ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

RIC-STIC-002
Guia d'Auditoria Infraestructures Crítiques

Fitxa del document

Títol	Guia d'Auditoria Infraestructures Crítiques

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	Gener 2025	

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi
1.1	27	30/07/2024	Canvis realitzats per les modificacions efectuades en el RIC-AD, pel que es disposa en el Decret [...], del [...], de modificació del Decret 418/2022, del 12-10-2022, d'aprovació del Reglament de Infraestructures Crítiques Principat d'Andorra: - Introducció dels calendaris de compliment a aplicar al RIC-AD. - Modificació del tipus d'auditoria i de l'equip d'auditoria.

Propietari del document: ANC-AD

PRÒLEG

L'ús massiu de les tecnologies de la informació i les telecomunicacions (TIC), en tots els àmbits de la societat, ha creat un nou espai, el ciberespai, on es produiran conflictes i agressions, i on hi ha ciberamenaces que atemptaran contra la seguretat nacional, l'estat de dret, la prosperitat econòmica, l'estat de benestar i el normal funcionament de la societat i de les administracions públiques i entitats privades.

La Llei 22/2022, de 9 de juny, , encomana a l´Agència Nacional de Ciberseguretat d´Andorra (ANC-AD) l'exercici de les funcions relatives a la seguretat de les tecnologies de la informació, i de protecció de les xarxes d´ informació alhora que confereix Secretari d'Estat de Transició Digital i Projectes Estratègics la responsabilitat de dirigir l´ANC-AD.

En definitiva, la sèrie de documents RIC-STIC s'elaboren (adaptats del CCN-CERT i del CNPIC) per donar compliment a les comeses de l´Agència Nacional de Ciberseguretat d´Andorra, conscients de la importància que té l' establiment d' un marc de referència en aquesta matèria que serveixi de suport perquè el personal de les entitats afectades, i en ocasions, ingrata tasca de proporcionar seguretat als sistemes de les TIC sota la seva responsabilitat.

Marc Rossell i Soler
Secretari d'Estat de Transformació digital i Telecomunicacions

ÍNDEX

1. MARC DE REFERÈNCIA

1. Aquesta guia estableix unes pautes de caràcter general que són aplicables a entitats de diferent naturalesa, dimensió i sensibilitat sense entrar en casuístiques particulars. S'espera que cada organització les particularitzi per a adaptar-les al seu entorn singular.
2. Aquesta guia d'auditoria del Reglament de Infraestructures Crítiques del Principat d'Andorra (d'ara endavant, el "RIC-AD"), s'enquadra dins dels requisits de Llei 22/2022, del 09 de juny, i el decret 417/2022 de 19 d´octubre de 2022, de mesures per a la seguretat de les xarxes i dels sistemes d'informació (d'ara endavant la "Llei NIS-AD"). Així mateix, està Guia d'Auditoria, està subjecta a una modificacions segons el determinat en el Decret [...], del [...], de modificació del Decret 418/2022, del 12-10-2022, d'aprovació del Reglament de Infraestructures Crítiques Principat d'Andorra.
3. Amb el present document es pretén orientar a aquelles infraestructures designades com a essencials en l'elaboració del seu informe d'auditoria.
4. En aquesta guia s'inclouen una sèrie de mesures organitzatives o gestió, operacionals o procedimentals, protecció o tècniques, que podran ser referents d'ajuda als operadors crítics per a la confecció d'algun dels punts dels continguts mínims del seu informe d'auditoria.

2. OBJECTE DE L'AUDITORIA

5. Donar compliment al que s'estableix al RIC-AD.
6. Emetre una opinió objectiva, basada en els principis d'integritat, presentació imparcial, deguda cura professional, confidencialitat, i enfocament basat en l'evidència, sobre aquest compliment de tal forma que permeti als responsables corresponents, prendre les mesures oportunes per a esmenar les deficiències identificades, si n'hi hagués, i atendre les observacions que pogués haver identificat l'Equip Auditor i en el seu cas, possibilitar l'obtenció de la corresponent certificació tal com disposa el RIC-AD.
7. L'objectiu final de l'auditoria és sustentar la confiança que mereix la infraestructura auditada sobre el nivell de seguretat implantat; tant internament com enfront de tercers, que poguessin estar relacionats, és a dir, calibrar la capacitat de la infraestructura per a garantir la integritat, disponibilitat i confidencialitat dels serveis prestats i la informació tractada, emmagatzemada o transmesa.

3. DESENVOLUPAMENT I EXECUCIÓ DE L'AUDITORIA

8. Com tota auditoria de sistemes de les tecnologies de la informació, que inclou normalment, els aspectes de seguretat dels sistemes, aquesta ha de realitzar-se d'una forma metodològica que permeti identificar clarament:
    - L'abast i objectiu de l'auditoria.

- Els recursos necessaris i apropiats per a realitzar l'auditoria (equip auditor).
- La planificació preliminar o requisits d'informació previs al desenvolupament del pla d'auditoria, i a l'execució de les proves que es considerin necessàries.
- L'establiment d'un pla d'auditoria detallat amb les activitats, revisions i proves d'auditoria previstes.
- La presentació, dels resultats individuals de les proves, a les persones involucrades amb aquests resultats, per a la seva confirmació sense valoracions respecte als resultats finals.
- L'avaluació global dels resultats de l'auditoria en relació a l'objectiu i abast definits i als requisits de la Llei NIS-AD.
- La confecció, presentació i emissió formal de l'Informe d'Auditoria.

9. La metodologia aplicada ha de permetre comprovar, a través dels registres i evidències d'auditoria, la consecució d'aquests passos, les limitacions que s'hagin pogut produir en el desenvolupament de les tasques, i les activitats realitzades.

10. Per a una consecució eficaç de l'auditoria, l'equip auditor verificarà que les mesures de seguretat per a la infraestructura auditada s'ajusten als principis bàsics de Llei NIS-AD i satisfan els requisits mínims de seguretat.

3.1 DEFINICIÓ DE L'ABAST I OBJECTIU DE L'AUDITORIA

11. L'objectiu i abast de l'auditoria han d'estar clarament definits, documentats i consensuats entre l'equip auditor i l'entitat a la qual li apliqui el RIC-AD.

12. Les auditories podran ser requerides per l´Autoritat Nacional Competent definides a la Llei NIS-AD sobre la seguretat de la infraestructura objecte d'aquestes. Per tant, és necessari establir amb claredat abans de concretar la realització de l'auditoria, l'objectiu i l'abast d'aquesta.

13. S'aplicarà el procediment de determinació de la conformitat que, amb caràcter ordinari, verifiqui el compliment dels requeriments contemplats al RIC-AD.

    - Les infraestructures a auditar:
        - Requeriran d'una auditoria externa per a la seva declaració de conformitat que haurà de realitzar-se anul·lament de forma ordinària o quan es produeixin modificacions substancials en el sistema de forma extraordinària en els terminis que marca el RIC-AD.

14. Considerant que les xarxes de comunicacions, tenen interconnexions amb altres entitats públiques i privades, la descripció detallada de l'abast de l'auditoria és essencial, és a dir, establir clarament l'extensió i el límit fins a on s'audita.

