Auditoria tècnica de seguretat de sistemes d'informació i comunicacions

PID_00239292

Rafael Estevan de Quesada

Temps mínim de dedicació recomanat: 4 hores

Universitat Oberta de Catalunya

Índex

Introducció

Ja hem comentat en el mòdul 1, d'introducció a l'auditoria de sistemes d'informació, que el procés d'auditoria, de manera general, és l'aplicació d'una revisió sistemàtica del compliment d'uns criteris d'auditoria. També hem vist que la tendència actual en la gestió més eficient i alineada amb el negoci (govern TIC) és incloure les activitats d'auditoria.

Auditories tècniques de seguretat davant auditories de certificació

En el mòdul 2 hem tractat l'aspecte més formal de les auditories que prenen la forma d'auditories de tercera part o de certificació. Les auditories de certificació són processos molt formals i compleixen un objectiu molt particular: es desitja que una entitat externa a l'auditat que, *a priori* no està determinada, pugui disposar de l'opinió d'un tercer sobre la manera com es gestiona la seguretat de la informació prenent com a referència un marc regulat i reconegut. No obstant això, per la seva necessitat d'estar molt formalitzada i regularitzada, no és aplicable quan es busquen uns objectius d'auditoria molt més concrets i profunds que simplement declarar si la manera com es gestiona la seguretat de la informació s'ajusta a un estàndard determinat. Aquesta visió pot ser suficient si ens plantegem una auditoria de tercera part, però quan es tracta d'auditories de primera o segona part, el client de l'auditoria necessita una resposta més concreta a preguntes més específiques, ja que vol tenir una visió detallada sobre la manera com s'està fent un aspecte concret de la gestió de la seguretat de la informació.

Per tant, en aquest context els sistemes per a la gestió de la seguretat estan sotmesos a un tipus d'auditoria més específica que la de certificació. En aquest tipus d'auditoria, que nosaltres denominarem *auditories tècniques de seguretat* –encara que també podríem anomenar-les més senzillament *auditories de sistemes d'informació*–, s'avaluaran controls específics contra uns criteris d'auditoria més precisos:

- Les polítiques pròpies de l'entitat auditada que descriguin el control.
- Els catàlegs de controls àmpliament reconeguts en l'ambient en què es trobi l'entitat.
- Les tècniques (organitzatives i també tecnològiques) més actuals per a la implementació de cada tipus concret de control.

Per tant, quan ens referim a una auditoria tècnica de seguretat, estarem parlant d'un procés sistemàtic, i tècnicament mesurable, de com una determinada política de seguretat d'una organització és aplicada en un àmbit concret, i els problemes que hi pot haver en la implementació dels controls.

Auditories tècniques de seguretat i sistemes de gestió de la seguretat de la informació

Les polítiques de seguretat d'una organització en què hi hagi un sistema de gestió de la seguretat madur haurien de constituir la pedra angular sobre la qual fer les auditories tècniques de seguretat.

Aquests documents s'han de tractar com a documents vius i han de reflectir, amb molta precisió, com l'organització protegeix els seus actius d'informació mitjançant la implantació de mecanismes (processos organitzatius i també tecnologia en què es basen) que s'han d'engegar. No obstant això, l'entorn i les necessitats de l'organització són canviants i, per tant, també la manera com es tracta la informació; així, doncs, les polítiques de seguretat s'han d'adaptar a aquests canvis.

Com a conclusió d'un procés d'auditoria, es donaran indicacions i recomanacions no solament del nivell d'alineament de les pràctiques amb les polítiques, sinó que també podran concloure sobre la correcció d'aquestes polítiques i la manera en què aquestes estan implementades tècnicament, procedimentalment o organitzativament.

En aquest sentit, cal destacar que aquest tipus d'auditories formen part integrant del cicle de gestió de la seguretat de la informació. La integració de les auditories en l'SGSI és òbvia participant en la fase de verificar (*check*) del model PDCA (vegeu el mòdul 2, en què es descriuen les característiques d'un SGSI segons la Norma ISO/IEC 27001) i no com un simple exercici arbitrari o acadèmic d'una organització. Involucra tot el personal que utlitzi un recurs dels sistemes d'informació de l'organització. El seu resultat resultarà d'interès no solament a la direcció de sistemes d'informació per a conèixer i mesurar, objectivament, el nivell de seguretat aconseguit, sinó també a la direcció de la part usuària dels sistemes, ja que li donarà una imatge del grau de confiabilitat que se'ls pot atorgar.

Nota

Des de 2013, l'ISO va eliminar de la norma ISO/IEC 27001 la referència explícita al model PDCA pel model de referència de millora contínua que ha de seguir tot SGSI certificat segons aquesta norma, però en la resta del curs ho continuarem emprant perquè és senzill, àmpliament conegut i explicat, i perquè és vàlid a l'hora d'implementar un SGSI conforme a la norma.

D'altra banda, tal com s'ha indicat, l'auditoria tècnica de seguretat és essencialment un examen de com d'eficientment s'ha implantat la política de seguretat d'una organització. Per descomptat, això pressuposa l'existència prèvia d'aquest tipus de polítiques. Aquests documents pretenen estandarditzar en l'organització les pràctiques de seguretat, i descriure els controls de seguretat que s'han d'implantar per a assegurar que, en tots els nivells de l'organització,

s'entengui com s'han de protegir els actius d'informació. No obstant això, en les organitzacions actuals és habitual la inexistència de documents que descriguin els controls de seguretat implantats.

Quan els controls de seguretat no estan descrits, o s'han implantat de manera informal i no planificada (per exemple, perquè no estan emmarcats en un sistema de gestió de la seguretat de la informació), pot ser que s'hi estiguin aplicant controls de manera incorrecta tant per l'abast com per la manera d'implantarlos. En aquests casos, una auditoria tècnica de seguretat també és apropiada, atès que permet comprovar la manera com estan implantats els controls; el resultat es pot emprar per a la planificació de subsegüents accions orientades a la implantació, en l'organització, d'un sistema de gestió de la seguretat. Per tant, és habitual que les auditories de seguretat formin part del procés d'anàlisi de riscos que se sol desenvolupar en la fase de planificar (*plan*) del model PDCA.

Establerts els objectius d'una auditoria tècnica de seguretat, és habitual que l'equip auditor treballi amb un gran coneixement dels actius i les infraestructures que s'han d'auditar, encara que no és completament necessari, com veurem més endavant. Segons l'objectiu concret que persegueixi una auditoria tècnica, l'equip auditor tindrà més o menys coneixement previ de l'entorn auditat. El procés d'auditoria de seguretat inclourà tasques com entrevistes amb el personal d'operació i manteniment d'aplicacions i sistemes; anàlisis de vulnerabilitats de xarxes, sistemes i aplicacions; comprovacions detallades de la parametrització de sistemes; etc.

1. Factors d'èxit d'una auditoria tècnica

Tota auditoria tindrà un client d'auditoria amb qui l'equip auditor n'haurà de pactar els objectius. Aquests objectius seran contra els quals s'avaluarà el resultat de l'auditoria per a determinar-ne l'èxit o fracàs. Per tant, l'èxit d'una auditoria dependrà, en gran manera, de la impressió general que tingui l'auditat dels resultats obtinguts. Entre els diferents factors d'èxit d'una auditoria, podem trobar:

- **Determinació correcta de l'abast de l'auditoria**. Aquest és el punt crític que determina l'èxit o el fracàs d'una auditoria. De fet, acostuma a ser el problema més gran amb el qual es trobarà l'equip auditor durant l'execució de l'auditoria. Com en qualsevol altre tipus de projecte, l'abast determina l'esforç, els recursos tècnics, logístics i humans necessaris, i les fases o tasques que s'han de dur a terme per a executar l'auditoria. Un abast mal definit, o en canvi, constant i no gestionat, pot fer fracassar l'auditoria i que els resultats que s'obtinguin no compleixin els objectius esperats pel client. L'existència d'aquest risc no implica que l'abast no evolucioni al llarg del desenvolupament de l'auditoria. Al contrari: és habitual que es vagi ajustant segons la progressió de l'auditoria. Certes constatacions, o la falta d'aquestes, poden redirigir l'auditoria cap a un altra banda. El risc es materialitza, realment, quan la modificació no està gestionada o es fa de manera incorrecta. Més endavant, en aquest mateix mòdul, aprofundirem en la determinació de l'abast de l'auditoria.

- **Planificació correcta de l'esforç i els recursos destinats**. Com en qualsevol altre tipus de projecte, és essencial una planificació correcta de les tasques que s'han de dur a terme i de l'ús dels recursos, tant humans com materials si són necessaris. Aquest aspecte incidirà més en l'èxit econòmic de l'auditoria, i no tan determinantment en el seu èxit tècnic.

- **Selecció correcta de l'equip auditor**. És important que l'equip auditor estigui compost per membres que disposin de prou perícia o habilitat tècnica en les àrees que siguin d'interès per l'abast que s'hagi determinat, o bé que es pugui disposar de les persones amb el perfil adequat en les fases del projecte que correspongui.

La composició de l'equip d'auditoria seria similar a la determinada anteriorment en el mòdul 1. Mentre que per a la composició d'un equip auditor en una auditoria de certificació sí que hi ha requisits, no hi ha requisits específics per a compondre un equip per a una auditoria tècnica. En tot cas, sí que podem afirmar que l'equip ha de combinar capacitats suficients. És recomanable

que hi hagi algun component de l'equip que tingui coneixements sobre els processos d'auditoria (a l'estil que s'exigeix en la Norma ISO 19011) i, a més, que hi hagi tants experts tècnics com aspectes diferents quedin sota l'abast.

D'altra banda, els requisits poden haver estat imposats pel client de l'auditoria. Encara que no hi hagi requisits per a la composició d'aquest equip, el client d'auditoria podria exigir alguna formació o experiència determinada per a alguns components de l'equip. Cal destacar que, en l'actualitat, en el mercat de l'auditoria de seguretat se solen exigir les certificacions de la ISACA[1] (CISA: *certified information systems auditor*) i de (ISC[2])2 (CISSP: *certified information systems security professional*) per a perfils més versàtils; quan es requereixen coneixements més específics, es recorre a certificacions sobre seguretat emeses per fabricants, per exemple: *Check Point Certified Security Expert* (CCSE), *Red Hat Certified Security Specialist* (RHCSS), del SANS *Institute*[3] GIAC *Systems and Network Auditor* (GSNA), *Cisco Certified Security Professional* (CCSP), *Microsoft Certified Systems Engineer* (MCSE), etc.

(1)Information Systems Audit and Control Association, www.isaca.org

(2)International Information Systems Security Certification Consortium

(3)El programa "Global Information Assurance Certification", www.giac.org

- **Col·laboració amb l'auditat**. És necessària la col·laboració de l'auditat tant abans d'afrontar l'auditoria com mentre s'executa.
  - Col·laboració abans de fer l'auditoria. Abans d'executar l'auditoria és necessària la complicitat amb l'auditat per a poder arribar a un acord quant a què s'espera de l'auditoria. Aquest punt està íntimament relacionat amb el primer factor d'èxit que hem explicat. Moltes auditories fetes fracassen en el moment de presentar resultats a la direcció que "va patrocinar" o va iniciar el projecte. La direcció no esperava el resultat que es va obtenir, no perquè fos tècnicament incorrecte o contrari a la realitat de l'organització, sinó simplement, o bé perquè el treball fet no es corresponia amb la idea que havia pensat, o bé perquè les conclusions obtingudes no li resultaven rellevants o suficients per a prendre les decisions adequades.

  - Col·laboració durant l'auditoria. De la mateixa manera, també és necessari comptar amb la col·laboració de l'auditat durant l'execució de l'auditoria. Moltes vegades les auditories són percebudes negativament pel personal de l'auditat. Segons el tipus d'auditoria que s'estigui fent, aquesta percepció negativa de l'auditoria provocarà una falta de col·laboració amb l'equip auditor i amb tota probabilitat comportarà la necessitat d'un esforç més gran per a l'execució de les diferents fases de l'auditoria.

Vegeu també

La composició de l'equip serà la determinada en el mòdul 2.

Auditories basades en entrevistes

La col·laboració durant l'auditoria és especialment important quan gran part de les activitats de l'auditoria es basen en entrevistes. Si l'entrevistat no facilita la informació demanada, o bé dóna respostes que no són confiables, seran necessàries més entrevistes amb un altre personal similar en funcions per a contrastar versions. Igualment, de vegades és necessària la col·laboració de l'auditat per a conèixer l'entorn o les infraestructures auditades. En cas que no es tingui aquesta col·laboració, l'equip auditor necessitarà dedicar

part dels seus esforços a adquirir un coneixement sobre l'entorn que el mateix auditat podria facilitar.

Per tant, per a estar en disposició de fer una auditoria amb prou garanties d'èxit, l'auditor en cap (o el cap del projecte) haurà d'avaluar correctament cadascun d'aquests factors abans d'afrontar fases més específiques de l'auditoria. Aquesta avaluació es pot considerar una anàlisi de riscos del projecte. El cap de projecte haurà d'identificar totes les possibles amenaces al seu projecte, establir la probabilitat que s'esdevinguin, determinar quin seria l'impacte i els possibles controls de seguretat que podria emprar l'equip auditor. D'aquesta manera s'haurà de fer una idea clara de tots els factors que poden incidir en el desenvolupament correcte del seu projecte i ha de tenir previst plans per a afrontar les contingències que prevegi.

2. Abast de l'auditoria tècnica

Per a garantir que una auditoria de seguretat sigui reeixida, abans de res se n'ha de determinar i consensuar l'abast amb el client; és necessari que sigui establert abans d'afrontar qualsevol altra activitat de l'auditoria.

De manera general, en qualsevol projecte, per a poder estimar els mitjans necessaris i el nivell d'esforç requerit per l'equip auditor i per l'auditat, és essencial determinar de manera detallada i realista l'abast del treball que s'ha de dur a terme. En l'àmbit de l'auditoria de seguretat, la determinació de l'abast també és essencial, ja que mostrarà la satisfacció de l'auditat i de l'equip auditor mentre està fent la seva assignació d'auditoria.

2.1. Característiques de l'abast d'una auditoria

L'abast de l'auditoria ha de ser vist com l'acord mutu entre auditor i auditat sobre què es farà en l'auditoria.

Una vegada determinat l'abast, s'han d'identificar correctament els aspectes rellevants següents sobre l'auditoria que s'ha de dur a terme:

- L'auditoria ha d'incloure no solament les àrees físiques de l'organització auditada, sinó també les funcionals (grups o àrees organitzatives), sistemes d'informació i comunicacions, processos de negoci, etc.

