

ANNEX II

SEGURETAT SISTEMES INFORMACIÓ

D'acord amb Real Decret 311/2022, de 3 de maig, pel qual es regula el Esquema Nacional de Seguretat (ENS), es té per objectiu determinar les polítiques de seguretat adients que estableixin els principis bàsics i requisits mínims per a la protecció dels sistemes d'informació i la informació continguda en ells als quals es troba sotmesa l'Administració pública.

1. Condicions de seguretat generals per empreses proveïdores que proporcionaran el servei amb Sistemes d'Informació de l'Ajuntament.

Atenent a serveis prestat per terceres parts a l'Ajuntament de Barcelona emprant els sistemes propis de l'Ajuntament, s'estableixen els següents requeriments per garantir el compliment del Esquema Nacional de Seguretat.

- a) **Dret d'auditoria:** per tal de vetllar per la qualitat del servei, el departament de Seguretat es reserva el dret d'auditar el servei prestat per l'empresa adjudicatària. Es contemplen tant auditories de seguretat periòdiques com auditories sobrevingudes si es considerés necessari. En qualsevol cas, si la realització de l'auditoria es realitzés en les instal·lacions de l'empresa adjudicatària, aquest haurà de garantir l'accés necessari, incondicional i irrevocable als documents necessaris a l'abast.

La realització de l'auditoria en cap moment eximirà l'empresa adjudicatària del compliment dels compromisos derivats de la prestació dels serveis.

A la finalització de l'auditoria, es revisaran els resultats i s'elaborarà un pla d'acció per corregir les desviacions i/o observacions detectades. El conjunt del resultat serà signat per ambdues parts.

L'empresa adjudicatària, d'acord amb el calendari establert al pla d'acció, es compromet a portar a terme les activitats establertes en el pla d'acció. Es podrà verificar que el pla d'acció s'ha implementat correctament.

- b) **Gestió d'incidents:** l'empresa adjudicatària informará al Departament de Seguretat de l'IMI de qualsevol incident de seguretat, seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona establert.

L'empresa adjudicatària col·laborarà amb el Departament de Seguretat de l'IMI en la resolució de qualsevol incident produït en el seu entorn, proporcionant totes les evidències requerides.

- c) **Confidencialitat:** l'empresa adjudicatària s'obliga a no difondre i a guardar el més absolut secret de tota la informació a la qual tingui accés en compliment del present contracte i a subministrar-la només al personal autoritzat per l'Ajuntament.

L'empresa adjudicatària queda expressament obligat a mantenir absoluta confidencialitat i reserva sobre qualsevol dada que pogués conèixer com a conseqüència de la participació en la present licitació, o, amb ocasió del compliment del contracte, especialment els de caràcter personal, que no podran copiar o utilitzar com a finalitat diferent a les que la informació te designada.

L'empresa adjudicatària serà responsable de les violacions del deure de secret que es puguin produir per part de les persones al seu càrrec. Així mateix, s'obliga a aplicar les mesures necessàries per a garantir l'eficàcia dels principis de mínim privilegi i necessitat de conèixer, per part de les persones participants en el desenvolupament del contracte.

Un cop finalitzat el present contracte, l'empresa adjudicatària es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per l'Ajuntament, així com qualsevol altre producte obtingut com a resultat del present contracte.

- d) **Accés a la informació:** tant si l'accés a les dades es fa als locals de l'Ajuntament de Barcelona, com si es fa de forma remota exclusivament a suports o sistemes d'informació de l'Ajuntament, l'empresa adjudicatària té prohibit incorporar les dades a d'altres sistemes o suports sense autorització expressa i haurà de complir amb les mesures de seguretat establertes per l'IMI.
- e) **Control d'accés local:** L'empresa adjudicatària haurà de protegir les estacions de treball i es compromet a complir les següents condicions:
- La informació revelada a qui intenta accedir ha de ser la mínima imprescindible. Els diàlegs d'accés proporcionaran únicament la informació indispensable.
 - El nombre d'intents permesos serà limitat, bloquejant l'accés una vegada efectuats un cert nombre de fallades consecutives.
 - S'hauran de enregistrar els accessos amb èxit i els fallits.
 - El sistema informarà a la persona usuària de les seves obligacions immediatament després d'obtenir l'accés.
- f) **Control d'accés remot:** l'empresa adjudicatària haurà de disposar dels mitjans materials i el maquinari necessari per a la connexió amb els Sistemes d'Informació de l'Ajuntament, sent els costos de connexió a càrrec de l'empresa adjudicatària.

