més credibilitat és el moviment de programari lliure. Amb una data de fundació relativament recent, s'han creat diverses comunitats amb uns objectius, cadascun lleugerament diferent, però que, quant a l'auditoria tècnica de seguretat en sistemes d'informació, ha aportat els seus propis marcs de treball i de vegades metodologies o guies per a millorar la seguretat que l'equip auditor ha de tenir en compte a l'hora de planificar la part tècnica de les seves auditories. Sense ànim de desacreditar altres moviments, projectes i comunitats que també existeixen i que aporten la seva pròpia visió de l'activitat d'auditoria, actualment els moviments que més destaquen són els següents:

2.1. ISECOM (Institute for Security and Open Methodologies)

L'ISECOM és una comunitat d'usuaris independents, creada el 2001, constituïda com una organització no governamental i sense ànim de lucre l'objectiu de la qual és la conscienciació, investigació i certificació en matèria de seguretat dels sistemes d'informació. Destaca perquè ha desenvolupat una metodologia (OSSTMM: *open source security testing methodology manual*) per a l'auditoria dels sistemes d'informació. En la seva versió 3 va canviar la seva visió, que fins aleshores estava orientada a donar una metodologia d'auditoria des de l'òptica de comprovar la seguretat dels sistemes davant atacs fets per una tercera part externa a l'organització.

Enllaç recomanat

La versió 3.0 està publicada, en anglès, en la URL http://www.isecom.org/mirror/OSSTMM.3.pdf

En la seva última revisió d'aquest material fins avui, la metodologia ha evolucionat encara més amb l'objectiu de proporcionar una valoració objectiva de la seguretat operacional d'una organització. L'OSSTMM pretén definir un mètode d'auditoria per determinar, de la manera més objectiva possible i de manera quantitativa, com de bé operen els controls de seguretat que s'han implantat per realment protegir la informació. És a dir, l'OSSTMM s'apropa més a una metodologia d'avaluació de riscos per poder buscar com avaluar l'eficàcia dels controls, no el seu simple compliment de guies de bones pràctiques, normes, documentació interna corporativa o aspectes normatius de compliment legal. La metodologia busca ser tan científica i repetible com sigui possible amb l'objectiu final d'avaluar numèricament el grau d'eficàcia de l'acompliment de la seguretat, i per aquesta raó considerem que és tant una metodologia d'auditoria com també d'avaluació de risc. L'execució d'un test segons l'OSSTMM facilita al final una puntuació (denominada RAV) que varia des de 0 fins a valors que poden superar 100, quan és 100 representa que hi ha un balanç òptim entre els controls existents i com s'opera enfront de les amenaces reals, mentre que un valor per sota de 100 representaria una situació en la qual els controls són ineficaços. Els valors superiors a 100 indicarien situacions en les quals la complexitat dels controls és superior al nivell òptim i,

a més d'incórrer en ineficiència, també poden produir-se problemes de gestió d'aquests que podrien provocar, fins i tot, situacions adverses per a la seguretat. En aquest sentit i com s'ha comentat, l'OSSTMM s'apropa més a una metodologia d'anàlisi de riscos que a una metodologia d'auditoria de seguretat, ja que el procés que estableix és molt tancat i orientat a l'avaluació de diferents aspectes amb l'objectiu final de realitzar el càlcul del RAV. Una organització pot emprar aquesta metodologia per a avaluar periòdicament l'estat de la seguretat, observar com evoluciona el nivell d'eficàcia dels controls i desenvolupar plans per ajustar-los amb l'objectiu d'apropar-se al valor objectiu 100. D'altra banda, en ser molt completa, té en compte gairebé tots els factors que poden incidir en la seguretat de la informació, per la qual cosa és una font d'informació interessant per a l'auditor de seguretat TIC a l'hora de realitzar les seves pròpies metodologies.

Per veure la manera en què pot ser emprat per un auditor, cal tenir present que l'OSSTMM, conceptualment, realitza una anàlisi molt metòdica d'un determinat entorn o abast. L'abast es defineix com el conjunt dels actius que es vol protegir i, a partir d'aquests, també les persones, els processos i els serveis que els empren, els mecanismes de protecció que els afecten, i els aspectes externs que els condicionen per al correcte funcionament, com ara la seva ubicació, els subministraments, els proveïdors, les normatives, els contractes, els proveïdors, etc. Aquest abast interactua o, en certa mesura, es produeixen fluxos d'informació tant dins mateix de l'abast com cap a l'exterior, en diferents nivells o, com la metodologia denomina, canals en els quals s'avalua la seguretat i que l'OSSTMM classifica de la següent manera:

a) Nivell PHYSEC - Seguretat física, que pot ser per dos canals:

- Humà: referent a les implicacions de les relacions de confiança entre les persones.

- Físic: referent a aspectes tangibles de seguretat (murs, càmeres, portes d'accés, etc.).

b) SPECSEC - Seguretat "radioelèctrica". Bàsicament tot allò referent a comunicacions sense fils i també aspectes de seguretat de la informació que poden ser rellevants mitjançant emanacions electromagnètiques (emissions de senyals radioelèctrics potser no intencionades que poden tenir implicacions de seguretat).

c) COMSEC - Seguretat de les comunicacions. En aquest aspecte, l'OSSTMM separa el que fa referència als canals:

- Telecomunicacions: qualsevol aspecte relacionat amb els sistemes d'informació relacionats amb el transport de veu (inclòs veu sobre IP, cen-

trals de commutació i senyalització, sistemes de registres de trucades, bústies de veu, etc.).

- Xarxes de dades: en aquest canal es considera, en general, tot el que s'entén per sistema d'informació i comunicació, quan la seva finalitat no està relacionada amb sistemes de veu.

Per avaluar la seguretat dels controls aplicats en cadascun d'aquests cinc canals, la metodologia que l'OSSTMM dóna és idèntica per a cadascun d'ells que sigui rellevant en els intercanvis d'informació, i tots ells passen per l'avaluació d'uns conceptes precisos. En la pràctica, òbviament no s'avalua de la mateixa manera cadascun d'aquests passos, i és aquí on l'OSSTMM és una bona font d'informació per afrontar l'avaluació d'aspectes sobre els quals un auditor tal vegada no estigui encara perfectament capacitat i necessiti una visió sobre com auditar determinats aspectes rellevants de la seguretat d'una infraestructura TIC:

- Seguretat de la informació existent sobre l'organització en mitjans públics, bàsicament informació publicada a Internet de manera intencionada o no i rellevant per a l'organització.

- Seguretat dels processos en què intervé el personal de l'organització, per tal d'avaluar en quina mesura és susceptible de ser atacada emprant tècniques d'enginyeria social.

- Seguretat vista des del punt de vista purament tècnic dels sistemes de l'organització exposats a Internet.

- Seguretat vista des del punt de vista purament tècnic dels sistemes de comunicacions de veu, inclòs veu sobre IP.

- Seguretat vista des del punt de vista purament tècnic de les comunicacions sense fil, incloent-hi xarxes Wi-Fi (802.11x), RFID, Bluetooth, infrarojos, etc.

- Seguretat física vista des del punt de vista purament tècnic.

2.2. OWASP (Open Web Application Security Project)

L'OWASP és una comunitat d'usuaris independent i molt activa iniciada el setembre de 2001. Està constituïda com una organització no governamental, sense ànim de lucre, que té per objectiu facilitar a les organitzacions la informació i els mitjans per a desenvolupar, adquirir i mantenir, de manera segu-

ra, aplicacions basades en tecnologies d'Internet, també anomenades comunament *aplicacions web*. Fonamentalment, la iniciativa facilita a la comunitat de seguretat TIC lliurables dels diferents tipus:

- guies i/o documentació,
- eines,
- codi per a ser emprat en entorns productius.

La visibilitat d'aquesta iniciativa ha crescut enormement en els últims anys a causa de l'auge de l'ús de tecnologies englobades en el que es coneix com a *web applications*, que ofereixn millors nivells d'estandardització i d'integració. Parlem del següent:

- Aplicacions web amb interfícies per a usuari amb independència del suport que emprin, tant si són ordinadors personals com si són dispositius personals com tauletes o *smartphones*.
- Interfícies entre sistemes basats en tecnologies web com a interfícies, anomenats *webservices* (diferents tecnologies com ara SOAP sobre HTTP, XML-RPC, JSON-RPC, etc.).

Per tant, tots els documents, metodologies i eines que l'OWASP facilita estan orientats a la seguretat en l'entorn d'aplicacions web però no descriu tècniques per a comprovar la seguretat d'altres aspectes en la gestió de la informació, com processos organitzatius, continuïtat de negoci, seguretat física, etc.

Aquesta organització, al contrari que la ISECOM, afronta la seguretat només de les aplicacions web, però des de tots els seus aspectes del cicle de vida, i considera que les seves recomanacions s'han d'incloure des de les etapes inicials del cicle de vida d'un sistema. Per tant, gran part dels seus esforços s'orienten a definir les característiques que han de tenir les aplicacions web per a garantir la seguretat de la informació que tracten. En aquest sentit, la iniciativa OWASP ha desenvolupat al llarg dels anys molts projectes, alguns amb més èxit que d'altres, gràcies al suport que han rebut per la comunitat tant a l'hora de continuar amb el seu desenvolupament com pel seu ús al món real. Actualment, dins de l'OWASP hi ha la tendència a potenciar més la part de *testing* que la de disseny i, en aquest sentit, és molt profitós per a un auditor de seguretat TIC. Inicialment, un dels seus projectes estrella dins de l'OWASP va ser l'elaboració d'una guia o d'un manual que recull aquestes característiques i que es pot utilitzar per a dissenyar, desenvolupar, desplegar o auditar aplicacions web, i que s'adreça a arquitectes de sistemes, programadors, consultors i auditors. No obstant això, en els darrers anys els projectes destinats a la comprovació de la seguretat han tingut molt més suport i desenvolupament per part de la comunitat.