- Els límits als esforços que s'han de fer en l'auditoria, tant lògics com físics, amb la finalitat de poder ajustar l'esforç d'auditoria des del punt de vista econòmic per aconseguir els objectius d'auditoria.

- Les dates i l'esforç del treball que ha de fer l'equip auditor per poder planificar les tasques tant de l'auditor com de l'auditat i afectar el mínim possible les seves activitats habituals.

- La llista de totes les accions que s'han de dur a terme durant l'auditoria. No es tracta tant de detallar exactament, sinó de conèixer des d'un punt de vista d'alt nivell quin tipus de proves s'hauran d'executar.

- Les expectatives que es deriven del projecte, especialment quin tipus de lliurables es faran. És essencial conèixer bé l'objectiu que té el client de

l'auditoria per poder complir amb les seves expectatives i que el seu resultat aporti valor.

En el cas d'un auditor extern, habitualment aquests aspectes es pacten entre auditat i auditor en un contracte; mentre que en el cas d'un auditor intern s'estableix en una assignació o instrucció de treball.

2.2. Determinació de l'abast

Qualsevol activitat involucrada en la gestió de la informació és susceptible de ser auditada, o bé per a comprovar com s'apliquen les polítiques i normes de seguretat de l'organització, o bé per a comparar la pràctica que es fa amb els codis de bones pràctiques existents. Per tant, qualsevol aspecte que es troba tractat dins dels catàlegs estàndard de controls de seguretat (per exemple, l'ISO/IEC 27002 o COBIT) és susceptible de ser auditat.

De manera general, desenvolupar l'abast d'un projecte d'auditoria és la tasca inicial on es decideixen els límits que s'aplicaran al treball que ha de dur a terme l'equip auditor, i els requisits tècnics necessaris i les tècniques. En una auditoria de seguretat, definir aquestes "fronteres" inclouria determinar:

- Quins processos de negoci de l'organització estan afectats per l'auditoria i quines parts d'aquests processos es revisaran? Tot el procés? Només la part exclusivament suportada pels sistemes d'informació? Ens centrarem en una auditoria de caràcter tècnic? O també es revisaran els processos?

- Quina àrea o quin tipus de controls de seguretat són els que s'han d'auditar? Estan clarament definits aquests controls o han d'emprar-se com a guies de referència de bones pràctiques o, fins i tot, directament l'opinió tècnica de l'auditor?

- En cas que s'hagin d'auditar infraestructures tècniques de tractament d'informació, quins sistemes físics, segments de xarxes o aplicacions estan sota l'abast?

- En cas que s'hagin d'auditar processos que tracten la informació i que són executats per diverses estructures organitzatives de l'auditat, quin personal de l'organització es troba afectat per l'auditoria i amb quin ens entrevistarem?

Determinar aquests aspectes condiciona totalment el treball que s'ha de fer posteriorment.

Cas pràctic: seguretat d'un banc

Plantegem-nos la revisió del sistema d'identificació i autenticació d'un banc mitjançant la "targeta de coordenades".

L'organització auditada ha millorat recentment els controls d'identificació i autenticació en la seva plataforma de banca electrònica i ha substituït l'antic esquema d'usuari/contrasenya a l'inici de l'aplicació per un sistema amb dues fases d'autenticació: una a l'inici mitjançant usuari/contrasenya i una segona autenticació en determinades operacions clau mitjançant l'ús d'una targeta de codis distribuïda als clients. La direcció està preocupada per la seguretat del sistema engegat i vol que una organització externa doni una estimació sobre la seguretat del nou sistema d'identificació i autenticació.

A l'hora de plantejar quin és l'abast real de l'auditoria proposada, l'equip auditor es pot plantejar dues opcions extremes:

- Ens podem fixar únicament en el procés tècnic propi de la identificació i autenticació, i delimitar el nostre treball d'auditoria a la revisió de la plataforma (servidors web) on corre l'aplicació en recerca de problemes/vulnerabilitats. L'abast del projecte seria, per tant, la plataforma tecnològica utlitzada i l'aplicació que s'hagi dissenyat sobre aquesta. Seríem davant una auditoria de seguretat purament tècnica.

- Una altra opció seria determinar un abast molt més ampli i revisar tots els processos que intervenen en el cicle complet de vida de la targeta de coordenades, des de la seva creació, passant per la distribució, el seu ús i la seva destrucció. Per tant, inclouria tasques com les següents:
  - Verificació de la seguretat dels algorismes que s'empren per a generar les targetes.
  - Revisió de la seguretat en el procés informàtic de creació.
  - Comprovació de la seguretat durant la impressió física de les targetes, especialment si la duen a terme empreses subcontractades.
  - Verificació de la confidencialitat durant el procés de distribució de les targetes.
  - Revisió de les clàusules de confidencialitat en els contractes amb empreses subcontractades que manegen aquestes targetes.
  - Identificació del nivell de formació necessària donat als usuaris,
  - Revisió de la implementació tècnica de la plataforma web on s'utlitza la targeta.

Com es veu, aquesta auditoria tindrà un abast molt més ampli que l'anterior i necessàriament l'equip auditor haurà de dedicar molts més recursos i esforços per dur-la a terme.

Respecte a la pregunta de quin dels dos enfocaments és més adequat, la resposta és que qualsevol de les dues opcions és vàlida, sempre que el client de l'auditoria en conegui l'abast i hi estigui d'acord. Per tant, abans d'iniciar si més no la planificació de tasques de l'auditoria, és essencial arribar a un acord amb la direcció de l'organització auditada, que rebrà l'informe d'auditoria per a determinar quines són les seves expectatives i necessitats. D'acord amb aquesta recollida d'informació, l'equip auditor podrà determinar quin punt intermedi entre les nostres dues opcions és el que realment vol l'auditat.

Gran part dels projectes d'auditoria de seguretat fallits ho són a causa d'algun tipus de problema a l'hora de definir-ne l'abast. És molt habitual que l'abast estigui inicialment mal definit o sigui ambigu, i això provoca, durant el desenvolupament de l'auditoria, que es desviïn els esforços i que s'incorri en sobrecostos o en lliuraments fora de termini o fins i tot que produeixin un resultat que no compleixi les expectatives dels patrocinadors de l'auditoria (usualment la direcció executiva d'una entitat).

Les raons per les quals l'abast del projecte es troba mal definit són molt diverses i depenen de cada escenari. Malgrat això es poden donar certes indicacions per a evitar les fallades més comunes:

- **Identificar les raons que mouen l'auditat a fer l'auditoria**. Generalment l'auditat duu a terme l'auditoria per una raó ben precisa i conèixer-la ens permetrà delimitar-ne les àrees d'interès. Algunes d'aquestes raons són:
  - Requisits legals o reguladors en el seu sector d'activitat.
  - Requisits imposats per una entitat asseguradora.

- Necessitat de garantir la protecció d'una infraestructura crítica (per exemple: instal·lacions de distribució d'aigua, electricitat, centrals elèctriques, etc.).
- Proporcionar a un tercer una garantia o nivell de confiança sobre la seguretat dels processos analitzats per l'auditor. Les auditories exigibles en el marc d'un SGSI es trobarien situades en aquest apartat, ja que l'objecte d'implantar un SGSI en la majoria dels casos és oferir a un tercer garanties sobre la seguretat en el tractament de la informació en l'organització on es troba implantat l'SGSI.
- Resposta a incidents de seguretat esdevinguts en el passat.
- Validació externa d'una auditoria feta internament.

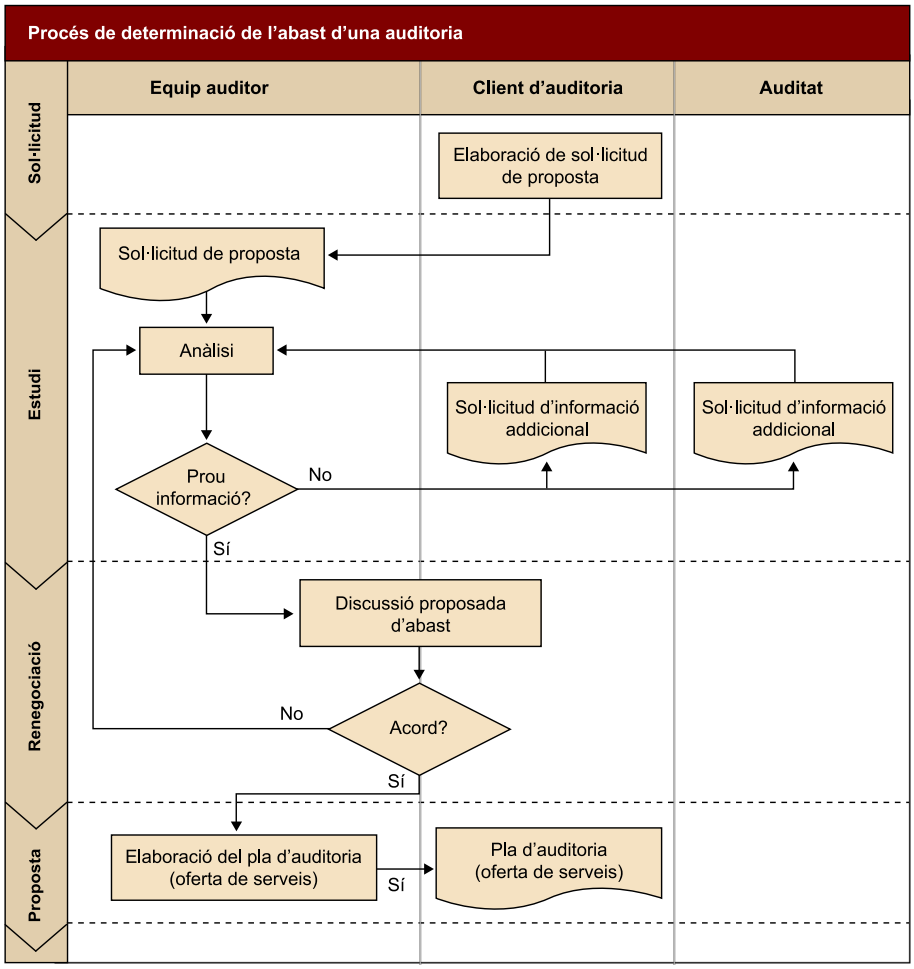
- **Identificar les limitacions aplicables al mateix auditat**. Totes les organitzacions tenen certes limitacions que li són imposades a l'hora d'afrontar una auditoria. Algunes poden ser:
  - Marc temporal en què s'ha de disposar d'una auditoria feta per un tercer.
  - Limitacions financeres a l'hora de dotar de recursos el projecte d'auditoria.
  - Limitacions quant a la dedicació del seu propi personal a l'auditoria.
  - Limitacions lògiques o físiques en la infraestructura que dóna suport al tractament de la informació.

- **Comprendre l'entorn en què es farà l'auditoria**. Com millor sigui la informació relativa a l'entorn en què es farà l'auditoria millor se'n podrà delimitar l'abast. Entre els aspectes de l'entorn que s'han de determinar, s'hi inclou:
  - Ubicació en què es farà l'auditoria.
  - Nombre i ubicació d'altres centres que s'han de visitar durant l'auditoria. D'aquest aspecte derivaran els requisits de viatges i desplaçaments necessaris.
  - Disponibilitat de documentació prèvia de l'auditat, com per exemple diverses polítiques de seguretat, diagrames de xarxa, documents de disseny d'aplicacions, descripció dels diferents entorns operatius, inventaris d'infraestructures, etc.
  - Disponibilitat del personal de l'organització auditada.

Perquè l'equip d'auditoria eviti errors en la determinació o el manteniment de l'abast de l'auditoria, és necessària una bona comunicació entre l'equip auditor i l'auditat, d'una banda, i també amb el client de l'auditoria, de l'altra, que pot ser el mateix. Aquest intercanvi s'ha de donar tant a l'inici com durant l'execució. Mitjançant informacions o informes preliminars, l'auditor ha de mantenir informat tant l'auditat com el client de l'auditoria dels progressos, i donar motiu al fet que se'n renegociï l'abast. Per descomptat, aquesta renegociació haurà de tenir en compte els recursos previstos inicialment per a l'auditoria, i ajustar-s'hi, o bé dotar l'auditoria de recursos addicionals.

2.3. Tècniques per a determinar-ne l'abast

La manera més senzilla de determinar l'abast d'una auditoria és recórrer al client de l'auditoria i, en cas necessari, al mateix auditat com a font d'informació més precisa. El procés de determinació de l'abast necessita la interacció entre l'auditor i el client de l'auditoria principalment. El diagrama del procés queda reflectit en la figura següent:



Procés de determinació de l'abast d'una auditoria

És recomanable que l'entitat que hagi de ser client de l'auditoria (el mateix auditat en cas d'auditories de primera part) doni indicacions inicials a l'equip auditor de quin n'ha de ser l'abast.

En els casos en què se sol·licita una auditoria feta per una entitat externa més independent i en què l'auditat té prou coneixement i conscienciació, en matèria de gestió de la seguretat de la informació, o bé simplement a causa de la necessitat de complir els procediments interns per a la contractació (de vegades, imposat per la implantació d'un sistema de gestió de la qualitat), l'auditat sol emetre un document en què s'especifiquen les característiques del servei que es vol contractar, en aquest cas una auditoria. Habitualment, aquests documents s'acostumen a denominar *sol·licitud de servei* (o en l'àmbit anglosaxó,

request for proposal –RFP– o també *statement of work* –SOW–) o, per exemple, en el camp de la contractació amb les administracions públiques a Espanya, *plec tècnic*.

Segons qui hagi redactat l'RFP, el document pot incloure un ventall molt ampli d'informació sobre les necessitats de l'auditat. El tipus i abast de l'auditoria sol·licitada dependrà, en gran manera, dels coneixements tècnics i de la comprensió dels aspectes que involucren una auditoria, o simplement de la voluntat de detallar les intencions de l'auditat. En tot cas, si existeix aquest document, serà la millor font d'informació per a començar a treballar i determinar l'abast de l'auditoria.

En cas que l'auditoria es faci internament, també és recomanable fer la preparació d'un document aprovat per la direcció de l'entitat auditada i que reflecteixi l'abast de l'auditoria que s'ha de dur a terme.