La connexió remota als sistemes de l'Ajuntament es realitzarà seguint els protocols establerts per l'IMI per als sistemes de l'Ajuntament.

- g) **Gestió de les persones, deures i obligacions:** el/la Cap de Projecte de l'empresa adjudicatària durà a terme de forma correcta la gestió de les persones i els aspectes relacionats amb la seguretat de la informació.

L'empresa adjudicatària està obligada a implantar i donar a conèixer al seu personal els mecanismes i controls necessaris per a garantir l'accessibilitat, la confidencialitat, integritat i la disponibilitat de la informació de l'Ajuntament, i de donar-los a conèixer al seu personal.

El/la Cap de Projecte de l'empresa adjudicatària, abans de l'inici de la prestació del servei objecte del contracte, haurà de notificar al seu personal qualsevol obligació a la que l'empresa estigui sotmesa per contracte i formar al seu personal en la política i instruccions de l'Ajuntament que els sigui d'aplicació.

El/la Cap de Projecte haurà d'informar a tothom que presti serveis dins del marc del contracte, dels deures i responsabilitats del seu lloc de treball en matèria de seguretat de la informació i protecció de dades de caràcter personal, especificant les mesures disciplinàries al fet que pertoqui i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Ajuntament.

El/la Cap de Projecte de l'empresa adjudicatària haurà de mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte on s'indicarà la data en què van rebre la formació en política i instruccions de l'Ajuntament, així com el document d'acceptació de les obligacions relatives a la seguretat de la informació.

El document d'acceptació de les obligacions signat per les persones adscrites a l'execució d'aquest contracte serà entregat al/la Cap de Projecte de l'Ajuntament, abans de ser donats els permisos per accedir als Sistemes d'Informació de l'Ajuntament o bé abans de ser facilitada la informació per al correcte compliment del servei contractat, i restarà en poder de l'empresa adjudicatària que haurà de presentar-los quan siguin requerits per l'Ajuntament.

Es contemplarà el deure de confidencialitat respecte de les dades a les que tingui accés, tant durant el període de duració del contracte, com posteriorment a la seva terminació.

L'empresa adjudicatària haurà de mantenir disponible en tot moment la informació o treballs resultants de l'objecte del contracte, amb la finalitat de comprovar el compliment de les mesures i controls previstos en aquest apartat.

- h) **Formació i conscienciació:** l'empresa adjudicatària realitzarà les accions necessàries per conscienciar regularment al personal sobre el seu paper i responsabilitat respecte a la seguretat dels sistemes. Es recordarà regularment instruccions sobre l'ús dels sistemes i tecnologies de la informació i comunicació per part de les persones al servei de l'Ajuntament de Barcelona; normativa de seguretat relativa al bon ús dels sistemes; normativa d'identificació i comunicació d'incidents, activitats o comportaments sospitosos que hagin de ser reportats per al seu tractament per personal especialitzat.

L'empresa adjudicatària haurà de formar regularment al personal en aquelles matèries que requereixin per a l'acompliment de les seves funcions, en particular en relació a configuració de sistemes, detecció i reacció a incidents, i gestió de la informació i dades personals en qualsevol tipus de suport.

L'Ajuntament podrà demanar evidències de les diferents accions de formació i conscienciació que l'empresa adjudicatària ha realitzat sobre les persones assignades a l'execució del contracte.

- i) **Protecció del lloc de treball:** quan el lloc de treball sigui buit, l'empresa adjudicatària haurà d'establir una política de "taules netes" respecte a la documentació de l'Ajuntament. Únicament es podrà disposar del material requerit per a l'activitat que s'està realitzant a cada moment.

En relació a la protecció d'equips l'empresa adjudicatària es compromet a que els equips que surtin, o puguin sortir de l'empresa adjudicatària, estaran protegits adequadament contra accessos no autoritzats en cas de pèrdua o robatori.