A dia d'avui, els projectes més interessants d'aquesta comunitat a l'hora de facilitar informació i eines a l'auditor de seguretat TIC són:

a) Documentació

- OWASP - *Developper Guide*, en la mesura que és el producte més antic de la iniciativa OWASP i amb visió més completa.
- OWASP - *Testing guide*.
- OWASP *Top Ten vulnerabilities*.

b) Eines

- OWASP ZAP (*Zed Attack Proxy*),
- OWASP OWTF (*Offensive Web Testing Framework*).

2.2.1. OWASP Top ten vulnerabilities

Aquest projecte no és, en si mateix, cap tipus de metodologia, sinó més aviat una eina per a l'educació i conscienciació, en matèria de seguretat, en les aplicacions web. Té per objecte recollir el consens a què ha arribat la comunitat per a identificar les deu fallades de seguretat més importants que se solen cometre a l'hora de dissenyar una aplicació web. El públic objectiu d'aquest *top ten* és molt ampli, per la qual cosa el grau de detall i la manera d'explicar volen ser tan didàctics com sigui possible. Es pretén, per mitjà d'aquesta iniciativa, que totes les parts involucrades en la gestió del cicle de vida d'una aplicació web coneguin quines vulnerabilitats s'han d'evitar.

Per la seva simplicitat i facilitat de comprensió, s'ha convertit en un referent de les vulnerabilitats que s'han d'evitar i és emprat, tant per clients d'auditories com pels mateixos auditors, com a referència dels objectius que ha de complir una auditoria que busqui avaluar la seguretat d'una aplicació web. Aquest ampli espectre d'ús fa que sigui interessant o gairebé imprescindible que un auditor de seguretat TIC el conegui.

L'última versió del 2013 (es preveu la seva revisió el 2016 o 2017) recull les següents vulnerabilitats (text oficial):

> "A1 - Injecció. Les fallades d'injecció, com ara SQL, US i LDAP, ocorren quan s'envien dades no confiables a un intèrpret com a part d'una ordre o consulta. Les dades hostils de l'atacant poden enganyar l'intèrpret en executar ordres no intencionades o accedir a dades no autoritzades.
>
> A2 - Pèrdua d'autenticació i gestió de sessions. Les funcions de l'aplicació relacionades amb autenticació i gestió de sessions amb freqüència s'implementen incorrectament, i permeten als atacants comprometre contrasenyes, claus, testimonis de sessions o explotar altres fallades d'implementació per assumir la identitat d'altres usuaris.
>
> A3 - Seqüència d'ordres en llocs creuats (XSS). Les fallades XSS ocorren cada vegada que una aplicació pren dades no confiables i les envia al navegador web sense una validació i codificació adients. XSS permet als atacants executar seqüències d'ordres en el navegador

de la víctima que poden segrestar les sessions d'usuari, destruir llocs web o dirigir a l'usuari cap a un lloc maliciós.

A4 - Referència directa insegura a objectes. Una referència directa a objectes ocorre quan un desenvolupador exposa una referència a un objecte d'implementació intern, com un fitxer, un directori, o una base de dades. Sense una verificació de control d'accés o una altra protecció, els atacants poden manipular aquestes referències per accedir a dades no autoritzades.

A5 - Configuració de seguretat incorrecta. Una bona seguretat requereix tenir definida i implementada una configuració segura per a l'aplicació, els marcs de treball, el servidor d'aplicació, el servidor web, la base de dades i la plataforma. Totes aquestes configuracions han de ser definides, implementades i mantingudes, ja que, en general, no són segures per defecte. Això inclou mantenir tot el programari actualitzat, incloses les llibreries de codi utilitzades per l'aplicació.

A6 - Exposició de dades sensibles. Moltes aplicacions web no protegeixen adequadament dades sensibles com ara números de targetes de crèdit o credencials d'autenticació. Els atacants poden robar o modificar aquestes dades per dur a terme fraus, robatoris d'identitat o altres delictes. Les dades sensibles requereixen mètodes de protecció addicionals com el xifratge de dades, així com també de precaucions especials en un intercanvi de dades amb el navegador.

A7 - Absència de control d'accés a funcions. La majoria d'aplicacions web verifiquen els drets d'accés a nivell de funció abans de fer visible en la mateixa interfície d'usuari. Malgrat això, les aplicacions necessiten verificar el control d'accés en el servidor quan s'accedeix a cada funció. Si les sol·licituds d'accés no es verifiquen, els atacants podran realitzar peticions sense l'autorització apropiada.

A8 - Falsificació de peticions en llocs creuats (CSRF). Un atac CSRF obliga el navegador d'una víctima autenticada a enviar una petició HTTP falsejada a una aplicació web vulnerable, incloent-hi la sessió de l'usuari i qualsevol altra informació d'autenticació inclosa automàticament. Això permet a l'atacant forçar el navegador de la víctima per generar ordres que l'aplicació vulnerable interpreta com a peticions legítimes provinents de la víctima.

A9 - Utilització de components amb vulnerabilitats conegudes. Alguns components com ara les llibreries, els marcs i altres mòduls de programari, gairebé sempre funcionen amb tots els privilegis. Si s'ataca un component vulnerable, això podria facilitar la intrusió en el servidor o una pèrdua seriosa de dades. Les aplicacions que utilitzin components amb vulnerabilitats conegudes afebleixen les defenses de l'aplicació i permeten ampliar el rang de possibles atacs i impactes.

A10 - Redireccions i reexpedicions no validades. Les aplicacions web sovint redirigeixen i reenvien els usuaris cap a altres pàgines o llocs web i utilitzen dades no confiables per a determinar la pàgina de destinació. Sense una validació apropiada, els atacants poden redirigir les víctimes cap a llocs de pesca o programari maliciós o utilitzar reexpedicions per a accedir a pàgines no autoritzades."

A més de conèixer el *top ten* de l'OWASP, l'auditor ha de conèixer també les tècniques per a construir aplicacions web segures, i les tècniques per a auditar l'ús o la implementació d'aquests controls.

2.2.2. La guia OWASP per al desenvolupament d'aplicacions web

Inicialment, el projecte original de l'OWASP era la creació d'una guia de desenvolupament segur d'aplicacions web (OWASP *Guide to building Security Web Applications and Web Services*, actualment denominat OWASP *Developper Guide*). És un dels projectes que més suport va rebre i el que tenia una orientació més generalista, ja que preveia tots els aspectes que s'han de tenir en compte a l'hora de garantir la seguretat de la informació tractada en el context d'una aplicació web. És a dir, des de decisions relatives a elements fonamentals d'arquitectura i disseny fins a regles i principis de desenvolupament i configuració i, finalment, la seva operació. Iniciada el 2002, l'OWASP (*Guide*

to building Secure Web Applications and Web Services) continua actualment en la versió oficial 2.0.1 de 2005, però la versió 3 es troba en un avançat estat de desenvolupament, tot i que encara no s'ha donat per finalitzada per la comunitat OWASP.

Aquest document té per objectiu mostrar els aspectes que cal tenir més en compte en una aplicació web, a l'hora de garantir la seguretat de la informació que maneja. Es tracta d'un catàleg de controls de seguretat que s'haurien d'adoptar en el disseny d'una aplicació web. Aquests controls recullen:

- L'explicació de conceptes de seguretat:
  - Tipus i tècniques d'atacs.
  - Definició d'arquitectures segures.
  - Anàlisi dels riscos derivats de les vulnerabilitats en aplicacions web.

- Un catàleg detallat dels requisits de seguretat que s'haurien d'incorporar en un disseny d'una aplicació web, i una explicació de com cal comprovar si estan implementats. Aquests requisits estan estructurats de la manera següent (en la versió 2.2):
  - Autenticació.
  - Autorització.
  - Gestió de sessions.
  - Validació de les dades d'entrada.
  - Injecció de codi d'intèrprets (SQL, LDAP, *shell code*, etc.).
  - Formes canòniques i tractament de codificacions UNICODE.
  - Mecanismes de registre d'activitat (traces d'auditoria) i de gestió de les condicions d'error.
  - Configuració del sistema de fitxers dels servidors web.
  - Prevenció dels desbordaments de memòria.
  - Protecció de les interfícies d'administració de l'aplicació.
  - Criptografia.
  - Procés d'instal·lació i configuració (en cas que es tracti d'aplicacions desenvolupades per un tercer).
  - Procés de manteniment. Aquest és l'únic apartat de la guia que fa referència a processos executats per personal a càrrec del manteniment de l'aplicació
  - Protecció contra denegació de servei.

A l'hora d'afrontar una auditoria emprant aquesta guia, l'equip auditor haurà de prendre-la com la referència dels requisits auditables. En si mateixa, la guia no facilita una metodologia per a fer una auditoria, sinó que constitueix una referència a la qual l'auditor s'ha de dirigir per a entendre més bé les aplicacions web, els atacs que poden patir i les tècniques o els elements de disseny que els resolen.

2.2.3. OWASP - *Testing guide*

Dins de l'àmbit de l'OWASP, s'ha desenvolupat el projecte OWASP - *Testing guide*, per tal de proporcionar un marc complet per a l'auditoria/proves d'aplicacions web. Des de la seva creació (avui ja està en la seva versió 4), aquest ha estat un dels projectes de l'OWASP que més suport ha aconseguit i ha fet que el seu contingut hagi evolucionat, s'hagi refinat i mantingut actualitzat amb l'evolució de la tecnologia i els escenaris reals de riscos. Aquesta guia es pretén ser una referència perquè les organitzacions l'emprin i l'integrin amb les seves pròpies metodologies o formes de treball. En aquest sentit, aquest material pot ser utilitzat per l'equip auditor per a desenvolupar el seu propi pla d'auditoria, la qual cosa facilitarà aquesta tasca.

La metodologia està clarament dividida en dues parts que han estat desenvolupades de manera successiva però que, a partir de l'última versió, s'han combinat en un únic document.