El pas següent podria valer en cas de no disposar de tota la informació en l'RFP. També seria necessari, i constituiria directament el primer en els casos en què el client de l'auditoria ni tan sols hagués facilitat una RFP o similar i, simplement, hagués transmès a l'auditor el seu desig de fer una auditoria sense donar gaires més indicacions. De fet, aquesta és una situació molt corrent. En aquesta fase, es tractaria d'aclarir amb el client de l'auditoria els dubtes que es tinguessin. El mètode més adequat seria una entrevista amb el client de l'auditoria o amb la persona o les persones assignades per a la gestió del projecte amb l'objectiu d'aclarir els punts següents:

- Obtenció per part de l'auditat d'informació no classificada sobre l'abast. Aquesta informació pot incloure:
  - Polítiques de seguretat que afectin les àrees que l'auditat vol revisar.
  - Documents tècnics que mostrin a un alt nivell l'abast de les infraestructures que s'han de revisar (diagrames de xarxa, inventaris de sistemes, arquitectures de sistemes).
- Determinar les àrees d'especial interès per al client de l'auditoria.
- Esbrinar motivacions del client que porten a la necessitat de fer una auditoria.
- Pactar el format o el tipus d'auditoria que s'ha de fer: fases, tècniques que s'hi han d'utilitzar, i especialment els tipus de lliurables que esperarà rebre el client de l'auditoria.
- Determinar la manera com es relacionarà l'equip auditor amb l'auditat i el client de l'auditoria per a informar sobre l'avenç, els resultats preliminars i la gestió del canvi de l'abast durant l'execució de l'auditoria.

És important l'intercanvi d'idees entre l'auditat i l'auditor per a consensuar la visió que tots dos tinguin sobre el treball que s'ha de fer. Per a aquest objectiu, acostuma a ser pràctic fer ús de qüestionaris de recollida d'informació. No obstant això, no s'ha de deixar de tenir en compte que una entrevista no ha de constituir un interrogatori de l'auditat o un avançament de qüestions que són objecte de l'auditoria. Encara que es disposi d'un qüestionari, l'auditor ha de tenir prou experiència per a conversar amb el seu interlocutor, obtenir la informació prevista i, per mitjà de la conversa, aclarir qualsevol dubte que li pugui plantejar la informació obtinguda.

Cas pràctic

La infraestructura d'una organització ha experimentat una forta evolució, i l'anterior responsable dels sistemes d'informació ha decidit abandonar l'organització. El nou director de sistemes d'informació ha plantejat a la direcció la necessitat de fer una auditoria de seguretat, per a conèixer el punt en què es troben les infraestructures i en quina mesura la seva operació pot impactar en la seguretat de la informació tractada per l'organització. No s'ha publicat cap document a l'hora de sol·licitar ofertes per a fer el servei.

D'unes primeres entrevistes no oficials entre el director de sistemes i el cap de l'equip auditor es va determinar que, *a priori*, l'abast afectaria únicament la revisió de les infraestructures en una modalitat en què l'equip auditor disposaria d'informació prèvia sobre aquestes infraestructures.

No obstant això, l'equip auditor, amb vista a planificar l'esforç i els recursos necessaris per a l'assignació, necessita determinar millor el seu coneixement previ. D'aquesta manera, s'ha decidit sol·licitar una entrevista amb el director de sistemes, i s'ha preparat un document qüestionari que haurà de guiar l'entrevista. La informació que s'ha considerat rellevant per a poder determinar l'abast de l'auditoria que l'organització necessita és:

- Quina o quines seran les persones de contacte en el projecte.
- Quantes ubicacions físiques de l'organització contenen sistemes que es considerin sota l'abast de l'auditoria.
- On estan situades.
- Quants empleats es troben en aquestes ubicacions i quants fan tasques relacionades amb la gestió de la infraestructura dels sistemes d'informació.
- Un esquema de l'arquitectura dels sistemes d'informació i, si és possible, un diagrama que ho mostri. Els diferents protocols de comunicacions emprats per a interconnectar els sistemes (únicament fins a la capa 4).
- Quantes estacions de treball s'estima que hi ha en cada ubicació. De quin tipus de sistemes operatius disposen.
- Quants servidors es troben en cada ubicació. Quin tipus de sistema operatiu tenen i quin tipus de serveis corre cadascun.
- Quin tipus de sistemes de seguretat perimetral lògica tenen (tallafocs, servidors intermediaris, IDS, IPS, etc.).
- Quin tipus de serveis s'ofereixen a l'exterior de la xarxa corporativa. Des de quins sistemes s'ofereix.
- Quin tipus de sistemes de comunicació hi ha per a la interconnexió de la xarxa corporativa amb altres xarxes: concretament, VPN, IPSec o SSL, accessos telefònics, connexions punt a punt amb terceres parts, etc.
- Quins mecanismes s'empren per a la identificació, autenticació i autorització dels accessos a la informació fets mitjançant infraestructures.

- Quines infraestructures de xarxes sense fil hi ha.

D'altra banda, l'equip auditor també haurà d'obtenir com a resultat d'aquesta entrevista informació sobre aspectes operatius que es faran durant l'execució de l'auditoria, com per exemple:

- Fases en què es vol desenvolupar l'estudi. L'equip auditor proposarà la seva metodologia, que el client de l'auditoria haurà d'aprovar.
- Resultats parcials i/o preliminars que el client vol obtenir.
- Forma i nombre de lliurables.
- Forma de procedir, en cas de detectar problemes greus que l'auditor consideri que afecten greument la seguretat de la informació.

Una vegada recollida adequadament la informació i analitzada juntament amb l'RFP (si n'hi ha), l'equip auditor estarà en disposició de redactar el contracte d'auditoria, si és una auditoria externa, o d'establir els termes d'assignació d'auditoria, si és interna.

3. Enfocament de l'abast de l'auditoria tècnica TIC

Ja hem vist, en el punt anterior, que el factor més crític per a l'èxit d'una auditoria serà determinar-ne l'abast i gestionar-ne les modificacions durant l'execució. Aquesta serà la característica que marca el tipus d'auditoria que es durà a terme. Per tant, fins i tot per a poder determinar correctament quin és l'abast de l'auditoria, és important aclarir com s'enfoca i orienta aquesta auditoria.

En l'apartat anterior es van tractar de manera concreta les fases o els passos a seguir per pactar amb el client de l'auditoria. En aquest es precisarà més concretament quins aspectes és essencial definir en l'abast d'una auditoria dins del context de l'àmbit de la gestió de seguretat de la informació en sistemes TIC. En aquest sentit, és important pactar amb el client de l'auditoria:

- Els aspectes tècnics dins de la gestió de seguretat de la informació que es tractaran en l'auditoria.

- El nivell d'informació prèvia de què disposarà l'equip auditor abans de realitzar l'auditoria, el qual veurem com afecta a l'hora d'enfocar el treball d'auditoria.

- L'esforç que l'equip auditor haurà de planificar i quantificar i la manera en què igualment impacta al final a l'hora de determinar l'abast.

3.1. Aspectes tècnics de l'abast

Com s'ha comentat, una auditoria de seguretat de la informació en TIC té per objectiu verificar la implantació correcta de controls de seguretat que una organització pot haver decidit implantar i per tant poden existir en un gran ventall d'àrees relacionades amb la gestió dels sistemes d'informació. Les normes que defineixen catàlegs de bones pràctiques recullen totes les àrees, per la qual cosa l'abast d'una les auditoria tècnica de seguretat pot dirigir-se en aquest àmbits es poden sobre qualsevol de classificar sobre la base dels objectius de control que es pretenen verificarpuede arribar a haver seleccionat. D'aquesta manera, des d'un punt de vista purament tècnic, l'abast d'una auditoria de seguretat TIC podria realitzar-se sobre qualsevol classificació bàsica, prenent com a criteri de selecció els diferents capítols o àrees d'interès de qualsevol dels catàlegs de controls existents al mercat, com per exemple, la norma ISO/IEC 27002, la qual té una orientació prou àmplia per a incloure tots els aspectes que són rellevants en la gestió de la seguretat de la informació TIC.

Norma ISO/IEC 27002

En el diagrama següent representem els diferents capítols de la Norma ISO/IEC 27002, que es poden fer servir com a referència a l'hora d'identificar des del punt de vista purament tècnic els aspectes de l'abast que es poden incloure.

En l'actualitat hi ha diverses normes i codis de bones pràctiques que donen un marc sobre les millors pràctiques de la indústria en relació amb els serveis de tecnologies de la informació, com per exemple: ITIL, conjunt de normes BS-15000 i el seu equivalent internacional ISO-20000, o el COBIT. Qualsevol de les diferents àrees descrites seran susceptibles de poder ser auditades, encara que algunes tindran més implicació sobre la qualitat del servei de TI ofert en l'organització, unes altres sobre el valor que les TI aporten al negoci i unes altres sobre la seguretat de la informació.

Nota sobre el capítol 17

Des de la revisió de 2013, la continuïtat de negoci completa ja no està inclosa com un control de seguretat de la informació, sinó que només es té en compte la garantia de la seguretat de la informació durant la gestió de la continuïtat de negoci. Hi ha una norma pròpia per a continuïtat de negoci, l'ISO/IEC 25999.

A continuació presentem diferents tipus d'abastos (només des del punt de vista tècnic, ja hem comentat que l'abast inclou més elements) que es poden donar en un ambient TIC i centrats en la seguretat de la informació. Com hem esmentat, en ser un entorn molt ampli, aquest llistat no pretén ser exhaustiu, però sí almenys rellevant i concorde al que en l'actualitat es realitza en el sector de la seguretat informàtica.

3.1.1. Revisió del compromís de la governança de la seguretat de la informació

L'objectiu d'aquest tipus d'auditoria seria comprovar el compromís i la direcció o governança de la direcció sobre la seguretat de la informació mitjançant la revisió formal de tots els documents que donen suport a la seguretat de la informació en l'organització en els diferents aspectes que són de la seva responsabilitat, i la manera en què es realitza el govern, el control i la millora de la seguretat de la informació. Es tractaria de comprovar, per tant, com es troben implementades les clàusules dels apartats 4, 5, 6 i 9 de la norma ISO/IEC 27001 i la manera en què s'implementen els controls dels capítols 4, 5, 6, 7 i 15 de la norma ISO/IEC 27002 (vegeu el diagrama anterior de capítols de la norma), la qual cosa estaria molt alineada amb el que seria una auditoria interna de verificació de l'SGSI (vegeu el mòdul 2 d'aquest curs). Els objectius d'aquesta auditoria serien els següents:

- Revisió del manteniment del document de política de seguretat i les revisions posteriors i de la resta de documentació que se'n derivi.
- Revisió de les anàlisis de riscos fetes per l'organització.
- Revisió de les reunions periòdiques dels comitès, grups de treball o similars creats per a donar suport directiu a la seguretat.
- Revisió de la política de classificació i tractament de la informació, i de la seva aplicació.
- Revisió de la política de gestió dels recursos humans en els aspectes relacionats amb la seguretat.

- Revisió de la gestió feta amb la subcontractació de serveis de TI, inclòs el control posterior a la contractació.

3.1.2. Revisió de la seguretat física

Àrees d'interès

Hi ha diverses àrees d'interès en la gestió de la seguretat de la informació: centres de càlcul, sales de comunicacions, sales d'operació, oficines d'usuaris, etc.

Aquesta auditoria tindria un caràcter més tècnic però limitat a la revisió dels controls de seguretat física aplicats a les diferents àrees d'interès en la gestió de la seguretat de la informació.

Els aspectes que s'han d'examinar han d'incloure revisions de tipus tècnic sobre com s'han implementat els controls tècnics i les revisions dels procediments aplicats per a gestionar aquests controls i les polítiques que s'hagin dictat per a guiar la implantació. Aquestes revisions enllaçarien amb la resta de polítiques i normes de l'organització amb l'objectiu de constituir un sistema de gestió de la seguretat de la informació coherent. Per tant, els objectius d'una auditoria d'aquest tipus serien:

- Revisió de la ubicació i les condicions de construcció de les diverses àrees segures, des de l'avaluació de l'elecció de la ubicació fins a l'avaluació de les característiques de construcció: si hi ha tanques de seguretat, finestres, identificacions externes, disposició i mesures de seguretat a les zones de càrrega i descàrrega, ubicació i mesures de seguretat a les sortides d'emergència, etc.

- Revisió dels mecanismes de control d'accés físic i dels procediments que els efectuen: com es lliuren les credencials d'accés, com s'empren, com es gestionen la pèrdua o l'oblit de les credencials, etc.

- Revisió de les característiques de disseny de les diferents sales tècniques segons el propòsit que tenen: sales de comunicacions, sales de servidors, magatzems de suports de còpies de seguretat, etc.
  - Elecció de materials.
  - Distribució del cablatge pel sòl tècnic o per la part alta de la sala.
  - Característiques dels *cabinets* d'equips (materials, controls d'accés físic a aquest nivell, connexió a terra, etc.).
  - Ubicació i mesures de seguretat de les entrades "oficials" i d'emergència.

- Revisió de la instal·lació elèctrica i del cablatge per a garantir la compatibilitat electromagnètica.

- Revisió dels controls de seguretat de les condicions d'entorn: subministrament elèctric, control de temperatura i humitat, i mecanismes de detecció i extinció d'incendis.

- Revisió dels procediments operatius aplicables a aquest tipus d'instal·lacions: normes d'entrada/sortida d'equips, normes de treball, procediments d'instal·lació/retirada d'equips, procediments d'accés a les sales, etc.

És molt interessant saber que, quant a la seguretat física, hi ha una tendència actual a externalitzar la gestió física dels equips informàtics servidors en grans centres de processament de dades (CPD o centres de càlcul); d'aquesta manera, s'estalvien costos i s'aconsegueixen nivells de protecció que de manera particular tindrien un cost molt elevat.

En aquest context, cada vegada més, les grans entitats que recorren a aquest tipus de servei exigeixen auditories de segona part contra la seguretat física dels centres de càlcul on han externalitzat serveis informàtics crítics per al negoci. Com en qualsevol altra auditoria, l'auditor es troba davant la necessitat de disposar d'uns criteris d'auditoria amb els quals contrastar les proves que reculli. El client d'auditoria podria haver elaborat unes normes físiques, o bé haver-les establert contractualment en el contracte d'externalització, però no és el més habitual en aquest tipus d'externalització. No obstant això, l'auditor disposa d'una norma que és interessant que conegui, la TIA-942 (*telecommunications infrastructure standard for data centres*, www.tia-942.org).

Aquesta norma, redactada per la Teleccomunications Industry Association (TIA), facilita estàndards per al disseny de centres de processament de dades en tots els seus aspectes o subsistemes funcionals (que també estan enumerats i estandarditzats):

- Sistema arquitectural. Condicions constructives i d'ubicació del mateix edifici, i de distribució i accés a les seves diferents estances.