Sense perjudici de les mesures generals que els afectin, es requereix a l'empresa adjudicatària que porti un inventari d'equips juntament amb una identificació de la persona responsable del mateix i un control regular que està positivament sota el seu control. Les persones usuàries hauran de disposar d'un canal de comunicació per informar al servei de gestió d'incidents de pèrdues o robatoris, que hauran de ser comunicades a l'IMI.

S'evitarà, en la mesura del possible, que l'equip contingui claus d'accés remot a l'organització. Es consideraran claus d'accés remot aquelles que habilitin un accés a altres equips de l'organització, o unes altres de naturalesa anàloga.

Adicionalment, els equips hauran de disposar de: solució d'antivirus actualitzada a la última versió i configurada per realitzar anàlisis regulars de l'equip; política d'actualització que instal·li els últims pegats de seguretat en un temps raonable, prioritzant les crítiques; Firewall habilitat restringint el trànsit d'entrada a l'equip al mínim necessari.

- j) **Comunicacions externes:** l'empresa adjudicatària disposarà dels mitjans materials i el maquinari necessari per a la connexió amb els Sistemes d'Informació de l'Administració Municipal, sent els costos de connexió a càrrec de l'empresa contractada.

La connexió és realitzarà seguint els protocols de seguretat per a les comunicacions externes establerts per l'Administració Municipal.

L'empresa adjudicatària serà la responsable de custodiar correctament els certificats digitals lliurats per la interconnexió segura de xarxes i de demanar la seva revocació una vegada finalitzada la prestació del servei. Així mateix, serà responsable subsidiària de l'ús dels certificats personals individuals lliurats als seus empleats pel desenvolupament del producte o servei.

k) **Protecció dels suports informàtics:** l'empresa adjudicatària haurà de gestionar els suports informàtics amb informació de l'Ajuntament de Barcelona seguint les següents pautes.

- **Etiquetat:** l'empresa adjudicatària es compromet a etiquetar els suports d'informació de manera que, sense revelar el seu contingut, s'indiqui el nivell de seguretat de la informació continguda de major qualificació. Les persones usuàries han d'estar capacitades per entendre el significat de les etiquetes, bé mitjançant simple inspecció, bé mitjançant el recurs a un repositori que ho expliqui.
- **Transport:** l'empresa adjudicatària garantirà que els dispositius romanen sota control i que satisfan els requisits de seguretat mentre estan sent desplaçats d'un lloc a un altre. L'empresa adjudicatària garantirà que es segueix el procediment de transport, de manera que s'haurà de disposar d'un registre de sortida que identifiqui al transportista que rep el suport per al seu trasllat i d'un registre d'entrada que identifiqui al transportista que el lliura, conjuntament amb un procediment rutinari que quadri les sortides amb les arribades i elevi les alarmes pertinents quan es detecti algun incident.
- **Esborrat i destrucció:** l'empresa adjudicatària haurà de seguir els estàndards i normes de l'IMI respecte a l'esborrat i destrucció de suports d'informació. S'aplicarà a tot tipus d'equips susceptibles d'emmagatzemar informació, incloent mitjans electrònics i no electrònics. Els suports que hagin de ser reutilitzats per a una altra informació o alliberats a una altra organització hauran de ser objecte d'un esborrat segur del seu contingut.

l) **Protecció de la informació:** s'hauran de contemplar els següents camps d'aplicació.

- **Neteja de documents:** l'empresa adjudicatària disposarà d'un procediment de neteja de documents, el qual retirarà d'aquests tota la informació addicional continguda en camps ocults, metadades, comentaris o revisions anteriors, excepte quan aquesta informació sigui pertinent per al receptor del document.

Aquesta mesura serà especialment rellevant quan el document es difongui àmpliament, com quan s'ofereix al públic en un servidor web o un altre tipus de repositori d'informació.

- **Protecció del correu electrònic:** en el cas de que l'empresa adjudicatària faci ús del seu correu electrònic corporatiu per gestionar informació de l'Ajuntament, l'haurà protegir enfront d'amenaques que li són pròpies: la informació distribuïda per mitjà de correu electrònic s'ha de protegir tant en el cos com els annexes; s'haurà de protegir la informació d'encaminament de missatges i establiment de connexions; no es permetrà la redirecció a dominis de correu públics fora del correu corporatiu de l'empresa adjudicatària; s'ha de protegir el correu electrònic front spam, programes nocius i codi de mòbil de tipus applet.