En una primera part, es descriu un marc de referència que comprèn les diferents tasques i tècniques de prova més apropiades a cada fase del cicle de vida d'una aplicació. En aquest sentit, descriu de manera general, com a possibles tècniques per a fer l'auditoria d'aplicacions web, les següents:

- **Inspeccions i revisions manuals**. Tasques fetes personalment pels auditors consultant documentació, entrevistant personal clau o duent a terme proves específiques sobre l'aplicació.

- **Anàlisi de riscos**. Per a estimar correctament l'impacte de les vulnerabilitats detectades, s'hi ha d'aplicar algun tipus de metodologia d'anàlisi de riscos com les que ja s'han comentat en mòduls anteriors.

- **Revisions de codi**. Examen detallat de parts del codi d'una aplicació.

- **Proves d'intrusió**. Proves en mode caixa negra en un sistema en producció o preproducció.

Un altre dels aspectes que el marc de referència mostra és el tipus de proves que s'han de dur a terme segons el punt en què es trobi l'aplicació dins del seu cicle de vida. De nou, el model de cicle emprat és similar al que també utilitza el NIST. Segons la fase en què es trobi l'aplicació, proposa una sèrie de comprovacions que cal dur a terme:

- **Fase 1. Inici**
  - Revisió de les polítiques i els estàndards aplicables.
  - Revisió dels criteris de mesurament dels factors de funcionament de l'aplicació que s'han d'utilitzar per a mesurar l'eficàcia de l'aplicació.

- **Fase 2. Definició i disseny**

  - Revisió dels requisits de l'aplicació per a comprovar la inclusió correcta dels requisits de seguretat (s'utilitzarà la guia OWASP que detalla els requisits recomanats).
  - Revisió dels dissenys d'arquitectura.
  - Revisió dels casos d'ús de l'aplicació.
  - Anàlisi de riscos de l'aplicació emprant els requisits, el disseny d'arquitectura i els casos d'ús.

- **Fase 3. Desenvolupament**
  - Revisió de codi: per a revisar la lògica de l'aplicació i de baix nivell per a detectar possibles vulnerabilitats, com les detallades en la guia OWASP.

- **Fase 4. Desplegament**
  - Prova d'intrusió en l'aplicació en preproducció, com a fase final del desplegament i com a part del conjunt de les proves per a l'acceptació del sistema.
  - Revisió de la configuració de l'aplicació.

- **Fase 5. Operació i manteniment**
  - Revisió del procés d'operació i manteniment per a comprovar que, des del punt de vista purament operatiu, no s'estan cometent errors.
  - Revisió periòdica de l'aplicació.
  - Revisió de les actualitzacions.

En la segona part, la metodologia de l'OWASP - *Testing guide* descriu tècnicament les proves que s'han de fer en una aplicació per a comprovar les vulnerabilitats més importants, per la qual cosa no es pot considerar una llista completa i tancada de totes les proves que s'han de dur a terme, tot i que sí que n'és una de molt completa. Aquesta llista s'ha de considerar un catàleg de proves i una font d'informació per a l'equip auditor a l'hora de dissenyar detalladament les proves que s'han de fer i incloure en el seu pla d'auditoria d'aplicacions web. Es refereix a proves d'aplicacions en mode de caixa negra i les organitza en les categories següents:

- Informació sobre l'aplicació revelada públicament, sense execució de cap tipus d'interacció fora del seu ús habitual o de la cerca a Internet.
- Aspectes de seguretat en la configuració de la plataforma.
- Procés de gestió de la identitat dels usuaris de l'aplicació.
- Procés de gestió del procés d'autenticació.
- Procés de gestió del marc d'autorització.
- Procés de gestió de la sessió d'usuari.
- Validació de les dades d'entrada.
- Tractament d'errors.
- Ús de la criptografia.
- Lògica de negoci (aquest és un dels aspectes de vegades oblidats en les auditories i fa referència al possible abús de la lògica de negoci implementada per l'aplicació i no tant a errors de programació).

- Revisió dels aspectes de seguretat en el costat client.
- Revisió de *webservices* emprats en aplicacions mòbils.
- Revisió d'aspectes de seguretat específics d'entorns desplegats i infraestructures en el núvol.
- Revisió de la preparació de l'aplicació enfront d'atacs de denegació de servei.

Com es pot comprovar, el catàleg de proves que ofereix és molt ampli, i l'equip auditor ha d'ajustar el conjunt de proves que s'han de dur a terme a l'abast determinat.

Finalment, la guia també facilita indicacions sobre l'elaboració de l'informe en el qual s'han de presentar els resultats.

2.2.4. Eines de l'OWASP

A més del mateix contingut de la guia, l'OWASP també promociona la creació d'eines sota llicència GPL per a l'estudi i prova d'aplicacions web. En aquest sentit, hi ha diverses iniciatives interessants pel nivell de desenvolupament aconseguit corresponen a:

- OWASP ZAP (*Zed Attack Proxy*). És una eina eminentment per a l'auditoria d'aplicacions web i és bàsica per a la realització de proves d'auditories web. És un servidor intermediari local amb funcionalitats d'anàlisi de seguretat que l'auditor empra per a monitorar, analitzar, interceptar i manipular qualsevol part dels paràmetres d'una comunicació HTTP entre el navegador client i l'aplicació web. Mitjançant aquesta anàlisi, l'auditor pot avaluar el comportament de l'aplicació i executar gran part de les proves dissenyades en el pla d'auditoria. És una eina molt flexible i versàtil que permet la seva ampliació amb mòduls, alguns dels quals permeten l'automatització de certs tipus de proves.

- OWASP OWTF (*Offensive Web Testing Framework*). Es tracta d'una aplicació web modular per a ajudar els auditors d'aplicacions web a unificar l'entorn d'execució de proves.

- OWASP ModSecurity CRS (*Core Set Ruleset*). ModSecurity és una eina de codi obert de seguretat WAF (*Web Applications Firewall*) que analitza el trànsit HTTP per a detectar i, segons la manera en què estigui operant, bloquejar el trànsit en cas d'identificar algun patró d'atac. És una eina basada en patrons o signatures. Aquest projecte OWASP proporciona un conjunt de regles per a la identificació d'atacs de diferents categories.

2.3. PTES (*penetration testing execution standard*)

Dins de les activitats d'auditoria de seguretat en sistemes d'informació, la realització d'un test d'intrusió (o *penetration testing*, en anglès) és un dels tipus de proves que, de manera més realista, avalua la situació de la seguretat d'una infraestructura TIC, encara que no ho realitza de manera sistemàtica per a tots els controls. Malgrat no facilitar la visió exhaustiva de la situació de tots els controls en els seus resultats, és una activitat que en el mercat de la seguretat de la informació s'empra com a exercici de prova real de l'eficàcia global i combinada dels controls de seguretat i també dels equips que els operen, en cas que es facin amb el seu desconeixement. Per aquesta raó, són eines molt populars per a augmentar, sobretot, la conscienciació en capes directives de l'organització i a més, en alguns casos, per a l'obtenció i el manteniment de determinades certificacions que requereixen de la realització periòdica d'aquest tipus de prova d'auditoria de seguretat TIC, com per exemple PCI.

Ja s'han comentat anteriorment diferents metodologies o marcs de treball a partir dels quals un equip auditor pot preparar la seva pròpia metodologia de test d'intrusió. No obstant això, hi ha una iniciativa de la comunitat de seguretat que busca facilitar una metodologia uniforme i consensuada per a l'execució d'aquest tipus de proves. És l'anomenada PTES (*penetration testing execution standard*). Sense estar explícitament recolzada per cap fabricant ni grup de desenvolupadors d'eines de seguretat conegudes, és important subratllar que aquesta metodologia s'empra en materials de divulgació generats per organitzacions tan conegudes com Offensive Security (recolzada per l'empresa Offsec Services Ltd.) o per col·laboradors de PTES que són o van ser membres de Rapid7, actualment propietària de la coneguda eina de *pentesting* "metasploit".

Enllaç recomanat

La pàgina web d'aquest projecte es troba en:
http://www.pentest-standard.org/

Fins al moment, la metodologia PTES no és un estàndard oficial recolzat per cap entitat d'estandardització, sinó una iniciativa governada des de l'esperit dels moviments col·laboratius d'Internet i no té en si mateixa la vocació de convertir-se en un estàndard oficial (almenys segons declaren els seus principals promotors). Per contra, pretén obtenir un estatus d'estàndard *de facto* que potser podria ser emprat per altres estàndards més oficials.

L'estàndard PTES està encara en fase de desenvolupament en algunes de les seves parts però, pel seu contingut, és interessant que els equips auditors el coneguin per poder desenvolupar els seus propis plans d'auditoria o metodologies de treball quan l'assignació que rebin sigui realitzar un test d'intrusió. El treball realitzat en el projecte PTES és molt ambiciós, ja que pretén incloure totes les fases d'un projecte de prova d'intrusió, des de les inicials de contacte amb l'auditat i client del projecte, fins a les finals de presentació de resultats. Comprèn les següents fases d'un projecte de prova d'intrusió:

1) Interaccions inicials (correspon a les accions necessàries per a establir, tant amb l'auditat com amb el client de l'auditoria, tots els elements rellevants per a la feina que cal desenvolupar en l'assignació d'auditoria.

2) Recollida d'intel·ligència (entenent *intel·ligència* com la informació rellevant i processada respecte a l'objectiu obtinguda de manera no intrusiva),

3) Modelatge d'amenaces,

4) Anàlisi de vulnerabilitats,

5) Explotació de vulnerabilitats,

6) Postexplotació de vulnerabilitats,

7) Elaboració d'informe de resultats.

Encara que no tots els seus apartats estan igualment desenvolupats, els més tècnics (del 2 al 6) proporcionen un nivell de detall i referències externes suficients perquè l'auditor pugui elaborar la seva pròpia metodologia i també seleccionar les eines adients. Alguns apartats importants com el 7, dedicat a la comunicació dels resultats, són molt escarits i necessiten ampliació, encara que l'essencial està disponible.

