

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PER LA CONTRACTACIÓ DEL SERVEI D'UNA PLATAFORMA SAAS DE GESTIÓ DE CERTIFICATS ELECTRÒNICS PER LA SOCIETAT MERCANTIL CORPORACIÓ CATALANA DE MITJANS AUDIOVISUALS, SA.

1.- OBJECTE DEL CONTRACTE

Constitueix l'objecte del present contracte la prestació del servei d'una Plataforma SAAS de Gestió de Certificats Electrònics amb l'objectiu d'homogeneïtzar el tractament dels mateixos, la centralització del seu dipòsit i salvaguarda en un repositori segur de manera que es millori l'operativa a nivell general pel que fa al control del cicle de vida, seguretat pel que fa als permisos usuari / certificat i a l'auditoria de tot aquest procés. Aquestes funcionalitats reduiran els temps i costos de suport als usuaris i també reduiran els temps dedicats al control amb un increment significatiu del nivell de seguretat.

2.- CARACTERÍSTIQUES TÈCNIQUES OBLIGATÒRIES DE LA SOLUCIÓ

- Solució SaaS
- Aplicació Client-Servidor
- Emmagatzematge segur de certificats.
- Disponible per a 100 usuaris corporatius. Amb possibilitat d'ampliació (cost addicional).
- Nombre de certificats il·limitats.
- Capacitat de processament criptogràfic 1000 operacions concurrents per segon.
- Alta disponibilitat: Fail-over i sincronització automàtica / No requereix elements externs addicionals.
- Actualitzacions: Sistema d'actualitzacions amb càrrega web de firmware / Upgrading i downgrading de versions
- Gestió de backups.
- Monitorització del sistema.
- Sistema d'usuaris locals i integració amb directori actiu o LDAP. SSO-SAML
- Consola d'administració web compatible amb tots els navegadors actuals.
- Agents per a sistemes operatius Windows-Linux i complement per als principals navegadors del mercat.

3.- FUNCIONALITATS MÍNIMES OBLIGATÒRIES DE LA SOLUCIÓ

- **Emmagatzematge:** Els certificats s'emmagatzemaran en un únic repositori segur i centralitzat.
- **Desplegament:** El desplegament dels agents es podrà realitzar de manera centralitzada i els usuaris finals no requereixen cap tipus de formació ja que ells seguiran usant els certificats de manera totalment transparent.



- **Utilització:** Establiment de polítiques d'ús, permisos d'ús als usuaris tenint un control total i centralitzat de qui, en quin moment, i per a què s'estan utilitzant els certificats instal·lats.
- **Monitorització:** Registre complet de totes les accions que realitza l'usuari. Mitjançant l'auditoria es podrà consultar les activitats d'un usuari i/o un certificat determinat.
- **Revocació:** Suspensió del permís d'ús del certificat a un usuari. D'aquesta manera no és necessari que la CA revoqui el certificat perquè l'usuari no l'utilitzi més.
- **Rotació:** Renovació de certificats de forma centralitzada.
- **Expiració:** Alertes per saber amb antelació quan expira un certificat.
- **Destrucció:** Destrucció de certificats centralment, garantint al 100% la destrucció del mateix i assegurant que no existeixen còpies.

4.- GARANTIA, MANTENIMENT I SUPORT

- **Actualitzacions** de noves versions del producte. Han d'estar incloses en el cost del servei.
- **Support.** Ha d'incloure un servei de manteniment de segon nivell 8x5, per tractament d'incidències.
- S' inclourà el servei de **manteniment del fabricant** així com el suport expert proporcionat pel contractista durant el temps de vida del contracte. Totes les actualitzacions estaran incloses.
- **Formació:** S'inclourà formació per l'equip que farà l'administració de l'eina.

5.- INCOMPLIMENT ANS

Els criteris de prioritització queden recollits en 2 tipus, normal i crítics.

