PLEC DE PRESCRIPCIONS TÈCNIQUES DELS SERVEIS DE CONTINUÏTAT, EVOLUCIÓ, MANTENIMENT I MILLORA DEL SISTEMA DE GESTIÓ DE LA SEGURETAT DE LA INFORMACIÓ ALINEAT AMB L'ESQUEMA NACIONAL DE SEGURETAT (ENS) A BARCELONA ACTIVA, AIXÍ COM LA REALITZACIÓ DE LES ACTIVITATS D'AUDITORIA QUE PERMETIN ASSOLIR I MANTENIR LA CERTIFICACIÓ CORRESPONENT (EXP. 23/26)

ANTECEDENTS

Barcelona Activa té la missió de promoure l'ocupació de qualitat, la iniciativa emprenedora, la competitivitat empresarial i la diversificació del teixit productiu, per a assolir un model econòmic sostenible, inclusiu i just. La nostra visió és fer de Barcelona una ciutat de referència per treballar, emprendre i viure amb valors socials i ambientals.

En aquest sentit, aquest contracte és necessari per tal de garantir el normal funcionament de l'activitat de Barcelona Activa mantenir en funcionament els sistemes i les aplicacions corporatives per donar compliment a la missió i objectius d'aquesta.

Barcelona Activa porta aproximadament dos anys d'execució del Pla d'Adequació a l'Esquema Nacional de Seguretat (ENS, en endavant) amb una implementació significativa de mesures organitzatives i tècniques, l'establiment de rols i Comitè de Seguretat de la Informació (COMSEG) i l'ús d'eines de suport a la gestió (p. ex., PILAR/INÉS). El present contracte té com a finalitat garantir la continuïtat d'aquest trajecte, la millora contínua i l'assoliment i manteniment de la certificació en l'ENS en la categoria que correspongui al seu abast.

OBJECTE DEL CONTRACTE

Establir les condicions tècniques que regiran la contractació, per part de Barcelona Activa, SAU (d'ara endavant "BA"), dels serveis següents:

- LOT 1: Servei de manteniment, evolució i seguiment del Pla d'Adequació a l'ENS, incloent auditories internes anuals i acompanyament a auditories externes.
- LOT 2: Servei d'auditories externes de certificació de l'ENS.

NORMATIVA

L'ENS, tal com està recollit en el seu art. 2, resulta d'aplicació a les entitats del sector públic, a les entitats del sector privat que els prestin serveis competencials i, en general, a la cadena de subministrament d'aquestes últimes, en la mesura que una anàlisi de riscos previ així ho determini.

A més, cal recordar que les mesures del ENS són així mateix d'aplicació per a aquelles entitats que determina la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades i garanties dels drets digitals, quan es realitzin tractaments de dades personals.

Finalment, l'ENS també és aplicable als sistemes que tracten informació classificada, podent resultar necessari adoptar mesures complementàries de seguretat, específiques per a aquests sistemes que així mateix estan subjectes a la Llei 9/1968, de 5 d'abril, de Secrets Oficials (*LSO), i les derivades dels compromisos internacionals contrets per Espanya, o conseqüència de la seva pertinença a organismes o fòrums internacionals.

L'ENS està regulat específicament per la següent normativa:

- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- Resolució de 27 de març de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció Tècnica de Seguretat d'Auditoria de la Seguretat dels Sistemes d'Informació.
- Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció de Seguretat de conformitat amb l'Esquema Nacional de Seguretat.
- Resolució de 7 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat d'Informe de l'Estat de la Seguretat.
- Resolució de 13 d'abril de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció Tècnica de Seguretat de Notificació d'Incidents de Seguretat.

La relació d'una altra normativa relacionada amb la ciberseguretat a Espanya pot consultar-se en el Codi de Dret de la Ciberseguretat editat pel BOE.

MESURES DE SEGURETAT, CONFIDENCIALITAT I PROTECCIÓ DE DADES

Durant l'execució del contracte cal donar compliment del RD 311/2022 (ENS) i guies CCN-STIC aplicables, així com al RGPD i LOPDGDD en els tractaments necessaris. I per últim, cal limitar l'accés a la informació estrictament necessària i registre d'accessos quan escaigui.

CONDICIONS GENERALS DEL SERVEI

- Lloc de prestació: preferentment en remot; reunions de kick-off, seguiment, auditories i proves podran requerir presencialitat a dependències de Barcelona Activa.
- Idioma de treball: català i/o castellà; documentació mínima en català.
- Coordinació: BA designarà un/a Responsable del Contracte i aquest juntament amb el Comitè de Seguretat de la Informació (COMSEG) realitzaran el seguiment.
- Eines: s'empraran les eines de BA i, si escau, les eines del CCN (PILAR, INÉS) o equivalents del CCN que permetin exportació/traspàs.
- Tots els entregables s'hauran de lliurar en format editable i PDF, en català, amb control de versions. Barcelona Activa disposarà d'un termini raonable per revisar i acceptar, o bé demanar correccions. Els criteris d'acceptació inclouen:
  - Completesa respecte a l'abast definit.
  - Traçabilitat a requisits ENS i evidències.
  - Claredat, exactitud i coherència amb l'estat real dels sistemes.
  - Correcció d'incidències i no conformitats en el termini acordat.
- Per tal de garantir una correcta execució caldrà complir ambles següents condicions d'execució, seguiment i qualitat del servei
  - Reunió de seguiment mensual amb acta i pla de treball actualitzat.
  - Quadre d'indicadors KPI/KRI trimestral per al COMSEG.
  - Gestió de riscos i registre d'incidents mantinguts al dia.
  - Mecanisme de control de canvis i gestió documental amb traçabilitat.