2.4. OISSG (Open Information Systems Security Group)

Finalment, val la pena esmentar l'OISSG com un altre projecte emmarcat dins del conjunt de metodologies sorgides del moviment de programari lliure per a proporcionar eines d'auditoria de sistemes.

L'OISSG és una comunitat d'usuaris independents, constituïda com una organització no governamental sense ànim de lucre, que té per objectiu facilitar a la comunitat informació rellevant en matèria d'avaluació de la seguretat de la informació mitjançant la publicació de guies, metodologies i eines.

L'OISSG destaca pel fet de ser un marc de referència per a les proves de seguretat denominat ***ISSAF*** **(*information systems security assessment framework*)**. La diferència amb altres marcs de referència rau en el gran nombre de proves que proposa i el gran nombre d'entorns que s'hi preveuen. No obstant això, té el problema que encara és en una fase recent de desenvolupament, amb la qual cosa alguns aspectes no estan completament desenvolupats. A finals del 2016, hi ha una versió del document en la seva versió 1, tot i que s'ha de considerar per ara com un esborrany, ja que diversos dels apartats estan incomplets o no han estat actualitzats quant als aspectes tecnològics (per exemple, els apartats

referents a Microsoft Windows només fan referència a les versions NT, 2000 i 2003, encara que molt del material explicat és totalment aplicable a versions més modernes d'aquest sistema operatiu).

El fet que encara estigui en fase de desenvolupament redueix, en gran manera, l'aplicabilitat de la metodologia de manera íntegra. No obstant això, és una font d'informació excel·lent perquè l'equip auditor prepari el pla d'auditoria i el disseny de les proves que s'han de dur a terme.

3. Norma PCI - DSS

Les principals empreses capdavanteres en el mercat de les targetes de crèdit (American Express, Discover Financial Services, JCB, MasterCard Worldwide i Visa International) han tingut sempre un interès per la protecció de la informació de les dades contingudes en les targetes i en les transaccions. Totes han elaborat, separadament, els seus propis programes per a conscienciar els seus comerços i clients en matèria de seguretat. Potser la més activa ha estat Visa, però finalment totes han col·laborat en l'elaboració d'un estàndard de seguretat que harmonitzi cadascun d'aquests programes i que serveixi, d'una manera conjunta, per a protegir les dades personals dels titulars de les targetes i la mateixa informació de les targetes. L'estàndard que han definit es denomina ***Payment Card Industry Data Security Standard*** **(PCI DSS)**. Per coordinar i harmonitzar els seus diferents programes de seguretat i mostrar més independència, aquestes empreses han creat l'organització **PCI Security Standards Council**, amb els objectius de donar suport a l'aplicació de l'estàndard PCI DSS mitjançant la publicació de les eines (bàsicament guies) per a la implementació de l'estàndard, i igualment mantenir i desenvolupar l'estàndard mateix. A més d'aquest estàndard, el Consell duu a terme altres activitats que també poden ser d'interès per a l'auditor i que mereixen la seva atenció.

Altres activitats que duu a terme el Consell

- Llista de requisits de seguretat i tècniques per a la seva avaluació, per a dispositius d'introducció del número personal secret (*PIN entry device*, que poden anar des de caixers automàtics, també coneguts com a *ATM*, fins a punts de vendes informatitzats), que recull un conjunt únic de requisits aplicables als fabricants per a poder protegir informació crítica manejada en aquests dispositius, com ara PIN, dades del titular de la targeta, etc. Així mateix, també ofereix una llista dels fabricants i els dispositius que compleixen aquest estàndard, i també dels laboratoris autoritzats per a fer les proves.

- Estàndard per a la seguretat de les aplicacions de pagament. Amb la finalitat de garantir que les aplicacions desenvolupades per un tercer i utilitzades per comerciants o proveïdors de serveis compleixen els requisits del PCI DSS, s'ha desenvolupat aquest estàndard i la llista d'aplicacions.

- Manteniment de la llista d'assessors de seguretat qualificats (QSA: *qualified security assessor*) per a fer revisions de la implantació del PCI DSS, i dels proveïdors de serveis d'anàlisi de vulnerabilitats (ASV: *approved scanning vendor*).

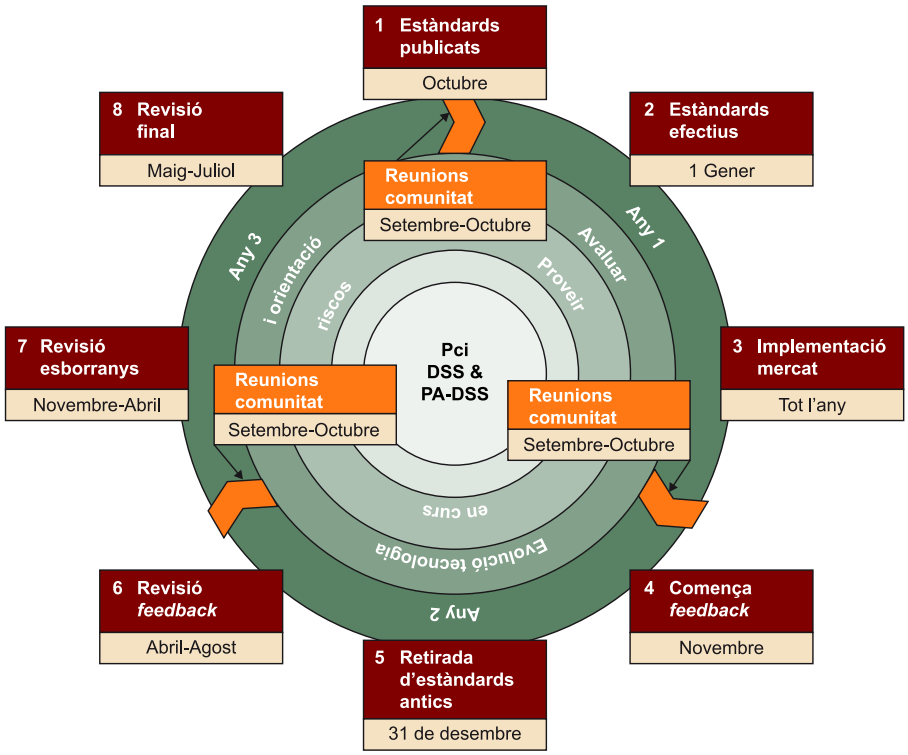
3.1. Manteniment de l'estàndard PCI - DSS

Indubtablement, el principal treball del PCI SS Council és el manteniment de l'estàndard PCI DSS.

El PCI DSS és un estàndard que està en contínua revisió i, amb data d'elaboració d'aquest material, l'última versió publicada era la 3.2, d'abril de 2016, però anualment pot rebre petites revisions i actualitzacions. No obstant això, el seu objectiu es manté des d'un inici i consisteix a facilitar un ampli

conjunt de requisits per a millorar la seguretat de les dades relacionades amb les targetes de crèdit. A partir de l'edició de la versió 2 de l'estàndard PCI-DSS, el PCI SS Council va decidir adoptar un model de revisió constant de l'estàndard per poder garantir que es vagi adequant al panorama d'amenaces contra la indústria de les targetes de crèdit i també que vagi beneficiant-se de les millores tecnològiques que es van introduint. Per a això, s'ha definit un model de revisió per a PCI-DSS i PA-DSS de tres anys amb vuit fases consecutives que asseguren una introducció gradual de noves versions i permeten a les organitzacions no quedar-se fora de compliment per un canvi de versió.

El gràfic següent mostra les diferents fases (es tracta d'una combinació entre fases i fites).



Font: PCI Security Standards Council

- Fase 1 (fita): l'estàndard es publica a finals del mes d'octubre. És completament vigent però les organitzacions no estan obligades a implementar-lo fins que no es faci efectiu.

- Fase 2 (fita): el nou estàndard es fa efectiu. A partir d'aquest moment, les organitzacions han d'emprar la nova versió, però hi ha un període de gràcia de 4 mesos per a fer la transició i, durant aquest període, les organitzacions poden mostrar encara el seu compliment de l'estàndard emprant la versió antiga. No obstant això, és recomanable que qualsevol modificació de controls de seguretat es realitzi amb el nou estàndard com a referència.

- Fase 3 (fase): el primer any (des de la publicació) es considera el període d'implementació. Durant aquesta fase, les organitzacions (tant les que han

d'implantar els controls com els QSA) han de familiaritzar-se amb el nou estàndard i implantar els sistemes d'informació d'acord amb la nova versió. És un període en què tota la indústria de les targetes de crèdit observa l'estàndard en el seu funcionament.

- Fase 4 (fase): l'octubre de l'any 1 de vigència del nou estàndard s'inicia oficialment el període de revisió que finalitzarà a finals de març de l'any 2. Totes les parts interessades tenen la possibilitat d'enviar al PCI SS Council els seus comentaris i suggeriments, especialment en tot allò que pugui fer referència a aspectes tecnològics o d'amenaces a les dades de targetes de crèdit.

- Fase 5 (fita): el 31 de desembre de l'any 2 es retira la versió anterior i les organitzacions només podran mostrar el compliment de l'estàndard amb la versió vigent.

- Fase 6 (fase): el PCI SS Council inicia oficialment la revisió de tots els comentaris rebuts a la nova versió. Típicament, el procés consisteix a avaluar la idoneïtat del comentari o suggeriment i incorporar-lo o elaborar una revisió categoritzant-lo com a "Aclariment", "Guia addicional" o "Requisit evolucionat". Aquest període comprèn d'abril a agost de l'any 2.

- Fase 7 (fase): des del final de la fase de revisió dels suggeriments de la comunitat fins a finals d'abril de l'any 3, internament el PCI SS Council elabora l'esborrany d'una possible nova versió.

