RIC-STIC-002_S
Guia Simplificada d'Auditoria Infraestructures Crítiques

(DOCUMENT SUBJECTE A MODIFICACIONS)

Gener 2023

Fitxa del document

Títol	Guia Simplificada d'auditoria Infraestructures Crítiques

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	25/1/23	26/1/23

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

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.

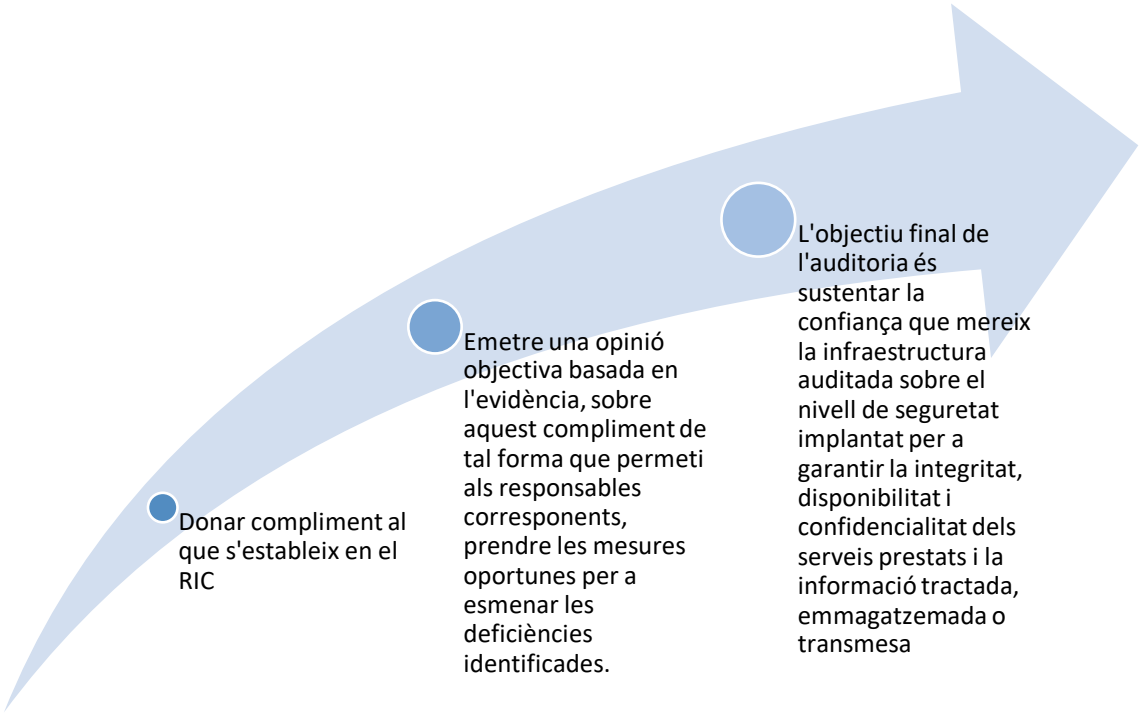
César Marquina Pérez de la Cruz
Ministre de Finances i portaveu del Govern