- Sistemes de telecomunicacions. Inclou cablatge estructurat intern de dades i l'accés de proveïdors de telecomunicacions.

- Sistema elèctric. Des de l'arribada del proveïdor fins a la distribució final en els bastidors (*racks*).

- Sistema mecànic. Aspectes relacionats amb el manteniment de les condicions mediambientals i, en general, de subministraments diferents dels elèctrics: aigua, gas, gasoil, etc.

El més interessant per a l'auditor és que aquesta norma és certificable i, tot i que ell no hagi de fer una auditoria de certificació, sí que li facilita un marc per a avaluar els centres actuals contra les especificacions que dóna la norma i

el nivell de disponibilitat que ofereixen. L'estàndard defineix una classificació per als centres de dades (des de *tier-1* fins a *tier-4*, per als quals donen la màxima seguretat). Cadascun es correspon amb un nivell diferent de disponibilitat que ofereix per les seves característiques:

Nivell	Disponibilitat	Característiques
Tier 1	99,671% (28,8 h/any d'indisponibilitat)	**Centre de càlcul bàsic** • Susceptible d'interrupcions tant planificades com no planificades. • Els sistemes de subministrament i comunicacions no disposen de cap tipus de redundància i/o existeixen diversos punts únics de fallada. • Les operacions de manteniment o errors requereixen posar en fora de servei la instal·lació.
Tier 2	99,741% (22 h/any d'indisponibilitat)	**Centre de càlcul amb components redundats** • Menys susceptibles a interrupcions que un *Tier* 1, tant planificades com no. • Els sistemes de subministrament i comunicacions disposen d'elements de respatller (per exemple, redundància o sistemes de suport alternatius), però estan connectats a una sola línia de distribució activa. • Hi ha redundància N + 1 (els necessaris més un) per als components de la infraestructura. • Les operacions de manteniment o els errors requereixen posar en fora de servei la instal·lació.
Tier 3	99,982% (1,6 h/any d'indisponibilitat)	**Centre de càlcul amb manteniment concurrent** • Permeten fer qualsevol activitat planejada sobre qualsevol component de la infraestructura sense interrupcions en l'operació. • Doble línia de distribució dels components, encara que només una d'activa en un moment determinat. • Capacitat suficient de tal manera que sigui possible fer manteniment o proves en una línia, encara que esdeveniments no planificats (errors o fallades espontànies) poden provocar interrupcions del servei per falta de capacitat.
Tier 4	99,995% (0,4 h/any d'indisponibilitat)	**Centre de càlcul amb tolerància a fallades** • Permeten fer qualsevol activitat planejada sobre qualsevol component de la infraestructura, o sofrir esdeveniments no planificats (errors o fallades) sense interrupcions de cap tipus. • Múltiples línies de distribució per als components de la infraestructura activa, totes elles. • Redundància completa 2(N + 1) (tot duplicat i amb elements de reserva addicionals).

Nivells de disponibilitat segons TIA/EIA 942

Aquesta classificació és aplicable als diferents subsistemes d'un CPD que l'estàndard defineix; en un dels annexos (annex G) es recullen tots els requisits que cada subsistema ha de complir per a cadascun dels nivells. Cal destacar que també es donen indicacions que incideixen sobre la classificació d'un CPD, però que no estan estrictament lligades al concepte de *disponibilitat*, com per exemple els controls d'accés i de monitoratge. L'estàndard estableix els diferents requisits en aquesta àrea per als diferents nivells, encara que no incideixen directament sobre la disponibilitat (limiten la possibilitat que un atacant extern pot provocar un incident que afecti la disponibilitat). L'auditor determinarà el nivell (*tier*) resultant d'un determinat CPD, fent l'anàlisi del nivell de disponibilitat de cadascun dels components i prenent el menor de tots ells.

Per tant, l'auditor pot fer una auditoria per a comprovar el nivell que correspon a la instal·lació i confrontar-lo, després, amb el client d'auditoria, que haurà de determinar si és adequat per als seus interessos.

3.1.3. Revisió de la seguretat perimetral de les xarxes de comunicacions

En molts entorns, quan es parla d'*auditories de seguretat* es pensa només en auditories que revisin l'eficàcia dels controls de seguretat implantats a les xarxes de comunicacions. És cert que són un dels tipus d'auditories més sol·licitats en el mercat –i destaquen per això–, però com estem veient al llarg de tot aquest curs, l'auditoria de seguretat de les TIC pot comportar més coses.

Aquest tipus d'auditories se centraran a avaluar la seguretat perimetral de les diferents subxarxes corporatives, amb un interès especial en el perímetre exterior. Es tractarà d'una manera més general de la revisió de la seguretat que s'ofereix a la informació quan es transmet per les xarxes de comunicacions de l'organització, tant en el perímetre (connexions a Internet, interconnexions amb xarxes d'altres organitzacions, etc.) com en l'organització interna (segmentació de la xarxa, interconnexions de LAN corporatives, etc.). Per tant, aquesta auditoria tindrà una orientació molt tècnica, encara que pot incloure aspectes de gestió d'algun tema molt concret que afecti la seguretat de les comunicacions, per exemple la revisió dels procediments que involucrin la gestió d'accessos remots (autorització, concessió, auditoria d'accessos remots, etc.). Els objectius específics d'aquest tipus d'auditoria serien (sense ser exhaustius):

- Determinar la implantació correcta de controls de filtratge de trànsit mitjançant enumeracions de xarxes i comprovació de la capacitat de filtratge implementada en els tallafocs corporatius.

- Revisar la seguretat en els accessos remots a les xarxes corporatives segons les diferents tecnologies existents.

- Identificar el nivell de vulnerabilitat dels sistemes de comunicacions i altres serveis presents a les xarxes corporatives per a comprovar l'eficàcia de la política de manteniment i la seva posada en pràctica per part de l'organització.

- Avaluar la implantació de les xarxes sense fil per a l'accés a la xarxa corporativa.

- Avaluar la seguretat d'aplicacions exposades a Internet o bé en xarxes de tercers amb la finalitat de detectar vulnerabilitats, problemes o errors de configuració.

Habitualment, dins d'aquest tipus d'auditories s'inclouran les conegudes auditories d'anàlisis de vulnerabilitats, o proves d'intrusions, o qualsevol de les seves variacions que veurem més endavant.

3.1.4. Revisió dels mecanismes de control de seguretat en aplicacions

Aquest tipus d'auditories també ha estat tradicionalment lligat a la idea general que es té sobre què és una auditoria tècnica de seguretat. Aquestes auditories de seguretat per a la verificació dels controls d'accés a la informació tractaran, principalment, de verificar la seguretat en el nivell d'aplicació, encara que també en revisaran la implementació en altres punts de l'arquitectura de sistemes com, per exemple, en l'accés al sistema operatiu o en l'accés a recursos d'informació a la xarxa.

Des del punt de vista tècnic, els mecanismes de control d'accés lògic a la informació es poden aplicar tant en l'accés de l'usuari a recursos de xarxa com en les mateixes aplicacions de tractament de la informació; així, doncs, si es tracta de verificar quins controls s'hi apliquen per a limitar l'accés a la informació, l'auditoria ha d'identificar tots els punts d'accés a la informació i tots els elements que intervinguin a l'hora de limitar-ne l'ús.

Així mateix, en la mateixa lògica de les aplicacions de tractament, també s'hi apliquen controls d'accés que implementen la política de l'organització quant als drets d'accés concedits als usuaris ja autenticats; és a dir, aquest tipus d'auditories també comprovaran si les aplicacions implementen correctament la lògica de negoci i els controls d'aplicació que s'hagin determinat per a evitar-ne l'ús fraudulent. Això és especialment rellevant en entorns de negoci sensibles, com ara el bancari.

D'altra banda, juntament amb la part tècnica dels controls, també hi estan involucrats els procediments que són necessaris per a gestionar aquests processos. Per tant, l'auditor haurà de comprovar les característiques dels procediments de gestió dels drets d'accés (sol·licitud, autorització, concessió, revocació, auditoria/monitoratge, etc.) i com són executats per l'organització.

Per tant, aquest tipus d'auditoria podrà incloure tant aspectes tècnics com organitzatius, però acostuma a ser més habitual concentrar-se en les revisions de les característiques tècniques d'aquests controls en el marc d'una auditoria tècnica de seguretat que tindria un abast superior al que estem comentant ara mateix. Aquest tipus d'auditoria, eminentment tècnica, inclourà una revisió de la seguretat perimetral de les xarxes de comunicacions com hem vist en l'apartat anterior, i també dels controls de seguretat aplicats en les aplicacions de tractament.

3.1.5. Revisió de la gestió del cicle de vida dels sistemes

Quan una organització afronta el desenvolupament o l'adquisició d'un sistema d'informació, de seguida sorgeix la temptació d'obviar les diverses fases que componen el cicle de vida del desenvolupament de sistema (en anglès *system development life cycle*, SDLC).

Hi ha diverses representacions o denominacions de les fases que componen aquest SDLC, però de manera general podem reflectir l'SDLC complet de la manera següent:

Hi ha diverses raons que comporten que una organització no compleixi aquest model. Habitualment es tracta de raons econòmiques, juntament amb planificacions temporals molt ajustades. No obstant això, l'omissió d'alguna d'aquestes fases pot comportar un risc tant per a la informació que aquests sistemes han de tractar, com sobre el suposat valor que aportarien a l'organització. En aquest context, és possible que es demani a l'equip auditor la revisió de l'execució del cicle de vida del desenvolupament d'algun tipus de sistema.

D'altra banda, l'auditor també pot estar involucrat en el mateix cicle de vida. Hem de recordar que, en les fases de definició de requisits, tant de negoci com d'usuari, s'han de recollir les necessitats de seguretat que ha de tenir el sistema. Els dissenys i les implementacions han de considerar aquests requisits, i implementar internament els controls que siguin necessaris i especificar els que, en el moment del desplegament, hagin de proveir altres infraestructures TIC de l'entorn en què s'integri el nou sistema. L'auditor pot participar en tot aquest procés d'incrustar la seguretat en el procés de desenvolupament en lloc de proporcionar-lo *a posteriori*. Es pot requerir a un auditor que executi proves per comprovar la implementació dels dissenys que compleixen els requisits de seguretat. En aquests casos, participarà en les funcions de proves a partir de la fase de proves d'integració de sistemes i podrà arribar fins a la fase final de proves d'acceptació.

D'altra banda, és convenient reconèixer que, en els últims temps, el procés de desenvolupament de programari ha evolucionat i ja no sempre s'aplica el tradicional model SDLC en cascada vist anteriorment. No obstant això, hi ha altres models coneguts com a "metodologies àgils de desenvolupament" les quals fonamentalment busquen reduir les iteracions entre recollida de requeriments i lliurament de producte, amb la finalitat d'aconseguir una col·laboració més estreta i flexible entre els equips de desenvolupament i els clients o usuaris del producte final. Hi ha múltiples metodologies, com ara SCRUMM, XP - *Extrem Programming*, *Kanban* i d'altres.

Totes han estat orientades, principalment, a la satisfacció de l'usuari i poc o gens a garantir la seguretat (tant de la informació com del procés), per la qual cosa no s'utilitzen àmpliament en entorns molt regulats on la seguretat física

(en anglès, *safety*) o la confiança en el resultat és crucial, com per exemple, en sectors crítics com l'industrial, nuclear, financer, instrumental mèdic, etc., encara que dia a dia es van introduint, amb el risc que això comporta.

A causa d'aquest dinamisme i aquesta rapidesa en el lliurament, el programari és propens a la introducció d'errors, però també permet detectar-los i aplicar-hi correccions abans. Respecte a la seguretat de la informació que tracten, aquesta situació és problemàtica. Quan s'empren aquest tipus de metodologies, és essencial inserir la seguretat en el procés. Per a això s'haurien de tenir en compte aspectes com els següents:

- En aquesta situació és important que hi hagi una anàlisi de riscos del procés que l'aplicació implementi i que, a més, vagi evolucionant a mesura que el producte ho faci. D'aquesta manera, es podrà valorar tant la necessitat d'una determinada freqüència d'auditoria com la priorització de la resolució dels problemes detectats davant de la contínua incorporació de noves funcionalitats.

- D'una manera o una altra, en algun moment s'ha de planejar una revisió de seguretat o auditoria tècnica que identifiqui problemes en el control de la informació tractada. Encara que aquestes metodologies es basin en cicles de desenvolupament molt curts, hi pot haver una planificació de més alt nivell que prevegi lliuraments més generals. Aquestes auditories de seguretat han d'alinear-se el màxim possible tant amb els cicles curts com amb els lliuraments d'alt nivell. Per tant, les implicacions més determinants respecte a les tradicionals auditories de seguretat rauen en el fet que tindran un abast més reduït i una freqüència d'aquestes més gran com més alineades estiguin amb els cicles de lliurament curts. Això no exclou la necessitat d'auditories completes amb una certa periodicitat que actuarien a manera d'avaluació global que garanteixi que problemes anteriorment resolts no hagin estat reintroduïts o s'expressin d'una manera diferent.

- Els resultats d'aquestes auditories han de ser incorporats en el procés de desenvolupament i prioritzats correctament pel responsable del producte. Aquest ha de ser molt conscient del valor de la informació i dels riscos que els problemes detectats impliquen.

- Els desenvolupadors han de ser capaços de produir programari sense errors de seguretat emprant eines que analitzin el codi abans del seu lliurament i corregint-lo en la iteració.

En qualsevol cas, la introducció de metodologies de desenvolupament àgil implica un desafiament molt elevat per a la seguretat, i tant els responsables de producte com els auditors han de ser conscients d'això i arribar a un acord en què la seguretat s'insereixi correctament en el procés.

3.1.6. Revisió dels plans de continuïtat de negoci

Un altre dels aspectes que són susceptibles de requerir una auditoria és la gestió de la continuïtat de negoci. A mesura que les TI han adquirit més pes en els processos de negoci de les organitzacions, la capacitat operativa i la supervivència d'una organització estan lligades d'una manera o una altra a la continuïtat dels serveis de TI.

En aquest sentit, les organitzacions solen requerir que es facin auditories dels seus processos de continuïtat de negoci perquè una organització externa els avaluï i determini si garanteixen adequadament la supervivència de l'organització en cas d'una contingència greu.