- Fase 8 (fase): en l'última fase, el PCI SS Council comparteix l'esborrany del nou estàndard amb un panel d'assessors per realitzar una última revisió i un ajust del text. Aquest període va de maig a finals de juliol de l'any 3.

D'aquesta manera, el PCI SS Council garanteix que l'estàndard estigui sempre alineat amb les millors pràctiques de seguretat i tecnologia del mercat.

3.2. Requeriments de l'estàndard PCI-DSS

Des d'un punt de vista global, podem dir que l'estàndard PCI-DSS tracta temes com la gestió de la seguretat, polítiques i procediments, arquitectura de xarxes, i disseny de programari. El seu contingut és senzill i està estructurat en els sis objectius de control següents i un total de 12 requeriments de seguretat d'alt nivell:

- **Construir i mantenir una arquitectura de xarxa segura**
  - Requisit 1. Instal·lar i mantenir una infraestructura tallafoc per a protegir les dades dels titulars de les targetes.
  - Requisit 2. No utilitzar els valors per defecte facilitats pels fabricants per a sistemes d'identificació o altres sistemes de seguretat.

- **Protegir les dades dels titulars de targetes**
  - Requisit 3. Protegir les dades emmagatzemades de les targetes.
  - Requisit 4. Xifrar la transmissió de dades de targetes per mitjà de xarxes públiques.

- **Mantenir un programa de gestió de les vulnerabilitats**
  - Requisit 5. Emprar i actualitzar regularment programari antivirus.
  - Requisit 6. Desenvolupar i mantenir sistemes i aplicacions segurs.

- **Implementar mesures robustes de control d'accés**
  - Requisit 7. Restringir l'accés a les dades de les targetes segons el principi de necessitat de conèixer per raons de negoci.
  - Requisit 8. Assignar una identificació única a cada persona amb accés.
  - Requisit 9. Restringir l'accés físic a llocs, dispositius i sistemes amb dades de targetes.

- **Monitorar i auditar regularment les xarxes**
  - Requisit 10. Registrar i monitorar tots els accessos a recursos de xarxa i sistemes que continguin dades de targetes.
  - Requisit 11. Auditar regularment els sistemes i processos.

- **Mantenir una política de seguretat de la informació**
  - Requisit 12. Mantenir una política que tracti específicament la seguretat de la informació.

Juntament amb aquests 12 requeriments, l'estàndard PCI-DSS defineix altres addicionals específics per a circumstàncies concretes, com per exemple en el cas de proveïdors de serveis d'allotjament compartit.

Aquests objectius de control i els seus 12 requeriments són desenvolupats amb més detall dins de l'estàndard. Com es pot comprovar, afronta la seguretat de la informació (en aquest cas, les dades de les targetes) des d'una perspectiva àmplia, com es fa en la Norma ISO/IEC 27001 o COBIT, encara que una mica més centrada en els controls aplicats en xarxes de dades, aplicacions i alguns processos al voltant de la gestió d'aquests. Com la definició de polítiques que descriguin la forma d'operar dels controls, o també els controls aplicables als recursos humans. No obstant això, s'eludeixen o no es tracten amb gaire profunditat aspectes com l'estructura organitzativa (comitès o estructures per la governança de la seguretat o esquemes de classificació i tractament de la informació) per a la gestió de la seguretat, la continuïtat de negoci o el compliment del marc legal que, en aquest cas, seria molt important en països com Espanya o altres de la Comunitat Europea amb una protecció de la privadesa i de la informació de caràcter personal, la qual és molt rellevant quan es parla d'informació relacionada amb targetes de crèdit i pagaments efectuats.

3.3. Aplicabilitat de l'estàndard PCI-DSS a la indústria

La norma PCI-DSS és de compliment obligat sempre que una organització tracti qualsevol d'aquestes dades de targetes de crèdit (alguns tenen un nivell de protecció més o menys elevat segons l'estàndard):

- Dades de titulars de la targeta:
  - numeració completa de la targeta,
  - nom i cognom,
  - data de venciment,
  - codi de servei.

- Dades confidencials:
  - dades emmagatzemades en la banda magnètica (conegudes com a "track1" i "track2"),
  - codi de seguretat imprès en la targeta,
  - PIN.

Per tant, és aplicable a les institucions financeres i comercials que fan ús dels serveis dels emissors de targetes de crèdit, i també proveïdors de serveis que processin, emmagatzemin o transmetin informació en nom d'institucions financeres, comercials o les mateixes empreses emissores de targetes de crèdit-durant una transacció econòmica amb una targeta. Aquest entorn és relativament complex i, en el moment de realitzar una transacció, de manera general, intervenen els següents actors:

- *Cardholder*: titular de la targeta. Es tracta de la persona a nom de qui està emesa la targeta i en principi n'és l'usuari. N'ha de conèixer el PIN i és responsable de la seva custòdia. En principi, l'usuari real i el titular de la targeta són la mateixa persona, però en la pràctica es donen molts casos en què no és així. De la mateixa manera, cal recordar que en els inicis de les targetes de crèdit no hi havia mecanismes per a realitzar verificacions *online* ni PIN, per la qual cosa l'autenticació es realitzava mitjançant la signatura manuscrita del titular de la targeta i un document acreditatiu de la seva identitat (als EUA això últim no succeeix, ja que no existeix l'obligació legal de disposar d'aquest tipus de document, però sí a Europa).

- *Merchant*: comerç. En termes generals, es tracta de qui desitja rebre un pagament per part del *cardholder* que utilitza la targeta, a canvi d'algun tipus de mercaderia o servei. El *merchant* pot voler fer la transacció en un lloc físic (una botiga) o en un lloc web.

- *Issuing Bank*: és el banc o entitat financera que contracta el *cardholder* per obtenir una targeta. És qui rep les peticions d'autorització i ha de donar indicacions de si es pot o no realitzar la transacció.

- *Acquiring Bank*: és el banc o entitat financera contractada pel *merchant* per tal que gestioni els pagaments que ha de rebre. Tant l'*issuing bank* com l'*acquiring bank* han de pertànyer a una associació de gestors de targetes.

- *Payment Processor*: entitat que contracta el *merchant* per fer d'intermediari amb *l'acquiring bank*. A més, pot realitzar tasques més avançades com ara processaments per lot, prevenció de frau, etc. No és gaire habitual sentir parlar d'ells, almenys a Espanya, ja que històricament els *acquiring banks* van haver d'implementar aquesta funció perquè al mercat no van sorgir organitzacions independents prou fortes per a realitzar aquesta labor i, en conseqüència, ells mateixos van implementar els mecanismes tècnics perquè els *merchants* poguessin emprar mecanismes d'autorització *online*. Als EUA sí que n'hi ha diversos que els *merchants* contracten directament, sobretot si són comerços que generaran moltes transaccions. En el passat, alguns van ser desgraciadament coneguts per haver sofert atacs de *hackers*. Actualment, a Espanya estan sorgint nous actors en aquest àmbit (Sagepay, Payvision, etc) al costat d'altres de tradicionals com Redsys (abans coneguda com SERMEPA, fusió de les àrees de processament de pagaments de Servired i 4B).

- *Card network*: cada tipus de targeta té una xarxa d'interconnexió per tal que, mitjançant el *payment processor*, es faci el procés d'autorització de l'operació.

A part d'aquests actors, que són els que intervenen en transaccions econòmiques amb targetes, qualsevol organització que finalment tracti una dada d'una targeta per prestar un servei també es veu afectada per la PCI-DSS. Per exemple, les empreses d'assistència que presten els seus serveis a un titular d'una targeta de crèdit poden veure's afectades per la PCI-DSS si en els seus processos operatius han de tractar la dada de la targeta de crèdit del client.

Totes aquestes entitats que finalment controlen les dades del *cardholder* hauran d'aplicar aquest estàndard en tots els elements dels seus sistemes TIC i processos operatius. Per *element del sistema* s'entén element de xarxa, servidors, aplicacions que estiguin incloses o connectades a un entorn de tractament de dades de targetes de crèdit. Mitjançant una segmentació de la xarxa adequada, les entitats podran limitar l'abast de la norma. Aquest entorn sobre el qual una organització ha d'aplicar la norma PCI-DSS és conegut com el CDE (*cardholder data environment*). A l'hora de realitzar una auditoria de compliment de PCI-DSS, l'auditor únicament ho farà sobre aquest abast, per la qual cosa és crític per a una organització afectada per la PCI-DSS el fet de conèixer molt bé els límits del seu CDE. Mitjançant aquesta correcta delimitació, aconseguirà optimitzar els controls que la norma l'obliga a implantar, els quals són molt exigents, i també a garantir que no existeixen fora d'aquest CDE punts en els

quals hi pugui haver tractaments de dades de targetes potencialment susceptibles de veure's afectats per un incident de seguretat degut en part a la incorrecta aplicació de la norma PCI-DSS.

3.4. Compliment i auditoria de l'estàndard PCI-DSS

Totes les parts que intervenen en les transaccions comercials amb targetes de crèdit han de complir la totalitat del PCI DSS. Però, a més d'adherir-s'hi (a la pràctica, aplicar tots els controls en tots els elements i processos dins del CDE), periòdicament han de fer unes auditories el tipus i la forma de presentació de les quals dependrà del seu nivell, i l'informe de les quals ha d'estar a disposició de les entitats emissores de les targetes i en certs casos en què el nivell és el més elevat fins i tot presentar-lo al PCI SS Council. D'aquesta manera, es demostrarà que es compleix l'estàndard[1]. El tipus d'auditoria que s'ha de fer depèn del nivell i de la seva classificació en *merchant* o "proveïdor de servei".

(1)Amb tot, aquest compliment no és cap garantia que no puguin succeir incidents greus. A manera d'exemple, recordem el cas protagonitzat per l'empresa Heartland Payemnt Services que, el gener de 2009, va cometre un error en què s'haurien pogut comprometre milions de dades de targetes de crèdit i que, per la seva condició de "PCI Compliant", va posar en dubte tot l'esquema d'auditories per mitjà de QSA ideat des del PCI SS Council.

