Finançat per:
Finançat per la Unió Europea NextGenerationEU
Pla de Recuperació, Transformació i Resiliència
incibe_
Agència de Ciberseguretat de Catalunya
Next Generation Catalunya
Generalitat de Catalunya
Amb la col·laboració de:
Localret

Plec de prescripcions tècniques (PPT) que regeix el contracte de serveis d'auditoria tècnica de ciberseguretat (Exp. 1403-0035/2025), basat en el lot 2 de l'acord marc de subministrament de solucions i serveis gestionats de seguretat TIC (Exp. 1431-0003/2025)

Reina Cristina, 9 08003 Barcelona Tel. 934861430 www.localret.cat consorci@localret.cat N.I.F.P5800043A

Contingut

Reina Cristina, 9 08003 Barcelona Tel. 934861430 www.localret.cat consorci@localret.cat N.I.F.P5800043A

Reina Cristina, 9 08003 Barcelona Tel. 934861430 www.localret.cat consorci@localret.cat N.I.F.P5800043A

1 INTRODUCCIÓ I CONTEXT

L'Agència de Ciberseguretat de Catalunya (d'ara endavant, Agència), establerta sota el marc de la Llei 15/2017, del 25 de juliol, és l'entitat que lidera i coordina els esforços de la Generalitat de Catalunya en la protecció de la informació i les infraestructures del país davant les ciberamenaces. En un món digitalitzat i interconnectat, la seguretat de la informació s'ha convertit en una prioritat estratègica, i l'Agència subratlla el compromís de Catalunya amb la promoció d'un entorn digital segur i de confiança.

Aquest contracte és finançat per Fons Europeus. El programa RETECH constitueix un dels nous eixos transversals de l'Agenda España Digital 2026 promoguts pel Ministerio de Asuntos Económicos y Transformación Digital, i està alineat amb dues de les principals fites de l'Agenda, com són, liderar la transformació digital de manera inclusiva i sostenible i focalitzar els esforços de digitalització en sectors econòmics clau. L'objectiu del Programa RETECH és impulsar xarxes territorials d'especialització tecnològica, articulant projectes regionals que s'orientin a la transformació i especialització digital, assegurant la coordinació, la col·laboració i la complementarietat.

Gràcies a aquest nou eix de l'Agenda España Digital 2026, es pretén liderar un canvi rupturista, de manera inclusiva i sostenible, focalitzant els esforços de digitalització en sectors econòmics clau. En definitiva, la iniciativa RETECH permetrà impulsar els projectes tractors proposats per les Comunitats i Ciutats Autònomes, fomentant l'intercanvi de coneixement i multiplicant les oportunitats de cada regió, a través de xarxes d'impacte nacional que permetin maximitzar l'equilibri territorial i la cohesió social entre elles.

Per fer efectiva la iniciativa RETECH amb total transparència i igualtat d'oportunitats per a totes les Comunitats i Ciutats Autònomes interessades, el Ministerio de Asuntos Económicos i Transformación Digital, a través de la Secretaria d'Estado de Digitalización e Inteligencia Artificial, va llançar una invitació pública destinada al desenvolupament de propostes de cooperació per finançar iniciatives emblemàtiques d'especialització territorial tecnològica dins de les seves competències.

En el cas de la comunitat autònoma de Catalunya l'Agència és l'entitat responsable de la implementació del Projecte RETECH CCAA i de les actuacions derivades de l'Acord RETECH a Catalunya. Per tant, li correspon concretar els múltiples subprojectes i accions de ciberseguretat que promouran el desenvolupament tecnològic i incrementaran la confiança digital tant del govern autonòmic com dels ciutadans i empreses del territori català.

Pel que fa a la Línia d'actuació Ciberseguretat de Retech Excel·lència Operativa sobre entitats del món local, aquesta té la missió de millorar el seu estat de protecció en l'àmbit de la ciberseguretat.

Aquesta iniciativa s'emmarca en el Programa RETECH i en el Pla de Recuperació, Transformació i Resiliència (PRTR), finançat per la Unió Europea a través dels fons NextGeneration EU, a través de l'Instituto Nacional de Ciberseguridad (d'ara endavant, INCIBE).

Reina Cristina, 9 08003 Barcelona Tel. 934861430 www.localret.cat consorci@localret.cat N.I.F.P5800043A

Els objectius del Projecte RETECH CCAA que es pretenen cobrir amb el desenvolupament d'aquesta iniciativa, són els següents:

- OE1 Cohesionar l'ecosistema de ciberseguretat nacional
- OE3 Fomentar la capacitació especialitzada en ciberseguretat
- OE4 Impulsar projectes innovadors, solucions i serveis avançats als reptes de ciberseguretat als quals s'enfronta la societat.

Aquests objectius estan en línia amb l'objectiu 248 del Pla de Recuperació, Transformació i Resiliència de la Decisió d'execució del Consell (CID): Desenvolupament de solucions i serveis d'elevat valor afegit en l'àmbit de la ciberseguretat.

Per aconseguir aquest propòsit, l'Agència té previst col·laborar amb entitats públiques especialitzades en l'àmbit del món local per generar una protecció efectiva davant les ciberamenaces actuals, així com per estructurar una administració cibersegura i garantir la ciberseguretat de les administracions locals i supramunicipals catalanes. En aquest sentit, ha establert una col·laboració amb el Consorci Localret que busca realitzar un diagnòstic de l'estat de situació en ciberseguretat de les administracions incloses en l'abast del conveni signat per ambdues entitats, establir-hi un pla de ciberseguretat i impulsar el nivell de formació i de compliment normatiu.

En coherència amb aquest marc de col·laboració, les actuacions previstes es duran a terme mitjançant un contracte basat dins de l'abast de l'acord marc "Acord marc de ciberseguretat" publicat el 25 de febrer del 2025 i promogut pel Consorci Localret, que té per objecte el subministrament, instal·lació i suport de productes, així com la prestació de serveis destinats a reforçar la seguretat TIC dels ens, organismes i entitats del sector públic local català.

Aquest acord marc constitueix una oferta integral de productes i serveis amb prou capacitat per donar resposta a les necessitats actuals i futures en matèria de ciberseguretat dels ens locals, recolzant el desplegament de qualsevol pla de seguretat de la informació i garantint l'ús de tecnologia homologada pel Centre Criptogràfic Nacional (CCN). La seva finalitat és permetre a les entitats beneficiàries contractar:

- Lot 1 –Solucions de seguretat TIC incloses al Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i la Comunicació (CPSTIC) del Centre Criptològic Nacional (CCN).
- Lot 2 – Serveis d'auditoria tècnica de ciberseguretat.
- Lot 3 – Serveis de gestió de la ciberseguretat.
- Lot 4 – Serveis de Centre d'Operacions de Seguretat (SOC).
- Lot 5 – Serveis d'adequació a l'Esquema Nacional de Seguretat (ENS).
- Lot 6 – Serveis de formació i conscienciació en ciberseguretat ad hoc.
- Lot 7 – Serveis de CSIRT (Computer Security Incident Response Team).

Concretament, l'actual basat és del lot 2 de l'acord marc, de serveis d'auditoria tècnica de ciberseguretat. Servei encarregat de valorar l'estat de seguretat de l'entitat, identificant vulnerabilitats i riscos que puguin afectar la integritat, confidencialitat i disponibilitat de la informació i els sistemes. Inclou l'anàlisi dels usuaris amb accés, la

Reina Cristina, 9 08003 Barcelona Tel. 934861430 www.localret.cat consorci@localret.cat N.I.F.P5800043A

revisió de l'actualització del programari, proves d'intrusió controlades, l'avaluació del pla de seguretat existent i l'exposició de dades personals.

2 OBJECTE DEL CONTRACTE

L'objecte dels serveis és la realització d'auditories tècniques de ciberseguretat per a les entitats de més de 50.000 habitants, diputacions i consells comarcal amb la finalitat d'identificar punts de millora que permetin incrementar la seva resiliència i reduir la superfície d'exposició davant les principals ciberamenaces que afecten les administracions locals.

També podran ser objecte del contracte alguns municipis de menys de 50.000 habitants, amb funcions, servei informàtic i requisits de ciberseguretat equivalents a consistoris de més de 50.000 habitants.

Aquestes actuacions s'emmarquen en el Model de Ciberseguretat de l'Agència de Ciberseguretat de Catalunya, concretament en les seves fases inicials de Diagnòstic i Identificació d'Iniciatives de Seguretat. Aquest enfocament permet establir les bases per al desplegament progressiu del model a les administracions locals i per a l'alineament amb les directrius estratègiques de l'Agència.

Les auditories es duran a terme en format de caixa grisa, combinant:

- Una avaluació interna, desenvolupada presencialment a les instal·lacions de les entitats, analitzant els sistemes, serveis i aplicacions amb connectivitat IP, tant en entorns locals com a través de xarxes privades virtuals.
- Una avaluació externa, executada de manera remota, orientada a la detecció d'actius públics exposats, vulnerabilitats de configuració i informació delicada accessible des d'internet.

Els objectius principals del servei són:

- Obtenir una visió completa del context de negoci, tecnològic i de ciberseguretat de cada entitat.
- Identificar el grau d'exposició de les entitats a les principals ciberamenaces del sector públic local.
- Detectar vulnerabilitats i riscos, proposant les mesures correctores i de mitigació adequades.
- Proporcionar recomanacions prioritzades, tant de caràcter tècnic com organitzatiu (protocols, procediments i bones pràctiques), que orientin les entitats en les actuacions necessàries per millorar la seva protecció i avançar cap al Perfil de Compliment Específic per a Requisits Fonamentals de Seguretat (PCE-RFS) de l'Esquema Nacional de Seguretat (ENS).
- Facilitar l'establiment del model de relació de les entitats amb els serveis de l'Agència.