Per tant, es tractarà d'avaluar de quina manera s'ha establert l'estudi de l'anàlisi d'impacte sobre el negoci (en anglès *business impact analysis*, BIA), com s'han determinat els paràmetres de l'RPO i l'RTO per a cadascun dels processos de negoci i l'estratègia de suport determinada, i posteriorment es revisarà la implantació dels plans de continuïtat que s'hagin derivat de l'estudi anterior.

En el diagrama següent, recordem els conceptes d'*RPO* (*recovery point objective*) i *RTO* (*recovery time objective*), que són els dos paràmetres bàsics que defineixen l'estratègia de continuïtat de negoci que ha d'abordar una entitat.

Aquest tipus de revisions requerirà, per tant, combinar proves tècniques –que determinin de quina manera s'ha previst el suport dels sistemes d'informació– amb proves no tècniques –entrevistes, visites, estudi de documentació– per a completar la revisió de la manera com l'organització gestiona la continuïtat.

3.1.7. Revisió de la capacitat de resposta davant incidents

Un altre dels pilars de la gestió de la seguretat que manté preparada l'organització en les situacions d'emergència és la manera com es gestionen els incidents de seguretat o com es respon davant d'aquests incidents. Juntament amb la gestió de la continuïtat de negoci, la gestió d'incidents forma el front de resposta davant situacions imprevistes que queden fora de la capacitat dels controls de seguretat implantats, ja sigui pel seu mal funcionament o perquè simplement no estan preparats per a protegir contra tot tipus de situacions de risc. L'auditor també pot ser requerit perquè avaluï els processos que l'organització hagi engegat per a gestionar aquest tipus de situacions. Les tècniques que utilitzaria diferiran de les que tractem generalment en aquest mòdul, ja que treballaria més amb simulacions. L'auditor podria comprovar l'efectivitat d'aquests processos posant-los a prova en situacions simulades. Aquestes tècniques queden lleugerament fora de l'abast d'aquest curs, però és interessant conèixer que aquesta també és una àrea en què pot participar un auditor de seguretat.

3.2. Impacte del coneixement previ en l'abast de l'auditoria

Tant si és una auditoria purament tècnica com si és una auditoria sobre algun altre aspecte, segons el coneixement previ que es tingui de la infraestructura que s'ha d'auditar, tindrà un clar impacte sobre com determinar l'abast i els objectius de l'auditoria.

La classificació que es presentarà té especial sentit en el cas d'auditories purament tècniques; en la resta, habitualment es tractarà sempre d'auditories en què l'equip auditor ha de disposar d'un coneixement previ elevat. En certes assignacions d'auditoria, no té sentit que l'auditor no disposi de certa informació sobre l'entorn que ha d'auditar, i li és impossible aconseguir els objectius d'auditoria.

En les auditories purament tècniques (per exemple, revisions de seguretat perimetral a la xarxa, revisió de controls d'accés lògic o físics), és legítim que el client d'auditoria vulgui obtenir, com a resultat, una avaluació pràctica de la seguretat dels seus sistemes d'informació quan s'han d'enfrontar a una situació de risc real mitjançant la confrontació dels controls implantats contra una amenaça simulada. Per tant, voldrà comprovar com es comporten els seus mecanismes de control en una hipotètica situació de risc. En aquests casos, se sol·licita a l'equip auditor que faci una auditoria en què se li facilitarà la mínima quantitat d'informació possible, amb la finalitat que se simuli una situació real en què els sistemes d'informació s'han d'enfrontar a un agent extern que vol accedir a informació de l'organització. Aquest tipus d'auditoria se sol denominar de *caixa negra* (*black box*), ja que per a l'equip auditor el sistema és una caixa negra en què, únicament, es pot examinar, donades unes determinades entrades, quines sortides produeix el sistema.

Les dues situacions anteriorment descrites són els dos extrems que es poden donar. Fixant-nos en el grau de coneixement que es té de les infraestructures que s'han de revisar, també es poden classificar les auditories en els tipus següents:

- ***White box***. L'equip auditor disposa, o pot disposar si ho sol·licita, de tot el coneixement (o gran part d'aquest coneixement) sobre les infraestructures o els processos que s'han d'auditar. No hi ha limitacions quant a la informació a la qual pot tenir accés (no més enllà, és clar, del que determinin els acords de confidencialitat) i el resultat de l'auditoria depèn, exclusivament, de la capacitat de l'auditor per a analitzar la informació recopilada. El valor afegit de l'auditoria ve d'aquesta anàlisi, no del procés de recopilar la informació.

- ***Black box***. Amb la finalitat de simular tan bé com sigui possible un escenari real, l'equip auditor no disposarà de cap informació sobre els sistemes d'informació que no sigui informació pública o informació que pugui anar extraient d'acord amb les diferents proves que es vagin desenvolupant. El

procés de recopilació de la informació constitueix una part del valor que l'auditoria aportarà al client.

Limitacions de les auditories *black box*

Una auditoria *black box* 100% autèntica presenta moltes limitacions. La principal és tenir la certesa que l'auditoria hagi examinat o posat a prova tots els mecanismes de control o hagi detectat tots els problemes potencials. En la pràctica, aquest tipus d'auditoria té un abast molt determinat i reduït a determinar de manera general si en un moment donat els sistemes d'informació són o no vulnerables a un agent extern. En aquest cas ens trobem amb el que es denomina una *prova d'intrusió* o *pen-test*. En aquest tipus d'auditoria preval l'efectivitat davant l'exhaustivitat, i el que es demana a l'equip auditor és que obtingui proves que la intrusió en els sistemes d'informació és possible. En aquests casos, com a part de la determinació de l'abast, l'equip auditor i l'auditat hauran de pactar les característiques que hauran de tenir les proves de la intrusió.

Una altra de les limitacions d'aquest tipus d'auditories és l'elevat cost, tant pel temps necessari com pels grans coneixements que exigeix a l'equip auditor.

- ***Grey box***. Se situa a mig camí entre els dos tipus d'auditoria anterior. En la pràctica representa la major part de les auditories fetes. S'hi combinen anàlisis fetes en mode caixa negra, que poden ser corroborades per l'auditat i posteriorment es continua l'avaluació a les àrees que han quedat fora de les proves de caixa negra. L'equip auditor va adquirint part del coneixement.

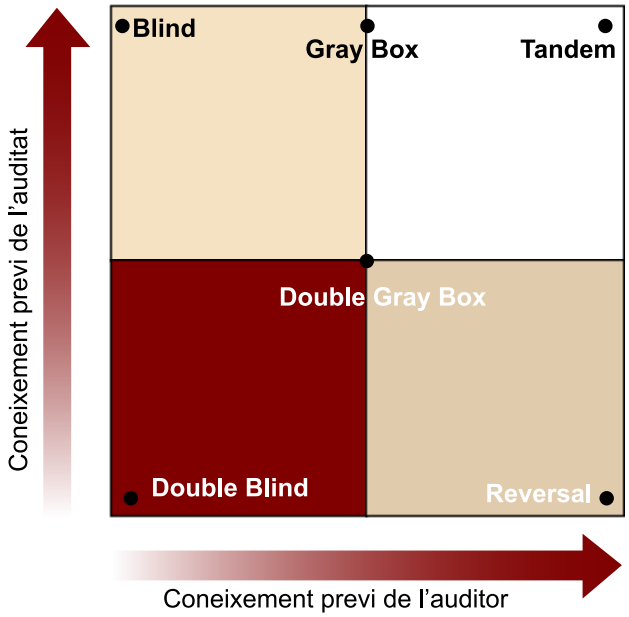
Quant a això, val la pena esmentar la metodologia OSSTMM. És interessant comprovar que l'OSSTMM classifica les auditories emprant aquesta idea però ampliant-la i, per tant, aplicant-la també al coneixement que té el personal responsable de l'operació i el manteniment de les infraestructures auditades.

Vegeu també

La metodologia OSSTM es tractarà en el mòdul 4.

En aquest sentit no s'ha d'oblidar que l'OSSTMM és una metodologia molt orientada a auditoria des del punt de vista extern de l'organització i, per tant, la seva classificació s'ha d'entendre com una classificació d'auditories de tipus tècnic d'avaluació de les mesures de seguretat dels sistemes d'informació exposats en xarxes públiques.

Es duu a terme una classificació de les auditories en les categories següents:



Classificació auditoria segons el coneixement. Font: OSSTMM

1) ***Blind***. L'auditor inicia l'auditoria sense un coneixement previ dels controls existents, de l'arquitectura dels sistemes, dels actius d'informació o dels diferents canals disponibles per a accedir a la informació. No obstant això, els sistemes d'informació avaluats són preparats amb anterioritat per l'auditat amb el coneixement del tipus de proves que l'auditor durà a terme.

Aquest tipus de proves són emprades habitualment tant per a examinar les capacitats d'un auditor, com per a avaluar la robustesa d'unes infraestructures després de la implantació d'algun tipus de mecanisme de control i que l'auditat vol posar a prova.

2) ***Double blind***. Aquest tipus es correspon exactament amb el mode de caixa negra esmentat anteriorment. L'auditor inicia l'auditoria sense un coneixement previ dels controls existents, de l'arquitectura dels sistemes, dels actius d'informació o dels diferents canals disponibles per a accedir a la informació. Els sistemes d'informació auditats no són preparats específicament per a l'auditoria, i el personal a càrrec de la seva operació i el seu manteniment no és advertit abans de l'auditoria. Habitualment, únicament el personal en el nivell de gestió és coneixedor de les activitats que l'equip auditor està duent a terme.

El principal objectiu d'aquest tipus d'auditories és comprovar de la manera més real possible de quina manera tant l'organització com els sistemes d'informació respondrien a un intent d'atac d'un intrús (recordem que l'Institute for Security and Open Methodologies, ISECOM, afronta l'auditoria com l'avaluació des de l'exterior). Com a objectiu addicional d'aquest tipus d'auditories, s'obté també una avaluació dels controls de detecció que s'hi hagin implantat. D'altra banda, s'ha de destacar que, atès que el coneixement de l'auditor és limitat, no es pot pretendre una avaluació en un entorn real de cadascuna de les mesures de seguretat implantades i que, per tant, les proves buscaran la consecució de la vulneració d'algun dels aspectes de seguretat (confidencialitat, integritat o

disponibilitat) de la informació manejada per l'organització mitjançant la recerca i posterior explotació de qualsevol tipus de debilitat o vulnerabilitat en les infraestructures auditades.

3) *Grey box*. L'auditor inicia l'auditoria amb un coneixement previ parcial dels controls existents, de l'arquitectura dels sistemes, dels actius d'informació o dels diferents canals disponibles per a accedir a la informació. Per la seva banda, els sistemes d'informació auditats estan preparats i el personal d'operació i manteniment està advertit del detall de les activitats que es duran a terme.

La naturalesa i els objectius d'aquest tipus de proves és comprovar l'eficiència dels controls implantats davant una situació tan propera com sigui possible a la realitat en què un atacant extern no disposa d'informació *a priori* de les infraestructures. No obstant això, per a disposar d'un resultat més exhaustiu que en el cas d'una auditoria de tipus *blind*, es facilita informació addicional a l'auditor per a concentrar les activitats a les àrees d'especial interès.

4) *Double grey box*. L'ISECOM identifica aquest tipus d'auditories com auditories de caixa blanca (*white box*), encara que es pot discutir molt sobre si és apropiat de denominar-les així.

En la *double grey box*, l'auditor inicia l'auditoria amb un coneixement previ parcial dels controls existents, de l'arquitectura dels sistemes, dels actius d'informació o dels diferents canals disponibles per a accedir a la informació. Per part de l'auditat, el personal d'operacions i manteniment es troba advertit del marc temporal en què es faran les proves, encara que sense el coneixement exacte de les tècniques que es faran servir, de manera que els sistemes no estan específicament preparats per a les proves. Aquest tipus d'auditories comproven tant les capacitats tècniques de l'auditor com l'eficàcia dels controls de detecció de l'auditat.

Tant en aquest cas com en les auditories de tipus *grey box*, en la fase inicial l'auditor i l'auditat intercanviaran informació sobre les característiques tècniques de les infraestructures provades; a més, durant el desenvolupament de les proves, es podrà anar millorant el grau de coneixement que l'auditor tingui sobre els sistemes auditats, tant per informació inferida de les proves com per informació addicional proporcionada per l'auditat.

Els objectius d'aquest tipus de proves són similars als obtinguts amb una auditoria de tipus *grey box*, amb el valor afegit que també es podrà comprovar l'eficàcia dels controls de detecció.

5) ***Tandem***. Aquest tipus d'auditories és denominat per ISECOM *crystal box*, ja que es correspon amb les auditories en què tant l'auditor com l'auditat disposen de tota la informació sobre la infraestructura que s'ha d'auditar i en un gran nombre d'ocasions les proves les duen a terme conjuntament o de manera coordinada segons un pla d'auditoria.

L'objectiu de l'auditoria serà l'avaluació exhaustiva dels controls de seguretat en alguna de les àrees, encara que òbviament no podrà avaluar completament els controls de detecció i encara menys els processos de l'organització per a gestionar les incidències.

6) ***Reversal***. Aquest tipus de proves d'auditoria té com a objectiu principal comprovar la preparació de l'organització a l'hora de gestionar les incidències de seguretat, ja que l'organització auditada no coneix res sobre el desenvolupament de les proves (almenys els seus nivells més operatius), mentre que l'auditor disposa de tota la informació que l'auditor li hagi facilitat.

Aquesta classificació l'ha d'utilitzar l'equip auditor per a determinar quin enfocament d'auditoria s'ha de prendre tenint en consideració l'abast de l'auditoria i els objectius que haurà de complir amb vista a satisfer les expectatives de l'auditat.

3.3. Impacte de l'esforç en l'abast

Hem vist que l'abast de les auditories està afectat pels aspectes purament tècnics a revisar i també pel nivell de coneixement previ de què es disposarà, així com, en certa mesura, pels matisos respecte a l'objectiu de l'auditoria que tingui el client.