ÍNDEX

1. MARC DE REFERÈNCIA

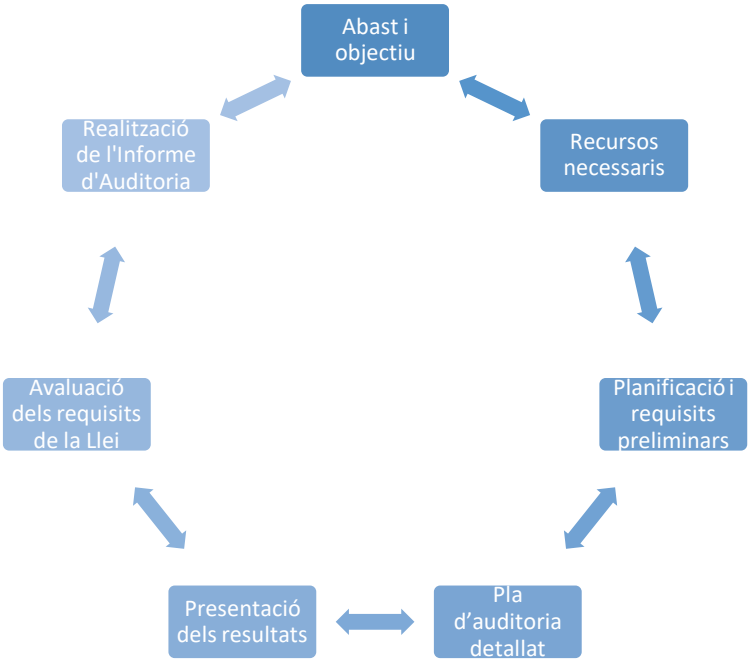
1. Aquesta guia d'auditoria del Reglament d'Infraestructures Crítiques del Principat d'Andorra (d'ara endavant, el RIC), de mesures per a la seguretat de les xarxes i dels sistemes d'informació (d'ara endavant la "Llei NIS-AD") estableix unes pautes de caràcter general.
2. Aquesta guia simplificada té l'objectiu de canalitzar d'una forma homogènia la realització de les auditories, establint unes premisses mínimes en la seva execució.
3. Les infraestructures, les quals es trobin compresos en l'àmbit d'aplicació el RIC seran objecte d'una auditoria regular ordinària anual, que verifiqui el compliment dels requeriments d'aquest Reglament.

2. OBJECTE DE L'AUDITORIA



3. DESENVOLUPAMENT I EXECUCIÓ DE L'AUDITORIA

4. Ha de realitzar-se d'una forma metodològica que permeti identificar:



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

<table>
<tr><th colspan="2">DEFINICIÓ DE L'ABAST I OBJECTIU DE L'AUDITORIA</th></tr>
<tr><td colspan="2">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 segons els següents criteris:</td></tr>
<tr><td colspan="2">Les auditories podran ser requerides per l´Autoritat Nacional Competent definides a la llei NIS-AD.</td></tr>
<tr><td colspan="2">Identificar els elements que entren dins de l'auditoria abans de començar-la.</td></tr>
<tr><td rowspan="2">S'aplicarà el procediment de determinació de la conformitat que verifiqui el compliment dels requeriments contemplats al RIC</td><td>Requeriran d'una autoavaluació per a la seva declaració de conformitat que haurà de realitzar-se anualment o quan es produeixin modificacions substancials en la infraestructura en els terminis que marca el RIC.</td></tr>
<tr><td>L'autoavaluació podrà ser desenvolupada pel mateix personal que administra la infraestructura o en qui aquest delegui.</td></tr>
<tr><td colspan="2">Si les xarxes de comunicacions, tenen interconnexions amb altres entitats públiques i privades cal establir clarament l'extensió i el límit fins a on s'audita.</td></tr>
<tr><td colspan="2">Si existeix alguna informació que no estarà accessible a l'equip auditor, que sigui una limitació per a realitzar l'auditoria d'acord amb el que es preveu en la llei NIS-AD, ha de reflectir-se en l'Informe d'Auditoria, informant a l´Autoritat Nacional Competent corresponent.</td></tr>
<tr><td colspan="2">Per a assegurar l´objectivitat de les tasques d'auditoria, no inclouran l'execució d'accions que puguin ser considerades com a responsabilitats de consultoria o similars.</td></tr>
</table>