Reina Cristina, 9 08003 Barcelona Tel. 934861430 www.localret.cat consorci@localret.cat N.I.F.P5800043A

Per donar context sobre la magnitud del servei, es preveu un volum global aproximat de 60 encàrrecs per cobrir les necessitats de totes les entitats, amb una distribució de sistemes a analitzar molt variada segons la dimensió de cada entitat, tal com segueix:

Nombre Servidors	
Petit <=10	18
Mitja >10 <40	21
Gran >=40 <150	11
Molt Gran >= 150 < 1500	9
1500	1

Aquesta diversitat de dimensions reforça la necessitat que el servei d'auditoria s'adapti a realitats molt diferents, incloent-hi recomanacions tant tècniques com organitzatives per a cada entitat segons el seu nivell de maduresa i complexitat.

En la present licitació es faran 15 encàrrecs tal com es detalla a l'apartat de lots i es preveuen noves licitacions per cobrir les necessitats de la resta d'entitats que sol·licitin el servei. S'inicia amb aquest basat per començar els diagnòstics més llargs que disposem de sol·licituds confirmades.

2.1 Abast i desenvolupament de les actuacions

El servei comprèn un conjunt estructurat d'actuacions que permeten conèixer en profunditat la realitat tecnològica i organitzativa de cada entitat, identificar riscos i vulnerabilitats i definir iniciatives de millora que incrementin el seu nivell de seguretat i resiliència davant de les principals ciberamenaces.

L'abast de les actuacions inclou activitats d'anàlisi tècnica i de consultoria estratègica, amb l'objectiu de disposar d'una visió completa i integrada de l'estat de la ciberseguretat de cada organització.

2.1.1 Recollida i anàlisi de la informació de context

En una primera fase, es durà a terme la recollida i tractament de la informació de context, mitjançant:

- Entrevistes amb els responsables tècnics i funcionals de l'entitat.
- Revisió de la documentació disponible: inventaris d'actius, polítiques i procediments de seguretat, organigrames TIC, plans de contingència i registres d'incidents.

Aquest procés permetrà contextualitzar l'entorn tecnològic i establir la base per a la resta d'activitats.

Reina Cristina, 9 08003 Barcelona Tel. 934861430 www.localret.cat consorci@localret.cat N.I.F.P5800043A

2.1.2 Avaluació tècnica integral

Aquesta avaluació tècnica integral, també anomenada diagnòstic, se centra a avaluar i validar de forma proactiva els mecanismes i controls existents a les entitats envers les principals ciberamenaces del sector. Aquesta avaluació es realitza mitjançant una anàlisi tècnica de febleses i riscos per a la cerca de vulnerabilitats que podrien ser explotades per un possible atacant, complementada amb una consultoria interna de l'arquitectura de seguretat de l'entitat. Addicionalment, s'aborda un diagnòstic del grau de compliment del Perfil de Compliment de Requisits Fonamentals (PCE-RFS) de l'ENS.

Aquest diagnòstic tindrà com a objectiu oferir una visió del grau d'exposició a les 5 principals amenaces identificades com a més rellevants per l'àmbit de les administracions locals i donar una visió global de l'estat de desplegament del perímetre de seguretat a l'entitat. S'identifiquen a continuació les 5 principals amenaces:

1. Desplegament manual de ransomware

   Els atacs de ransomware busquen accedir als sistemes de les víctimes per robar i exfiltrar informació valuosa. Els ciberdelinqüents sovint amenacen de publicar dades confidencials per augmentar la pressió, i el xifratge es converteix en un pas secundari.

2. Compromís de comptes d'usuari legítims de plataformes de correu

   La seguretat dels comptes d'usuari legítims a plataformes de correu electrònic es veu compromesa per atacs que busquen adquirir el control d'aquests comptes i suplantar la identitat de les persones afectades.

3. Compromís d'aplicacions web

   Els atacs a aplicacions web inclouen tècniques diverses com les Webshells, el Defacement i el Black SEO.

4. Intrusions per accessos derivats de troians

   Els troians són la porta d'entrada per a tota mena de programari que proporcioni als ciberdelinqüents accessos no autoritzats a xarxes corporatives. Aquesta informació pot ser utilitzada per desplegar de manera manual ransomware, seleccionant estratègicament els sistemes objectius per maximitzar l'impacte.

5. Credencials compromeses per infostealers

   Un cop les credencials han estat compromeses per un infostealer, els ciberdelinqüents poden fer servir per accedir a sistemes o xarxes corporatives. Aquest accés pot facilitar el desplegament manual de ransomware, cosa que permet als atacants escollir els objectius més valuosos per maximitzar l'impacte.

A tal efecte, s'executarà una avaluació tècnica completa que comprèn:

- Anàlisi interna, que inclourà, l'anàlisi de l'arquitectura, configuracions i controls de seguretat de l'entitat, una prova d'intrusió controlada i una avaluació del compliment del PCE-RFS.
- Anàlisi externa, que estarà, d'una banda, orientada a l'obtenció d'informació mitjançant tècniques OSINT i a la revisió de la seguretat reputacional, incloent-hi la detecció de filtracions de credencials, la identificació de dominis similars o maliciosos i la comprovació d'actius públics. D'altra banda, inclourà l'avaluació de la superfície d'exposició pública de l'organització per identificar vulnerabilitats i riscos en els actius publicats.

L'avaluació es realitzarà considerant uns conjunts de controls referenciats als dominis i controls del NIST Cybersecurity Framework (CSF), així com funcionalitats definides en el perímetre de seguretat de l'Agència de Ciberseguretat de Catalunya, que defineix les capacitats esperades de prevenció, detecció, resposta i recuperació dins l'àmbit del Model Integral de Ciberseguretat.

L'avaluació es desenvoluparà seguint una matriu de controls estructurada segons aquests dos marcs de referència, amb l'objectiu d'obtenir una visió homogènia del nivell de maduresa i cobertura de les capacitats de seguretat de cada entitat.

2.1.3 Avaluació del compliment ENS (PCE-RFS)

El servei inclourà una avaluació específica del nivell de compliment de l'Esquema Nacional de Seguretat (ENS), a partir del Perfil de Compliment Específic de Requeriments Fonamentals de Seguretat (PCE-RFS). Aquesta anàlisi es durà a terme amb el suport d'eines i qüestionaris automatitzats de l'Agència, cosa que permet comparar resultats, consolidar indicadors i identificar desviacions i oportunitats de millora.

2.1.4 Elaboració de l'informe de diagnòstic

Amb tota la informació recollida, s'elaborarà un informe de diagnòstic integral que reflectirà el grau d'exposició de l'entitat a les 5 principals amenaces, els resultats de les anàlisis tècniques, d'arquitectura i dels controls, el grau de desplegament de perímetre i el grau de nivell de compliment respecte al PCE-RFS.

A tal efecte, l'adjudicatari haurà d'utilitzar la plantilla "Informe diagnòstic inicial" disponibles a l'annex 5.

2.1.5 Definició d'iniciatives de millora

A partir dels resultats del diagnòstic, es proposarà un conjunt d'iniciatives de seguretat prioritzades, alineades amb el catàleg de l'Agència de Ciberseguretat de Catalunya, que inclouran descripció, abast funcional i tècnic, recursos estimats i previsió de cost orientativa per facilitar-ne la futura execució.

A tal efecte, l'adjudicatari haurà d'utilitzar la plantilla de "Presentació de resultats executius del diagnòstic i iniciatives de seguretat" disponibles a l'annex 6.

2.1.6 Metodologia i coordinació

Totes les activitats es duran a terme d'acord amb les metodologies, eines, controls i directrius establertes per Consorci Localret i l'Agència, assegurant la coherència, homogeneïtat i comparabilitat dels resultats.

El procés de treball inclourà reunions periòdiques de seguiment per garantir la qualitat de les actuacions i lliurables, la coordinació amb altres serveis en curs i l'alineació amb els objectius del Model Integral de Ciberseguretat de l'Agència.

En l'aplicació de la metodologia de l'Agència i l'elaboració dels lliurables corresponents, l'adjudicatari disposarà d'accés a un espai de l'Agència on podrà accedir als documents, eines i plantilles previstes. L'adjudicatari haurà d'utilitzar aquest espai com a repositori on compartir tota la informació vinculada a la metodologia de l'Agència.

La direcció i supervisió dels equips de treball, així com el control de la qualitat de l'activitat desenvolupada i dels productes resultants seran responsabilitat de l'adjudicatari i formaran part intrínseca de les seves funcions.

3 LOTS

Per garantir la viabilitat del compliment de terminis del projecte i la qualitat del servei es divideix el contracte en 8 lots.

Cada lot, excepte el Lot 1, inclou dos ajuntaments, un de més de 150 servidors i un de menys de 150 servidors.