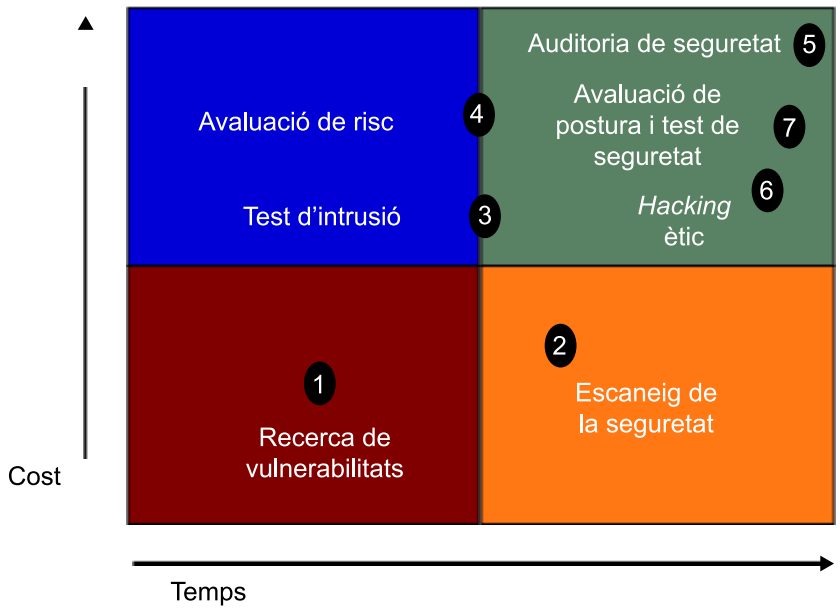
De cada combinació de tipus d'auditoria que hem repassat tenim un ampli ventall dels diferents tipus de treballs que un auditor de seguretat de la informació pot arribar a dur a terme. Cadascuna d'aquestes assignacions d'auditories té un cost que l'entitat auditora ha de conèixer i ha de preveure, i que ha d'estar disposada a assumir. Per tant, l'esforç (cost en temps necessari i recursos tècnics i humans necessaris) és l'altre gran paràmetre pel qual es poden classificar les auditories. Els dos primers criteris de classificació ens serviran per a determinar millor l'abast i l'objectiu de l'auditoria i, finalment, els recursos disponibles d'auditoria (avaluats en persones, coneixements i temps) ens determinaran les tècniques que s'hi han d'aplicar. De totes maneres, l'entitat auditora ha de ser capaç de fer aquest exercici de comparar abast i recursos que es poden mobilitzar per a poder determinar si es troba en disposició d'aconseguir els objectius d'auditoria que s'han pactat amb el client. Ja hem dit que aquest és un dels factors crítics per a l'èxit de l'auditoria, i també podem afirmar que és un dels més afectats quan es fan canvis no gestionats en l'abast de l'auditoria. Tot canvi de l'abast ha de comportar una nova avaluació dels recursos necessaris i contrastar-los amb el total previst per a l'assignació. Si no es poden complir els objectius amb el pressupost previst, l'equip auditor

ho hauria de comunicar al client de l'auditoria, ja que es podria incórrer en un elevat risc d'auditoria (vegeu el mòdul 1 per a revisar-ne el significat) si no es dediquen els recursos necessaris.

Les tècniques per a determinar els recursos necessaris i el seu ús no difereixen de les que s'empren per a la planificació i gestió de qualsevol altre tipus de projecte, per la qual cosa no entrarem en els detalls sobre tècniques de gestió de projectes[4]. És una temàtica molt àmplia sobre la qual hi ha literatura especialitzada.

(4)Per a obtenir més informació sobre gestió de projectes, es recomana consultar la guia àmpliament reconeguda del *Project Management Body of Knowledge* (PMBOK), l'estàndard per a la gestió de projectes desenvolupat pel Project Management Institute (PMI).

Per tant, el pressupost previst per a l'assignació de l'auditoria i el seu abast determinaran les fases i proves d'auditoria, i també les tècniques que s'hi utilitzaran. Quan ens trobem davant auditories purament tècniques que avaluen la implantació de controls de seguretat, per distingir les diferents tècniques i les seves implicacions, ens fixarem de nou en l'OSSTM, que ofereix la classificació que examinarem a continuació:



Classificació de les auditories segons el cost i el temps. Font: OSSTMM

Aquesta classificació presenta una visió massa tècnica, però ens serveix com a referència per a comprovar que hi ha diferents formes d'abordar l'auditoria de seguretat dels sistemes d'informació. Emprarem la terminologia utilitzada per l'OSSTMM, encara que alguna de les denominacions pot induir a confusió; no obstant això, la distinció entre cadascuna de les auditories és completament coherent.

1) Recerca de vulnerabilitats. Quan els recursos involucrats siguin molt reduïts, l'auditoria es podrà limitar a comprovacions automàtiques d'un sistema dins d'una xarxa, mitjançant eines que automatitzin les tasques i facin ús de fonts d'informació externa, o bases de dades que recullin les vulnerabilitats conegudes dels sistemes involucrats.

2) Escaneig de la seguretat. No es diferencien gaire de l'auditoria de recerca de vulnerabilitats, excepte per la intervenció de l'equip auditor a l'hora d'analitzar els resultats. Les eines de recerca de vulnerabilitats generen massa "falsos positius". La gran majoria d'eines d'aquest tipus examinen els sistemes des del seu exterior i per això solen generar més avisos dels que finalment resulten significatius. Per tant, són necessàries verificacions manuals de falsos positius, la identificació dels punts febles de la xarxa i l'anàlisi professional individualitzada.

Terminologia

Les auditories d'escaneig de la seguretat també se solen denominar *anàlisi de vulnerabilitats*.

3) Test d'intrusió. Des del punt de vista dels recursos d'auditoria necessaris, aquest tipus d'auditoria està limitada en el temps. A més, els requisits de capacitat de l'equip auditor són elevats, ja que s'han d'enfrontar a una infraestructura de la qual no es té informació inicial. Aquest tipus de proves acostumen a estar limitades tant en el temps com en els objectius, que consisteixen a evidenciar d'alguna manera el compromís de la seguretat de la informació manejada (modificar algun arxiu en algun sistema, facilitar en l'informe final d'auditoria detalls d'arquitectures, etc.).

Test d'intrusió

Cal recordar que un test d'intrusió és una auditoria de seguretat de tipus tècnic sense coneixement previ de l'equip auditor.

4) Avaluació de risc. Els anteriors tipus d'auditories es refereixen a avaluacions purament tècniques de la seguretat; no examinen en cap cas la implantació de controls que són aplicables als processos organitzatius en l'auditat. No obstant això, sabem que els controls de seguretat poden ser de diferents tipus. Aquest tipus d'auditoria es combinarà amb auditories d'escaneig de seguretat i es farà específicament una avaluació del risc combinant aquests resultats tècnics amb entrevistes i investigació de nivell mitjà, que inclou la justificació de negocis, les justificacions legals i les justificacions específiques de la indústria.

5) Auditoria de seguretat. Des del punt de vista eminentment tècnic, l'OSSTMM entén l'auditoria de seguretat com una auditoria tècnica de la seguretat dels sistemes d'informació i, per tant, fa referència a la inspecció manual amb privilegis administratius del sistema operatiu i dels programes d'aplicació del sistema o dels sistemes dins d'una xarxa o xarxes. Per tant, com més extensa sigui la infraestructura i més exhaustiva sigui l'auditoria volguda, més recursos d'auditoria es requeriran.

6) *Hacking* ètic. Es refereix generalment als tests d'intrusió, l'objectiu dels quals és obtenir trofeus a la xarxa dins del temps predeterminat de durada del projecte. La diferència amb els tests d'intrusió és que la seva durada pot ser més gran, ja que es combinaran diferents tècniques.

Tècniques de *hacking* ètic

Les tècniques que es poden emprar en les auditories de *hacking* ètic són tan dispars com l'enginyeria social o l'anàlisi de vulnerabilitats.

7) Test de seguretat. Finalment tindrem les auditories similars a una avaluació de risc, però amb un abast més ampli que no es limita a les implicacions tècniques, legals i de normativa del sector. S'avaluaran els diferents processos de negoci que influeixin sobre la seguretat de la informació sota l'abast de l'auditoria.

Avaluació de postura

L'avaluació de postura és l'equivalent militar dels tests de seguretat.

El coneixement del tipus d'auditoria que s'ha de fer permetrà a l'equip auditor determinar i pactar amb l'auditat l'abast de l'auditoria, els terminis per a executar-la i els recursos necessaris.

4. Planificació d'una auditoria tècnica de seguretat

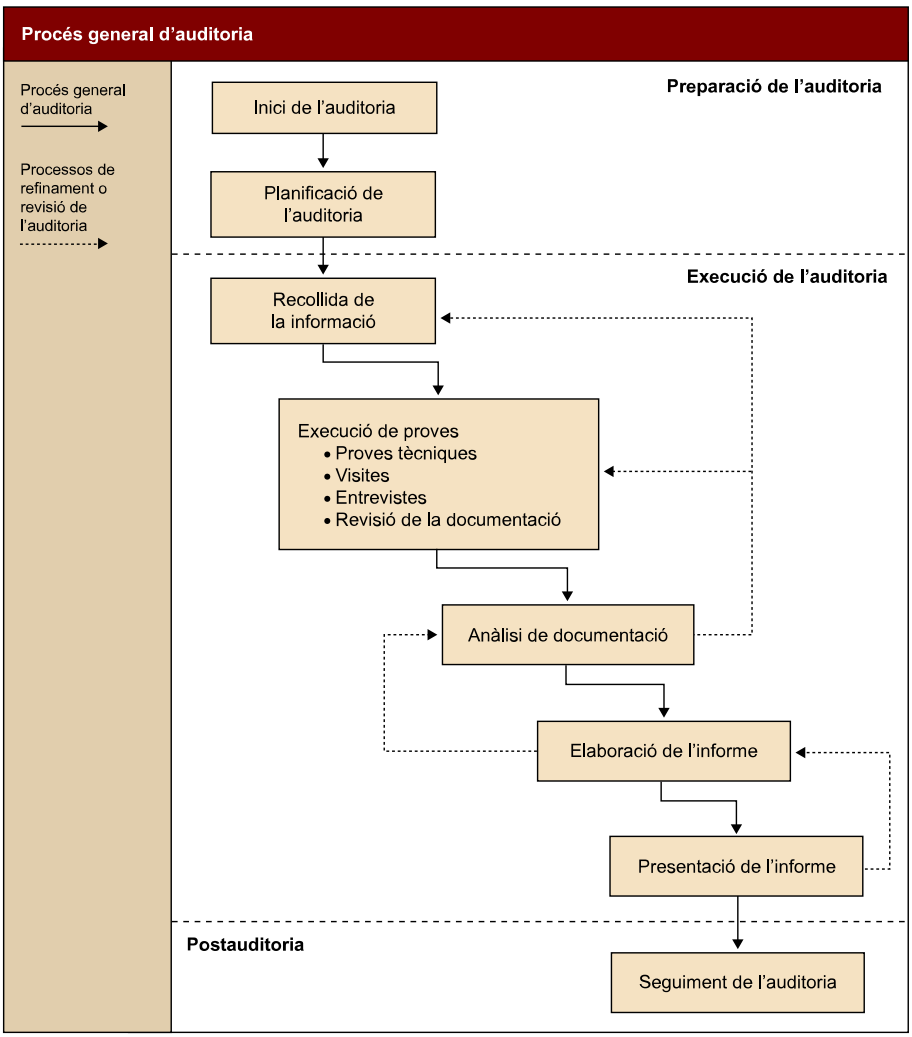
La planificació d'auditoria que us proposem aquí és genèrica i cada equip auditor l'haurà d'aplicar al seu cas particular. No obstant això, podem afirmar que per a adherir-se a les metodologies més reconegudes, sigui quin sigui el tipus d'auditoria que s'hi afronti, s'hauran d'executar les fases següents:

Vegeu també

La planificació d'auditoria apareix descrita en el mòdul 4.

- Definició del pla d'auditoria i iniciació del projecte
- Execució de l'auditoria
- Recol·lecció d'informació prèvia
- Execució de les proves d'auditoria
- Anàlisi de la informació
- Elaboració i presentació de l'informe
- Seguiment de l'auditoria

L'esquema general d'una auditoria seria el que mostra el diagrama següent.



Procés general d'una auditoria

Cal destacar que aquesta organització de l'auditoria està recollida també en l'estàndard per a l'auditoria de sistemes de gestió ISO 19011, per la qual cosa podem concloure que el procés d'auditoria té aspectes independents de l'objecte que s'està auditant.

Examinem una mica més detalladament quines activitats s'inclouran en cadascuna d'aquestes fases.

4.1. Definició del pla d'auditoria

Una vegada establert amb l'auditat l'abast de l'auditoria, s'hauran de fer les accions següents:

Establiment de l'abast

L'abast d'una auditoria es plasma en un document en cas que l'equip auditor sigui extern, per exemple en una oferta de prestació de serveis professionals, o s'estableix per a la creació d'un projecte intern d'auditoria, en el cas d'una auditoria interna.

a) L'equip auditor haurà d'obtenir el compromís i el suport de la direcció de l'organització auditada per dur a terme l'acció d'auditoria.

Nota

És convenient que l'acord de confidencialitat sigui revisat per un assessor legal per tal que inclogui tots els aspectes legals, com per exemple, la protecció de dades de caràcter personal.

El document de compromís per part de la direcció

En cas que es faci una auditoria externa, s'hi ha de reflectir el compromís de l'auditor amb el deure de secret professional. Aquest tipus de document se sol denominar ***acord de confidencialitat*** (en anglès, *non-disclosure agreement*). Si es tracta d'auditories internes, l'habitual serà que tot el personal de l'organització hagi signat un acord de confidencialitat en els termes que hi siguin aplicables segons les funcions laborals que han de dur a terme.

Se sol denominar ***carta d'auditoria*** o ***carta d'assignació d'auditoria*** el document que descriu l'assignació de tasques que l'equip auditor ha de dur a terme. S'hi indiquen temes com l'objectiu de l'auditoria, l'abast, els criteris per a determinar l'èxit o no de l'auditoria, el material que s'ha de lliurar en finalitzar l'auditoria, el nivell d'accés a la informació que es facilitarà a l'auditor, els procediments de comunicació entre l'auditor i l'auditat, etc. Quan es tracta d'auditories de tipus tècnic, hi ha un altre aspecte que cal establir: el tipus de proves i la manera com es desenvoluparan. Això és especialment important en cas que s'hagin d'incloure proves que puguin causar la interrupció d'algun servei. En aquests casos, gràcies a aquest document, l'equip auditor es trobarà lliure de responsabilitats.

En una auditoria externa, aquest document no se sol denominar *carta d'auditoria* i el contingut acostuma a estar establert en la mateixa oferta de serveis professionals. Però, en el cas d'una auditoria interna, l'estatus de l'auditor pot quedar indefinit i, per tant, és molt important que la direcció que impulsa l'acció d'auditoria doni suport oficialment a l'equip auditor mitjançant la signatura d'aquest tipus de document d'ús exclusivament intern.

b) L'equip auditor haurà de definir el pla d'auditoria. Aquest ha de determinar amb exactitud el següent:

- Terminis temporals:
  - Dates d'inici i finalització dels períodes de prova.
  - Períodes del dia per a fer les proves.
  - Periodicitat del pla d'auditoria. Establir la periodicitat converteix el pla en un programa d'auditoria (pot estar lligat al contingut d'algun element d'SGSI).

