



PLEC DE PRESCRIPCIONS TÈCNIQUES (PPT) PER A LA LICITACIÓ DEL CONTRACTE DE SERVEIS D'ASSESSORAMENT, CONSULTORIA, ASSISTÈNCIA TÈCNICA I JURÍDICA PER A L'ELABORACIÓ D'UN PLA D'ADEQUACIÓ I POSTERIOR CERTIFICACIÓ DE L'ESQUEMA NACIONAL DE SEGURETAT A BARCELONA ACTIVA

1. ANTECEDENTS

Barcelona Activa (BA d'ara en endavant) té la missió de contribuir a la millora de la qualitat de vida de les persones promovent la competitivitat econòmica de la ciutat i el reequilibri dels territoris, a través del foment de l'ocupació de qualitat, l'impuls a l'emprenedoria i el suport a un teixit empresarial plural, divers i sostenible, des d'una perspectiva econòmica, social i ambiental.

La nostra visió és fer de Barcelona una ciutat de referència internacional per treballar, emprendre i viure amb valors socials i ambientals. Una de les principals prioritats municipals dels darrers anys ha estat la lluita contra l'atur i la precarietat laboral. Fomentar l'ocupació de qualitat és essencial per a la ciutat i constitueix un element clau per a la millora de la cohesió social i l'avenç cap a un nou model de desenvolupament just i sostenible.

Per aconseguir-ho, BA acompanya les persones en el seu procés de recerca de feina basant-se en els eixos que la defineixen (persona, aspectes psicosocials i mercat de treball), per tal d'augmentar les seves oportunitats d'accedir a un lloc de treball de qualitat.

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

L'Esquema Nacional de Seguretat (ENS d'ara en endavant) estableix les directrius bàsiques i els requisits mínims que han de complir els sistemes d'informació utilitzats per les administracions públiques espanyoles, incloent-hi BA. Això inclou la protecció de la informació i els recursos associats, així com la garantia de la seva integritat, disponibilitat, confidencialitat i autenticitat.

2. NORMATIVA QUE REGULA L'ENS

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.



3. OBJECTIUS DEL CONTRACTE

- Crear les condicions necessàries de seguretat en l'ús dels mitjans electrònics, a través de mesures per garantir la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics, que permeti l'exercici de drets i el compliment de deures a través d'aquests mitjans.
- Promoure la gestió continuada de la seguretat.
- Promoure la prevenció, detecció i correcció per a una millor resiliència a l'escenari de ciberamenaces i ciberatacs.
- Promoure un tractament homogeni de la seguretat que faciliti la cooperació en la prestació de serveis públics digitals quan hi participen diverses entitats. Això suposa proporcionar els elements comuns que han de guiar l'actuació de Barcelona Activa i dels seus proveïdors tecnològics en matèria de seguretat de les tecnologies de la informació.
- Servir de model de bones pràctiques, en línia amb allò que s'ha apuntat en les recomanacions de l'OCDE Digital Security Risk Management per Economic and Social Prosperity OECD Recommendation and Companion Document.
- Obtenir la certificació de conformitat amb l'ENS amb la categoria que correspongui.

4. CARACTERÍSTIQUES DEL SERVEI

A) Preparar i aprovar la Política de Seguretat i la Normativa Interna corresponent, incloent els objectius i missió de l'organització, el marc regulatori de les activitats, la definició de rols de seguretat, l'estructura i composició del comitè per a la gestió i coordinació de la seguretat, les directrius d'estructuració de la documentació de la seguretat i els riscos derivats del tractament de dades personals.

Guies de suport:

- o CCN-STIC 801, 805 i 821

Documents a lliurar:

- o Política de Seguretat (revisió i/o millora d'aquesta) - *Política*
- o Normativa Interna aplicable - *Registre*
- o Acta de constitució del Comitè de Seguretat (composició, rols, funcions, etc) – *Acta*

La **Política de Seguretat** és un document d'alt nivell, mitjançant el qual l'entitat defineix el seu compromís respecte a la seguretat de la informació i la dels serveis prestats. En aquesta Política es descriuran els mecanismes implementats per a la gestió continuada de la seguretat i s'establiran els responsables de vetllar pel seu compliment.

La **Normativa Interna**, comprendrà aquell conjunt de normes, de caràcter intern a l'organització, que prescriurà el comportament exigible als usuaris del sistema d'informació quant a l'ús dels mitjans electrònics que l'entitat posa a la seva disposició.