Incidència normal: No implica l'aturada total del servei o que no comprometen la seguretat del mateix.

Incidència crítica: Implica l'aturada total del servei o que pot comprometre la seguretat del servei.

Per que respecta, als temps de resposta i resolució s'ha de donar el servei següent:

Tipus	Temps de resposta	Temps de solució
Peticions	16 hores	72 hores
Incidència normal	4 hores	48 hores
Incidència crítica	1 hora	24 hores

Totes les desviacions a la baixa al nivell de compliment del servei estaran associades a una compensació. Per establir-la compensació es defineixen dos nivells d'incompliment: lleu i greu.

Incompliment	Lleu	Greu
Temps resposta. Excedit incidència normal	Entre 48 i 72 hores	Mes de 72 hores
Temps resposta. Excedit incidència crítica	Entre 8 i 24 hores	Mes de 24 hores
% disponibilitat	Entre 98% i 99,5%	Menor 98%

Sempre que els nivells de servei no siguin complerts, PROVEÏDOR haurà de compensar CLIENT. Les compensacions per incompliment del servei queden recollides a continuació:

Incompliment	Penalització Lleu	Penalització Greu
Temps resposta. Excedit incidència normal	1% de descompte en la propera factura. Màxim 10% acumulable.	4% de descompte en la propera factura. Màxim 20% acumulable.
Temps resposta. Excedit incidència crítica	1% de descompte en la propera factura. Màxim 10% acumulable.	4% de descompte en la propera factura. Màxim 20% acumulable.
% disponibilitat inferior al demanat	2% de descompte en la propera factura. Màxim 10% acumulable.	10% de descompte en la propera factura. Màxim 100% acumulable.

D'altra banda, la reiteració d'incompliments tant lleus com greus tindrà penalitzacions addicionals.

En cas que es donin més 3 incompliments lleus en el termini d'una setmana, seran considerats amb caràcter general com un incompliment greu.

En cas que es donin més de 3 incompliments greus en el termini d'un mes estarà justificada la resolució unilateral del contracte.

L'acord de nivell de servei tindrà validesa durant tot el període de temps que duri la prestació del servei.

6.- E-LEARNING

Quan l'objecte del contracte requereixi la formació en la utilització d'una eina de propòsit específic, es subministrarà un curs bàsic de formació a importar en la plataforma de formació de la CCMA que asseguri una transferència de coneixement i la formació continua dels empleats.

7.- PROTECCIÓ DE DADES I ENS

No es podrà transferir cap informació sobre els treballs a persones o entitats no explícitament esmentats en aquest sentit en el contracte sense el consentiment, per escrit, de la CCMA.

Si derivat de l'execució de l'objecte del contracte resultant d'aquest procés de adjudicació s'accedís a qualsevol de les bases de dades de caràcter personal, la



empresa adjudicatària, en compliment del que disposa RGPD, no podrà utilitzar les dades de caràcter personal a què tingui accés o a les quals la CCMA, els hi hagi facilitat, amb fi diferent del que figuri al contracte, ni cedir-los, ni tan sols per al seu conservació a terceres persones.

L'empresa adjudicatària no revelarà a persones alienes a la relació contractual, cap informació a què hagi tingut accés com a conseqüència de la realització de l'estipulat en aquest plec.

L'empresa adjudicatària declara tenir incorporades les mesures d'índole tècnica i organitzatives necessàries per garantir la seguretat que determina l'ENS.

Un cop finalitzada la relació contractual, les dades de caràcter personal tractades per l'adjudicatària, així com el resultat del tractament obtingut, han de ser destruïts o tornats en el moment en què aquesta ho sol·liciti.

L'empresa adjudicatària respondrà davant de CCMA per l'ús fraudulent de les dades de caràcter personal propietat d'aquesta entitat, així com per l'ús no acord amb el contingut del contracte, mitjançant la corresponent indemnització per danys i perjudicis ocasionats, assumint les despeses que es poguessin ocasionar com a conseqüència d'actuacions judicials i sancions que a el seu cas poguessin dictar per tercers.