Els lots són els següents:

- Lot 1 – Servei de diagnosis de l'Ajuntament de Barcelona.
- Lot 2 – Servei de diagnosis de l'Ajuntament de l'Hospitalet de Llobregat i l'Ajuntament de Tarragona.
- Lot 3 – Servei de diagnosis de l'Ajuntament de Sant Boi de Llobregat i l'Ajuntament de Santa Coloma de Gramenet.
- Lot 4 – Servei de diagnosis de l'Ajuntament de Granollers i l'Ajuntament de Rubí.
- Lot 5 – Servei de diagnosis de l'Ajuntament de Sant Cugat del Vallès i l'Ajuntament de Vilanova i la Geltrú.
- Lot 6 – Servei de diagnosis de l'Ajuntament de Reus i l'Ajuntament de Lleida.
- Lot 7 – Servei de diagnosis de l'Ajuntament de Girona i l'Ajuntament de Cornellà de Llobregat.
- Lot 8 – Servei de diagnosis de l'Ajuntament de Terrassa i l'Ajuntament del Prat de Llobregat.

Aquesta divisió en lots permetrà l'execució en paral·lel per complir el calendari i la planificació del projecte, així com el foment de la competència efectiva evitant contractes excessivament grans que podrien limitar la concurrència.

Reina Cristina, 9 08003 Barcelona Tel. 934861430 www.localret.cat consorci@localret.cat N.I.F.P5800043A

En el cas que, per causes justificades per algun ajuntament, no fos possible dur a terme la diagnosi prevista, s'assignarà una altra entitat local amb un volum de servidors i característiques similars.

Tots aquests encàrrecs hauran d'estar completament executats i lliurats abans de meitats del mes de març de 2026.

Els lots s'adjudicaran segons l'ordre següent: lot 1, lot 2, lot 3, lot 4, lot 5, lot 6, lot 7 i lot 8. Els lots s'adjudicaran a l'empresa que hagi presentat la millor oferta que no hagi estat adjudicatària de cap dels lots precedents.

4 CRONOLOGIA DEL PROJECTE

En aquest apartat es mostren de manera ordenada les diferents fases que conformen el projecte, des de les reunions inicials fins al lliurament final dels resultats.

L'objectiu global és avaluar la capacitat de l'organització per resistir, detectar i recuperar-se davant un intent de desplegament de ransomware, analitzant tant la superfície d'exposició externa com la infraestructura interna i els mecanismes de protecció, detecció i resposta existents.

Cada fase del projecte estableix portes de validació que asseguren la coherència dels lliurables i la qualitat dels resultats obtinguts.

Durant tot el període d'execució, l'adjudicatari haurà d'informar quinzenalment sobre l'estat d'evolució dels treballs, incloent-hi els avenços, incidències, troballes rellevants i possibles bloquejos que puguin afectar el calendari.

Aquesta estructura seqüenciada garanteix una execució controlada, traçable i orientada a resultats, amb un seguiment constant per part del Consorci Localret i una validació prèvia abans de la presentació final a les entitats auditades.

4.1 Reunió inicial presencial amb Consorci Localret

Aquesta trobada es durà a terme a les instal·lacions de Consorci Localret dins un termini màxim de quinze dies naturals des de l'adjudicació del contracte.

La seva finalitat serà establir el marc general d'execució del projecte i garantir una comprensió comuna entre totes les parts implicades.

Durant la sessió es revisaran els aspectes següents:

- L'abast concret de les auditories i la metodologia general prevista.
- Els canals de comunicació i coordinació entre les parts.
- Els procediments de seguiment, la periodicitat i el calendari global d'execució.
- Els rols i responsabilitats de Consorci Localret, de l'adjudicatari i de les entitats auditades.
- Els criteris generals per a la gestió documental, la validació de lliurables i la resolució d'incidències.
- Presentació i formació en el model de ciberseguretat i en les metodologies de l'Agència.

L'adjudicatari aixecarà acta de la reunió, on constaran els acords i compromisos adoptats, els responsables designats i el calendari de treball global.

Aquesta acta haurà de ser validada per totes les parts.

4.2 Reunió inicial de presentació amb cada entitat auditada (amb participació opcional de Consorci Localret)

Abans de l'inici del servei d'anàlisi integral, l'adjudicatari haurà de participar en una reunió virtual o presencial amb cadascuna de les entitats auditades, amb l'objectiu de garantir una correcta planificació de les activitats i establir els canals de comunicació i treball.

La presència de Consorci Localret serà opcional, segons es consideri convenient en cada cas.

Aquesta sessió tindrà com a objectius principals:

- Presentar l'equip d'auditors i els interlocutors designats per ambdues parts.
- Exposar la planificació específica de l'auditoria, incloent-hi l'abast, la metodologia, el conjunt d'activitats i el tipus de proves previstes.
- Definir el calendari de treball, les finestres horàries de proves i la disponibilitat dels equips tècnics, amb l'objectiu de minimitzar l'impacte en el servei.
- Establir el protocol d'actuació en cas d'incidència i el procediment per a la comunicació de vulnerabilitats crítiques (Avís Primerenc), incloent-hi punts de contacte, temps de resposta i condicions per a l'aturada immediata de l'exercici (p. ex. compromís d'un sistema crític o indici d'incident real).
- Validar la llista de contactes de totes les parts implicades (auditors i responsables de l'entitat).
- Identificar la documentació i la informació que l'entitat haurà de preparar per facilitar la feina de l'equip auditor i contextualitzar l'estat actual de l'organització en matèria tecnològica i de seguretat de la informació.

  Aquesta documentació podrà incloure, entre d'altres:

  - Inventaris d'actius tecnològics (servidors, estacions de treball, xarxes, dominis, serveis al núvol i còpies de seguretat).
  - Polítiques i procediments de seguretat de la informació.
  - Organigrama TIC i assignació de rols i responsabilitats.
  - Plans de contingència i registres d'incidents.
  - Evidències bàsiques dels controls de seguretat implantats (configuracions, informes d'auditoria o revisions de vulnerabilitats).
  - Determinar els permisos temporals, dades o accés que caldrà facilitar a l'adjudicatari per al correcte desenvolupament de l'auditoria.

L'adjudicatari haurà d'aixecar acta de la reunió, on constin de manera clara i estructurada tots els acords assolits, compromisos, responsables designats, calendari, protocols establerts i documentació a lliurar per part de l'entitat.

Aquesta acta s'haurà de lliurar tant a Consorci Localret com a l'entitat auditada dins dels dos dies hàbils següents a la celebració de la reunió.

4.3 Reunió o reunions tècniques per a la recollida de dades

La fase de recollida de dades té com a finalitat establir una base de coneixement completa i fiable sobre la realitat tecnològica, organitzativa i procedimental de cada entitat. Aquesta tasca és essencial per garantir que les activitats d'anàlisi tècnica i de diagnòstic parteixin d'informació contrastada, actualitzada i coherent amb la situació real de l'organització.

Aquestes reunions seran presencials o virtuals segons necessitats del servei.

4.3.1 Objectius de les reunions tècniques

Durant aquesta fase, l'adjudicatari durà a terme una o diverses reunions tècniques amb els responsables tècnics, funcionals i de seguretat de l'entitat, amb els objectius següents:

- Contextualitzar l'entorn TIC i conèixer l'abast real dels sistemes i serveis crítics.
- Identificar dependències operatives i punts sensibles.
- Validar els contactes de referència per a la coordinació de les proves.
- Confirmar la disponibilitat i adequació de la documentació necessària per a l'auditoria.
- Sol·licitar, si escau, documentació complementària no facilitada prèviament per assegurar la correcta execució de les activitats de diagnòstic.

4.3.2 Suport en el qüestionari PCE-RFS

L'adjudicatari proporcionarà suport directe a l'entitat en la resposta del qüestionari del Perfil de Compliment Específic de Requeriments Fonamentals de Seguretat (PCE-RFS), mitjançant el servei i formulari interactiu ENS360 de l'Agència de Ciberseguretat de Catalunya.

Aquesta eina proporciona un qüestionari i procés estructurat de recollida d'informació del compliment del PCE-RFS, i genera un seguit d'indicadors i recomanacions que l'adjudicatari haurà d'utilitzar en l'avaluació integral.

Les tasques de l'adjudicatari son:

- Personalitzar el qüestionari amb la informació de l'entitat.
- Planificar, dintre del calendari d'entrevistes i sessions de treball previstes amb l'entitat, l'espai necessari per omplir el qüestionari amb els responsables corresponents.
- Assessorar i acompanyar a l'entitat durant tot el procés de resposta.

- Incorporar comentaris qualitatius o aclariments per a cada resposta, especialment en els casos en què s'observin excepcions, limitacions o accions en curs.
- Resoldre dubtes interpretatius i si s'escau validar les respostes amb les evidències documentals o operatives existents.
- Validar la integritat i coherència de les respostes amb la informació disponible d'altres controls i anàlisis tècniques.
- Revisar la qualitat abans del tancament del formulari, verificant que totes les preguntes hagin estat contestades, comprovant coherència entre respostes i comentaris associats, i que les dades recollides reflecteixen la realitat de l'entitat.
- Enviar al servei ENS360 de l'Agència el qüestionari completat (en el format ENS360_ENTITAT_DATA.pdf), per al seu processament, valoració i generació d'indicadors.
- La informació i indicadors que el servei ENS 360 proporcionarà automàticament a l'adjudicatari correspondran a:
    - Indicadors quantitatius:
        - Percentatge de compliment general
        - Percentatge de compliment per domini de seguretat de l'ENS
        - Percentatge de compliment per subdomini
        - Compliment ponderat respecte a la mitja de nivell de compliment del sector al qual pertany l'entitat
    - Diversos gràfics i visualitzacions del nivell de compliment per subdomini i marc de control
    - Resum executiu per entitat:
        - Punts forts (àrees amb alt nivell de compliment o bones pràctiques consolidades)
        - Punts febles (àrees amb baix compliment o mancances crítiques)
        - Recomanacions prioritzades.
        - Valoració global de l'estat de situació a mode conclusió
- L'adjudicatari haurà de:
    - Incorporar aquesta informació facilitada pel servei ENS 360 en l'informe de diagnòstic de l'entitat.
    - Utilitzar les recomanacions generades com a base per a la definició de les iniciatives de seguretat previstes en el Pla d'iniciatives o projectes de seguretat, respecte a la millora del compliment de l'ENS.
    - Complementar o matisar les recomanacions automàtiques amb les seves pròpies observacions, adaptant-les a la realitat organitzativa i als recursos disponibles de cada entitat.