- Procediments de comunicació amb els responsables de projecte en l'auditat, especialment per a la comunicació del descobriment de vulnerabilitats crítiques o situacions de frau, així com qualsevol protocol que pugui sol·licitar o necessitar l'auditat sobre comunicació d'inici i fi de proves, especialment quan es tracta de proves tècniques en entorns productius.

- Inventariat de les polítiques corporatives que afectin l'auditoria i que han de ser comprovades pel procés d'auditoria.

- Documentació de les proves que s'han de fer, indicant-hi:

- Objectiu de la prova: es tracta d'identificar quin requisit de les polítiques de seguretat de l'auditat, o en cas que no n'hi hagi, quin requisit d'un catàleg de bones pràctiques s'ha d'auditar. Per aquesta raó en aquesta fase l'equip auditor haurà d'estudiar les polítiques i els catàlegs de bones pràctiques que siguin aplicables a l'abast de l'auditoria.

- Manera com es farà la prova: descripció, almenys succinta, del procediment i de les tècniques d'auditoria que s'hi aplicaran per a comprovar el requisit o els requisits auditats.

- Eines o requisits específics necessaris per a fer la prova.

Documentació de proves

Cal notar que si l'abast de l'auditoria és molt ampli, la documentació de les proves pot ser un procés molt laboriós. Òbviament, el treball previ no ha de sobrecarregar l'esforç total dedicat a l'auditoria. Per tant, la documentació de les proves s'ha de fer d'una manera proporcionada a l'esforç total. Si l'abast és molt ampli, les proves que s'han de fer es poden descriure d'una manera més general, encara que no se n'haurà de sacrificar l'exhaustivitat a l'hora de cobrir les àrees comprovades; potser sí que es podrà descriure cada tipus de prova d'una manera no totalment descriptiva i ser més indicatiu de l'objectiu de la prova i de les tècniques que s'hi apliquin.

El pla d'auditoria haurà d'estar aprovat tant pel cap de l'equip auditor com per l'entitat auditada.

Cas pràctic: pla d'auditoria

Una entitat financera ha desenvolupat una nova aplicació bancària per a ús dels seus clients a través d'Internet. Es tracta d'una aplicació en tres capes amb un frontal (*front-end*) constituït per un servidor web. Abans de passar l'aplicació a producció, i en el marc de les proves d'acceptació d'usuari, la direcció vol que una entitat externa faci una auditoria de seguretat de l'aplicació.

L'equip auditor, una vegada signats els acords de confidencialitat i la carta d'auditoria materialitzada en l'oferta de serveis professionals, facilita a la direcció de l'auditat un pla d'auditoria amb el contingut (resumit) següent:

Pla d'auditoria d'una aplicació web

1. Informació general

1.1. Objectiu del pla

L'objectiu general de l'auditoria que s'ha de fer serà identificar errors de programació o de configuració en l'aplicació BANCA-*ONLINE* accessible des del portal del banc XXXX en l'URL: http://banca-online.xxxx.com.

L'objecte d'aquest document és recopilar els diferents aspectes que s'han de revisar dins de l'aplicació sota auditoria. S'hi han de descriure tots els aspectes rellevants que es revisaran.

Aquest document constituirà la guia que es farà servir per a la coordinació entre equip auditor i XXXX a l'hora de planificar, programar les proves que s'han de dur a terme i gestionar les autoritzacions que calguin per a l'auditoria.

Aquest pla no pretén recopilar el detall de totes i cadascuna de les proves que es faran, sinó que l'objectiu és descriure detalladament l'estratègia de prova que se seguirà. Aquesta estratègia està basada en els principis per a la programació segura d'aplicacions web descrits per l'organització independent Open Web Application Security Project (OWASP). Per tant, s'hi descriuran detalladament el tipus de proves que es faran, encara que no s'hi indicarà explícitament en quines parts de l'aplicació es faran les proves perquè l'abast és massa ampli.

1.2. Abast

Aquesta auditoria se cenyirà a revisar els controls de seguretat aplicats en la capa d'aplicació, és a dir, no s'analitzarà la plataforma tecnològica que dóna suport a l'aplicació (sistema operatiu o altres aplicacions diferents de les mateixes aplicacions, com per exemple servidors web, servidors d'aplicacions, etc.), tret que la direcció de

projecte de XXXX indiqui el contrari; en aquest cas, s'actualitzarà aquest document. Sí que s'ha de destacar que la determinació de la plataforma tecnològica emprada constitueix una de les proves que s'han de fer perquè constitueix una de les informacions emprades per a les proves subsegüents. No obstant això, una vegada determinada, no es verificaran les possibles vulnerabilitats que pugui tenir aquesta plataforma.

Aquest pla d'auditoria s'executarà previsiblement entre les dates DD/MM/AAAA i DD/MM/AAAA.

Nota

El més apropiat seria que l'equip auditor donés un cronograma del desenvolupament de les proves, però almenys com a mínim s'ha de donar un marc temporal delimitat per a la fase de proves.

1.3. Visió general del sistema sota prova

El sistema sota prova es correspon amb el següent:

- L'aplicació sota estudi és accessible des del portal de XXXX en l'URL: http://www.xxxx.com a partir de l'enllaç: http://banca-online.xxxx.com
  Es revisarà l'aplicació de BANCA-*ONLINE* en la part d'operativa destinada a clients particulars, i se n'exclouran se expressament totes les operatives destinades a empreses o relacionades amb la gestió de valors cotitzats en borsa.
  No es faran proves que puguin afectar sistemes no inclosos sota l'abast de l'auditoria.

- L'aplicació facilita accés a totes les operatives de l'aplicació BANCA-*ONLINE* i permet comprovar-ne el funcionament.

- L'aplicació es troba a PRODUCCIÓ; per tant, totes les proves es coordinaran amb XXXX mitjançant la gestió de les autoritzacions apropiades en els casos que consideri necessari l'equip de projecte conjunt d'EQUIP AUDITOR i XXXX amb els departaments adequats.

1.4. Documents de referència

Per a la redacció d'aquest document s'han pres com a referència els documents següents:

- Oferta del projecte <codi identificatiu de l'oferta.

- Guia OWASP en la seva versió oficial i estable: conté la descripció dels aspectes que es comprovaran en aquest projecte.

- Guia OWASP de verificació en la versió oficial i estable: conté una relació del marc de prova i de les proves que s'han de fer en una aplicació web.

2. Procediments de control de les proves

2.1. Entorn de prova requerit

Per a dur a terme les proves anteriorment descrites cal l'entorn següent:

- Les aplicacions de BANCA-*ONLINE* de XXXX (en la versió clients particulars) han d'estar actives durant el període que es determini per a la realització de les proves.

- Un o més llocs clients des d'on es faran les proves interactuant amb l'aplicació a partir de comunicacions sobre Internet. Aquests llocs estaran situats a les instal·lacions d'EQUIP AUDITOR al c/ YYYYYY. L'adreça IP des de la qual es faran les proves és: XXX.XXX.XXX.XXX

- En els llocs clients s'utilitzarà el programari d'auditoria necessari per a fer les proves. En la definició de cadascuna de les proves es detallaran les eines necessàries.

- Procediment de comunicació d'inici i fi de proves. Com que l'entorn a prova és un entorn en producció i està monitoritzat amb eines de seguretat, és necessari que, abans d'iniciar qualsevol prova, es planifiqui la intervenció amb el centre de control operatiu. Amb anterioritat a la data prevista per a les proves, se n'haurà d'obtenir l'autorització i un número d'intervenció. A l'inici de les proves, es comunicarà al centre de control operatiu mitjançant l'enviament d'un correu electrònic a l'adreça soc@xxxxx.com, informant del nom de l'empresa auditora, la persona de contacte en l'organització, el número d'intervenció, l'adreça IP (una o

diverses), una indicació de si es realitzaran proves automatitzades i un telèfon de contacte per a casos d'emergència. Igualment, es realitzarà una trucada telefònica al 902xxxyyy informant del número d'intervenció. En finalitzar el termini previst per a les proves, es comunicarà la finalització mitjançant un correu electrònic a l'adreça indicada anteriorment.

2.3. Gestió de les incidències

En cas que durant l'execució del pla d'auditoria es detecti una vulnerabilitat greu que pugui comprometre la seguretat (confidencialitat, disponibilitat o integritat) de l'aplicació, s'han de comunicar a XXXX la incidència i les circumstàncies que la van provocar.

Abans de l'inici de l'execució de les proves s'hauran de determinar amb exactitud els procediments que s'utilitzaran, els *point of contact* (POC) adequats i els períodes en què estaran disponibles i els mitjans que es faran servir en cada cas. En cas que XXXX tingui ja definida una manera de procedir, s'acturarà de la manera que es tingui prevista en aquests procediments. En cas contrari, es procedirà de la manera següent:

1) El procediment de comunicació urgent de les incidències s'activarà quan un auditor d'EQUIP AUDITOR detecti, ja sigui mitjançant la realització d'una prova, o bé per qualsevol altra circumstància, una vulnerabilitat greu.

S'entén per *vulnerabilitat greu* qualsevol aspecte del funcionament de l'aplicació que causi:

- Una filtració d'informació confidencial
- Una modificació no autoritzada d'informació
- Un malfuncionament de l'aplicació que causi, o pugui causar si fos explotada de manera adequada, una denegació de servei
- En general, qualsevol incident que pugui situar el sistema en un estat inoperable.

En aquest cas i una vegada comprovada l'existència de la vulnerabilitat, l'auditor es posarà en contacte amb el POC per les vies previstes per a informar de la situació i les circumstàncies que ho provoquen.

2) El detall de la incidència es documenta en l'informe d'auditoria.

3. Definició de les proves

A continuació es presenten el conjunt de proves que es faran per a l'auditoria dins de l'abast determinat anteriorment.

3.1. Estratègia de prova

Aquest pla d'auditoria se centra en la comprovació de la implementació dels controls de seguretat en la capa d'aplicació, és a dir, en els controls que la mateixa aplicació ha d'implementar per a garantir la confidencialitat, integritat i disponibilitat de la informació que és tractada des d'aquesta. Com que l'aplicació que es pretén auditar té una arquitectura de tres capes basada en tecnologies web, s'ha pres com a referència la metodologia OWASP. Aquesta metodologia ens facilita una guia detallada amb els conceptes necessaris per a dissenyar, desenvolupar, desplegar o auditar aplicacions web. Per tant, l'estratègia emprada per a dissenyar les proves d'aquest pla d'auditoria deriva d'aquesta metodologia.

D'aquesta manera, s'han organitzat diferents fases de proves amb objectius diferents que detallem a continuació:

- INF - Recollida d'informació
- LOG - Estudi de la lògica de negoci
- AUT -; Revisió del procés d'identificació i autenticació
- SES - Revisió de la gestió de sessions
- VAL - Revisió de la validació de les dades d'entrada
- DOS - Revisió de situacions de denegació de servei

3.2. Recollida d'informació

L'objectiu d'aquesta fase és la comprovació de la informació relativa a l'aplicació auditada que es pot obtenir de manera legítima emprant els diversos canals existents a Internet.

3.2.1. Prova [INF-001] - Identificació del servidor web

Requisit a provar

Identificar el tipus de servidor web que allotja la capa de presentació de l'aplicació. Si es determina correctament la versió exacta del programari del servidor web, es poden determinar les vulnerabilitats públiques existents en el moment de l'auditoria i la política d'apedaçament/manteniment dels sistemes de suport de l'aplicació.

Descripció de la prova

Connectar amb el servei HTTP en el port 80 (o un altre si s'utlitza) i determinar l'aplicació i versió del servidor web. Per a això s'utilitzaran les eines següents:

- Netcat. Per a recollir el bàner exposat pel servidor.
- HTTPRINT. Per a examinar la resposta del servidor a diverses peticions http i comparar-la contra diverses "firmes" mantingudes en el catàleg de l'aplicació HTTPRINT.

Resultats esperats

S'hauran d'identificar els aspectes següents:

- Nom de l'aplicació
- Fabricant
- Versió
- Nivell d'apedaçament

3.2.2. Prova [INF-002] - Identificació de l'aplicació

Requisit a provar

Identificar totes les aplicacions web / portals servits des d'un servidor web concret.

Quan l'objectiu de l'auditoria consisteix en la comprovació de manera general de la seguretat d'una infraestructura, és important inventariar i identificar les diferents aplicacions que s'ofereixen, ja que cadascuna és susceptible de ser examinada de manera diferent. En cas que ja estigui determinada l'aplicació que s'ha d'auditar, aquesta prova no tindrà sentit.

Descripció de la prova

1) Investigar si hi ha diferents URL base que allotgen diferents aplicacions web.

2) Investigar si en la IP hi ha altres aplicacions instal·lades en altres ports diferents dels estàndards (80, 443, 8080, 8000). Emprar per a això l'eina NMAP.

3) Per a identificar hosts virtuals i trobar noms de dominis assignats a la IP auditada:

- Comprovar la possibilitat de fer transferències de zona en el servidor DNS del domini examinat
- Comprovar la possibilitat de fer una resolució inversa de noms (*reverse DNS query*)
- Connectar amb serveis a Internet per a examinar registres DNS, o directament cercadors tradicionals.

Pàgines web

Algunes "eines": www.live.com, www.dnsstuff.com, www.google.com, etc.

Resultats esperats

S'hauran d'identificar, per a cadascuna de les IP examinades dins de l'àmbit del projecte, els dominis, els subdominis i els URL d'entrada a les aplicacions identificades.

El pla continuaria amb tot el detall de les proves que s'han de fer.

4.2. Execució de l'auditoria

Una vegada que l'equip auditor i l'auditat han aprovat el pla d'auditoria, els auditors estan en disposició d'iniciar el seu treball.

Malgrat que l'execució és completament depenent de l'abast, l'enfocament i el tipus d'auditoria, podem identificar certes fases que es compleixen de manera general en qualsevol tipus d'auditoria.

A continuació repassarem les subfases que componen l'execució de l'auditoria.

4.2.1. Recol·lecció d'informació prèvia

Aquesta subfase permetrà a l'equip auditor preparar l'execució de les proves identificades en el pla d'auditoria. Les activitats que es duran a terme inclouen:

- Recopilar tota la informació rellevant per a entendre correctament l'entorn que s'ha d'auditar:
  - Els requisits del negoci i els riscos associats.
  - Lleis i regulacions.