15. Les mesures de seguretat a auditar poden abastar mesures de naturalesa diversa (organitzativa, física i lògica, entre altres). Per tant, com a part de la definició de

l'abast de l'auditoria, és necessari abans de començar-la, identificar els elements que entren dins d'aquesta.

16. És imprescindible que es defineixi, preliminarment, si existeix alguna informació que, per indicació del Responsable de la Infraestructura o del de Seguretat, no estarà accessible a l'equip auditor, devent avaluar si aquesta és una limitació per a realitzar l'auditoria d'acord amb el que es preveu en la Ll-ei NIS-AD. Si és així, i es decideix continuar amb el procés d'auditoria, aquesta limitació ha de reflectir-se en l'Informe d'Auditoria, informant a l´Autoritat Nacional Competent corresponent.

17. Per a assegurar l´objectivitat de les tasques d'auditoria no inclouran en cap cas l'execució d'accions que puguin ser considerades com a responsabilitats de consultoria o similars, com ara implantació o modificació d'aplicacions relacionades amb la infraestructura auditada, redacció de documents requerits pel RIC-AD o procediments d'actuació, així com recomanacions particulars sobre productes o solucions concretes, entre altres.

3.2 EQUIP AUDITOR

1. L'equip auditor extern haurà d'estar compost per professionals (Responsable d'auditoria, auditors, i experts tècnics, alguns poden actuar amb ambdós rols a la vegada) que garanteixi que es disposa dels coneixements suficients, d'acord amb l'abast establert, per a assegurar l'adequada i ajustada realització del RIC-AD. Aquest equip d'auditoria extern haurà de ser independent a l'organització auditada i ha de tindre experiència en l'àmbit de la seguretat de la informació.

2. Aquest equip extern és necessari complir amb els següents requisits:

    - L'organització auditada serà participant de l'auditoria, sent col·laboradora en tot moment. Mentre que l'equip auditor extern serà l'encarregat de la realització de l'auditoria, de l'emissió de l'informe, i conseqüentment, dels resultats de l'auditoria. El pla d'auditoria ha d'establir amb claredat la responsabilitat i assignació de funcions a cada integrant de l'equip auditor.
    - La propietat dels documents de treball i de les evidències, així com la responsabilitat per l'emissió de l'informe i el seu contingut han de ser sempre inequívoques tant en l'obertura de l'auditoria, com en el seu informe final.
    - A l'ésser una auditoria executada per un equip extern, els integrants hauran de signar les preceptives clàusules de confidencialitat, incloent-hi les clàusules aplicables de la legislació de tractament de dades de caràcter personal.
    - En cas de necessitar la incorporació d'experts tècnics independents, aquests també han de signar una clàusula de confidencialitat.

3. L'equip auditor, en el disseny de les seves proves i revisions, no ha de limitar-se a la revisió de documents, ja que l'objectiu de l'auditoria és obtenir evidències

eficaces per a avaluar i sustentar si, en la pràctica, les mesures de seguretat auditades són adequades per a protegir la integritat, disponibilitat, i confidencialitat de la informació tractada, emmagatzemada o transmesa per la infraestructura auditada.

4. Els components de l'equip d'auditoria hauran de tenir una formació suficient en auditoria de sistemes d'informació, i en seguretat, segons s'estableix en els requisits mínims. Si es considera necessari per la complexitat tecnològica o dimensions de l'entorn a auditar, es podran incorporar experts.

5. El responsable d´auditoria haurà d'assegurar que:

   - Disposa dels coneixements tècnics necessaris per a abordar l'auditoria d'una forma eficient.
   - Es realitzen les accions necessàries, en l'etapa preliminar, per a garantir que tots els integrants de l'equip entenen i coneixen l'estructura organitzativa i tècnica de la infraestructura a auditar, els serveis que presta, i l'objectiu i l'abast de l'auditoria.
   - Tots els auditors coneixen la Llei NIS-AD i, en la mesura de les tasques assignades, els requisits de seguretat d'una altra legislació aplicable, i en particular, la relativa a tractament de dades de caràcter personal LQPD.
   - S'ha dut a terme el pla d'auditoria previst i aprovat, i que les desviacions al programa, o les seves modificacions, estan degudament fonamentades i registrades.

3.3 PLANIFICACIÓ DE L'AUDITORIA

6. Per a la realització de l'auditoria és necessari realitzar una planificació preliminar que, fonamentalment, consisteix a establir els requisits d'informació i documentació necessaris i imprescindibles per a:

   - Establir i desenvolupar el pla d'auditoria.
   - Concretar els coneixements necessaris de l'equip d'auditoria.
   - Definir l'agenda de revisions, reunions i entrevistes.
   - Definir les revisions i proves a realitzar.
   - Adjudicar les tasques als components de l'equip auditor i experts.
   - Els criteris d'auditoria i qualsevol document de referència.

7. La documentació mínima a requerir per a concretar la planificació detalladament de l'auditoria del compliment de la Llei NIS-AD és:

   - Documents signats per l'òrgan superior corresponent que mostrin el coneixement i l'aprovació formal de les decisions en matèria de política de seguretat.
   - Organigrama dels serveis o àrees afectades, amb descripció de funcions i responsabilitats.
   - Identificació dels responsables: de la informació, dels serveis, de la seguretat i de la infraestructura.

- Descripció detallada de la infraestructura a auditar (programari, maquinari, comunicacions, equipament auxiliar, ubicacions i similars).
- Categoria de la infraestructura segons el RIC-AD, incloent-hi els criteris d'identificació i valor dels nivells de les dimensions de seguretat que seran aplicables a la infraestructura.
- La Política de Seguretat.
- La Política de Signatura Electrònica i Certificats (si s'empren aquestes tecnologies).
- La Normativa de Seguretat.
- Descripció detallada del sistema de gestió de la seguretat i la documentació que el substancia.
- Informes amb el desenvolupament i resultat de l'apreciació del risc, incloent-hi la identificació d'escenaris de risc, la seva anàlisi i avaluació.
- La Declaració d´aplicabilitat.
- Decisions adoptades per a tractar els riscos.
- Relació de les mesures de seguretat implantades per requisits legals o com a resultat de l'apreciació del risc.
- Relació de registres d'activitat quant a les mesures de seguretat implantades i estat d'implantació.
- Informes d'altres auditories prèvies (1 any si existeixen), de seguretat relacionats amb els sistemes i serveis inclosos en l'abast de l'auditoria.
- Informes de seguiment de deficiències detectades en auditories prèvies de seguretat, i relacionades amb la infraestructura a auditar.
- Llista de proveïdors externs els serveis dels quals es veuen afectats o entren dins de l'abast de l'auditoria, i evidències del control realitzat sobre aquests serveis.

8. Amb el propòsit d'agilitzar i escurçar en la mesura del possible els temps d'auditoria en l'entitat auditada, és recomanable que aquesta faci arribar al responsable d´auditoria la documentació requerida en l'apartat anterior amb l'antelació suficient.