Per l'execució d'aquestes tasques l'adjudicatari podrà comptar amb el suport del servei d'adequació a l'ENS prestat per altres proveïdors a l'entitat en el marc dels projectes finançats amb fons Retech.

4.3.3 Validació i coherència de la informació

Abans de la seva incorporació a l'anàlisi tècnica i documental, tota la informació recollida serà validada conjuntament amb l'entitat, assegurant la seva traçabilitat, coherència i actualització.

Aquesta validació constitueix un requisit previ essencial per poder iniciar amb garanties les actuacions tècniques.

4.3.4 Confirmació de l'abast i exclusions

En aquesta fase també s'haurà de confirmar i documentar:

- Rangs d'IP, subxarxes, servidors, estacions de treball, sistemes de còpia de seguretat, entorns de virtualització, aplicacions crítiques i serveis que formen part de l'objectiu.
- Una llista clara d'elements exclosos, com ara sistemes no accessibles per raons legals, operatives o de seguretat (ex. entorns de producció sensibles o terminals de pagament).
- Els llindars d'impacte i els criteris d'aturada immediata de l'exercici.

4.3.5 Gestió d'accessos i control d'usuaris auditors

Per garantir la seguretat dels accessos:

- Es registrarà prèviament la totalitat dels comptes i privilegis que utilitzaran els equips d'auditors.
- S'establiran mecanismes d'autenticació i control temporal que garanteixin la traçabilitat.
- Es preveurà la supressió immediata dels comptes un cop finalitzades les proves.

4.3.6 Gestió d'incidències i comunicació

Durant l'execució de les proves:

- Es disposarà d'un equip de resposta a incidències, intern o externalitzat, disponible durant i després de l'exercici.
- Es mantindrà una llista actualitzada de contactes d'emergència, incloent-hi personal tècnic, responsables i proveïdors crítics.
- Es definiran canals de comunicació prefixats i protocols d'activació.

4.3.7 Conformitat legal i protecció de dades

Abans de començar les proves, es revisarà i verificarà la conformitat legal de l'exercici, especialment quan es puguin veure afectades dades personals.

S'establiran mesures de:

- Minimització i anonimització de dades que apareguin en els lliurables.

Reina Cristina, 9 08003 Barcelona Tel. 934861430 www.localret.cat consorci@localret.cat N.I.F.P5800043A

- Tractament segur d'evidències sensibles, en compliment del Reglament (UE) 2016/679 (RGPD) i de la Llei Orgànica 3/2018 (LOPDGDD).

4.3.8 Proves prèvies i validació operativa

Quan sigui possible:

- Es faran proves prèvies en entorns no productius o de simulació per validar configuracions i comportaments.
- Si escau, es programarà una prova pilot limitada per verificar procediments, temps de resposta i coordinació operativa amb l'equip tècnic de l'entitat.

4.3.9 Resultat final de la fase

A la finalització d'aquesta fase, entitat i empresa adjudicatària hauran de disposar d'un coneixement compartit de l'abast, de les responsabilitats i de les condicions de seguretat.

Això garantirà que les proves s'executin en un entorn controlat, segur i traçable, amb totes les condicions prèvies degudament tancades i documentades.

4.4 Reunions de seguiment

Durant el període d'execució, es preveu la realització de reunions de seguiment amb el Consorci Localret, preferentment en format virtual. La seva freqüència serà mensual quan la durada del projecte així ho requereixi, o en el nombre que s'acordi segons les necessitats i el calendari establert. Aquestes trobades serviran per monitorar l'estat de les auditories, revisar l'acompliment de les fites, analitzar incidències, supervisar la qualitat de les actuacions i lliurables, i validar possibles ajustos o millores.

Consorci Localret o l'adjudicatari podran sol·licitar trobades extraordinàries si es detecten necessitats específiques, com ara la resolució d'incidències urgents o la revisió de vulnerabilitats crítiques.

4.5 Informes d'evolució quinzenals

L'adjudicatari haurà de lliurar, amb una periodicitat quinzenal, un informe d'evolució que permeti al Consorci Localret fer un seguiment continuat de l'estat dels treballs i l'assoliment de les fites previstes.

Aquest informe haurà d'incloure, com a mínim:

- la fase o estat actual de cada auditoria o actuació,
- els principals indicadors d'execució i avenç,
- les troballes o incidències detectades,
- les accions correctives o preventives proposades,
- els bloquejos identificats que puguin afectar el calendari o provocar l'allargament dels terminis d'execució,

Reina Cristina, 9 08003 Barcelona Tel. 934861430 www.localret.cat consorci@localret.cat N.I.F.P5800043A

- i la data estimada de finalització de cada fase o tasca en curs.

Els informes s'hauran de lliurar en format electrònic i d'acord amb el model o estructura que determini el Consorci Localret, amb l'objectiu d'unificar la informació i facilitar-ne el seguiment tècnic.

4.6 Anàlisi externa

L'anàlisi externa es planteja amb un doble abast. D'una banda, inclourà totes aquelles activitats que l'adjudicatari podrà dur a terme de manera remota, sense necessitat d'accés físic, orientades a l'anàlisi OSINT i de seguretat reputacional: recerca en fonts obertes, detecció de filtracions de credencials, identificació de dominis similars o maliciosos. D'altra banda, es avaluarà la superfície d'exposició pública de l'organització per identificar vulnerabilitats i riscos potencials en tots aquells actius connectats a Internet que disposin d'una adreça IP pública pròpia o associada a un domini de titularitat de l'entitat.

Queden exclosos els serveis allotjats íntegrament en modalitat SaaS gestionada per tercers (Office 365, plataformes de nòmina, etc.), on la seguretat recau en el proveïdor.

L'auditoria es durà a terme en mode caixa grisa, amb informació bàsica facilitada per l'entitat (dominis, subdominis i actius).

L'adjudicatari executarà una tasca prèvia de descoberta i d'inventari d'actius, que es validarà amb l'entitat en una reunió inicial.

4.6.1 Metodologia i referències

La metodologia combinarà escanejos automàtics i revisions manuals, quan sigui necessari, d'acord amb marcs reconeguts (OWASP, NIST, MITRE ATT&CK). No es limitarà a enumerar serveis, sinó avaluar-ne el risc real.

4.6.2 Activitats mínimes remotes (OSINT i altres)

L'anàlisi externa inclourà, com a mínim, les activitats següents, totes elles executables de forma remota i sense accés físic:

- Recerca en fonts obertes (OSINT): anàlisi de xarxes socials, fòrums, blogs i altres canals públics relacionats amb l'entitat per detectar suplantacions, perfils falsos, campanyes hostils o mencions que puguin implicar riscos reputacionals o de seguretat.
- Identificació i verificació de filtracions de credencials o dades en bases públiques de leaks, així com en entorns de deep web i dark web, i monitoratge de mercats il·lícits per detectar la venda d'informació vinculada a l'entitat.
- Anàlisi de DNS, subdominis i whois, incloent-hi la detecció de subdominis no controlats, mal protegits o aparcats, així com la validació de configuracions i possibles riscos d'exposició.

- Revisió de possibles exposicions en repositoris de codi públics (GitHub, GitLab, Bitbucket) i anàlisi de metadades en documents publicats per l'entitat (p. ex., a webs corporatives).
- Detecció de configuracions incorrectes i serveis exposats amb eines OSINT com Shodan, Censys, Zoomeye o Google Dorks, incloent-hi revisions bàsiques de configuració de serveis al núvol sota control de l'entitat (AWS, Azure, GCP).
- Identificació de dominis similars o dominis maliciosos potencialment utilitzables per a phishing o suplantació.
- Revisió de la reputació i configuració de correu electrònic i dominis: validació de registres SPF, DKIM i DMARC, detecció en llistes negres (blacklists) i verificació de bones pràctiques de seguretat.
- Anàlisi de l'empremta digital dels usuaris (xarxes socials i altres fonts públiques) per identificar vectors potencials d'enginyeria social i riscos de seguretat associats.

4.6.3 Anàlisi tècnica per IP i servei

L'anàlisi tècnica dels actius detectats amb IP pública es realitzarà seguint metodologies i estàndards reconeguts internacionalment (p. ex. OWASP, OSSTMM, PTES), amb l'objectiu de garantir una auditoria professional, rigorosa i repetible.

De cada IP i servei identificat s'avaluarà com a mínim:

- Identificació i mapatge de serveis i ports oberts, incloent-hi la detecció de possibles serveis amagats o no documentats.
- Enumeració de tecnologies, versions i sistemes operatius per establir el context de l'auditoria.
- Detecció de vulnerabilitats conegudes (CVE) i configuracions insegures, amb priorització segons el nivell de risc i l'impacte potencial.
- Verificació de serveis no declarats o no autoritzats, que puguin ampliar la superfície d'exposició.
- Avaluació de les mesures de defensa existents, incloent-hi sistemes de detecció i prevenció d'intrusions, tallafocs i mecanismes de segmentació de xarxa.
- Revisió de bones pràctiques i compliment normatiu, com ara alineament amb ENS, ISO/IEC 27001, NIST o altres marcs aplicables al sector públic.