B) Identificar i categoritzar l'abast dels sistemes d'informació i serveis atenent a la valoració de la informació que es tracta i dels serveis que es presten.

Guies de suport:

- o CCN-STIC 803
- o *Fitxa de descripció de cada servei (plantilla de serveis proporcionada pel CCN)*

Documents a lliurar:

- o Acta abast, categorització i SOA – *Acta*
- o Categoria del Sistema - *Informe*
- o Catàleg d'Identificació de l'abast del sistema, informació dels serveis i valoració de les dimensions de seguretat - *Informe*
- o Fitxes dels serveis (segons la plantilla de serveis del CCN) – *Informe*

C) Realitzar l'anàlisi de riscos, incloent la valoració de les mesures de seguretat existents.

Eines a utilitzar:

- o *Eines PILAR i INÉS del CCN o pròpia amb possible traspass a les eines del CCN*

Guies de suport:

- o CCN-STIC 470 i 882

Documents a lliurar:

- o Anàlisi de Riscos incloent la valoració de les mesures de seguretat existents - *Informe*



- Fitxer de l'Anàlisi de Riscos apte per importar-lo a l'eina PILAR del CCN (amb l'anàlisi efectuat) - *Fitxer*

D) Preparar i aprovar la Declaració d'aplicabilitat de les mesures de l'Annex II de l'ENS.

Guies de suport:

- CCN-STIC 804 i 819
- Annex II del ENS – *Relació de mesures aplicables de l'ENS*

Documents a lliurar:

- Declaració d'Aplicabilitat a l'ENS - *Registre*

E) Auditar la seguretat per verificar el compliment dels requisits de l'ENS (Auditories Internes de l'ENS).

Guies de suport:

- CCN-STIC 802 i 808

Documents a lliurar:

- *Acta de la reunió inicial de l'auditoria (Kick Off) - Acta*
- *Informe de l'auditoria i acta de la reunió final – Informe i Acta*

F) Desenvolupar un Pla de Millora de la Seguretat sobre la base de l'informe d'insuficiències detectades, diagnòstic de la situació actual, recomanacions d'adequació a les polítiques, requeriments, mesures de seguretat tècniques, organitzatives i jurídiques establerts en l'ENS i terminis d'execució.

Documents a lliurar:

- Pla de Millora de Seguretat incloent l'Informe de Deficiències - *Informe*
- Pla d'Adequació a l'ENS definitiu – *Informe*

El **Pla de millora de la seguretat** identificarà les tasques que serà necessari realitzar per a esmenar les deficiències del sistema, planificar-les i assignar-los els recursos necessaris (personals i/o econòmics, segons sigui el cas).

L'**informe de deficiències** del sistema (GAP analysis), recollirà l'estat de compliment de les mesures de seguretat, reflectint el nivell actual de maduresa de les mesures de la declaració d'aplicabilitat. Aquest informe es pot completar també amb aquelles mesures que serà necessari implantar per a garantir el compliment de la normativa de protecció de dades. L'informe contindrà, per tant, el que es consideren riscos residuals del sistema que hauran de ser acceptats formalment pels Responsables dels Serveis i pels Responsables de la Informació.

G) Suport en la Implementació del Pla de Millora: caldrà realitzar accions d'assessorament, acompanyament, control i formació en les tasques de millora identificades en el Pla de Millora.

Documents a lliurar:

- Actes de les reunions de les sessions de control i sessions formatives – *Actes*

H) Formació i conscienciació al personal de BA envers a l'impacte i implicació de l'aplicació de l'ENS en el dia a dia del personal.

Documents a lliurar:

- Actes de les sessions formatives – *Actes*

I) Informar sobre l'estat de la seguretat al CCN a través de l'eina INÉS.

Eines a utilitzar:

- *Eines PILAR i INÉS del CCN o pròpia amb possible traspàs a les eines del CCN*

Documents a lliurar:

- Elaboració de l'Informe Nacional de l'Estat de la Seguretat amb l'eina INÉS del CCN – *Informe*

J) Disseny d'un Pla d'Auditories, en el qual es planificarà, s'establirà, s'implementarà i es mantindran els diversos programes d'auditoria per a les posteriors auditories internes (anuals) i externes (biennals) de l'ENS.