9. Segons la disponibilitat d'aquesta documentació, i d'acord amb els Responsables de la Infraestructura i del Responsable de la Seguretat, el responsable d´auditoria determinarà si és necessari rebre una còpia, o bé, segons el cas, és suficient amb una presentació d'aquesta documentació, per part d'aquests responsables.

10. No obstant això, és aconsellable per a una planificació ajustada de les proves detalladament, que es pugui disposar de còpies (en suport electrònic) d'alguna d'elles com a evidència, o per a facilitar la planificació de les proves i assignació de tasques als integrants de l'equip auditor. En tots els casos l'equip auditor mantindrà una llista actualitzada de la documentació sol·licitada i la seva situació per permetre l'accés per a la seva revisió.

11. Cada entorn a auditar serà diferent i amb les seves pròpies configuracions i estructura organitzativa, per tant, és necessari tenir-les en compte a l'hora de:

    a) dissenyar les revisions i proves d'auditoria,

b) definir en què consistirà cadascuna d'elles,
c) i establir els recursos necessaris (de l'equip d'auditoria i dels serveis auditats).

12. Per a la planificació de l'auditoria es tindran en compte les següents premisses:

- Els criteris organitzatius de l'òrgan responsable de la infraestructura auditada i la descripció de les funcions del personal afectats per aquesta infraestructura.
- Els criteris que poden auditar-se mitjançant la revisió de documentació, observació, entrevistes, qüestionaris o mostreig.
- La selecció de mesures de seguretat a verificar quant al seu compliment tal com han estat aprovades.
- Les revisions que haurien de realitzar-se mitjançant l'execució de proves tècniques (accessos, visualització de registres, edició de paràmetres de seguretat, observació i fotografia, si és aplicable, de les mesures de seguretat física, etc.), establint mostres d'elements a revisar. L'objectiu, en aquest cas, és comprovar el compliment i l'observança de determinades normes de seguretat.
- Les proves podran realitzar-se sobre la base de mostres, però l'equip auditor ha de sustentar que la mostra d'elements seleccionada per a una prova determinada, és prou representativa, per a garantir la solvència dels resultats.
- Les evidències que s'espera obtenir en cada prova i quins són ineludibles per a documentar la realització de la prova, documentant aquelles que per restriccions de propietat industrial o seguretat no sigui factible la seva obtenció, encara que sí la seva verificació per l'auditor.
- Assignació de tasques a cada integrant de l'equip d'auditoria segons la seva qualificació i experiència, i assignació de tasques als experts. Haurà de deixar-se constància de la supervisió del seu treball.
- Si existeixen informes recents d'auditoria prèvies (internes o externes) que hagin inclòs la revisió d'elements afectats per la present auditoria, aquests podran considerar-se en la planificació i no repetir proves, sempre que:
  - D'acord amb la informació inicial rebuda, no s'hagin modificat les mesures de seguretat, i es pugui tenir accés a les evidències de les proves realitzades en el seu moment. Si les mesures s'han modificat, per qualsevol circumstància, ja sigui per raons de millora contínua, o per a solucionar deficiències identificades en l'auditoria anterior, la mesura de seguretat es tornarà a revisar.
  - Aquestes auditories prèvies hagin tingut un grau d´objectivitat i qualificació sense incidències.

3.4 EVIDÈNCIES DE L'AUDITORIA

13. Les evidències d'auditoria poden obtenir-se a través de la inclusió dels següents mètodes i procediments en el pla de l'auditoria, tenint com a referència així mateix la Llei NIS-AD:

- Gestió del Risc.

Tipus de proves: sustentació metodològica de la identificació d'escenaris de risc, la seva anàlisi i avaluació, la seva coherència i documentació, i verificació de l'inventari d'actius. - Metodologia d'anàlisi i gestió de riscos dels sistemes d'informació o en altres metodologies d'apreciació del risc reconegudes internacionalment. En aquest apartat no és aplicable la selecció de mostres.

- El marc organitzatiu i la segregació de funcions.

Tipus de proves: documentació de les polítiques i procediments (accessibilitat pel personal al qual afecta i actualització); la comunicació de les normes, de les responsabilitats i de la conscienciació del personal afectat sobre aquestes normes, polítiques i procediments. Es recomana que, a l'efecte d'una avaluació més representativa, es va entreveure no sols a càrrecs jeràrquics, sinó també a un altre personal de manera aleatòria.

- El marc operacional (Planificació, Control d'accessos, explotació, serveis externs, continuïtat del servei, i monitoratge de la infraestructura).

Tipus de proves: avaluació, entre altres, de les proves fefaents de la continuïtat del servei, amb inclusió o no dels serveis externs; les autoritzacions i sol·licituds d'accés, el registre i seguiment dels incidents de seguretat; l'adequació dels drets d'accés que considerin la segregació de funcions, avaluació del control de capacitat dels sistemes, els mecanismes de control per a l'accés físic, la revisió dels registres d'activitat, la seva revisió i supervisió; la fortalesa de les mesures de seguretat de les comunicacions enfront d'atacs interns o externs; el control de canvis en aplicacions i sistemes; el compliment de contractes de propietat intel·lectual, etc.

- Les mesures de protecció (Protecció de les instal·lacions i infraestructures, Gestió del personal, Protecció d'equips, de les comunicacions, dels suports d'informació, de les aplicacions informàtiques, de la informació, i dels serveis).

Tipus de proves: avaluació, entre altres, de les proves fefaents de la protecció dels elements referenciats.

- La Declaració d'Aplicabilitat que recull les mesures de seguretat que són rellevants per a la infraestructura subjecte a l'auditoria.

Tipus de proves: evidència documental de la Declaració d'Aplicabilitat incloent totes les mesures de seguretat que són aplicables globalment o sistemàticament.

- Els processos de millora contínua de la seguretat.

Tipus de proves: avaluar el cicle de maduresa del sistema de gestió de la seguretat de la infraestructura auditada, criteris per a la revisió, no conformitats detectades, derivades o no d'accions, accions correctives i preventives, i agenda de millores.

- L'aplicació dels models de clàusula administrativa particular a incloure en les prescripcions administratives dels contractes corresponents (segons una mostra seleccionada d'aquests).

14. Per a definir els mètodes i procediments d'auditoria (verificació de les mesures de seguretat), l'equip auditor pot utilitzar guies i qüestionaris d'auditoria disponibles en associacions i col·lectius d'auditors, i les guies que pugui proporcionar l'ANC-AD que siguin aplicables a la infraestructura auditada. Aquestes guies poden ser una bona base per a l'abast de l'auditoria, dissenyar proves adequades, mantenint sempre un criteri analític i de proporcionalitat.

15. El responsable de l´auditoria ha de valorar quina informació o documentació complementària és necessari sol·licitar al començament de l'auditoria, per a assegurar que es té un coneixement fidel de l'estat de la seguretat al començament d'aquesta, com poden ser, entre altres possibles i segons es consideri aplicable:

    - Llista del personal que ha deixat l'entitat recentment.
    - Còpia del registre d'incidències.
    - Còpia del registre d'activitat dels usuaris.
    - Registres de formació del personal afectat per la infraestructura auditada.