Els resultats de l'anàlisi inclouran les evidències i la traçabilitat de les proves realitzades, així com recomanacions prioritzades segons criticitat i alineades amb bones pràctiques establertes, indicant també el nivell de facilitat d'implementació de cada mesura correctiva i una estimació dels costos associats a la seva aplicació. Tota aquesta informació s'haurà de lliurar amb el detall necessari perquè l'entitat pugui reproduir i validar els resultats de manera autònoma.

4.7 Anàlisi interna

L'anàlisi interna té per objectiu proporcionar una avaluació exhaustiva i pràctica de la resistència de l'entitat davant d'un atac amb un elevat impacte, amb especial èmfasi en la simulació de desplegament manual de ransomware.

Aquesta comprovació es realitza partint de la premissa que un agent maliciós ha obtingut ja un accés intern mínim a la infraestructura; no s'investigarà en aquesta fase l'origen o vector inicial d'entrada, sinó que la prioritat serà avaluar la profunditat d'explotació i l'impacte potencial des d'aquest punt d'accés.

L'auditoria interna es durà a terme en mode caixa grisa, d'acord amb la metodologia d'avaluació de l'exposició de l'amenaça de l'Agència, utilitzant la informació bàsica facilitada per l'entitat per planificar i executar les proves de manera controlada.

Les proves es realitzaran in situ, amb connectivitat directa des de punts de xarxa acordats amb l'entitat (un amb visibilitat a totes les VLANs o punts separats per segment). No es faran connexions remotes externes, per garantir el màxim control i seguretat de l'execució.

L'activitat d'anàlisi interna inclou, entre altres, les següents tasques:

- Validació de la coherència de les dades recollides: validar i contrastar la informació obtinguda en les entrevistes i en els qüestionaris amb les evidències tècniques observades in situ o a través d'eines d'anàlisi (inventaris, configuracions, llistats d'usuaris, logs i captures).
- Descobriment de la superfície interna: escaneig controlat per identificar xarxes internes, rangs d'IPs, dispositius, ports oberts i serveis exposats dins de l'entorn, amb l'objectiu d'establir el mapa d'actius vulnerables i les seves relacions.
- Anàlisi de configuracions i controls: revisió de la configuració de controladors de domini, servidors crítics, sistemes de còpia de seguretat, entorns de virtualització i estacions de treball per determinar debilitats en polítiques d'accés, segregació de xarxes i proteccions existents.

Aquest enfocament garanteix que l'auditoria interna cobreix tota la superfície d'atac interna i híbrida (on-premise, cloud i storage), així com els accessos interns i remots, proporcionant una visió completa dels riscos i vulnerabilitats reals.

S'escometrà una anàlisi exhaustiva de tota la xarxa interna per identificar vulnerabilitats i vectors d'explotació. Aquesta anàlisi inclou: mapatge d'IPs i subxarxes, escaneig de ports i serveis, identificació de dispositius i sistemes exposats, inventariat de serveis i versions, detecció de serveis cloud i integracions amb tercers, i comprovació de configuracions crítiques (controladors de domini, servidors, entorns de virtualització i sistemes de còpies de seguretat), entorns de wifi. Les proves d'escaneig i descoberta s'executaran de manera controlada (sense provocar DoS), es correlacionaran amb la informació obtinguda a les entrevistes i amb els inventaris proporcionats, i s'inclouran en la bitàcola d'evidències per a la seva validació i posterior anàlisi. Els resultats serviran per prioritzar vulnerabilitats, definir vectors utilitzats en el posterior intent de desplegament de ransomware i fonamentar les recomanacions incloses en els lliurables.

4.7.1 Abast de l'anàlisi interna

L'auditoria interna comprendrà l'avaluació dels equips, sistemes i infraestructures internes de l'organització, amb la finalitat d'identificar vulnerabilitats, configuracions insegures i riscos operatius que puguin facilitar un atac o un desplegament de ransomware.

L'abast inclourà, com a mínim:

- Servidors físics i virtuals, com a actius prioritaris del sistema d'informació.
- Dispositius de xarxa (switches, routers, tallafocs, balancejadors i proxys), per revisar la seva configuració general, actualització i coherència amb la política de segmentació de la xarxa.
- Sistemes d'emmagatzematge (NAS, SAN, cabines o solucions similars) i els seus mecanismes de protecció, permisos i accés.
- VLANs i segments interns, incloent-hi les interconnexions amb la DMZ i els serveis externs.
- Xarxes Wi-Fi corporatives i d'invitats, per comprovar la seva separació i el nivell de seguretat aplicat.
- Sistemes industrials o d'operació (OT), si n'hi ha, i la seva integració o dependència respecte a la xarxa corporativa.
- Infraestructura i serveis al núvol sota control de l'entitat, sempre que siguin accessibles des de la xarxa interna.
- Altres dispositius amb connectivitat, com estacions de treball, portàtils, impressores multifunció o dispositius IoT, quan siguin rellevants per a la seguretat global.

L'anàlisi tindrà un enfocament de nivell diagnòstic, orientat a detectar riscos evidents i vulnerabilitats crítiques, establint una visió global de la postura de seguretat interna i la seva capacitat de resiliència davant amenaces de tipus ransomware.

4.7.2 Proves d'intrusió i explotació controlada

Es requereix l'execució de proves d'intrusió i explotació orientades a reproduir el cicle d'un atac que aspiraria a desplegar ransomware (p. ex. elevació de privilegis, moviment lateral, exfiltració de credencials i tractament de còpies de seguretat), sempre amb les cauteles i límits acordats per evitar afectació a la disponibilitat.

L'objectiu principal serà simular un intent de desplegament manual de ransomware partint de la premissa que un atacant ja ha obtingut accés intern a la infraestructura. Aquesta comprovació no inclourà la recerca dels vectors d'entrada, sinó que avaluarà la profunditat d'explotació i l'impacte potencial des d'un accés compromès, identificant punts crítics com controladors de domini, sistemes de còpies de seguretat i plataformes de virtualització.

Les proves es faran amb enfocament de caixa grisa, seguint metodologies reconegudes (UKC, NIST SP800-115, MITRE ATT&CKi cobrint descoberta i visibilitat de xarxa, identificació de ports i serveis, anàlisi de vulnerabilitats, explotació controlada i proves de resistència.

La prova haurà de cobrir com a mínim les següents activitats:

- Visibilitat i descobriment de xarxa.
- Identificació de ports i serveis de xarxa.
- Anàlisi i descobriment de vulnerabilitats.
- Password cracking.
- Fase de penetració utilitzant les principals vulnerabilitats descobertes.
- Prova de capacitats (tècniques, CVE i eines) associades a les principals amenaces facilitades per l'Agència.
- Proves bàsiques de WIFI si aplica (visibilitat, enumeració, proves d'accés basic).
- Documentació del procés / processos d'intrusió, les vulnerabilitats detectades i les recomanacions corresponents, i l'avaluació del grau d'exposició segons les capacitats (tècniques, CVE i eines) vinculades al top5 d'amenaces esmentades de l'àmbit.

Totes les proves hauran de garantir la continuïtat del servei (sense provocar DoS) i definir prèviament, d'acord amb l'entitat i amb Consorci Localret, l'abast, les exclusions i les finestres de prova. Els resultats i les evidències obtingudes s'integraran a l'informe de diagnòstic de l'entitat, incloent-hi la matriu NIST aplicada, la bitàcola d'accions i les recomanacions prioritzades.

4.7.3 Avaluació de vulnerabilitats i configuracions dels equips , servidors i perifèrics

L'auditoria analitzarà els equips interns de l'organització prioritzant servidors físics i virtuals com a elements crítics de la infraestructura.

L'objectiu és identificar vulnerabilitats i configuracions insegures que puguin comprometre la seguretat de la informació.

Consistirà en la descoberta i inventari detallat dels equips i serveis actius.

S'utilitzaran eines automàtiques d'escaneig per trobar serveis exposats, ports oberts i protocols insegurs. Aquesta activitat inclourà també la revisió de versions de sistema operatiu obsolet, l'estat de pegats, firmware i aplicacions instal·lades, amb especial atenció a plataformes de virtualització, així com a les interfícies d'administració que puguin ser accessibles des de la xarxa interna.

Es revisaran aspectes com les polítiques de bloqueig de sessió, el xifratge de disc i de comunicacions, la configuració de protocols segurs (TLS) i la desactivació de serveis innecessaris o insegurs. Es validaran els mecanismes de protecció desplegats en els endpoints: antivirus i EDR (estat, cobertura i capacitat de detecció), tallafocs locals i coherència amb els de xarxa, monitoratge d'integritat i eines de control de canvis.

De manera complementària, i segons l'abast i els objectius definits per a cada entitat, es podran incloure també altres dispositius com estacions de treball, portàtils, impressores multifunció o qualsevol altre equip amb capacitat de processament i connectivitat a la xarxa corporativa.

4.7.4 Revisió de la seguretat dels usuaris i l'autenticació

L'auditoria avaluarà en profunditat del marc de gestió d'identitats i control d'accés de l'entitat, amb l'objectiu de verificar no només l'existència de polítiques i procediments, sinó també la seva eficàcia real i el grau de compliment pràctic.