3.2 EQUIP AUDITOR

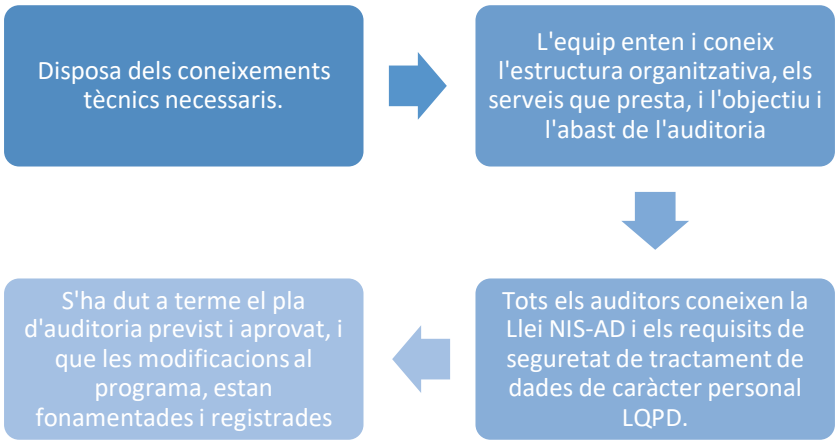
Responsable d'auditoria

Auditors interns i/o externs

Experts tècnics

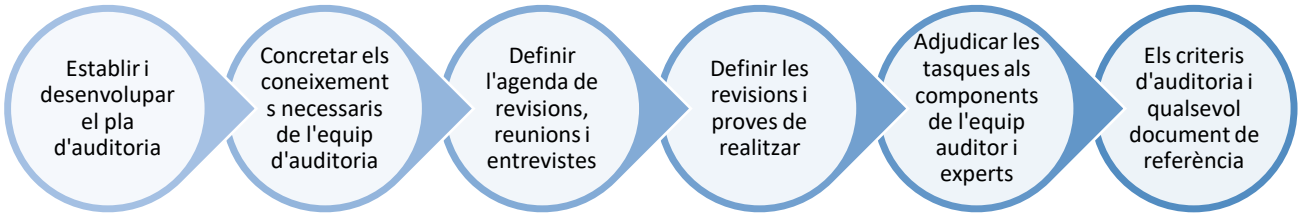
EQUIP AUDITOR
És necessari complir amb els següents requisits:
El pla d'auditoria ha d'establir amb claredat la responsabilitat dels equips que participen i l'assignació de funcions a cada integrant de l'equip auditor.
La propietat dels documents de treball i evidències, l'emissió de l'informe i el seu contingut han de ser sempre inequívoques tant en l'obertura de l'auditoria, com en el informe final.
Han de signar les perspectives clàusules de confidencialitat tant els auditors externs com els tècnics independents liderats per un equip intern.
L'equip auditor té com a objectiu obtenir evidències eficaces per a avaluar i sustentar si les mesures de seguretat auditades són adequades.
Els components de l'equip d'auditoria hauran de tenir una formació suficient en auditoria de sistemes d'informació i en seguretat.

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



3.3 PLANIFICACIÓ DE L'AUDITORIA

6. Per a la realització de l'auditoria és necessari realitzar una planificació preliminar:

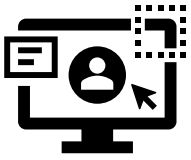


PLANIFICACIÓ AUDITORIA
Documents mínims per a l'elaboració del pla de auditoria
Documents signats per l'òrgan superior corresponent que mostrin el coneixement i l'aprovació formal de les decisions en matèria de política de seguretat.
Organigrama dels serveis o àrees afectades, amb descripció de funcions i responsabilitats.
Identificació dels responsables: de la informació, dels serveis, de la seguretat i de la infraestructura.
Descripció detallada de la infraestructura a auditar.
Categoria del sistema segons el RIC, incloent-hi els criteris d'identificació i valor dels nivells de les dimensions de seguretat que seran aplicable al sistema.
Política de Seguretat.
Política de Signatura Electrònica i Certificats.
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, 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.
Informes d'altres auditories prèvies 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 el sistema 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.