16. Aquest tipus d'evidències poden assistir a l'auditor en l'avaluació de si determinades mesures de seguretat s'han realitzat consistent i homogèniament.

17. Durant la definició de les proves a realitzar, es valorarà si és necessari sol·licitar comptes d'accés a la infraestructura auditada per a alguns integrants de l'equip auditor, encara que haurà de minimitzar-se la necessitat d'intervenció directa per part de l'equip auditor en els sistemes del client, podent en el seu cas requerir que la verificació tècnica sigui realitzada per personal especialitzat de l'organització auditada sota supervisió de l'equip auditor.

18. Per a la realització de les proves d'auditoria, l'auditor tindrà en compte com a normes generals, les següents premisses:

    - La planificació de les proves a realitzar, especialment les d'observació i proves tècniques, és un element privatiu de l'equip auditor. Per tant, aquest no té obligació d'anticipar-les al personal auditat, excepte en el que concerneix l'agenda o disponibilitat d'elements per a l'execució de la prova.
    - En la realització de determinades proves com la verificació documental d'autoritzacions, aprovacions o contractes, l'auditor podrà requerir la revisió dels documents. Aquests documents, en suport electrònic podran ser originals o constituir algun dels tipus de còpia, en relació a l'evidència a la qual hagin de servir a l'efecte de verificació (per exemple, en el cas en què, determinat document, pugui servir com a evidència d'una conclusió a incorporar en l'informe d'auditoria).

- La mostra seleccionada de mesures o documentació ha de ser suficient i rellevant per a satisfer el compliment objectiu de la prova, dins de l'abast i objectiu de l'auditoria. El responsable de l'auditoria pot decidir que s'ampliï la mostra si considera que la grandària d'aquesta no és suficient.
- L'equip auditor en avaluar no prejutjarà les mesures existents i deurà sempre considerar, objectivament, si s'ajusten al que es preveu al RIC-AD que resultin d'aplicació, així com d'aquells requisits específics que poguessin documentar-se en guies en funció del context intern o extern de la infraestructura i si són efectives per a tractar realment els riscos identificats en l'Anàlisi de Riscos.
- Davant l'absència de determinada mesura, s'investigarà i analitzarà si existeixen altres mesures compensatòries, i en el seu cas, s'avaluarà l'eficàcia d'aquestes últimes. Quan s'hagi avaluat la implantació i efectivitat d'una mesura de seguretat sense detectar no conformitats (sempre de manera interna per la pròpia entitat), es prosseguirà amb el pla d'auditoria, assumint, per tant, la seva conformitat.
- Les entrevistes no es plantejaran de manera inductiva (conduir a una contestació concreta), sinó obertes (com es realitza determinada activitat o es concreta en la pràctica determinada mesura de seguretat). És a dir: no s'han de realitzar preguntes on la resposta, afirmativa o negativa segons el cas, estigui implícita en la pregunta, excepte per a confirmar les troballes de conformitat o de no conformitat amb els criteris d'auditoria obtinguts a partir de les evidències.
- Es ponderaran les respostes de les entrevistes, podent donar lloc a la realització de proves complementàries que no estaven previstes.

19. Per a les evidències l'auditor tindrà en compte com a normes generals, les següents:

    - L'evidència recollida ha de ser suficient i rellevant perquè:
        - si no hi ha incidències a comunicar, s'acrediti la realització adequada de la prova i els seus resultats.
        - si hi ha troballes de no conformitat (considerades internament per l´entitat) a incloure en l'informe, s'evidenciï clarament l'incompliment persistent o una indiscutible deficiència de seguretat, i no aquelles situacions excepcionals o puntuals, si estan reportades, controlades, i aprovades, tret que l'excepcionalitat no hagués d'haver estat aprovada, pel risc que pogués implicar, segons el judici objectiu i sustentat de l'auditor.
    - La verificació de la documentació haurà de fonamentar-se en les conclusions de la revisió, i els possibles aclariments rebuts posteriorment.
    - Les conclusions o informació recollida en una entrevista, per a poder ser considerades com a evidències d'auditoria, hauran de correspondre a una declaració de fets, de personal que intervingui directament en el procediment.

- Els correus electrònics, en la mesura que involucri a diverses persones dins de l'abast de l'auditoria, poden servir, en determinats casos, també com a prova d'auditoria.
- Les proves d'observació (per exemple, seguretat física) hauran d'estar documentades detallant la data i lloc o actiu observat.
- Les evidències que es recullin han d'evitar, en la mesura del possible, contenir dades de caràcter personal, o si és necessari com a evidència, que els continguin, ha d'utilitzar-se algun mecanisme (supressió, ratllat, etc.) que impedeixi la seva divulgació.
- Els documents de treball de l'equip auditor (planificació, documentació revisada, evidències, actes de reunions, llistats, còpies de pantalles, i evidències similars del treball realitzat, en suport electrònic) hauran de mantenir-se com a mínim durant els dos anys següents degudament referenciats i arxivats, així com custodiats i protegits, ja que poden ser requerits per l´Autoritat Nacional Competent.
- Quan l'equip auditor, en el curs de les seves observacions, descobreix una irregularitat significativa de fàcil resolució, pot informar immediatament el Responsable de la Seguretat perquè prengui les mesures correctives oportunes anotant a l´informe final la mesura correctiva presa.

3.5 ELABORACIÓ I PRESENTACIÓ DE LES TROBALLES DE L'AUDITORIA

20. L'objectiu principal de la presentació dels resultats de les revisions i proves, abans de l'emissió de l'informe d'auditoria, és confirmar els fets i les situacions detectades o identificades com a resultat de les proves i revisions realitzades. Aquesta presentació tindrà un caràcter objectiu, sense valoracions subjectives, ni al·ludint a la valoració dels resultats finals a plasmar en l'informe, que és l'opinió professional de l'auditor.

21. Aquesta presentació és fonamental per a l'eficàcia de l'informe d'auditoria posterior, en confirmar que els resultats, de les revisions i les proves, són certs, i que no existeix una altra informació, que per no haver estat considerada o no estar disponible en el seu moment, podria canviar l'avaluació del compliment de determinat requisit de seguretat.

22. Tots els resultats de proves, relacionats entre si o que es refereixin a una mateixa no conformitat, seran agrupats en l'informe, encara que s'inclogui un detall de les deficiències de manera individual, en un annex a l'Informe d'Auditoria.

3.6 PRESENTACIÓ DE L'INFORME D'AUDITORIA

23. Una vegada confirmats els fets i deficiències resultants de les revisions i proves d'auditoria, es recolliran en un informe que haurà de presentar-se al Responsable de la Infraestructura i al Responsable de la Seguretat. Els informes d'auditoria seran analitzats pel Responsable de Seguretat competent, que elevarà les conclusions al Responsable de la Infraestructura perquè adopti les accions correctives adequades.

24. L'informe d'auditoria haurà de dictaminar sobre l'adequació de les mesures exigides. Deurà, igualment, incloure les dades, fets i observacions en què es basin els dictàmens aconseguits.