8.- INFORMACIÓ SOBRE L'ARQUITECTURA DE SEGURETAT.

Serà requisit obligatori que el prestador de serveis, quan sigui rellevant per al servei prestat, especialment a l'efecte de definició de requisits d'interconnexió, aporte la informació necessària sobre el sistema que suporta els serveis, respecte a l'arquitectura de seguretat, a fi de facilitar a l'entitat CCMA contractant el compliment de les seves obligacions, com ara la realització de l'Anàlisi de Riscos o el subsegüent Pla de Tractament de Riscos.

Així mateix, aportarà els diagrames de xarxa, esquemes d'elements físics, esquemes d'interconnexió i esquemes lògics de sistemes que mostrin a l'entitat client la infraestructura física i lògica de què forma part el servei objecte de contractació.

Tot això serà exigible sempre que els requisits esmentats no estiguin adequadament coberts per la Declaració o Certificació de Conformitat amb l'ENS que pogués posseir el proveïdor, amb relació als sistemes d'informació utilitzats per a la prestació dels serveis contractats.

9.- UBICACIÓ DE LA INFORMACIÓ

Per tal que l'entitat destinatària dels serveis conegui amb precisió la ubicació dels sistemes d'informació concernits en la prestació i la seva informació, el prestador de serveis aportarà la documentació que detalli els tractaments d'informació, s'executaran en sistemes i instal·lacions pròpies o en proveïdors cloud.

El prestador del servei, ha d'indicar les mesures de seguretat física associades. Les exigències anteriors podran ser evidenciades a través de les corresponents Declaracions o Certificacions de Conformitat amb l'ENS de les que el proveïdor fos titular.

10.- MESURES DE SEGURETAT IMPLEMENTADES.

La CCMA destinatària dels serveis podrà requerir el prestador, a més de la corresponent Declaració o Certificació de Conformitat amb l'ENS, el detall de la Declaració d'Aplicabilitat i, si escau, de les mesures compensatòries i complementàries de vigilància utilitzades si així es determinen.

De aquesta forma, la CCMA podrà donar conformitat als seus propis requisits de l'ENS i conèixer si hi ha mesures de seguretat addicionals o complementàries a les exigides per la categoria del/s seu/s sistema/s.

Les exigències anteriors podran ser evidenciades a través de les corresponents Declaracions o Certificacions de Conformitat amb l'ENS de les que el proveïdor fos titular.

11.- COMPLIMENT DE LA NORMATIVA VIGENT DE PROTECCIÓ DE DADES.

En aquells casos en què els serveis prestats impliquin el tractament de dades personals, serà necessari la implementació de funcionalitats que garanteixin el compliment de la normativa vigent per part de la CCMA.

Per exemple, mesures destinades a complir amb els principis bàsics del tractament i que permetin garantir els drets dels interessats (accés, rectificació, supressió i bloqueig de dades).

A més de l'anterior, quan sigui procedent, el proveïdor de serveis estarà obligat a complir les obligacions que estableix la normativa de protecció de dades pels Encarregats de Tractament.

12.- INCIDENT DE SEGURETAT

Les entitats públiques tenen l'obligació de notificar al CCN-CERT els incidents de seguretat que puguin tenir un impacte significatiu, tal com prescriu l'art. ENS i desenvolupa la 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.

D'altra banda, la Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual es aprova la Instrucció Tècnica de Seguretat de conformitat amb l'Esquema Nacional de seguretat, prescriu que l'ENS també és aplicable a les entitats privades quan prestin serveis o proveeixin solucions a les entitats públiques als que resulti exigible el compliment de l'Esquema Nacional de Seguretat.

Aplicabilitat de l'ENS a aquestes empreses privades suposa també l'obligació de notificar a l'entitat pública contractant a què prestin servei els incidents de seguretat, que puguin afectar la seguretat dels sistemes objecte del servei.