Documents a lliurar:

- Informe del Pla d'Auditories – *Informe*

K) Acompanyament a les auditories externes (Certificació de l'ENS). L'empresa adjudicatària haurà de preparar la documentació corresponent, contactar amb les entitats pertinents i acompanyar a **BA** en tot el procés d'auditoria externa per a la obtenció de la certificació de l'ENS.

L) Marc documental (Polítiques, Normatives, Procediments, plantilles de registres, etc). Es treballaran i s'entregarà a **BA** la documentació associada que es generi durant el procés d'implantació de l'SGSI (o Sistema de Gestió de Seguretat de la Informació consisteix en el conjunt de polítiques, procediments i directrius al costat dels recursos i activitats associats que són administrats col·lectivament per una organització, en la cerca de protegir els seus actius d'informació essencials). *Seguint les guies de referència del CCN-CERT i l'AEPD, es considera que el marc de normes a contemplar requereix els desenvolupaments de documentació següents:*

Marc normatiu:

- Normativa de control d'accés lògic
- Normativa d'accés a Internet
- Normativa d'ús del correu electrònic
- Normativa per treballar fora de les instal·lacions
- Normativa d'ús de dispositius mòbils
- Normativa de gestió de suports
- Normativa de seguretat dels equips
- Normativa de control de seguretat a l'operativa
- Normativa de conformitat legal
- Normativa de gestió de tercers
- Normativa de classificació de la informació
- Normativa de seguretat física a sales CPD i edificis
- Normativa de gestió d'incidències
- Normativa de gestió de claus criptogràfiques

Marc procedimental:

- Procediment de gestió i aprovació de la documentació
- Procediment de classificació, marcatge i etiquetatge d'informació suports
- Procediment de contractació de personal
- Procediment de contractació i seguiment de serveis externs
- Procediment de gestió de la formació i conscienciació
- Procediment d'altres, baixes i modificacions d'usuaris
- Procediment de gestió del canvi i configuració segura dels sistemes
- Procediment de gestió del manteniment de maquinari i programari
- Procediment d'entrada i eixida d'equipament i suports
- Procediment de còpies de seguretat i restauració
- Procediment de gestió d'incidentes i bretxes de seguretat
- Procediment de pas a producció
- Informes Pla de Continuitat
- Procediment de control d'accés físic
- Procediment de digitalització de documents
- Procediments de copiat autèntic i conversió entre documents electrònics, així com des de paper o altres mitjans físics a formats electrònics
- Procediment de drets ARCOP
- Procediment sobre legitimació del tractament i altres principis
- Procediment sobre compliment del deure informació
- Procediment de comunicació a l'autoritat de control

5. CALENDARITZACIÓ I TERMINIS D'EXECUCIÓ PARCIALS

En el decurs del primer mes d'execució del contracte, caldrà:

- Agendar un Kick-off Meeting amb el Responsable de Ciberseguretat de Barcelona Activa
- Agendar una reunió de traspass d'informació



- Definir el sistema i el seu abast
- Crear el Comitè de Seguretat de la Informació (COMSEG)
- Revisar la Política de Seguretat i Normativa Interna

A partir del segon mes d'execució del contracte, s'iniciarà l'esbaltiment del projecte en ple funcionament, que estima que calgui una dedicació de fins a 250 hores anuals (50 hores perfil de cap de projecte i 200 hores perfil de consultor/a sènior).

6. CONDICIONS I ESPECIFICACIONS TÈCNIQUES

6.1. Característiques generals de prestació dels serveis i ubicació

Amb caràcter general, la prestació dels serveis del contracte es realitzarà únicament a les instal·lacions de l'empresa adjudicatària, excepte en el cas de les reunions de kick-off, seguiment, actes i reunions que requereixin presencialitat, que es planificaran a les instal·lacions de BA, sempre que aquesta ho consideri necessari.

6.2. Sistemes de gestió

L'empresa adjudicatària podrà disposar, sempre i únicament quan estigui justificat i sigui necessari per a l'execució de les prestacions que formen part de l'objecte d'aquest contracte i només si BA ho considera oportú, d'un accés als programes de gestió corporativa.

Aquest accés serà limitat a allò estrictament necessari per al desenvolupament de les tasques objecte del contracte.

Marc Puente Vila-Massana
Director de Tecnologia