25. Ates que l'informe d'auditoria es basarà en el compliment aconseguit del prescrit en el RIC-AD i en concret en les mesures de seguretat que resultin d'aplicació, així com d'aquells requisits específics que poguessin documentar-se en guies en funció del context intern o extern de la infraestructura, identificant, en el seu cas, les troballes de conformitat, no conformitat i observacions que es detectin, així com els registres, declaracions de fets o qualsevol altra informació pertinent i verificable en què es basin les conclusions aconseguides.

26. Les troballes de no conformitat es classificaran atenent els següents graus:

    - "No Conformitat Menor": Es documentarà una "No Conformitat Menor" davant l'absència o la fallada en la implantació o manteniment d'un o més dels requisits del RIC-AD, incloent-hi qualsevol situació que pogués, sobre la base d'una evidència objectiva, sustentar un dubte significatiu sobre la conformitat de la infraestructura amb un o més de tals requisits.
    - "No Conformitat Major": Es documentarà una "No Conformitat Major" quan es detectin "No Conformitats Menors" en relació amb qualsevol dels preceptes continguts en la Llei NIS-AD, o en el Marc organitzatiu, o en algun dels subgrups que integren el Marc operacional o les Mesures de protecció (Planificació, Control d'Accessos, Explotació, Serveis Externs, Continuïtat del Servei, Monitoratge del Sistema, Protecció de les Infraestructures, Gestió del Personal, Protecció d'Equips, Comunicacions, Suports d'Informació, Aplicacions Informàtiques, Informació o Serveis) que, avaluades en el seu conjunt, puguin implicar l'incompliment de l'objectiu del Grup o Subgrup considerats.

27. Es documentarà una Observació quan es trobin evidències de, una feblesa, una vulnerabilitat o una situació que, sense comprometre qualsevol àrea de la infraestructura de gestió definida al RIC-AD o per l'organització, pugui, en l'actualitat o en el futur, derivar en un problema.

28. L'informe d'Auditoria haurà de contenir la informació adequada i suficient per a facilitar i justificar la decisió per obtenir la corresponent certificació, com a mínim:

    - Existeix un sistema de gestió de la seguretat de la informació, documentat i amb un procés regular d'aprovació per part de la direcció.
    - La Política de Seguretat respon a la missió i objectius de seguretat de l'organització.
    - L'organització defineix els rols i funcions dels responsables de la informació, els serveis, els actius i la seguretat de la infraestructura, detallant procediments per a la resolució de conflictes entre aquests responsables quan pugui donar-se aquest supòsit, i verificant que s'han designat persones per a aquests rols sota el principi de "separació de funcions".

- S'ha realitzat una apreciació del risc, incloent-hi la identificació d'escenaris de risc, l'anàlisi de les conseqüències i la seva probabilitat, i l'avaluació de la seva acceptabilitat o inacceptabilitat per a l'organització, amb revisió i aprovació regular.
- Detall del nivell de seguretat en cadascuna de les dimensions recollides en el RIC-AD.
- Es compleixen les mesures de seguretat en funció de les condicions d'aplicació en cada cas.
- Una referència a la versió de la Declaració d'Aplicabilitat, que inclogui el nivell en cada dimensió per a cada mesura de seguretat del RIC-AD aplicable.
- Existeix un procés de millora contínua de la gestió de la seguretat.
- Les àrees organitzatives, mòduls o funcions de la infraestructura cobertes per l'auditoria, incloent-hi els requisits de certificació i les ubicacions que van ser auditades, les pistes d'auditoria seguides i les metodologies d'auditoria utilitzades.
- Els detalls de les conformitats i no conformitats identificades es justificaran mitjançant evidències objectives i la seva correspondència amb els requisits del RIC-AD o altres documents requerits per a la Certificació.
- El dictamen per part de l´equip d´auditoria sobre si la infraestructura auditada ha de ser certificada o no, amb informació que suporti aquesta conclusió.

29. L'equip auditor no lliurarà ni concedirà accés a l'informe d'auditoria a tercers diferents dels indicats en el paràgraf anterior, excepte per imperatiu legal o mandat judicial.

30. L'Informe d'Auditoria es presentarà en format electrònic i estant degudament signat pel responsable de l´auditoria, la direcció de l´entitat i serà remés a l´Autoritat Nacional Competent a través del DSI (Delegat de la seguretat de la informació) al repositori electrònic habilitat per cada entitat per part de l´ANC-AD. L'esquema de l'informe inclourà com a mínim:

    - Data d'emissió de l'informe.
    - Una secció d'abast, detallant la seva extensió i limitacions, i incloent l'objectiu de l'auditoria, amb la deguda identificació de la infraestructura o infraestructures auditades.
    - Breu descripció del procés metodològic aplicat per a realitzar l'auditoria.
    - Identificació de la documentació revisada.
    - Indicació de si hi ha hagut alguna limitació en la realització de l'auditoria, que impedeixin a l'equip auditor formar-se una opinió sobre determinats criteris de l'auditoria, incloses mesures de seguretat.
    - Una secció d'informe executiu resumint els punts forts, les febleses (resum de les no conformitats i observacions) i oportunitats de millora, i incloent un resum general del grau de compliment.

- Les recomanacions en cap cas hauran de ser tancades, sinó suggeriments generals de les diferents alternatives possibles, quan sigui aplicable, a considerar pels responsables de la seguretat.
- Les recomanacions estaran sempre basades en l'existència d'un risc i sustentades degudament, o ben relacionades amb un incompliment fefaent i precís dels requisits bàsics i mínims.
- En annexos es podrà descriure els detalls i resultats de les proves que permeten arribar a les conclusions de l'informe executiu, agrupant-los pels apartats de l'informe executiu.
- L'informe també podrà incloure com a annex les contestacions del Responsable de la Seguretat als comentaris abocats en l'informe, o les accions que es prendran per a solucionar les deficiències, si n'hi hagués.
- L'Informe d'Auditoria haurà de ser signat digitalment pel responsable de l´auditoria, i indicar els participants en l'equip d'auditoria en un annex o a continuació de la seva signatura.

3.7 DICTAMEN FINAL DE L'INFORME D'AUDITORIA

31. El dictamen final de l'informe d'Auditoria per part de l´ANC-AD i si s´escau de l´Autoritat Nacional Competent si s´escau serà un dels següents:

    - "FAVORABLE": Quan no s'evidenciï cap "No Conformitat Major" o "No Conformitat Menor", el que comporta obtenir la Certificació de Conformitat corresponent.
    - "FAVORABLE AMB NO CONFORMITATS": Quan s'evidenciïn "No Conformitats Menors" i/o "No Conformitats Majors". En aquest cas, l'entitat titular responsable de la infraestructura auditada haurà de presentar, en el termini màxim d'un mes, un Pla d'Accions Correctives (PAC) sobre tals desviacions a l'Autoritat Nacional Competent per a la seva avaluació.
    - "DESFAVORABLE": Quan existeixi un número significatiu de "No Conformitats Majors" la solució de les quals no pugui evidenciar-se a través d'un Pla d'Accions Correctives i requereix la comprovació in-situ de la seva correcta implantació a través d'una auditoria extraordinària si es creu necessari per part de l´ANC-AD.