7. Cada entorn a auditar serà diferent per tant cal tenir en compte:

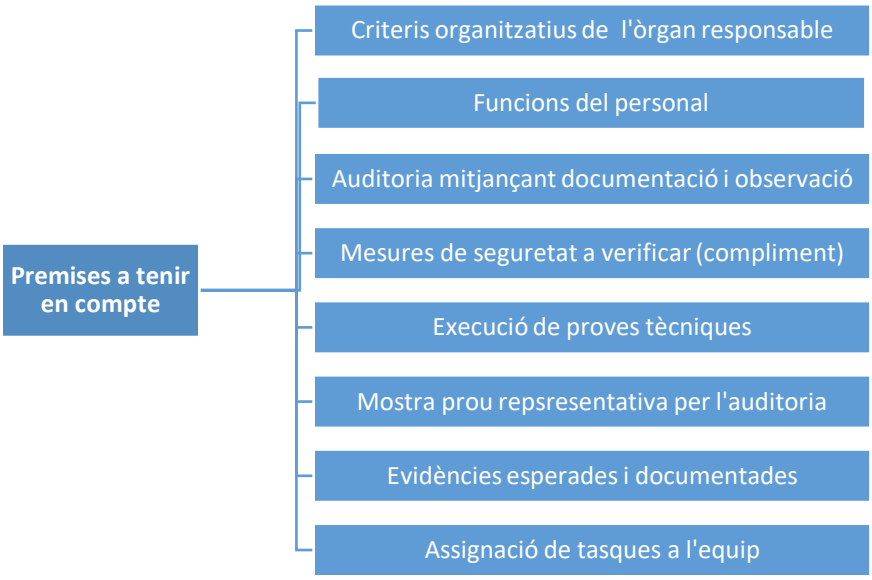
Dissenyar les revisions i proves

Definir en que consistiran



Establir els recursos

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



3.4 EVIDÈNCIES DE L'AUDITORIA

9. Les evidències d'auditoria poden obtenir-se a través de la inclusió dels següents mètodes i procediments en el Pla de l'auditoria intern:

Gestió del Risc

Marc organitzatiu i la segregació de funcions

- Documentació de les polítiques i procediments
- Comunicació de les normes, responsabilitats i conscienciació del personal

Marc operacional

- Avaluació de les proves de la continuïtat del servei
- Autoritzacions i sol·licituds d'accés
- Registre i seguiment dels incidents de seguretat
- Adequació dels drets d'accés
- Avaluació del control de capacitat dels sistemes
- Mecanismes de control per a l'accés físic
- Fortalesa de les mesures de seguretat de les comunicacions
- Revisió dels registres d'activitat
- Control de canvis en aplicacions i sistemes
- Compliment de contractes de propietat intel·lectual, etc