- Identificació de càrrecs/rols/funcions per a detectar les entrevistes necessàries i el personal que hi haurà d'assistir:
  - L'estructura organitzacional.
  - Els rols i les responsabilitats.

- Identificació i estudi de la documentació existent de l'auditat que sigui rellevant per a l'auditoria:
  - Polítiques i procediments.
  - Descripció dels entorns de tractament de la informació i estudi de les vulnerabilitats conegudes que hi siguin aplicables.
  - Descripció de les mesures de control establertes.

4.2.2. Execució de les proves d'auditoria

Una vegada recopilada tota la informació necessària, l'equip auditor desenvoluparà de manera efectiva el conjunt de proves documentades en el pla d'auditoria. Tal com s'ha comentat, per a la realització d'una auditoria de seguretat, segons l'abast, l'enfocament i el tipus, les proves que s'hi han de practicar seran:

- **Revisió de la documentació**, com per exemple les polítiques que s'han d'auditar per a comprovar-ne la idoneïtat, tenint en compte l'entorn de

l'auditat i les millors pràctiques reconegudes per la indústria. Així mateix, s'ha de revisar un altre tipus de documentació rellevant per al projecte, com ara inventaris, documents de disseny, procediments operatius, etc.

- **Realització d'entrevistes** per a comprovar si el personal coneix les polítiques i les aplica. Poden ser necessàries diverses entrevistes dins d'un mateix nivell funcional, amb l'objectiu de detectar incongruència, oblits o intents d'amagar la manera habitual de procedir.

Desenvolupament de l'entrevista

Les entrevistes es desenvoluparan habitualment en instal·lacions pròpies de l'auditat per a interrompre el menys possible les operacions normals de l'organització i s'hauran de fer sempre al personal més representatiu i més ben preparat per a cobrir els aspectes que es volen analitzar. El desenvolupament de les entrevistes s'ha de fer en un to no amenaçador per a l'entrevistat i, encara que es tracti d'una auditoria, s'ha de transmetre la idea que constitueix una oportunitat per a millorar algun aspecte de la seguretat i/o l'eficiència dels procediments.

- **Execució de proves tècniques** per a comprovar la manera com estan implantats els controls tècnics d'acord tant amb les polítiques com amb les bones pràctiques de la indústria. Les àrees més habituals que s'examinaran en aquest tipus de proves seran:
  - Funcionament dels sistemes i les comunicacions (amb especial importància per al control i l'ús d'accessos remots).
  - Configuració dels sistemes (servidors, llocs de treball o elements de la infraestructura de comunicacions).
  - Revisió de registres d'activitat de sistemes.

  Durant l'execució d'aquestes proves és possible que l'equip auditor detecti vulnerabilitats tècniques que, per la seva criticitat especial, s'hauran de transmetre amb agilitat a l'auditat.
- **Realització de visites** per a examinar aspectes de seguretat física i/o comprovar *in situ* la manera com actuen els sistemes d'informació.

És important que a mesura que es desenvolupa el pla d'auditoria, l'equip auditor vigili si, d'acord amb la nova informació que es va adquirint, no hi ha canvis substancials que impliquin, o bé una modificació de l'abast, o bé l'execució de proves diferents de les inicialment plantejades. En un primer moment, aquests punts han de ser discutits per l'equip internament i posteriorment concretats amb l'auditat, ja que poden implicar la necessitat de dotar de més recursos l'auditoria.

4.2.3. Anàlisi de la informació

En realitat, el procés d'anàlisi s'inicia des del mateix moment en què comença l'execució de l'auditoria i únicament finalitza amb l'acceptació per l'auditat de l'última revisió de l'informe d'auditoria. No obstant això, quan el desenvolupament de les proves es troba en un estat avançat, l'equip auditor les haurà de

compaginar amb l'anàlisi de la informació recopilada. Aquesta anàlisi feta en paral·lel amb l'execució de proves permet anar refinant les successives proves, tant les purament tècniques com aquelles altres que requereixin noves entrevistes, visites o documentació addicional de l'auditat.

Durant la fase d'anàlisi, un dels aspectes que l'auditor haurà d'anar avaluant és la importància relativa o el risc de no-conformitat del problema que detecti. En aquest sentit haurà d'emprar tècniques d'anàlisis de risc consistents a aplicar la coneguda equació del risc:

El risc és proporcional a tres factors:

- Al valor de l'actiu d'informació involucrat.
- A la probabilitat que una amenaça pugui aprofitar una vulnerabilitat o problema que hem detectat durant l'auditoria.
- A l'impacte que pugui arribar a provocar l'explotació de la vulnerabilitat.

Per a poder valorar adequadament les proves oposades en l'auditoria i poder relativitzar-les, serà necessari fer aquest exercici. Cal destacar que, per a la valoració de constatacions d'auditoria referents a vulnerabilitats en sistemes d'informació, hi ha un mètode àmpliament utilitzat, el *common vulnerability scoring system* (CVSS), que tractarem en el mòdul 5.

A l'hora d'analitzar la informació recopilada, podem, d'una manera general, separar-la en dues grans àrees:

1) Revisió de polítiques. Tal com hem exposat moltes vegades (no ens cansarem de repetir-ho), la pedra angular d'un programa efectiu de seguretat de la informació són les seves polítiques de seguretat, tant les generalistes com les més específiques dissenyades amb un abast reduït orientat a una temàtica o un entorn de sistemes d'informació determinat, ben redactades, comunicades i completes. Aquestes polítiques serveixen d'origen per a tota la resta de documentació: directives, estàndards, procediments, guies, etc. Per tant, és important analitzar-les amb l'objecte de respondre a les preguntes següents:

- Existeixen i són a l'abast del personal que hi està afectat?

- Com n'és de bo el seu contingut? En aquest sentit és important que les polítiques siguin concises, clares i no han de generar confusió i introduir nous problemes en l'organització. La qualitat i l'efectivitat d'una política ens les determinarà la manera com es responguin les preguntes següents (les 5 W del periodisme):
  - ***W**hat*: quina és la temàtica de la política i quin és l'actiu d'informació que es pretén protegir?

- ***Who***: qui és el responsable d'emetre la política i qui hi està afectat?
- ***Where***: a quines parts de l'organització afecta la política?
- ***Why***: per què és rellevant la política?
- ***How***: com es protegeix l'actiu d'informació?

2) Revisió de la informació recopilada durant les proves. Les proves tindran un caràcter essencialment tècnic, però també s'hauran d'analitzar els resultats d'entrevistes i visites, per a contestar les preguntes: com es distribueixen, com es comuniquen i com s'apliquen les polítiques de seguretat? Com en són d'efectius els controls de seguretat?

Domini del procés d'anàlisi

El procés d'anàlisi d'aquest tipus d'informació és tan ampli i respon a unes casuístiques tan diverses, que és difícil dominar-lo mitjançant un llibre o una metodologia.

De manera general podem destacar que l'anàlisi dels resultats ha de buscar identificar el següent:

- Incompliments dels controls de seguretat implantats que s'haurien de trobar documentats en les polítiques.

- Vulnerabilitats en la manera com estan implantats els controls, especialment quan es tracta de controls la implantació dels quals es fa per mitjans tècnics.

D'aquesta manera, l'anàlisi dels resultats de les proves proporcionarà la visió de l'efectivitat i l'eficiència dels controls de seguretat.

4.3. *Reporting* de l'auditoria

Una vegada fetes les diferents proves planificades i l'anàlisi de la informació obtinguda, l'equip auditor està en disposició de transmetre al client auditat les conclusions de l'auditoria. Aquesta fase és crítica, ja que un equip auditor amb capacitat insuficient de transmetre les seves conclusions al client no aconseguirà cobrir els objectius de l'auditoria.

Els auditors han d'elaborar un informe tan simple i directe com sigui possible, i sempre facilitant la informació rellevant, i les diferents constatacions. Al mateix temps, ha de facilitar de manera senzilla la manera de resoldre les deficiències que s'hi han trobat.

L'informe final d'auditoria pot seguir qualsevol esquema, però el triat ha d'incloure o tractar d'una manera o una altra els aspectes següents:

1) Resum executiu. Quan es desenvolupa l'informe, i una vegada analitzada la informació recollida durant l'auditoria, és recomanable començar per aquest punt, ja que la direcció pot requerir una primera versió de les conclusions d'auditoria. Sovint, aquesta part de l'informe és l'única que llegiran alguns dels seus destinataris, per la qual cosa n'haurà de reflectir de manera resumida el contingut. Per tant, inclourà una introducció, una visió general de la metodo-

logia emprada, les principals conclusions que se n'hagin obtingut i les recomanacions més rellevants que l'equip auditor pugui donar. El llenguatge emprat serà el més directe i comprensible per a un públic ampli.

És recomanable incloure en el resum executiu tant les fortaleses com les debilitats o fallades detectades per a facilitar una conclusió mesurada de l'auditoria.

2) Metodologia emprada. S'ha de fer una explicació breu de la metodologia que s'ha emprat. S'ha de fer referència als estàndards que s'han utilitzat, o bé, si s'utilitzen estàndards propis, s'han d'explicar i s'han de detallar els objectius, les fases i les tècniques que s'han utilitzat per a fer l'auditoria. El receptor de l'informe ha de conèixer amb quins criteris i de quina manera s'ha fet el treball. En aquest apartat pot fer referència al pla d'auditoria si constituïa un lliurable de l'assignació d'auditoria (que encara que sempre ha d'existir, almenys internament, per a l'equip auditor, pot ser que no sempre es lliuri a l'auditat) o, si no n'hi ha, una explicació de les proves sense entrar en tots els detalls. Es consignaran les entrevistes que s'haguessin realitzat (persones, llocs i dates), les proves tècniques realitzades amb els seus respectius objectius i les eines emprades, així com els terminis en els quals van tenir lloc les proves.

3) Llista detallada de les constatacions. Aquest apartat contindrà detalladament els resultats del procés d'auditoria, que no s'han de confondre amb els resultats de les proves d'auditoria. Com a resultat, es recolliran totes les troballes realitzades, tenint molt en compte que l'auditor ha d'entendre bé la diferència entre una troballa i un resultat d'una prova. No sempre hi ha una relació directa 1 a 1 entre prova d'auditoria i troballa, ja que els resultats de diverses proves poden posar de manifest un incompliment d'una política o una mala implementació d'un control. Per exemple, la detecció de múltiples pedaços (*patch*) sense instal·lar no implica una troballa per cadascun d'ells, sinó una única troballa que seria el manteniment incorrecte del sistema. A l'informe només s'hi han de consignar les troballes, mentre que, si s'estima oportú i interessant, els resultats de les proves es recollirien en un annex tècnic a l'informe. La manera concreta com s'organitzi aquest apartat dependrà exclusivament de l'abast de l'auditoria i del detall al qual s'hagi arribat. Per claredat és recomanable facilitar inicialment un llistat de les troballes indicant-ne la classificació respecte a la importància i posteriorment, en fulls independents, cada troballa de manera separada i amb més detall. De cada troballa s'haurà d'indicar quina és la problemàtica (política que s'incompleix, vulnerabilitat trobada, etc.) de la qual s'han trobat evidències i es mostraran aquestes (sense entrar en el detall de com es van obtenir, què pot deixar-se per a un annex tècnic amb els resultats de les proves). És convenient facilitar una avaluació de la importància o l'impacte que podria causar en l'organització i d'aquesta manera classificar-ne la criticitat. La tècnica emprada és l'esmentada anteriorment en la fase d'anàlisi: estimar el risc fent ús d'alguna de les metodologies d'anàlisi

de riscos, encara que com més senzilla i fàcil de transmetre a l'auditat, millor. Aquesta informació es podrà incloure en l'informe. És de gran utilitat donar una classificació de la importància de les constatacions, ja que serà emprada pel destinatari de l'informe per a fer el seguiment de la resolució o millora.

Subjectivitat de la classificació de les constatacions

No s'ha de perdre de vista que la classificació de la criticitat d'una constatació és sempre un acte subjectiu que, malgrat que sigui necessària una opinió de l'auditor, sempre hauria de ser pactat amb l'auditat, ja que ell és el millor coneixedor del possible impacte en el seu negoci de la constatació.

Exemple de classificació de les constatacions

Una possible classificació de les constatacions podria ser la següent:

ID	Nivell	Explicació
5	Crític	Necessita una resolució immediata.
4	Important	S'ha de resoldre quan sigui possible (per exemple, planificar una propera parada del sistema, a fi de resoldre el problema).
3	Moderadament important	Ha de ser gestionat de la manera que el client consideri convenient, utilitzant els seus procediments de canvi, però no ha de ser ignorat ni assumit per l'organització.
2	Lleugerament important	Ha de ser gestionat en la propera "reconfiguració" planificada, però no ha de ser ignorat ni assumit per l'organització.
1	A títol informatiu en aquest moment	És recomanable que sigui gestionat en la "reconfiguració" planificada i no és recomanable que sigui ignorat, encara que podria ser assumit per l'organització després de la seva avaluació mitjançant una anàlisi de riscos.

4) Annexos. En els annexos s'ha de recopilar la informació que doni suport a les constatacions descrites en el cos de l'informe. Per tant, han d'incorporar les sortides de les eines que s'utilitzen, els resultats de les llistes de control (*checklist*) que s'hagin dut a terme, les actes de les reunions que s'hagin fet, etc. També hi han d'incloure els detalls de la resolució recomanada a les constatacions quan per la seva complexitat requereixin una explicació més extensa.

El cos de l'informe no s'ha de saturar d'informació que, malgrat que sigui rellevant i útil per la profunditat i el detall exhaustius, en podria sobrecarregar el contingut i desviar l'atenció del destinatari del contingut de la constatació cap als detalls del descobriment o la resolució.

4.4. Seguiment de l'auditoria

Una vegada feta l'auditoria i lliurat l'informe, la responsabilitat d'adoptar les mesures que es recomanin recau en l'organització auditada. No està exclosa la participació de l'equip auditor en les tasques o en els projectes que se'n derivin; encara que la seva capacitat per a involucrar-s'hi és molt alta i participa

en tasques d'implementació, la seva independència pot quedar compromesa a l'hora de tornar a auditar l'organització. Per tant, el més habitual és que l'equip auditor assisteixi l'organització en la presa de decisions, en el seguiment de les activitats que se'n derivin i, una vegada finalitzada la implantació de recomanacions, en la revisió de la implantació de les recomanacions.