32. La Certificació de Conformitat amb el RIC-AD únicament podrà expedir-se si el dictamen fos "FAVORABLE" o, si havent estat "FAVORABLE AMB NO CONFORMITATS", el Pla d'Accions Correctives presentat per l'entitat titular de la infraestructura, tracta i resol les desviacions evidenciades, a criteri de l'ANC-AD.

33. Davant un dictamen "DESFAVORABLE", l'entitat titular de la infraestructura auditada, en un termini no superior a 3 mesos des de la data d'emissió de l'Informe d'Auditoria, haurà de sotmetre's a una Auditoria Extraordinària si es creu necessari per part de l´ANC-AD, exclusivament sobre les desviacions evidenciades que, de resultar satisfactori, permetrà l'expedició del corresponent Certificat de Conformitat amb el RIC-AD.

34. En cas d'una infraestructura certificada sobre el qual es detectin No Conformitats Majors, durant el període de resolució de les No Conformitats Majors el Certificat de Conformitat quedarà en suspens. En cas de no tancar les No Conformitats Majors en un termini de sis mesos el Certificat de Conformitat quedaria revocat i l'entitat auditada haurà d'eliminar el Distintiu de Conformitat de la seva entitat fins a la seva pròxima recertificació.

35. En el cas que les conclusions de l'auditoria incloguin no conformitats, l'organització auditada haurà de remetre a l'ANC-AD per a la seva aprovació un pla detallant les accions correctives que s'implementaran per a atacar la causa arrel de les no conformitats i evitar futures ocurrències. En el cas d'auditories de certificació, no podrà emetre's el Certificat de Conformitat fins a la recepció dels Plans d'Accions Correctives de totes les No Conformitats detallades en l'informe i, opcionalment, per a les observacions.

3.8 CALENDARIS DE CUMPLIMENT D'APLICACIÓ DEL RIC-AD

36. Aquesta guia d'auditoria té, com un dels seus objectius, determinar periòdicament el nivell mínim de seguretat exigit i la data límit per al seu compliment. De tal manera es confecciona una taula amb el calendari de compliment del RIC-AD, al costat dels nivells mínims:

NIVELL EXIGIT RIC-AD	NIVELL MÍNIM RIC-AD	DATA LÍMIT COMPLIMENT MÍNIM RIC-AD
2,3	2	01/03/2025
3	2,6	30/09/2025
4	3,6	31/03/2027
5	4,6	31/03/2028

37. Tal com es mostra en l'última columna de l'anterior taula, es determina la data d'inici d'un expedient sancionador i a la imposició de sancions després de la instrucció prèvia de l'expedient que es generi de conformitat amb el que es preveu a la Llei NIS-AD. La sanció es deu al fet que existeix una falta d'adopció de les mesures per esmenar les deficiències que hagin estat detectades en l'auditoria externa.

38. Així mateix, Les entitats crítiques i les entitats equivalents a entitats crítiques disposen d'un termini de 18 mesos a comptar a la data d'entrada en vigor del RIC-AD per adaptar-se al compliment de les obligacions contingues a l'article 12 apartat 5, exclusivament pel que es refereix a l'exigència de l'auditoria de seguretat externa prevista per a les entitats subcontractades.

3.9 GARANTIES MÍNIMES DELS DE SERVEIS I/O TECNOLOGIES I/O PRODUCTES

39. Les entitats crítiques i els seus equivalents han d'assegurar-se que els seus proveïdors subcontractats ofereixin suficients garanties sobre els serveis, tecnologies i productes proporcionats. Aquests serveis i productes han d'estar registrats en el registre de components certificats de l'ANC-AD, que s'elabora segons criteris rellevants, inclosos els internacionalment reconeguts.

40. Si una entitat crítica no pot accedir a serveis o productes del registre, pot sol·licitar a l'ANC-AD autorització per a usar-los, justificant la necessitat. L'ANC-AD té un mes per a avaluar la sol·licitud; si no hi ha resposta, es considera denegada.

41. Per a la contractació de serveis o productes, les entitats crítiques han d'exigir als proveïdors una auditoria de seguretat externa amb menys de 18 mesos d'antiguitat, realitzada segons normes internacionals de ciberseguretat. Si no poden trobar un proveïdor amb aquesta auditoria, poden demanar autorització a l'ANC-AD per a contractar el proveïdor seleccionat, justificant l'elecció.

42. A més, han de requerir a les entitats subcontractades auditories de seguretat externes amb menys de 18 mesos d'antiguitat a l'inici de la subcontractació. També poden sol·licitar excepcions a l'ANC-AD si no troben proveïdors amb aquesta auditoria.

43. Finalment, les entitats crítiques han de proporcionar anualment a l'ANC-AD un resum de les contractacions i subcontractacions realitzades, esmentant els components certificats contractats, i informar sobre les auditories externes i els marcs utilitzats.

3.10 EXEMPLE MESURES DE SEGURETAT

44. A continuació es mostra un registre d'exemples de mesures de seguretat aplicades a actius físics i de seguretat de la informació:

	ACTIUS	
	FÍSICS	SISTEMES D'INFORMACIÓ
ORGANITZATIVES O DE GESTIÓ		
Anàlisis de Riscs	Avaluació i valoració de les amenaces, impactes i probabilitats per obtenir un nivell de risc	
Planificació	Identificació d'objectius i programació de les activitats per aconseguir-los	
Definició de rols i responsabilitats	Assignació de responsabilitats en matèria de seguretat	
Cos normatiu	Elaboració de polítiques, estàndards i procediments de seguretat	
Compliment normatiu	Identificació de normativa aplicable i compliment amb les mateixes	

Certificació, acreditació i avaluació de seguretat	Revisions periòdiques dels sistemes per avaluar el seu nivell de seguretat	
OPERACIONALS O PROCEDIMENTALS		
Gestió d'actius i de la configuració	Identificació d'actius, control d'inventari	
Formació i conscienciació	Plans de formació i conscienciació en seguretat	
Plans de contingència	Plans de contingència informàtiques i físiques	
Supervisió continua	Avaluació/auditoria continua dels sistemes	
Seguretat del personal	Processos de selecció, règim intern i procediments de cessament	
Gestió d'accessos – Gestió d'usuaris	Altes, baixes i modificacions	
Gestió d'accessos – Control d'accessos temporals	De persones i vehicles	Identificadors d'usuari temporal dels sistemes
Gestió d'accessos – Control d'entrada i sortida	Paqueteria i correspondència	Suports, equips i informació
Procediments operacionals del personal de seguretat	Control de rondes de seguretat	No aplica
Evacuació	Pla d'evacuació	No aplica
DE PROTECCIÓ O TÈCNIQUES		
Mesures de prevenció i detecció		
Anti-intrusió	Seguretat física i electrònica perimetral, sistemes de detecció perimetral	Firewalls, DMZs, IPSs, segmentació de xarxes, protecció de llocs de treball, xifrat, VPNs
Control d'accessos (inclou autenticació)	De persones, vehicles i mercaderies	Registre d'usuaris, gestió de privilegis, gestió de claus secretes, revisió de drets d'accés
Instal·lació i configuració segura	Configuració segura dels equips i sistemes amb caràcter previ a la seva entrada en operació, manteniment d'equips i control dels canvis.	
Protecció davant de malware	No aplica	Instal·lació d'antivirus, antispyware
Desenvolupament d'aplicacions	No aplica	Desenvolupament basat en millors pràctiques, auditories preproducció
Mesures de coordinació i monitorització		
Monitorització	Sistemes de vídeo vigilància	Sistemes de integritat de software i sistemes de monitorització i gestió de logs

Coordinació (gestió d'incidències)	Centre de control, central d'alarmes, sistemes de comunicació	Creació d'equips de resposta a incidents, infraestructures SOC

Taula.1: Exemple de Mesura de Seguretat.