Ja s'ha dit que el compliment amb la totalitat dels requisits de l'estàndard és obligatori, però hi ha un nivell d'exigència diferent quant als mecanismes per a acreditar el compliment, o per a afirmar que s'és "PCI Compliant". És a dir, tots els aspectes de la norma són de compliment obligat, amb independència de la grandària d'una organització. Només es poden excloure controls específics si, per la naturalesa de l'activitat que realitza l'organització, realment no són aplicables. Per exemple, si l'organització no desenvolupa programari, hi pot haver determinats controls que no li siguin aplicables o si realment mai no arriba a emmagatzemar dades de targetes en cap sistema d'informació. No obstant això, sí que hi ha una distinció en la manera en què les organitzacions han de mostrar a la indústria el seu nivell de compliment, especialment cap a les entitats emissores de targetes (VISA, American Express, Mastercard, etc.), que pot ser més o menys complex o exigent a l'hora de facilitar evidències i l'informe de comunicació de compliment. Cada marca determina el nivell de demostració del compliment segons paràmetres com el volum de transaccions i determinades circumstàncies (que comentarem a continuació), així com el rol que es té en la cadena d'operació de les dades de les targetes.

En el cas de VISA, les institucions financeres i comercials, denominades *merchants*, estan classificades d'aquesta manera:

Nivell	Descripció
1	Qualsevol *merchant* que compleixi algun dels aspectes següents: • Accepti més de 6.000.000 de transaccions anuals, independentment del canal pel qual arribin. • Hagi sofert un atac/intrusió en els seus sistemes que hagi comportat l'accés a dades d'algun compte. • Hagi determinat adherir-se a aquest nivell.
2	Qualsevol *merchant* que accepti entre 1.000.000 i 6.000.000 de transaccions anuals, independentment del canal pel qual arribin.
3	Qualsevol *merchant* que accepti entre 20.000 i 1.000.000 de transaccions anuals per canal de comerç electrònic.
4	Qualsevol *merchant* que accepti menys de 20.000 de transaccions anuals per canal de comerç electrònic, o menys d'1.000.000 de transaccions anuals, independentment del canal.

Els proveïdors de servei es classifiquen d'aquesta manera:

Nivell	Descripció
1	Tots els involucrats amb la xarxa d'intercanvi de dades financeres (com VisaNet) i totes les passarel·les de pagament.
2	Qualsevol proveïdor de servei que no sigui de nivell 1 i que emmagatzemi, processi o transmeti més d'1.000.000 de comptes o transaccions anuals.
3	Qualsevol proveïdor de servei que no sigui de nivell 1 i que emmagatzemi, processi o transmeti menys d'1.000.000 de comptes o transaccions anuals.

Passarel·les de pagament

Les passarel·les de pagament són entitats que participen en la transacció de pagament i faciliten al *merchant* un "accés" a un punt de la xarxa d'intercanvi de dades financeres perquè es processi la transacció, especialment en entorns de comerç electrònic.

D'acord amb aquesta classificació, s'exigeixen diferents períodes i tipus d'auditoria que s'han de dur a terme.

Nivell	Tipus d'auditoria
1	Auditoria completa anual feta per un assessor qualificat (QSA: *qualified security assessor*) pel PCS DSS Council. Escaneig de xarxa trimestral fet per un proveïdor de servei d'escaneig de xarxes qualificat (ASV: *approved scanning vendor*) pel **PCI SS Council**.
2 3 4	Auditoria completa anual feta internament. Escaneig de xarxa trimestral fet per un ASV qualificat (autoritzat) pel **PCI SS Council**.

Per als proveïdors de servei, la periodicitat i el tipus són:

Nivell	Tipus d'auditoria
1 2	Auditoria completa anual feta per un QSA qualificat (autoritzat) pel PCS-DSS Council. Escaneig de xarxa trimestral fet per un ASV qualificat (autoritzat) pel **PCI SS Council**.
3	Auditoria completa anual feta internament. Escaneig de xarxa trimestral fet per un ASV qualificat (autoritzat) pel **PCI SS Council**.

Com es pot observar, aquest és un sector altament organitzat i estandarditzat, perquè també s'ha estandarditzat el tipus d'auditoria que s'ha de dur a terme. En aquest sentit, el **PCI SS Council** ha desenvolupat una metodologia per a cadascuna d'aquestes auditories, i ha publicat les metodologies següents:

- **Procediments per a auditoria de compliment del PCI DSS**. Aquests procediments estan inclosos en la norma PCI-DSS des de la versió 2, on es facilita a l'equip auditor el conjunt d'eines per a fer l'auditoria:
  - Indicacions per a determinar l'abast: la norma dóna algunes indicacions sobre com delimitar el CDE, tot i que encara és un punt en el qual, en la pràctica, hi pot haver divergències d'interpretació entre auditors.
  - Per a tots i cadascun dels punts de la norma es facilita, juntament amb el seu enunciat, les indicacions per a l'auditor sobre la manera en què s'ha de realitzar la comprovació del compliment. Igualment, a les organitzacions se'ls faciliten indicacions o recomanacions sobre la manera en què han d'implementar cadascun dels detalls dels controls, de manera que estiguin alineats tant el control com la revisió que ha de realitzar l'auditor posteriorment.

  S'ha de tenir en compte que, en alguns casos, les proves proposades per la metodologia poden ser complexes de fer i no es resoldran en una simple entrevista o comprovació tècnica. En aquests casos, la perícia de l'equip auditor li servirà per a determinar quines proves addicionals s'han de dur a terme.
- **Procediments per a fer els escaneigs de xarxa exigits pel PCI DSS**. El PCI SS Council facilita a l'equip auditor les diferents fases que s'han de seguir en l'escaneig de xarxa exigit en els termes del PCI DSS; es tracta, en realitat, d'una anàlisi de vulnerabilitats dels sistemes exposats a Internet de l'organització.

  El document no inclou el detall tècnic, i sí que estableix que tots els tipus de sistemes que s'exigeixen siguin escanejats. Per tant, només pot ser pres com la referència dels punts que s'han d'analitzar. L'equip auditor haurà de tenir el coneixement tècnic necessari per a fer l'escaneig.

- **Qüestionari per a l'autoavaluació del compliment del PCI DSS**. Aquest document té un àmbit d'aplicació menor per a l'equip auditor, ja que es tracta d'una guia perquè els *merchant* o proveïdors de serveis facin ells mateixos l'auditoria. Per tant, és més senzill que els procediments d'auditoria de compliment del PCI DSS complet. També és interessant destacar que el

PCI SS Council ha previst quatre nivells diferents de qüestionari, segons certes característiques del comerciant, per la qual cosa s'haurà d'analitzar en cada cas quin és el que aplica.

- **Document d'ajuda a la implantació prioritzada i progressiva del PCI DSS**. El PCI DSS ha preparat una guia per a ajudar als implantadors de l'estàndard. Aquesta guia organitza els diferents requisits de l'estàndard en quatre nivells o fites. D'aquesta manera, es poden planificar de manera progressiva i prioritzada, d'una manera coherent amb el PCI SS Council, els diferents requisits i per tant les accions que s'han de dur a terme. En tot cas, això no implica que s'hagin de complir tots els requisits.
  L'equip auditor ha de fer servir aquestes metodologies i aquests materials en cas d'una assignació relacionada amb la conformitat d'una entitat contra la PCI DSS i, en altres casos, els pot prendre com a referència per a preparar el seu propi pla d'auditoria.

4. Estàndards d'auditoria de la ISACA

La **Information Systems Audit and Control Association (ISACA)**, iniciada el 1967, és actualment una de les associacions més reconegudes mundialment com a font d'informació, estudi i desenvolupament en matèria d'auditoria de sistemes d'informació, de govern de les tecnologies de la informació, i és l'emissora de dues de les certificacions professionals més reconegudes internacionalment: el Certified Information Systems Auditor (CISA®) i el Certified Information Security Manager (CISM®).

El govern de TI, que s'ha introduït en el mòdul 1 d'aquest curs, s'ha d'entendre com el conjunt de tècniques, processos i estructures corporatius incorporats a la cultura corporativa, i integrats amb la resta de pràctiques de govern corporatiu, que tenen com a objectiu assegurar que les tecnologies de la informació proporcionen adequadament suport als objectius de negoci, maximitzen les inversions en TI i gestionen els riscos i les oportunitats que aquestes noves tecnologies presenten per al negoci.

4.1. COBIT

El concepte de *govern de les tecnologies de la informació* (*information technologies governance*) és central en la filosofia de la ISACA, fins al punt que, el 1998, va decidir promoure la creació de l'**IT Governance Institute (ITGI)** per a centrar les seves activitats en aquesta àrea. Actualment, l'ITGI és el responsable del manteniment i la promoció de l'estàndard COBIT, i constitueix una referència en matèria de govern de TI. La ISACA està més centrada en la gestió dels aspectes relacionats amb l'auditoria i el control dels sistemes d'informació.

Des del punt de vista de la ISACA, el bon govern de les tecnologies de la informació (TI) es basa en cinc àrees clau:

- **Alineació estratègica**. S'ha de garantir el vincle entre els plans de negoci i de TI; definir, mantenir i validar la proposta de valor de TI, i alinear les operacions de TI amb les operacions de l'empresa.

- **Lliurament de valor**. Les TI han d'aportar valor al llarg del seu cicle de vida, i s'ha d'assegurar que generin els beneficis promesos en l'estratègia global de l'organització, concentrant-se a optimitzar els costos i a oferir el valor intrínsec de les TIC.

- **Administració de recursos**. La gestió de les TI ha de ser correcta, de manera que la inversió sigui òptima, i també l'administració adequada dels recursos crítics de TI: aplicacions, informació, infraestructura i persones.

Els temes clau es refereixen a l'optimització del coneixement i de la infraestructura.