L'anàlisi inclourà la revisió detallada de les polítiques de contrasenyes, comprovant longitud, complexitat, historial, caducitat i l'ús de mecanismes de bloqueig davant intents d'autenticació fallits. Es contrastarà la seva coherència amb les bones pràctiques i normatives aplicables (ENS, ISO 27001, NIST, etc.). Es durà a terme una identificació de comptes orfes o inactius, de comptes amb privilegis excessius i la seva correcta assignació segons el principi de mínim privilegi i la segregació adequada de rols (SoD).

També s'avaluarà la implementació i eficàcia dels mecanismes d'autenticació multifactor (MFA) en tots els serveis crítics, validant la seva configuració i cobertura. Es revisaran els processos d'alta, modificació i baixa d'usuaris, incloent-hi els temps de reacció davant canvis de rol, incorporacions i sortides de personal, així com els controls establerts per evitar accessos indeguts tant en entorns interns com remots.

L'auditoria comprovarà la gestió dels comptes privilegiats i de servei, incloent-hi la revisió dels mecanismes de control i rotació de credencials. Es validarà que els accessos dels administradors i comptes crítics disposen de traçabilitat completa, amb registres íntegres i centralitzats, i que aquests logs es custodien adequadament i són utilitzats per a la detecció i resposta davant incidents.

Per fer-ho, s'analitzaran les configuracions en els sistemes de directoris (Active Directory, LDAP o equivalents), els informes de permisos i els registres d'accés. Es realitzaran mostrejos i entrevistes per comprovar que els procediments establerts s'apliquen realment a la pràctica, i que les revisions periòdiques de permisos es duen a terme i documenten adequadament.

La revisió de la gestió d'usuaris i permisos inclourà la identificació de comptes per defecte o innecessaris, comptes amb privilegis excessius, l'adequació al principi de mínim privilegi i l'aplicació de mecanismes d'autenticació robustos. S'analitzarà la presència de credencials febles o per defecte, la reutilització de contrasenyes entre serveis i la protecció dels secrets emmagatzemats en els equips.

L'objectiu és determinar la resistència real de l'entorn d'identitats davant tècniques d'atac habituals, així com la seva capacitat de detecció i resposta.

4.7.5 Anàlisi de l'arquitectura de seguretat i controls

L'avaluació es realitzarà considerant els dominis i controls del NIST Cybersecurity Framework (CSF), així com funcionalitats definides en el perímetre de seguretat de l'Agència de Ciberseguretat de Catalunya.

L'avaluació es desenvoluparà mitjançant entrevistes, seguint una matriu de controls estructurada segons aquests dos marcs de referència, analitzant la documentació proporcionada i tenint en compte els resultats de les proves tècniques executades.

L'avaluació abastarà, com a mínim, els següents dominis:

- Seguretat en la xarxa
- Protecció de sistemes d'informació
- Protecció del lloc de treball
- Serveis IT de ciberseguretat
- Gestió d'identitats, control d'accés i autoritzacions
- Elements de seguretat transversals
- Gestió d'incidents i resposta
- Correu electrònic
- Còpies de seguretat i mecanismes de recuperació
- Contingència i continuïtat del servei

La descripció detallada dels controls, activitats i funcionalitats associades al perímetre es poden consultar a la plantilla oficial de l'informe de diagnòstic definida per l'Agència de Ciberseguretat de Catalunya (annex 5).

Per a la correcta execució de l'anàlisi, s'utilitzaran els formularis per a la recollida i ampliació de la informació de les entitats i els qüestionaris d'avaluació definits per l'Agència, que permeten garantir l'homogeneïtat metodològica i la traçabilitat dels resultats entre entitats.

Aquests formularis i plantilles es presentaran en detall durant la primera reunió d'inici de contracte.

Aquesta estructura permetrà establir una correspondència directa entre els controls avaluats i els apartats de la plantilla d'informe de diagnòstic oficial de l'Agència, garantint la traçabilitat i la comparabilitat dels resultats entre entitats.

4.7.6 Anàlisi del SIEM/SOC

Si l'entitat disposa de SIEM/SOC l'auditoria avaluarà de manera integral l'eficàcia de l'arquitectura de seguretat i la seva capacitat per detectar i respondre a incidents. En cap cas l'actuació consisteix a fer proves específiques exclusives sobre el SIEM/SOC com a objectiu aïllat; en canvi, les activitats pròpies de l'auditoria i de l'intent controlat de desplegament d'un ransomware generaran processos i artefactes que el SIEM/SOC hauria de detectar en condicions operatives reals. La finalitat de la validació és comprovar si aquestes accions han estat identificades i gestionades pel sistema de monitoratge i resposta.

Es vol comprovar:

- Cobertura i coherència dels controls interns de seguretat, verificant que els actius crítics estan protegits segons les polítiques establertes i que no existeixen buits de seguretat rellevants.
- Capacitat operativa per detectar i respondre a incidents (accés inicial, moviment lateral, escalada i indicadors d'intent d'encriptació), mitjançant la revisió del flux de telemetria: recepció i integritat dels logs dels actius rellevants, processos de normalització, correlació d'esdeveniments, llindars d'alerta i mecanismes d'orquestració i resposta.

- Retenció, custòdia i integritat dels registres de seguretat, assegurant el compliment dels requisits legals i normatius aplicables (ENS, ISO 27001, NIS2, RGPD) i la disponibilitat de la informació necessària per a la investigació d'incidents.

La validació consistirà a contrastar les proves executades amb la informació registrada pel sistema de monitoratge, determinar si s'han generat alertes i examinar la corresponent cadena d'escalat i resposta.

4.7.7 Revisió i validació de còpies de seguretat

S'avaluarà l'estratègia de còpies de seguretat de l'organització, verificant la seva cobertura respecte a tots els actius crítics (servidors, bases de dades i aplicacions) i la freqüència de les còpies (completes, incrementals, diferencials), comprovant que és adequada als requisits de continuïtat de negoci. Es revisarà la segregació de les còpies per evitar que un incident intern o un atac (p. ex. ransomware) pugui afectar simultàniament els backups i la infraestructura de producció; això inclou la validació de l'existència de còpies offline, immutables o ubicades en entorns externs i segurs.

També s'analitzarà la configuració del xifratge de les còpies (tan en repòs com en trànsit) i la gestió de claus associades, així com els mecanismes de control d'accés al sistema de backup, verificant que només personal autoritzat hi té accés i que s'apliquen el principi de mínim privilegi i mecanismes d'autenticació forts.

Un element clau serà la revisió de les proves periòdiques de restauració, amb mostrejos per validar que les còpies es poden recuperar de manera efectiva.

Finalment, es revisaran els riscos de seguretat associats al sistema de backup, com ara vulnerabilitats en els servidors o software de còpia, configuracions per defecte no corregides, manca de monitoratge i alertes, o absència de plans de contingència en cas de fallada del sistema principal de còpia. L'objectiu és garantir que la política de backups no només existeix sobre el paper, sinó que és eficaç, resilient i alineada amb les millors pràctiques i els estàndards normatius (ENS, ISO 27001, NIST), aportant garanties reals de continuïtat de negoci i recuperació davant incidents greus.

4.8 Reunió de validació amb Consorci Localret

Abans de dur a terme la reunió de tancament amb l'entitat auditada, l'adjudicatari haurà de participar obligatòriament en una sessió de validació prèvia amb el Consorci Localret, amb l'objectiu de revisar i validar els resultats i els lliuraments corresponents a aquella auditoria.

En aquest punt, l'adjudicatari haurà d'entregar la totalitat de la documentació final generada en el marc de l'auditoria per a la seva revisió, incloent-hi informes, evidències, annexos, recomanacions i qualsevol altre material previst al contracte o sol·licitat durant el procés.

L'objectiu d'aquesta reunió és:

- Revisar la qualitat tècnica i formal dels informes finals i de la documentació que es preveu lliurar a l'entitat.
- Detectar possibles ajustos o millores abans de la presentació final a l'entitat auditada.
- Comprovar la correcta integració de les observacions recollides durant la reunió amb l'entitat.
- Verificar la traçabilitat i coherència dels resultats respecte a la metodologia i criteris definits en el contracte.
- Avaluar incidències, lliçons apreses i aspectes de millora de cara a futures auditories.

Aquesta sessió tindrà un caràcter intern de seguiment i validació, i no implicarà cap modificació dels resultats validats amb l'entitat, sinó la seva consolidació dins el conjunt documental del projecte.

En cas que s'identifiquin mancances, errors formals o necessitats de correcció, l'adjudicatari haurà d'esmenar-les en el termini establert pel Consorci Localret, no podent-se celebrar la reunió de tancament amb l'entitat fins a la validació final dels documents.

L'adjudicatari aixecarà acta de la reunió, que inclourà els acords, observacions i validacions efectuades per Consorci Localret. Aquesta acta servirà com a registre de control de qualitat i formarà part de la documentació final del contracte.

4.9 Reunió de tancament amb l'entitat auditada

Un cop validats els resultats amb el Consorci Localret, l'adjudicatari durà a terme una reunió de tancament individual amb la mateixa entitat auditada.

Aquesta sessió tindrà caràcter virtual o presencial segons disponibilitat i logística, i podrà comptar amb la presència opcional de Consorci Localret, segons es consideri oportú.

L'objectiu d'aquesta reunió és:

• Presentar els resultats i les conclusions tècniques de l'exercici de diagnòstic.

• Validar les evidències principals i els resultats del PCE-RFS.

• Alinear expectatives respecte a les recomanacions i a les següents passes de millora.