ANNEX A. GLOSSARI

Auditoria

Procés sistemàtic, independent i documentat per a obtenir evidències d'auditoria i avaluar-les de manera objectiva amb la finalitat de determinar el grau en què es compleixen els criteris d'auditoria.
Les auditories internes, denominades en alguns casos auditories de primera part, es realitzen per la pròpia organització, o en el seu nom, per a la revisió per direcció i per a altres propòsits interns (per exemple, per a confirmar l'eficàcia del sistema de gestió o per a obtenir informació per a la millora del sistema de gestió). Les auditories internes poden formar la base per a una autodeclaració de conformitat d'una organització.
Quan dos o més sistemes de gestió de disciplines diferents s'auditen junts, es denomina auditoria combinada.
(Adaptat de la UNE-EN-ISO 19011:2012, definició 3.1).

Auditoria de sistemes d'informació

1) L'Auditoria de sistemes d'informació és el procés metodològic, realitzat amb independència dels elements auditats i amb objectivitat, de recollir, agrupar i avaluar evidències per a determinar si els sistemes o tecnologies de la informació salvaguarden els actius, mantenen la integritat de les dades, contribueixen a l'assoliment dels fins de l'organització i utilitzen eficientment els recursos.

2) L'activitat d'auditoria ha d'avaluar les exposicions al risc referides al govern, operacions i sistema d'informació de l'organització, en relació amb la fiabilitat i integritat de la informació, l'eficàcia i eficiència de les operacions, la protecció d'actius, i el compliment de lleis, regulacions i contractes.

Abast de l'auditoria

Extensió i límits d'una auditoria. L'abast d'una auditoria inclou generalment una descripció de les ubicacions, les unitats de l'organització, les activitats i els processos, així com el període de temps cobert (adaptat de la UNE-EN-ISO 19011:2012, definició 3.14).

Elements als quals comprèn l'auditoria del RIC-AD: els sistemes que estaran en revisió, l'entitat responsable d'aquests sistemes, els elements de l'estructura tecnològica, personal vinculat als elements anteriors, períodes de temps. Dins del context d'aquesta guia té una relació directa amb la Declaració d'Aplicabilitat.

Antispyware

Programari que detecta y elimina spyware (veure "spyware")

Auditor

Persona que duu a terme una auditoria (adaptat de la UNE-EN-ISO 19011:2012, definició 3.8).

El professional amb formació i experiència contrastable sobre les matèries a auditar, que reuneix les condicions, a més de les de coneixements i competència, d'actuar de manera independent. Fa les tasques d'auditoria.

Auditor intern

Pertany a una unitat independent dins de l'entitat al qual pertanyen els elements objecte de l'auditoria, amb funcions i autoritat clarament definides, que pot no tenir responsabilitats operatives, directives o de gestió dels processos, sistemes o àrees auditats.

Auditor extern

És independent laboralment a l'organisme on realitzarà l'auditoria.

Comprovació

1) Verificar, confirmar la veracitat o exactitud d'alguna cosa.

2) Dins del context d'aquesta guia, són verificacions de la realització de controls, de l'establiment de mesures de seguretat, i de documentació de polítiques, entre altres, dins dels requeriments establerts per la norma de referència en l'auditoria.

Conformitat

Compliment d'un requisit (UNE-EN-ISO 19011:2012).

Control / Controls

1) Regulació, manual o automàtica, sobre un sistema.

2) Mecanisme o procediment que evita, prevé, o detecta un risc.

3) En el context d'una auditoria, aquests poden ser classificats en preventius, detectius i correctius.

Criteri d'auditoria

Conjunt de polítiques, procediments o requisits usats com a referència enfront de la qual es compara l'evidència d'auditoria (UNE-ISO/IEC 19011:2012)

Compliment

Veure "prova de compliment".

Dictamen

Opinió i judici que es forma o s'emet sobre alguna cosa.

Dictamen d'auditoria

Veure "informe d'auditoria".

DMZ

És una subxarxa d'àrea local situada entre la xarxa privada d'una organització i la xarxa externa.

Efectivitat / Eficàcia

Capacitat d'aconseguir l'efecte que es desitja o s'espera.

Evidencia d'auditoria

Registres, declaracions de fets o qualsevol altra informació que és pertinent per a les troballes d'auditoria i que és verificable. L'evidència d'auditoria pot ser qualitativa o quantitativa (UNE-EN-ISO 19011:2012).

Les evidències consisteixen, principalment, en les demostracions i testimoniatges (documentals, automatitzades, etc.) dels resultats de l'aplicació dels procediments d'auditoria (proves). Aquestes han de ser suficients per a suportar les conclusions de l'auditor. Per a això han d'acreditar determinades situacions o fets objectius quant als fets als quals es refereixen. L'avaluació d'aquestes evidències correspon a l'auditor per a documentar la seva troballa.

Expert tècnic

Persona que aporta experiència o coneixements tècnics específics a l'equip auditor. El coneixement o experiència específics són els relacionats amb l'organització, el procés o l'activitat a auditar.

Firewalls

En informàtica, un tallafocs és la part d'un sistema informàtic o una xarxa informàtica que està dissenyada per a bloquejar l'accés no autoritzat.

Guia

Persona designada per l'auditat per a assistir a l'equip auditor.

Informe d'auditoria

És el producte final de les tasques realitzades en una auditoria. En l'informe l'auditor comunica, a qui correspongui, els resultats de les tasques realitzades, amb els resultats obtinguts.

Limitacions al abast

Són aquells registres o documents, o elements de l'abast de l'auditoria, als quals, encara que previstos en les revisions planificades, per a aconseguir els objectius de l'auditoria, l'auditor no ha pogut tenir accés, per diferents raons, i la restricció d'accés de les quals pot impactar en les conclusions de l'auditoria. Han d'estar reflectides en l'informe d'auditoria. Dins del context d'aquesta guia d'auditoria, encara que podrien sorgir en la definició de l'abast, aquesta situació hauria de ser excepcional. Si les restriccions sorgeixen en la fase inicial de delimitació de

l'abast, l'auditor ha d'indicar-lo, a més d'en l'informe final, en la planificació. Així mateix, si sorgeix en la fase inicial, ha d'indicar-se el possible impacte en la realització de l'auditoria, i l'obtenció de les conclusions en relació a l'objectiu de l'auditoria. És convenient que en tots els casos, l'auditor requereixi que es comuniqui per escrit, la restricció d'accés a registres, documents o elements a auditar, i justificats per l'objectiu de l'auditoria.