- **Administració de riscos**. La gestió de les TI i les decisions d'inversió requereixen la presa de consciència dels riscos per part dels alts executius de l'empresa, un clar enteniment del desig de risc que té l'empresa, la comprensió dels requisits de compliment, la transparència dels riscos significatius per a l'empresa, i la inclusió de les responsabilitats d'administració de riscos dins de l'organització.

- **Mesurament de l'acompliment**. És necessari rastrejar i monitorar l'estratègia d'implementació, la terminació del projecte, l'ús dels recursos, l'acompliment dels processos i el lliurament del servei, amb l'ús, per exemple, de quadres de comandament (*balanced scorecards*).

L'estàndard COBIT[2] ajuda a aconseguir aquests objectius, mitjançant un marc de referència que proporciona a la gerència de TI els aspectes següents:

(2)A data de realització d'aquest material, l'última versió de COBIT era la 5.

- Estableix un enllaç mesurable entre els requisits de negoci de l'organització i els objectius de la gestió de TI, i manté sota control els riscos inherents a l'ús de les TI.

- Organitza la majoria de les activitats de les TI en un model de referència reconegut de manera general i mantingut per una organització de prestigi reconegut.

- Defineix els objectius de control de la gestió de TI que s'han de tenir en consideració.

- Facilita eines per a:
  - Establir objectius i calcular mètriques per a poder mesurar l'eficàcia i l'eficiència de les TI.
  - Modelar l'organització de la gestió de TI d'acord amb un model de maduresa que permeti comparar l'organització amb altres del seu entorn.
  - Aclarir els diferents rols i responsabilitats en la gestió de TI.

L'estàndard organitza els processos de govern de TI i els de gestió de TI (*IT management*), com un dels aspectes integrats en el mateix marc de definició. Es diferencia de la governança de la gestió en el fet que en el primer es tenen en compte les necessitats de negoci, s'avaluen els riscos i es monitoriza l'acompliment, mentre que la segona dissenya, construeix i opera conformement als principis de la governança.

Els grans processos que defineix el COBIT (en la seva última versió 5) són:

a) Processos de govern TI per a avaluar, orientar i supervisar

- EDM01 - Assegurar l'establiment del marc de govern,
- EDM02 - Assegurar el lliurament de beneficis,
- EDM03 - Assegurar l'optimització del risc,
- EDM04 - Assegurar l'optimització dels recursos,
- EDM05 - Assegurar la transparència cap a les parts interessades;

b) Processos de gestió TI que estan agrupats en diferents grups de processos

- APO - Alinear, planificar i organitzar:
  - APO01 Gestionar el marc de gestió de TI,
  - APO02 Gestionar l'estratègia,
  - APO03 Gestionar l'arquitectura empresarial,
  - APO04 Gestionar la innovació,
  - APO05 Gestionar el dossier,
  - APO06 Gestionar el pressupost i els costos,
  - APO07 Gestionar els recursos humans,
  - APO08 Gestionar les relacions,
  - APO09 Gestionar els acords de servei,
  - APO10 Gestionar els proveïdors,
  - APO11 Gestionar la qualitat,
  - APO12 Gestionar el risc,
  - APO13 Gestionar la seguretat;

- BAI - Construir, adquirir i implantar
  - BAI01 Gestionar els programes i projectes,
  - BAI02 Gestionar la definició de requisits,
  - BAI03 Gestionar la identificació i la construcció de solucions,
  - BAI04 Gestionar la disponibilitat i la capacitat,
  - BAI05 Gestionar la introducció de canvis organitzatius,
  - BAI06 Gestionar els canvis,
  - BAI07 Gestionar l'acceptació del canvi i de la transició,
  - BAI08 Gestionar el coneixement,
  - BAI09 Gestionar els actius,
  - BAI010 Gestionar la configuració;

- DSS - Lliurar, donar servei i suport
  - DSS01 Gestionar les operacions,
  - DSS02 Gestionar les peticions i els incidents del servei,
  - DSS03 Gestionar els problemes,
  - DSS04 Gestionar la continuïtat,
  - DSS05 Gestionar els serveis de seguretat,
  - DSS06 Gestionar els controls dels processos del negoci;

- MEA - Supervisar, avaluar i valorar
  - MEA01 Supervisar, avaluar i valorar el rendiment i la conformitat,

- MEA02 Supervisar, avaluar i valorar el sistema de control intern,
- MEA03 Supervisar, avaluar i valorar la conformitat amb els requeriments externs.

Dins de cadascuna d'aquestes àrees, es detallen els processos que constitueixen els mecanismes que proporcionen el control sobre el govern de TI. Posteriorment, cadascun dels processos es descompon en un cert nombre d'objectius de control. Dins dels aspectes que donen suport al govern de TI, hi ha la seguretat de la informació; per aquesta raó, COBIT es considera un marc de referència també per a la gestió de la seguretat de la informació. A més, com es pot observar, la seva manera d'organitzar el catàleg de controls és similar al proporcionat per l'ISO/IEC 27002:2005, i hi ha diferents treballs (de la mateixa ISACA) que fan un mapatge dels controls de la Norma ISO contra els controls de COBIT.

Dins de cadascuna d'aquestes àrees, es defineixen un conjunt de controls de seguretat que conformen el catàleg COBIT de controls de seguretat. Els controls COBIT estan organitzats d'acord amb els diferents processos de TI anteriorment descrits; cadascun afecta tant algun dels criteris d'informació com algun dels recursos de TI. La informació que es facilita en cadascun és molt completa (comparada amb les guies per a la implementació que es proporcionen en l'estàndard ISO/IEC 27002) i inclou matrius RACI[3] per a distribuir responsabilitats entre diferents actors típics en una organització, ajudes per a establir mètriques, i un esquema per a mesurar el grau de maduresa de la implantació del control basat en cinc nivells:

(3)Matrius per a l'assignació de responsabilitats R-*responsible*, A-*accountable*, C-*consulted*, I-*informed*.

- 0 – No existeix
- 1 – Inicial/*ad hoc*
- 2 – Repetible però intuïtiu
- 3 – Procés definit
- 4 – Administrable i mesurable
- 5 – Optimitzat

Nota

Aquest esquema està molt alineat amb el model CMMI (*capability maturity model integration*) del Software Engineering Institute (SEI) de la Universitat Carnegie-Mellon, per a la millora dels processos.

4.2. Reglamentació de l'activitat d'auditoria de TI per part d'ISACA

En l'àmbit de l'auditoria, una de les iniciatives més interessant d'ISACA, i en relació amb l'auditoria dels controls COBIT i l'auditoria en general dels sistemes d'informació, és la publicació de documents de referència sobre auditoria i control. Entre aquests, hi destaquen els estàndards, les guies i els procediments per a l'auditoria dels sistemes d'informació. La ISACA ha creat un marc de pràctiques professionals per a l'auditoria i verificació de sistemes TIC, al qual denomina *ITAF -IT Assurance Framework-*, que divideix el seu marc per a estandarditzar les auditories en tres nivells: estàndards, guies o directrius d'auditoria TI en general, i també més específiques per a l'auditoria dels controls de COBIT, i procediments.

4.2.1. Estàndards d'auditoria de la ISACA

Aquestes normes defineixen els requisits obligatoris per a la realització d'una auditoria i l'elaboració d'informes d'auditoria. Les normes són aplicables a auditors certificats per la ISACA (CISA). El seu propòsit fonamental és donar les pautes que l'auditor ha de seguir, des d'un punt de vista del comportament i l'actitud davant el seu treball, encara que també algunes de les normes corresponen a aspectes més específics del desenvolupament de l'auditoria. Addicionalment, n'hi ha dues més, però no són rellevants quant a definir els patrons; per això, el treball de l'auditor s'ha de guiar. Les normes establertes per la ISACA per al treball de l'auditor de TI són, en línies generals, les següents:

Enllaç recomanat

ISACA manté al dia aquests estàndards i es poden trobar en: http://www.isaca.org/knowledge-center/itaf-is-assurance-audit-/is-audit-and-assurance/pages/it-audit-and-assurance-guidelines-spanish.aspx

a) Sèrie 1000 - Normes generals. Són principis generals sobre els quals un auditor ha de guiar el seu comportament:

- 1001 Estatut de la funció d'auditoria. La direcció de l'organització auditada ha de documentar i aprovar un "estatut d'auditoria" o "carta de compromís" que reflecteixi el propòsit i l'abast de l'auditoria i la relació entre auditor i auditat a l'hora de presentar resultats.

- 1002 Independència organitzativa. L'equip auditor ha de ser totalment independent de l'estructura organitzativa respecte de l'àrea o activitat que s'està auditant.

- 1003 Independència professional. L'equip auditor ha de tenir total independència professional respecte de l'àrea o activitat que s'està auditant.

- 1004 Expectativa raonable. En afrontar una assignació, l'auditor ha de ser prou crític per a determinar si les circumstàncies fan raonable la consecució dels objectius.

- 1005 Cura professional deguda. L'auditor de SI ha de complir amb el codi d'ètica professional de l'ISACA, els seus estàndards d'auditoria i qualsevol altre estàndard professional aplicable en realitzar tasques d'auditoria.

- 1006 Competència. L'equip auditor ha d'estar format per membres que tinguin l'adequada capacitació professional per realitzar l'auditoria i, igualment, mantenir al dia els seus coneixements professionals.

- 1007 Afirmacions. L'auditor ha de revisar les afirmacions amb les quals el tema serà avaluat per a determinar que aquestes siguin auditables, suficients, vàlides i rellevants.

- 1008 Criteris. Els criteris d'auditoria que esculli l'auditor, amb els quals serà avaluat el tema, han de tenir un origen confiable (per exemple, estàndards o bones pràctiques de la indústria), ser objectius, complets, rellevants, me-

surables, comprensibles, autoritzats i compresos o disponibles pels destinataris de la comunicació.

b) Sèrie 1200 - Normes sobre execució. Es refereixen en concret a l'execució (planificació, definició d'abastos, supervisió, riscos, etc.)