Dins de les polítiques d'ús del correu electrònic s'inclou la limitació a l'ús com a suport de comunicació privada i el realitzar activitats de conscienciació i formació relatives a l'ús del correu personal per detectar malware o phishing.

El responsable del contracte de l'Ajuntament avaluarà si el contracte ha de gestionar informació sensible, especialment protegida en relació a la protecció de dades personals, confidencial de l'Ajuntament o de les tecnologies municipals (adreces IP, usuaris, credencials,...)

En cas afirmatiu, l'Ajuntament facilitarà a l'empresa adjudicatària un correu electrònic de l'Ajuntament (@ext.bcn.cat) el qual es convertirà en la via de comunicació entre l'empresa adjudicatària i l'Ajuntament.

Aquesta mesura vol evitar que les empreses externes retinguin informació confidencial de l'Ajuntament en servidors de correu aliens a l'entorn municipal, durant i sobretot, un cop finalitzat el contracte.

- m) **Protecció de les instal·lacions:** les instal·lacions de l'empresa adjudicatària hauran de disposar de certes condicions de seguretat física per evitar els accessos físics als repositoris d'informació, segons la sensibilitat de dita informació i per garantir que la informació de l'Ajuntament no pugui ser visible i/o audible des de l'exterior de les instal·lacions.
- n) **Gestió d'excepcions:** qualsevol excepció als anteriors apartats no recollida en el present document en el moment de la contractació o que ocorri en el transcurs del servei, haurà de ser comunicada per mitjà dels canals oficials al Departament de Seguretat de l'IMI per al seu corresponent tractament i valoració. S'haurà de presentar de forma clara i concisa l'objecte de l'excepció així com la modificació desitjada pel sol·licitant amb la seva deguda justificació.

Al ser un Sistema d'Informació de l'Ajuntament de nivell mig, també son obligatòries les següents clàusules:

- a) **Dimensionament:** l'empresa adjudicatària ha de garantir que disposa de les persones necessàries i amb les qualificacions professionals adients per garantir la correcta prestació del servei.
- b) **Anàlisis forenses:** l'execució d'anàlisis forenses serà responsabilitat exclusiva del Departament de Seguretat de l'IMI . L'empresa adjudicatària haurà de col·laborar proporcionant la informació requerida i el coneixements de les plataformes i tecnològics que facin falta. Les peticions de col·laboració es realitzaran a través dels procediments i canals establerts entre el Departament de Seguretat de l'IMI i l'empresa proveïdora.
- c) **Control accés local:** sumat a les obligacions anteriors, s'haurà de informar a la persona usuària de l'últim accés efectuat amb la seva identitat.
- d) **Mitjans alternatius:** l'empresa adjudicatària garantirà l'existència i disponibilitat de mitjans alternatius de tractament de la informació per al cas que fallin els mitjans habituals. Aquests mitjans alternatius hauran d'estar

subjectes a les mateixes garanties de protecció que les detallades anteriorment. Igualment, s'haurà d'establir un temps màxim perquè els equips alternatius entrin en funcionament.

e) **Protecció dels suports informàtics:** addicionalment a les obligacions establertes anteriorment:

- **Esborrat i destrucció:** en cas de que la naturalesa del suport no permeti un esborrat segur o quan així ho requereixi el procediment associat al tipus d'informació continguda, s'hauran de destruir de forma segura els suports fent us dels productes certificats per l'IMI.
- **Criptografia:** qualsevol informació corporativa que requereixi ser xifrada a la seva ubicació d'emmagatzemament, en particular a tots els dispositius extraïbles del tipus CD, DVD, discos USB, o uns altres de naturalesa anàloga, han de seguir els estàndards de seguretat, custòdia i protecció de les claus establerts pel Departament de Seguretat de l'IMI.

Qualsevol requeriment criptogràfic de plataformes que s'hagin de produir referents amb la informació municipal o corporativa, l'empresa adjudicatària haurà de presentar-les per ser validades pel Departament de Seguretat de l'IMI i/o seguir els estàndards i normes de l'IMI.