LOT 1 MANTENIMENT I EVOLUCIÓ DEL PLA D'ADEQUACIÓ A L'ENS

Objecte i resultats esperats

Assegurar la gestió continuada de la seguretat, la revisió i evolució del Pla d'Adequació a l'ENS, la realització d'auditories internes anuals, el seguiment d'indicadors i l'acompanyament a BA durant el procés d'auditoria externa fins a la certificació i en els cicles de manteniment.

Tasques principals:

- Revisió, manteniment i evolució del marc documental ENS (PSI, Normativa interna, procediments, registres i COMSEG).
- Actualització de l'abast i la categorització dels sistemes i serveis (segons CCN-STIC 803).
- Anàlisi i gestió de riscos periòdica
- Actualització de la Declaració d'Aplicabilitat (Annex II ENS).
- Planificació i execució d'auditories internes anuals (CCN-STIC 802/808), amb informes i plans correctius.
- Disseny i manteniment del Pla de Millora i del Pla d'Auditories (internes i externes).
- Acompanyament integral en auditories internes i externes: preparació d'evidències, suport en sessions i resposta a no conformitats i observacions.
- Execució de campanyes de formació i conscienciació; suport al Pla de Comunicació Interna.
- Elaboració i càrrega de l'Informe Nacional de l'Estat de la Seguretat a INÉS (segons ITS aplicable).
- Assessorament tècnic i jurídic transversal en mesures organitzatives i tècniques (incloses privadesa i protecció de dades).
- Execució de tasques complementàries i no previstes necessàries per assegurar el manteniment del compliment ENS.

Així mateix, l'adjudicatària del LOT 1 impartirà accions de formació i conscienciació planificades amb Barcelona Activa i establirà un pla de transferència de coneixement perquè l'organització assoleixi autonomia operativa en els processos ENS.

Entregables de LOT 1:
- PSI revisada i normativa interna actualitzada, amb acta de COMSEG.
- Actes del COMSEG i reunions de seguiment.
- Informe d'abast, categorització i catàleg de serveis actualitzat.
- Informe d'Anàlisi de Riscos i fitxer exportable per a PILAR.
- Declaració d'Aplicabilitat actualitzada (Annex II ENS).
- Informe d'Auditoria Interna anual i acta de tancament.
- Pla de Millora i Pla d'Auditories amb calendari.
- Actes i materials de formació i conscienciació.
- Procediments revisats i actualitzats.
- Informe INÉS anual preparat i/o presentat.
- Quadre de comandament trimestral d'indicadors de seguretat (KPI/KRI).
- Altres documents necessaris per mantenir la conformitat amb l'ENS.

Metodologia i referències normatives

S'aplicaran els requisits del Reial decret 311/2022 (ENS) i les Instruccions Tècniques de Seguretat corresponents, així com les guies CCN-STIC (p. ex., 802, 803, 804, 805, 808, 821, 470, 882 actuals i futures) i bones pràctiques ISO/IEC 27001/27002 quan aportin valor.

Nivell de servei (SLA) de LOT 1
- Cal definir un canal de notificació i registre d'incidents definit i acordat amb Barcelona Activa
- Resposta a consultes ordinàries: ≤ 1 dia laborable.
- Resposta a incidents greus: immediata en horari laboral; disponibilitat per a coordinació d'emergència.
- Caldrà redactar i entregar un informe post-incident amb causes arrel, impacte i mesures correctives
- Entrega d'informes d'auditoria interna: ≤ 15 dies laborables des del tancament del treball de camp.
- Actualització trimestral d'indicadors i Pla de Millora.

LOT 2 Auditories externes de certificació de l'ENS

Objecte i independència

Realització d'auditories externes de certificació de l'ENS, en el marc del RD 311/2022 i guies CCN-STIC aplicables, per part d'una entitat independent i acreditada per l'Entitat Nacional d'Acreditació (ENAC) o reconeguda com a OAT, i diferent de la que dugui a terme les activitats de consultoria de LOT 1. L'empresa adjudicatària del LOT 2 no podrà haver participat en implantació, manteniment ni auditoria interna dels sistemes objecte de l'auditoria de certificació de l'ENS.

Tasques principals:

- Planificació de l'auditoria (pla d'auditoria, abast, criteris, cronograma, mostreig).
- Revisió documental: PSI, normativa interna, abast/categorització, DA, anàlisi de riscos, evidències tècniques.
- Entrevistes, inspeccions i proves sobre el SGSI i controls (organitzatius, físics i lògics).
- Informe d'auditoria amb resultats, no conformitats (NC), observacions i oportunitats de millora.
- Verificació d'accions correctives i diligència per a l'emissió (o renovació) del certificat.
- Auditories de seguiment (manteniment) segons cicle de certificació.

Entregables de LOT 2

- Pla d'auditoria i agenda detallada.
- Informe d'auditoria de certificació (resultats, NC, evidències).
- Informe de seguiment de NC i validació de correccions.
- Certificat de conformitat ENS o informe de no certificació amb motius i recomanacions.

Calendarització: la càrrega dependrà de l'abast i la categoria del sistema, segons proposta de l'entitat auditora.

INCOMPATIBILITATS I INDEPENDÈNCIA ENTRE LOTS

Les empreses només es poden presentar a un dels dos lots i mai als dos. L'adjudicatària del LOT 2 haurà de garantir independència total respecte de qualsevol activitat d'implantació, manteniment o auditoria interna relacionada amb l'abast objecte de certificació, sense que hagi participat en aquests serveis durant els darrers 24 mesos.

VIDsigner code: 672FA63C93764A8B90...

- 16/03/2026 13:09:07

Xavier Galceran Esteve

Xavier Galceran Esteve
Responsable de Ciberseguretat