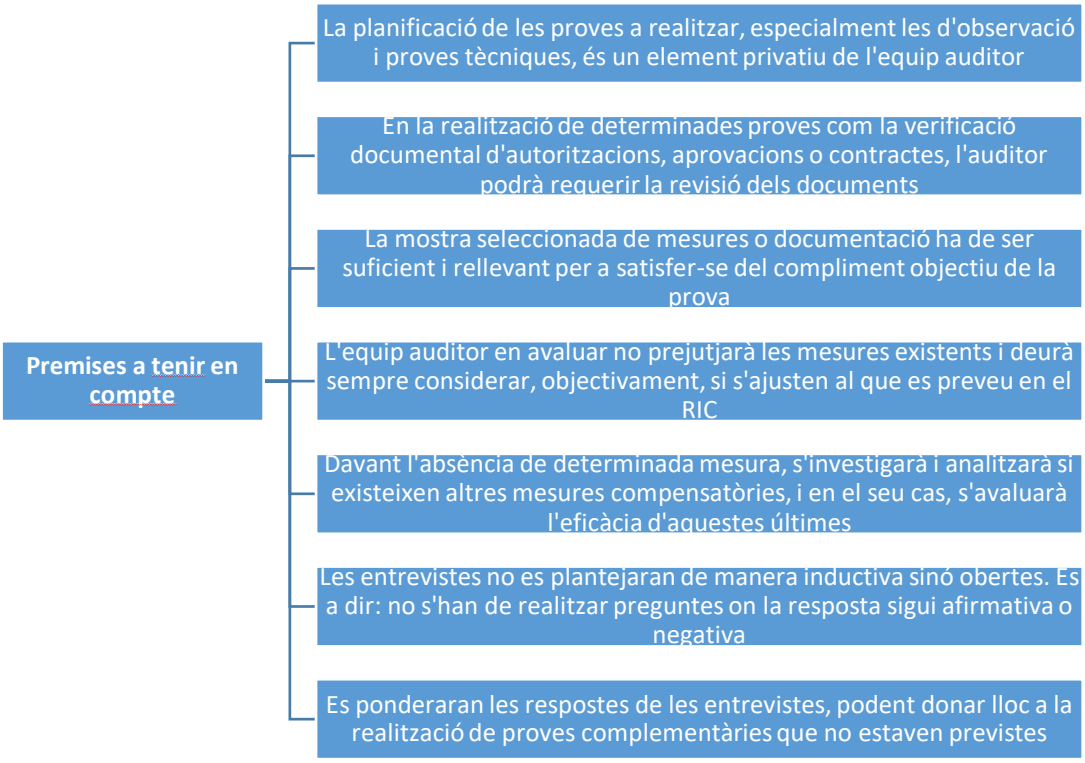
Mesures de protecció

Declaració d'Aplicabilitat

Processos de millora continua de la seguretat

- Avaluar el cicle de maduresa del sistema de gestió de la seguretat
- No conformitats detectades, derivades o no d'accions
- Accions correctives i preventives
- Agenda de millores

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



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

- L'evidència recollida ha de ser suficient i rellevant
  - 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 a incloure en l'informe, s'evidencií clarament l'incompliment persistent o una indiscutible deficiència de seguretat
- La verificació de la documentació haurà de fonamentar-se en les conclusions de la revisió
- Les conclusions o informació recollida en una entrevista hauran de correspondre a una declaració de fets
- Els correus electrònics, en la mesura que involucri a diverses persones dins de l'abast de l'auditoria, poden servir com a prova d'auditoria
- Les proves d'observació hauran d'estar documentades detallant la data i lloc o actiu observat
- Els documents de treball de l'equip auditor hauran de mantenir-se com a mínim durant els dos anys següents degudament referenciats i arxivats
- Quan l'equip auditor descobreix una irregularitat significativa de fàcil resolució, pot informar immediatament el Responsable de la Seguretat

3.5 ELABORACIÓ I PRESENTACIÓ DE LES TROBALLES DE L'AUDITORIA

Objectiu
L'objectiu principal de la presentació dels resultats de les revisions i proves, és confirmar els fets i les situacions detectades o identificades com a resultat de les proves i revisions realitzades

Presentació
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

Resultats
Tots els resultats de proves, relacionats entre si o que es refereixin a una mateixa no conformitat, seran agrupats en un annex a l'Informe d'Auditoria

3.6 PRESENTACIÓ DE L'INFORME D'AUDITORIA

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

No Conformitat Menor

- Es documentarà davant l'absència o la fallada en la implantació o manteniment d'un o més dels requisits de el RIC, 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