IPS

Un sistema de prevenció d'intrusos és un programari que exerceix el control d'accés en una xarxa informàtica per a protegir els sistemes computacionals d'atacs i abusos.

Log

Per a referir-se a l'enregistrament seqüencial en un arxiu o en una base de dades de tots els esdeveniments (o accions) que afecten un procés particular.

No conformitat

Incompliment d'un requisit (UNE-EN-ISO 19011:2012).

Malware

Programari maliciós o programari nociu.

Objectivitat

Veure "opinió independent i objectiva".

Objectiu de l'auditoria

1) Les fites específiques que ha d'aconseguir l'auditoria.

2) En el context d'aquesta guia, arribar amb concloure si es compleix amb el requerits per les normes de referència.

Observació

Veure "probes de auditoria".

Opinió independent i objectiva

1) Independent: Que no té dependència, que no depèn d'un altre.

2) Objectiva: Que pertany o relatiu a l'objecte en si mateix, amb independència de la pròpia manera de pensar o de sentir.

3) L'auditor ha de jutjar i opinar sobre els resultats de l'auditoria, en funció de l'objectiu i abast d'aquesta, lliure de tota parcialitat o biaix que pugui afectar de manera negativa en els resultats de l'auditoria, i que pugui conduir a una interpretació errònia dels fets identificats.

Pla d'auditoria

Descripció detallada (pas a pas) dels procediments d'auditoria (documentació, proves, etc.) que s'han de realitzar durant l'execució del treball d'auditoria per a aconseguir l'objectiu d'aquesta. En el pla de l'auditoria també s'inclou l'assignació de tasques, dates de realització de les tasques, i recursos necessaris per a desenvolupar l'auditoria.

Principis de segregació de funcions

1) Principi: Norma o idea fonamental que regeix el pensament o la conducta.

2) La separació o segregació de funcions és una regla bàsica en els controls: evitar que una persona pugui dominar tot un procés, de tal forma que errors o omissions, o incompliments de controls no puguin ser identificats. Per tant, l'auditor ha d'identificar on no es compleix amb aquesta norma fonamental, per a avaluar l'impacte en l'efectivitat dels controls.

Procediments d'auditoria

Comprenen el procés d'auditoria: habitualment al·ludeixen als processos relacionats amb la definició de les proves, la seva planificació i la seva execució. Les proves d'auditoria poden ser de compliment o substantives, segons el seu objectiu. Així mateix, les tècniques d'auditoria utilitzades en qualsevol tipus de les proves esmentades anteriorment poden ser: observació de la realització de tasques, revisió de documentació, entrevistes, realització de proves tècniques, revisió d'evidències del compliment de controls, etc. Entre aquestes últimes es poden incloure els criteris per a la selecció de mostres d'elements a revisar en determinades proves.

Proves d'auditoria

1) Permeten obtenir evidència i verificar la consistència dels controls existents i també mesurar el risc per deficiència d'aquests o per la seva absència.

2) Es dissenyen i planifiquen per a assegurar que els controls es dissenyen adequadament i funcionen de manera efectiva i continuada.

Proves de compliment

Permeten determinar si un control s'està realitzant de la forma prevista en les normes i polítiques de seguretat establertes per l'entitat responsable de la SI (seguretat de la informació). El seu objectiu principal és determinar si el control es realitza i si els seus resultats són efectius.

Proves substantives

Permeten confirmar l'exactitud de determinades situacions o fets, però fonamentalment permeten substanciar l'impacte i abast d'una deficiència, o incidència de seguretat (en el context d'aquesta guia), amb projecció sobre la integritat de determinada informació o d'un procés. Exemple: en la revisió d'un

inventari de còpies de seguretat, una prova de compliment pot determinar si els controls previstos s'estan complint o no, però amb una prova substantiva, es podria determinar quants, i /o quins elements no estan inclosos en l'inventari.

Recomanacions

Poden ser part de l'informe d'auditoria, on a més d'incloure les conclusions de les tasques d'auditoria realitzades, i identificar les deficiències observades, es poden incloure suggeriments concrets per a la solució de les fallades identificades.

Requisit

1) Circumstancia o condició necessària per a alguna cosa.

2) Dins del context d'aquesta guia, són les condicions, en ocasions mínimes, a complir pels auditors.

3) A l´auditoria se sol indicar que existeixen "requisits" o mandats mínims que ha de complir el procés d'auditoria, com ara establir l'abast i objectiu de l'auditoria, realitzar un programa d'auditoria, i les proves relacionades, així com l'emissió d'un informe, entre altres.

Responsabilitat

1) Obligació o deure de realitzar alguna acció.

2) Dins del context d'una auditoria, s'han d'establir, per exemple, responsabilitats mínimes per a la funció d'auditoria, responsabilitats del compliment de la metodologia d'auditoria, i els seus requisits mínims.

3) L'auditor és responsable de l'opinió i les conclusions abocades en l'informe d'auditoria.

Satisfacció d'auditoria

1) Satisfer: Complir, omplir uns certs requisits o exigències.

2) Dins del context de l'auditoria, es refereix al fet que el programa o pla d'auditoria, ha de complir amb els objectius d'auditoria, i les tasques realitzades amb aquest.

Selecció de mostres

Es poden aplicar criteris de mostreig estadístic o no, per a seleccionar elements a revisar en una determinada prova. La qualitat de la mostra i de la selecció dels elements de la mostra pot facilitar l'anàlisi dels resultats d'una prova i també la sustentació d'una conclusió d'auditoria. S'utilitza fonamentalment quan existeix una població homogènia d'elements a seleccionar, per exemple: comptes d'usuaris.

SOC

El Centre d'Operacions de Seguretat, SOC, es refereix a l'equip responsable de garantir la seguretat de la informació.

Software

És el conjunt dels programes informàtics (en anglès software), procediments i documentació que fan alguna tasca en un ordinador.

Spyware

Són aplicacions (programes informàtics) que recopilen informació sobre una persona o una organització sense que aquesta ho sàpiga.

Suficiència de les evidències

Les evidències que suporten una conclusió han de ser suficients (bastantes), i rellevants (significatius), per a suportar les conclusions i opinió del auditor.

Supervisió

1) Exercir la inspecció superior en treballs realitzats per altres.

2) Les tasques de l'equip d'auditoria han de ser supervisades pel responsable de l'auditoria per a assegurar que s'ha complert amb l'objectiu de l'auditoria dins de l'abast previst.

Troballa d'auditoria

Resultats de l'avaluació de l'evidència d'auditoria enfront dels criteris d'auditoria. Les troballes d'auditoria poden indicar conformitat o no conformitat. Poden conduir a la identificació d'oportunitats de millora o al registre de bones pràctiques. Si els requisits d'auditoria es seleccionen d'entre els requisits establerts, la troballa d'auditoria es denomina "compliment" o "no compliment" (UNE-EN-ISO 19011:2012).

Verificació

Qualsevol de les accions d'auditoria encaminades a la comprovació l'acarament, el contrast i l'examen d'evidències, registres i documents.