- 1201 Planificació de l'assignació. L'equip auditor ha de planificar i reflectir adequadament en un document, pla o programa, el desenvolupament de l'auditoria, de manera que es compleixi amb els objectius previstos i amb les lleis i normes professionals d'auditoria que li siguin aplicables (entre elles, aquestes mateixes). Aquest document estarà basat en una anàlisi de riscos que minimitzi el risc que l'auditoria obtingui uns resultats erronis.

- 1202 Avaluació de risc en planificació. En una planificació general o estratègica de les activitats d'auditoria d'una organització, s'han d'emprar tècniques d'anàlisi de riscos per a la planificació tàctica de les auditories i, d'aquesta manera, gestionar més eficientment els recursos d'auditoria.

- 1203 Acompliment i supervisió. L'execució de l'auditoria es farà seguint un pla d'auditoria, de manera supervisada i documentada, a partir de l'obtenció d'evidències que donin suport a les conclusions d'auditoria.

- 1204 Materialitat. La materialitat o importància relativa en les auditories pot ser considerada como la magnitud d'un error en la informació obtinguda durant una auditoria, que podria portar l'auditor a prendre una decisió basant-se en aquesta informació. Per tant, està relacionada amb el risc d'auditoria. A major nivell de materialitat, menor serà el risc d'auditoria. L'auditor tindrà en compte aquest aspecte a l'hora de planificar els recursos, el temps i els tipus de procediments d'auditoria aplicats. Això implica també que l'auditor ha de deduir els riscos que es derivin de la falta de controls o errors en la seva implementació, considerant aquest concepte de materialitat i si són suficients les evidències obtingudes.

- 1205 Evidència. Les conclusions de l'auditor han d'estar basades en les evidències d'auditoria, recollides en la seva assignació, que siguin suficients, apropiades i de confiança.

- 1206 Ús del treball d'altres experts. L'auditor podrà emprar el treball d'altres equips auditors, sempre que tingui la certesa del seu nivell de professionalitat i coneixements, i haurà de recórrer a realitzar proves addicionals quan les evidències aportades per altres equips auditors no siguin suficients.

- 1207 Irregularitats i actes il·legals. L'equip auditor ha de ser conscient que hi ha un cert nivell de risc d'irregularitats i accions fraudulentes en l'àrea a auditar (especialment, si és una àrea amb impacte financer) durant i fins i tot després d'haver realitzat el seu treball. Per això, quan realitzi la seva

auditoria, ha de parar gran atenció a detectar situacions que poguessin manifestar o conduir a alguna situació irregular o fraudulenta, i sempre basar-se en evidències d'auditoria suficients. Finalment, si es detecta una situació fraudulenta o il·legal, s'haurà de comunicar sense demora al nivell de gerència adequat. Aquesta norma reflecteix la gran relació que l'ISACA té amb altres organitzacions d'auditoria, especialment amb l'auditoria de comptes.

c) Sèrie 1400 - Normes sobre la comunicació. Fan referència als tipus de comunicació, les vies i el contingut de la informació a comunicar:

- 1401 Comunicacions. En finalitzar l'auditoria, l'equip auditor haurà de subministrar un informe d'auditoria signat que tracti els següents aspectes:
  - destinataris de l'informe,
  - nivell de restriccions aplicables al document (el seu nivell de classificació: secret, confidencial, ús restringit, etc.),
  - el període de cobertura de les seves conclusions,
  - la identificació de l'abast (organització, objectius, naturalesa, dates i extensió de les proves realitzades),
  - les troballes, conclusions i recomanacions, que hauran d'estar degudament recolzades per evidències suficients.
- 1402 Activitats de seguiment. L'equip auditor haurà d'informar-se de com l'organització ha decidit tractar les conclusions emeses en l'informe, i si les decisions són les oportunes o no.

Els auditors, especialment si es tracta d'auditors certificats per la ISACA (és a dir, els CISA®), han de prendre aquestes normes com les regles sobre les quals construir els seus propis plans d'auditoria, les seves pròpies metodologies a l'hora d'executar-les, i el seu codi de conducta i professionalitat. Com que es tracta d'una norma, no explica explícitament el com, sinó que simplement ens diu què ha de constituir l'auditoria. Per a ajudar els auditors a poder complir l'estàndard ISACA d'auditoria, l'associació ha desenvolupat unes guies de directrius d'auditoria.

4.2.2. Les guies o directrius d'auditoria

Com a directrius d'auditoria, es poden destacar dos tipus de directrius que la ISACA ha publicat. Es tracta de les directrius d'auditoria per al compliment de la Norma d'auditoria ISACA, a l'hora de fer tasques d'auditoria en diferents àmbits relacionats amb la seguretat i la gestió de TI en general, i després per a comprovar la implantació dels controls COBIT.

Directrius per a l'auditoria de TI

Les **directrius d'auditoria de TI per al compliment de l'estàndard ISACA** faciliten a l'equip auditor una guia per a poder aplicar els estàndards d'auditoria. Per tant, han de ser aplicats segons el parer de l'auditor; en cas que no s'hi apliqui alguna de les directrius, l'equip auditor ha de conèixer la raó que ho motiva, sense que això impliqui que no s'hagi de complir l'estàndard d'auditoria. L'estàndard és de compliment obligat per als auditors CISA®. De la mateixa manera que els estàndards d'auditoria es dirigeixen tant a aspectes relacionats amb l'actitud de l'auditor davant la seva feina com a aspectes del desenvolupament d'una auditoria, les guies i les directrius també tracten de manera diferenciada aquests aspectes.

Addicionalment, com que tenen com a objectiu proporcionar més detalls sobre l'aplicació de l'estàndard ISACA d'auditoria, donen certs detalls sobre l'auditoria d'algunes de les tecnologies de la informació més rellevants en l'entorn corporatiu actual.

Directrius d'auditoria de COBIT

D'altra banda, s'han de destacar les **directrius d'auditoria de COBIT**, o com s'indica en l'última versió disponible únicament en anglès, "**IT Assurance Guide – Using COBIT**".

Aquestes directrius d'auditoria contenen una descripció del marc referencial COBIT i un conjunt de directrius per a comprovar la implantació dels diferents controls de seguretat COBIT. Aquestes directrius es van actualitzant en la mesura que l'estàndard COBIT evoluciona.

Les directrius d'auditoria d'ISACA proporcionen guies per a preparar plans d'auditoria que s'integren en el marc referencial de COBIT i en els objectius de control detallats del COBIT. S'han d'usar juntament amb aquests dos últims, i a partir d'aquí es poden desenvolupar programes específics d'auditoria. No obstant això, les directrius no són exhaustives ni definitives; no ho poden incloure tot ni es poden aplicar a tot; així, doncs, s'han d'ajustar a les condicions específiques.

La ISACA entén l'auditoria com el procés pel qual comprova el control de la gerència sobre les TI amb els objectius següents:

- Proporcionar a la direcció de l'auditat, amb un assegurament raonable, que s'estan cobrint els objectius de control.
- On hi hagi debilitats de control significatives, justificar els riscos resultants.
- Aconsellar la direcció de l'auditat sobre accions correctores necessàries.

En aquest sentit, per a ISACA el procés d'auditoria de TI s'organitza generalment en les fases següents:

- Entendre els riscos relacionats amb els requisits del negoci i les mesures rellevants de control, mitjançant la identificació de processos de TI i la seva documentació.

- Avaluació de la pertinència dels controls establerts.

- Aplicar proves de compliment del control, per a saber si estan establerts i funcionen com s'espera, de manera consistent i contínua.

- Aplicar proves de comprovació de l'eficàcia del control, ja que hi ha el risc que els objectius de control no s'estiguin complint.

Com es pot observar, la planificació s'ajusta a la mostrada en aquest document.

Les directrius d'auditoria de COBIT faciliten a l'auditor una guia per a comparar la manera com l'organització fa els processos específics de TI amb els objectius de control de COBIT recomanats per a ajudar l'auditat a identificar en quins casos els controls són suficients, o per a assessorar-los respecte als processos que requereixen ser millorats.

No obstant això, hi ha quatre coses que les directrius no són:

- Les directrius d'auditoria no pretenen ser una eina per a crear el pla global d'auditoria que consideraria una àmplia gamma de factors, incloent-hi debilitats anteriors, riscos de l'organització, incidents coneguts, nous esdeveniments i selecció d'estratègies. Tot i que el marc referencial i els objectius de control ofereixen algunes orientacions i són força detallades, l'abast de les directrius no inclouen una guia precisa per a activitats específiques.

- Les directrius d'auditoria no estan dissenyades com a instrument per a ensenyar les bases de l'auditoria, tot i que incorporin els elements normalment acceptats de l'auditoria general i de TI.

- Les directrius d'auditoria no pretenen explicar detalladament la manera com es poden utilitzar les eines tècniques per a fonamentar i automatitzar els processos d'auditoria de TI, en matèria de planejament, avaluació, anàlisi i documentació (que estan incloses, però no es limiten a aquestes, en les tècniques d'auditoria assistides per ordinador). Hi ha un enorme potencial per a usar la tecnologia d'informació dirigida a augmentar l'eficiència i l'efectivitat de les auditories, però una orientació en aquest sentit tampoc no és dins de l'abast de les directrius.

- Les directrius d'auditoria no són exhaustives ni definitives, però es desenvolupen juntament amb COBIT i els seus objectius de control detallats.

Les directrius d'auditoria estan organitzades com a objectiu de control d'alt nivell de COBIT. Per a cadascun d'aquests objectius de control, les directrius faciliten a l'auditor la informació següent:

- Els interlocutors més adequats i la relació de documentació rellevant habitualment existent en les organitzacions per a poder entendre millor la situació.

- Les comprovacions i els aspectes que s'han de revisar per a avaluar la idoneïtat i la suficiència dels controls implantats.