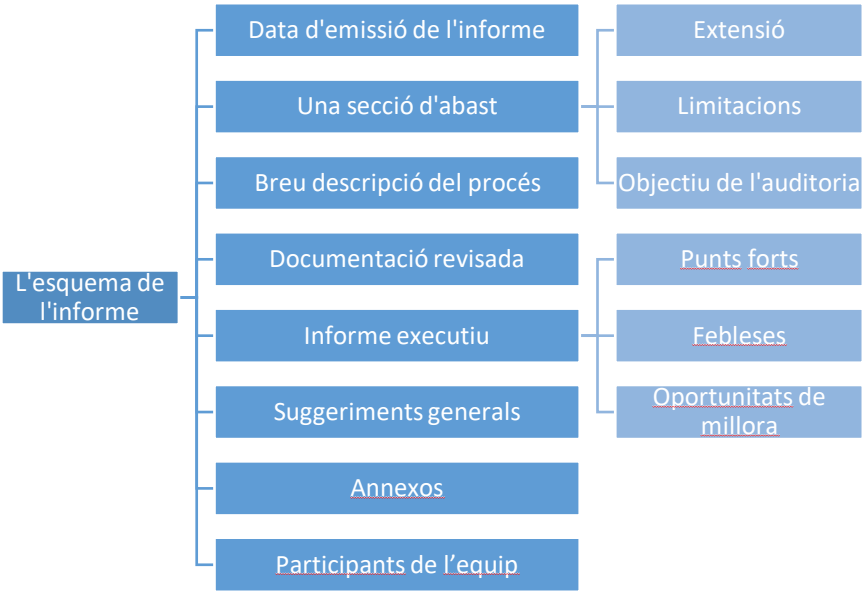
No Conformitat Major

- Es documentarà una 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 que, avaluades en el seu conjunt, puguin implicar l'incompliment de l'objectiu del Grup o Subgrup considerats

13. L'informe d'Auditoria haurà de contenir la informació adequada i suficient per a facilitar i justificar la corresponent certificació:

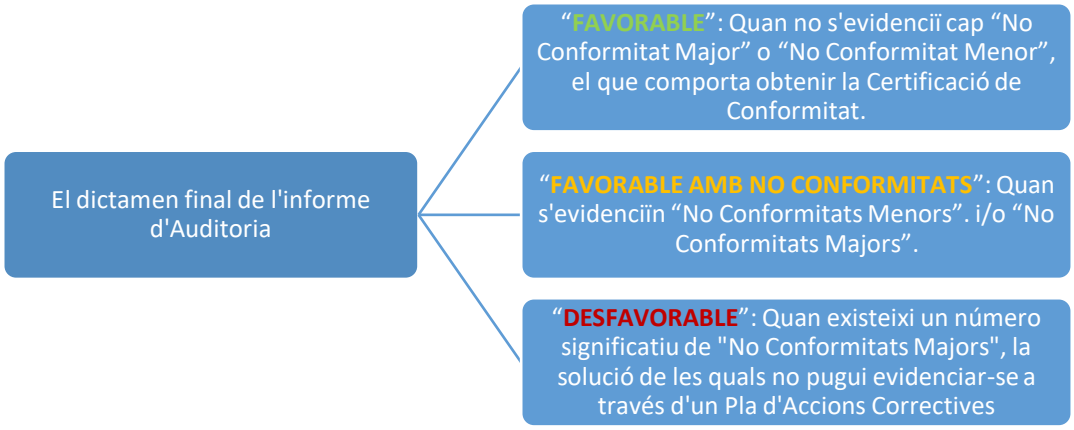
- **Sistema de gestió de la seguretat de la informació**
  - Documentat
  - Procés regular d'aprovació per part de la direcció.
- **Política de Seguretat**
- **Organització**
  - Rols i funcions dels responsables de la informació
  - Serveis
  - Actius
  - Seguretat del sistema d'informació
- **Apreciació del risc**
  - Escenaris de risc
  - Anàlisi de les conseqüències i la seva probabilitat
  - Avaluació de la seva acceptabilitat o inacceptabilitat per a l'organització
  - Revisió i aprovació regular.
- **Detall del nivell de seguretat**
- **Mesures de seguretat**
- **Declaració d'Aplicabilitat**
- **Procés de millora contínua de la gestió de la seguretat.**
- **Àrees organitzatives, mòduls o funcions del sistema d'informació**
- **Conformitats i no conformitats identificades.**
- **El dictamen per part de l´equip d´auditoria**

14. L'Informe d'Auditoria ha d'estar degudament signat pel responsable de l´auditoria, la direcció de l´entitat i serà remés a l´Autoritat Nacional Competent, incloent:



3.7 DICTAMEN FINAL DE L'INFORME D'AUDITORIA

15 El dictamen final de l'informe d'Auditoria per part de l´ANC-AD serà un dels següents:



3.8 EXEMPLE MESURES DE SEGURETAT

16. 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.