13.- PORTABILITAT DE LA INFORMACIÓ

Serà necessari implementar mecanismes que garanteixin la portabilitat de la informació amb l'objectiu de facilitar a la CCMA el procés de gestió del canvi davant el cessament o baixa dels serveis subministrats per part del prestador de servei.

Igualment, el prestador de serveis haurà de certificar que, en causar baixa el servei subministrat, les dades emmagatzemades han estat eliminades de manera segura una vegada finalitzat el procés de portabilitat.

14.- CADENA DE SUBCONTRACTACIÓ I ELS SEUS CANVIS.

L'entitat proveïdora del servei haurà de tenir una documentació que detalli clarament els elements que formen part de la cadena de subcontractació, així com les implicacions derivades de qualsevol canvi o modificació que pugui patir algun baula d'aquesta cadena.

El proveïdor haurà d'assegurar que els sistemes de informació de les empreses subcontractades són conformes amb l'ENS en allò que respecte als serveis que afectin l'entitat pública contractant, per la qual cosa el contingut del present document resultarà així mateix d'aplicació a la cadena de subministrament del proveïdor.

En aquest sentit, l'entitat pública destinatària dels serveis podrà requerir del prestador, a més de la corresponent Declaració o Certificació de Conformitat amb l'ENS, el detall de la Declaració d'Aplicabilitat i, si escau, de les mesures compensatòries i complementàries de vigilància utilitzades.

15.- CAPACITAT I DIMENSIONAMENT DEL SISTEMA.

S'haurà de disposar d'un sistema de gestió de la capacitat amb millora contínua, que proporcioni, de forma periòdica, informació relacionada amb el sistema que suporta els serveis, com ara capacitat, dimensionament i rendiment del sistema. Anàlogament, la CCMA podrà requerir del prestador, a més de la corresponent Declaració o Certificació de Conformitat amb l'ENS, el detall de la Declaració d'Aplicabilitat i, si escau, de les mesures compensatòries i complementàries de vigilància utilitzades.

16.- SEGUIMENT DELS ACORDS DE NIVELL DE SERVEI.

El proveïdor del servei, utilitzarà eines de monitorització o informes diaris de manera que l'entitat pública client en pugui fer un seguiment i gestió del compliment dels Acords de Nivell de Servei (SLA) contractats.

El prestador de servei serà proactiu en aquest àmbit, aportant aquestes dades amb total transparència i gestionant els incompliments diligentment.

17.- CONTINUÏTAT

Per tal que la CCMA pugui garantir la continuïtat dels serveis prestats pel prestador, caldrà que aquest li faciliti la informació necessària per establir el pla de continuïtat tal com s'exigeix a l'ENS.

18.- ANÀLISI I EXPLOTACIÓ DE REGISTRES.

Perquè els registres (logs) generats pels serveis contractats i que el proveïdor haurà de posar a disposició de la CCMA, tant en la seva utilització com en la seva gestió, puguin ser degudament analitzats i explotats, es recomana establir funcionalitats que permetin definir alertes i regles, de manera que es faciliti el anàlisi de la informació registrada. Aquestes funcionalitats permetran a la CCMA detectar situacions d'alerta davant d'una

possible utilització indeguda dels serveis, de manera que sigui possible depurar i analitzar incidències o accions realitzades.

19.- CONTROLS PERIÒDICS

Per tal de facilitar la realització dels controls periòdics exigits per al compliment de les exigències establertes a l'ENS, el proveïdor de serveis ha de proporcionar els mecanismes i les funcionalitats que permetin a la CCMA conèixer i analitzar els controls duts a terme per part del proveïdor de serveis. Alguns d'aquests controls seran, per exemple: auditories de seguretat, informes de hacking ètic, renovació de certificacions de seguretat, etc.

Sant Joan Despí, desembre de 2024