L'adjudicatari aixecarà acta de la sessió, recollint els acords, comentaris i validacions efectuades per l'entitat. Aquesta acta es lliurarà tant a Consorci Localret com a l'entitat auditada dins dels tres dies hàbils següents a la reunió.

4.10 Reunió de tancament i lliurament final del contracte

Un cop finalitzades totes les auditories, se celebrarà una sessió de tancament global de caràcter presencial a la seu de Consorci Localret, el termini límit per aquesta reunió serà durant la darrera setmana del mes de març.

L'objectiu d'aquesta reunió serà:

- Presentar els resultats consolidats del conjunt d'auditories.
- Formalitzar el lliurament final de la documentació i dels informes generals.
- Exposar les conclusions globals, tendències observades i recomanacions prioritzades per a futures actuacions de millora dins el Model Integral de Ciberseguretat.
- Analitzar els indicadors agregats de maduresa i nivell de compliment de les entitats participants.

L'adjudicatari aixecarà acta formal d'aquesta sessió, validada per totes les parts, com a constància dels acords adoptats, del lliurament complet dels productes contractats i de la correcta execució del servei.

5 LLIURABLES

Els informes resultants de l'auditoria seran l'evidència formal de les activitats executades i dels resultats obtinguts. Tots els informes previstos en aquest plec s'hauran de lliurar tant a l'entitat auditada com a Consorci Localret, assegurant en tot moment la traçabilitat i homogeneïtat de la informació.

Aquests documents constitueixen els lliurables contractuals del servei i tindran caràcter acreditatiu a efectes de seguiment, control i justificació davant els òrgans coordinadors del programa.

Els documents s'hauran de lliurar, com a mínim, en els formats següents:

- PDF signat digitalment, que constituirà la versió oficial i definitiva, hauran d'incloure metadades completes (autor, data, versió) i, en el cas dels PDFs, s'hauran de protegir contra modificacions no autoritzades.
- Format editable (Word i Excel o similar), per tal que l'entitat pugui treballar la informació, elaborar filtres i fer-ne ús en processos interns de seguiment o justificació.

Tots els documents generats s'ajustaran a la normativa vigent en matèria de protecció de dades (RGPD i LOPDGDD), així com a les darreres versions disponibles dels marcs i estàndards citats (ENS, CCN-STIC, NIST, ISO/IEC 27001, CIS)

Així mateix, tots els informes hauran d'estar clarament identificats, datats i estructurats per garantir-ne la traçabilitat i facilitar-ne la utilització en processos de justificació i auditoria dels fons Next Generation EU i hauran d'incloure els logotips oficials requerits per als projectes NextGenerationEU(Unió Europea – NextGenerationEU, Govern d'Espanya, Generalitat de Catalunya i altres que corresponguin), garantint la correcta visibilitat i compliment de les normes de comunicació institucional. El disseny gràfic i la disposició d'aquests elements es poden consultar en l'annex 4.

5.1 Informes segons format de l'Agència

Els informes i documents que formen part del model de treball de l'Agència de Ciberseguretat de Catalunya tenen com a finalitat garantir una presentació homogènia, traçable i comparable dels resultats de les auditories realitzades a les entitats locals.

L'empresa adjudicatària haurà de generar, emplenar i lliurar obligatòriament tots els documents definits per l'Agència, seguint estrictament les plantilles i instruccions oficials que aquesta faciliti, i assegurant que la informació reflecteix fidelment les troballes, resultats i recomanacions derivades de cada auditoria.

A diferència dels informes que cada adjudicatari pot elaborar amb el seu propi estil (com l'informe tècnic i l'executiu), els documents inclosos en el model de l'Agència tenen caràcter únic, obligatori i normalitzat, amb l'objectiu de permetre la comparació dels resultats entre entitats i garantir la coherència global de la informació sectorialment.

Relació de documents obligatoris, segons els models presentats en els annexos 5 i 6:

1. Informe de diagnòstic: document que exposa el grau d'exposició de cada entitat a les principals ciberamenaces, incloent-hi els resultats de les proves tècniques, l'anàlisi de l'arquitectura de seguretat i la valoració del nivell d'adequació a l'Esquema Nacional de Seguretat (ENS) i al Perfil de Compliment Específic (PCE-RFS). Aquest informe serà puntual. Presentat en l'annex 5.
2. Full de ruta d'iniciatives i presentació de resultats executius: informe que recull el conjunt d'iniciatives prioritzades i projectes de millora necessaris per reduir la superfície d'exposició, desplegar els models de perímetre de l'Agència i avançar en el compliment de l'ENS. Inclourà una estimació orientativa dels costos associats i dels recursos necessaris, amb lliurament puntual. Presentat en l'annex 6.

Relació de documents obligatoris, segons els models que es presentaran durant la primera reunió amb el Consorci Localret:

3. Context de l'entitat: documentació que reculli tota la informació de context recopilada durant la fase de diagnòstic, incloent-hi l'organització, els actius, l'entorn tecnològic, els serveis i les dependències.
4. Documents de treball per valorar el nivell d'exposició a les amenaces: formularis de treball elaborats a partir de la plantilla de l'Agència, que reflecteixin les proves i els resultats obtinguts durant el diagnòstic i que permetin calcular el grau d'exposició a les principals ciberamenaces. La seva elaboració serà puntual.
5. Bitàcola d'activitat: registre detallat de totes les accions executades durant les activitats d'avaluació, incloent-hi dates, participants, eines utilitzades i incidències observades. Aquest document es generarà de manera puntual.
6. Avís primerenc: comunicació formal excepcional adreçada a l'Agència i a l'entitat en cas d'identificar vulnerabilitats crítiques durant l'execució de les proves, fora del cicle habitual d'informes. La seva emissió tindrà caràcter puntual.

7. Informe d'incidència: document d'emissió immediata en cas que una activitat d'avaluació generi una incidència o interrupció en els sistemes de l'entitat, detallant la causa, la casuística i les mesures correctores aplicades. Aquest informe tindrà caràcter puntual.
8. Informes de seguiment: documents periòdics que informen sobre l'estat de les tasques, la planificació, els avenços, les possibles desviacions i els riscos detectats durant l'execució de les activitats. La seva periodicitat serà setmanal.

5.2 Pla d'Iniciatives o projectes de seguretat

Les iniciatives o projectes de seguretat tenen com a finalitat oferir a l'entitat un full de ruta estructurat i accionable, amb les actuacions necessàries per corregir les vulnerabilitats detectades i enfortir progressivament la seva capacitat de protecció, detecció, resposta i resiliència davant les principals ciberamenaces.

Aquestes actuacions constitueixen la fase d'Identificació d'Iniciatives de Seguretat, d'acord amb el Model de Ciberseguretat de l'Agència de Ciberseguretat de Catalunya, i s'obtenen del catàleg oficial d'iniciatives de l'Agència, que agrupa les accions de millora recomanades per a les administracions locals.

Per garantir l'homogeneïtat metodològica i facilitar el seguiment posterior, cada iniciativa haurà de contextualitzar, com a mínim, els aspectes següents:

- Antecedents i motivació, explicant la seva relació amb les deficiències o vulnerabilitats detectades al diagnòstic.
- Abast i aplicabilitat, detallant el conjunt d'actius, sistemes o processos que es veuran afectats i les dependències existents.
- Estratègia de desplegament, descrivint les fases, accions i actors implicats, així com possibles adaptacions o ampliacions segons la realitat i maduresa de l'entitat.
- Estimació de costos i recursos, aportant una visió orientativa del pressupost necessari, esforços humans i tecnològics, així com de les possibles fonts de finançament o suport (propis, subvencions o programes coordinats amb Consorci Localret i l'Agència).
- Prioritat i horitzó temporal, assignant una classificació segons el nivell de criticitat (molt alta, alta o mitjana) i un termini recomanat d'execució (curt, mitjà o llarg).
- Beneficis esperats, destacant l'impacte sobre la reducció de riscos, l'increment de la resiliència i l'alineament amb els requeriments de l'ENS i el Perfil de Compliment Específic (PCE-RFS).

Les mesures proposades inclouran tant actuacions tècniques (p. ex. actualitzacions de programari, reforç de configuracions, desplegament de mecanismes de protecció avançats, segmentació o gestió de vulnerabilitats) com organitzatives (p. ex. protocols interns, polítiques de seguretat, procediments de resposta a incidents, formació i conscienciació).

El conjunt d'iniciatives es lliuraran dintre de la Presentació de resultats executius de diagnòstic i iniciatives de seguretat, amb la plantilla disponible en l'annex 6, en la pàgina 10. La plantilla inclou totes les accions previstes, amb contingut ja disponible que haurà

d'adaptar, millorar i completar d'acord amb el diagnòstic, al context i a la realitat de cada entitat.

Es facilitarà a l'entitat la presentació en format PDF i editable, per tal que aquesta pugui utilitzar-la com a instrument viu de planificació, seguiment i actualització de les actuacions de millora en matèria de ciberseguretat.

5.3 Informe tècnic detallat

L'informe tècnic detallat haurà de recollir, amb un nivell d'exhaustivitat suficient, totes les activitats executades, els resultats obtinguts i les evidències recopilades durant l'execució de les proves.

L'objectiu del document és proporcionar una traçabilitat completa del procés d'auditoria, de manera que qualsevol troballa pugui ser reproduïda, verificada i contrastada posteriorment per l'entitat o per tercers degudament autoritzats.

Aquest informe, atesa la seva naturalesa tècnica, podrà ser cedit per l'entitat a terceres parts encarregades de la correcció de vulnerabilitats o riscos, garantint sempre la confidencialitat i l'ús exclusiu per a finalitats de millora de la seguretat.

Cada adjudicatari podrà definir el format i disseny de l'informe, però com a mínim haurà d'incloure els apartats següents:

- Metodologia i abast
  - Descripció de la metodologia emprada i dels marcs de referència utilitzats.
  - Enumeració de les eines i versions emprades en cada fase.
  - Limitacions o condicions específiques establertes amb l'entitat per a la realització de les proves.

- Inventari d'actius i mapa de xarxa
  - Llistat complet dels actius avaluats (servidors, estacions, dispositius, aplicacions, serveis, etc.).
  - Classificació dels actius per nivell de criticitat i relació amb serveis o processos de negoci.
  - Mapa de xarxa resultant de la descoberta d'actius i serveis, amb la topologia observada (VLANs, segments, DMZ, connexions externes).

- Resultats i vulnerabilitats identificades
  - Resum de resultats obtinguts per cada actiu o servei analitzat.
  - Relació de vulnerabilitats detectades (CVE/CWE), configuracions insegures i serveis exposats.
  - Evidències visuals (captures, sortides d'eines o logs) que acreditin cada troballa.
  - Justificació tècnica en cas de falsos positius o vulnerabilitats no explotables.

- Classificació i anàlisi de riscos
  - Valoració del risc associat a cada vulnerabilitat utilitzant CVSS v3.1 o equivalent.

- Assignació d'un identificador únic i descripció de l'impacte sobre la confidencialitat, integritat i disponibilitat (CIA).
- Valoració de la dificultat de correcció (baixa, mitjana o alta).
- Recomanacions de mitigació i referències normatives aplicables.

- Cronologia i traçabilitat
  - Dates i franges horàries d'execució de les proves.
  - Correspondència entre proves realitzades i possibles impactes o incidències observades.
  - Referència a les finestres operatives acordades amb l'entitat.

- Matriu de riscos i dependències
  - Representació visual de la distribució de vulnerabilitats per severitat.
  - Identificació dels actius més exposats i de les dependències entre vulnerabilitats.
  - Descripció dels possibles escenaris d'explotació o cadenes d'atac.

- Annexos tècnics
  - Sortides completes de les eines d'escaneig, registres i fitxers de configuració analitzats.
  - Scripts o procediments de prova utilitzats, amb paràmetres i resultats.
  - Captures de trànsit o evidències tècniques complementàries.

5.4 Fitxer Excel de troballes

A més de l'informe en format PDF signat digitalment i la versió editable (Word o equivalent), l'adjudicatari haurà de lliurar un fitxer Excel estructurat amb totes les vulnerabilitats i troballes identificades, per facilitar-ne el filtratge i la gestió interna.

Com a mínim, aquest fitxer haurà d'incloure els següents camps:

- ID de la troballa.
- Descripció breu i actiu afectat.
- Tipus d'actiu i localització/segment.
- Severitat (CVSS) i impacte CIA.
- Eina utilitzada i validació manual (sí/no).
- Evidència o referència a annexos tècnics.
- Dependències amb altres vulnerabilitats.
- Dificultat de correcció i recomanació de mitigació.
- Referències normatives (ENS, CCN-STIC, NIST, CIS, ISO, CVE/CWE).
- Responsable intern assignat (si escau).
- Estat de correcció (pendent, en curs, corregit, validat).
- Data límit proposada i observacions addicionals.

Aquest Excel tindrà com a finalitat actuar com a eina operativa de gestió de vulnerabilitats, que permet a l'entitat prioritzar, fer seguiment i validar la correcció de les troballes identificades.

Reina Cristina, 9 08003 Barcelona Tel. 934861430 www.localret.cat consorci@localret.cat N.I.F.P5800043A

5.5 Informe executiu

A partir de la informació recollida a l'informe tècnic detalla, s'elaborarà l'informe executiu que té com a objectiu oferir una visió clara, sintetitzada i accessible de l'estat de seguretat de l'entitat, dirigida a càrrecs directius i responsables polítics.

L'informe executiu haurà de ser apte per a la seva presentació pública o institucional, amb llenguatge no tècnic i contingut visualment accessible.

El document recull els resultats principals de l'auditoria i els contextualitza en relació amb els marcs de referència internacionals i nacionals, en especial el NIST Cybersecurity Framework (CSF) i l'Esquema Nacional de Seguretat (ENS), de manera que permeti avaluar el grau de maduresa de l'organització i situar-la dins del seu entorn de referència.

L'informe presentarà un resum executiu de les vulnerabilitats i riscos identificats, mostrant la seva distribució segons criticitat i l'impacte potencial sobre els serveis essencials de l'entitat. La informació es representarà de manera agregada i visual, mitjançant matrius de risc i gràfics de distribució que permetin identificar de forma immediata les àrees més crítiques.

La presentació dels resultats es farà en correspondència amb les cinc funcions principals del NIST CSF (Identify, Protect, Detect, Respond, Recover), posant de manifest el nivell de maduresa assolit en cadascuna d'elles. Al mateix temps, es valorarà el grau de compliment dels requeriments essencials de l'ENS, destacant les desviacions més rellevants i les mesures necessàries per avançar cap al perfil de compliment adequat.

Finalment, l'informe executiu oferirà una sèrie de recomanacions prioritzades, tant tècniques com organitzatives, estructurades en un full de ruta de curt, mitjà i llarg termini, amb l'objectiu d'enfortir la resiliència de l'entitat i millorar la seva posició relativa dins del sector públic local. Aquest full de ruta constituirà una eina estratègica per a la presa de decisions, orientada a reduir riscos i a assegurar el compliment normatiu i les bones pràctiques de ciberseguretat.

5.6 Informe per a la justificació dels fons NextGenerationEU

Aquest informe té com a finalitat proporcionar als òrgans coordinadors tota la informació necessària per elaborar la memòria justificativa dels fons NextGenerationEU, demostrant de manera clara, verificable i objectiva l'execució de les activitats i l'impacte real sobre la resiliència digital i la millora de la ciberseguretat.

S'elaboraran dos tipus d'informes diferenciats amb l'objectiu de garantir una visió completa i traçable dels resultats del projecte.

5.6.1 Informe individual per entitat

Document que resumeix l'execució i els resultats de l'auditoria per a una entitat concreta, i que servirà com a base per a la seva justificació pròpia dels fons.

Aquest informe haurà d'incloure, com a mínim:

- Dades generals de l'entitat (nom, dimensió, volum d'actius, abast del diagnòstic i dates d'execució).
- Descripció sintètica de les activitats executades: diagnòstic, proves tècniques, anàlisi de controls i elaboració d'iniciatives de seguretat.
- Recursos humans implicats (nombre de tècnics, perfils professionals, hores de dedicació i rols principals).
- Reunions i fites principals durant el procés d'execució.
- Actius, sistemes i serveis analitzats, amb nombre total de troballes detectades i classificació per nivell de gravetat.
- Indicadors específics de l'entitat:
- Dominis i sistemes de còpia de seguretat compromesos.
- Tècniques MITRE ATT&CK provades i eines emprades.
- Vulnerabilitats avaluades, CVEs explotades i credencials exfiltrades.
- Controls de seguretat analitzats i evidències revisades.
- Alertes o deteccions registrades pel SIEM/SOC.
- Temps mínim fins al compromís del domini.
- Iniciatives de seguretat identificades i prioritzades, amb estimació de costos i horitzó temporal.
- Correspondència amb els objectius del programa NextGenerationEU i grau d'alineament amb l'Esquema Nacional de Seguretat (ENS).
- Valoració qualitativa de l'impacte sobre la resiliència digital i recomanacions de millora.
- Resultat de l'enquesta de satisfacció de l'entitat.

5.6.2 Informe global consolidat

Document únic que presenta de manera agregada els resultats de totes les entitats participants en el programa.

Haurà de permetre una visió sectorial del progrés global i servirà per a la justificació centralitzada dels fons i la comunicació institucional.

Aquest informe haurà d'incloure, com a mínim:

- Resum executiu dels objectius, metodologia i abast global del programa.
- Nombre total d'entitats avaluades i volum d'actius dins l'abast.
- Síntesi agregada de resultats i principals troballes:
- Vulnerabilitats identificades per nivell de gravetat.
- Nombre de dominis i sistemes de backup compromesos.
- Tècniques MITRE ATT&CK més freqüents i eines utilitzades.
- Vulnerabilitats i CVEs avaluades o explotades.
- Controls de seguretat i evidències revisades.
- Deteccions realitzades pels SIEM/SOC.
- Indicadors globals del programa:
- Entitats completades.
- Actius analitzats.

- Vulnerabilitats totals i mitjanes per entitat.
- Temps mitjà fins al compromís.
- Nombre total de lliurables generats (informes, presentacions, bitàcoles, etc.).
- Reunions de seguiment internes i amb Consorci Localret.
- Resultats globals de les enquestes de satisfacció.
- Valoració global de l'impacte del programa:
- Increment del nivell de maduresa i compliment ENS.
- Reducció de la superfície d'exposició i millora de la resiliència digital.
- Conclusions generals i recomanacions estratègiques per a la continuïtat del programa.

Tant els informes individuals com el consolidat hauran d'incloure un resum executiu i una presentació gràfica agregada amb els principals indicadors i resultats.

Carles Giné Sabaté
Àrea de Transformació Digital i Tecnologies
(ciberseguretat)