Consorci
Administració Oberta
de Catalunya

Plec de prescripcions tècniques.

Desplegament i manteniment de hub de xarxes privades virtuals entre centres de dades

Generalitat
de Catalunya

Consorci de governs locals
per a la societat de la informació

1. Índex

2. Objecte del contracte

El Consorci AOC proporciona diferents aplicacions i serveis de negoci que es troben ubicades a infraestructura resident a diferents Centres d'Operació. Aquests serveis i aplicacions necessiten interaccionar en molts casos amb altres serveis i aplicacions ubicades a un altre dels Centres d'Operació extern. Els serveis requerits facilitaran aquesta interacció amb la configuració d'una nova arquitectura de comunicacions de xarxes privades virtuals. Els serveis que es requereixen són els següents:

- Serveis de configuració de dos equips Cisco Firepower 2110 per tal de desplegar les xarxes privades virtuals necessàries (VPN, *Virtual Private Networks*)
- Serveis de configuració de les comunicacions internes per a enrutar el tràfic intern i extern d'aquestes xarxes privades
- Serveis d'operació i suport de la solució i equips associats (explotació, manteniment, administració i monitoratge)
- Bossa d'hores per potencials futures tasques de reconfiguració i/o ampliació de la solució per noves necessitats del servei

3. Descripció del serveis requerits

3.1 Objectiu

L'AOC necessita desplegar una solució de xarxes privades virtuals que garanteixi les comunicacions entre Centres d'Operació que permeti l'accessibilitat entre serveis ubicats a diferents ubicacions de la infraestructura tecnològica de negoci no accessibles via la xarxa Internet i que es realitzi amb els màxims requeriments de seguretat possible.

Per assolir aquest objectiu la solució requerida es fonamenta en la utilització d'equips tallafocs de nova generació com són els esmentats a l'objecte de contracte i ubicats al Centre de Dades *on-premise*, així i com, la configuració dels elements disponibles als altes Centre d'operació residents a *clouds* públics.

Els equips on es centrarà la configuració de la solució ja es troben disponibles i no són part del present contracte.

3.2 Requeriments

La solució que cal desplegar ha de permetre les següents característiques funcionals:

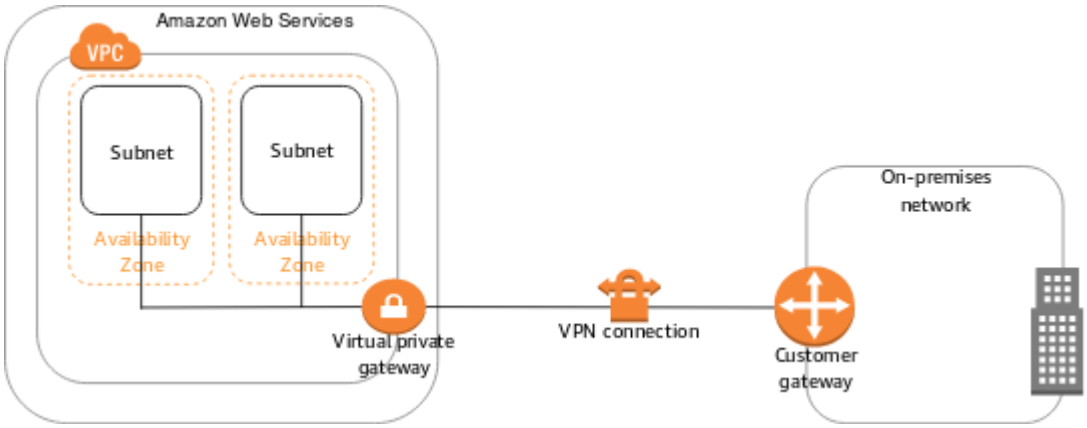
- *Setup* dels equips tallafocs disponibles per la solució
- Configuració específica dels equips en mode tallafocs de nivell 7
- Configuració de les funcions de xarxa privada virtual amb compatibilitat a les solucions dels altres Centre d'Operació (AWS i Azure)
- Possibilitat d'ampliació de la solució i configuració de processos de *Disaster recovery*

- Capacitat de monitorització externa de la solució amb els serveis de *monitoring* de l'AOC (OP5)
- Administració externa segons procediments interns de l'AOC
- Operació i suport de la solució fins a la data de devolució del servei
- Es requereix la capacitat de demanar noves tasques de reconfiguració i redisseny en funció de necessitats de negoci amb imputació a una bossa d'hores que ha d'oferir el proveïdor

La solució a desplegar ha de permetre la configuració i operació del servei en diferents arquitectures, a futur, si es requereix. La finalitat principal és establir una solució permanent i segura entre el Centre de Dades *on-premise* i la infraestructura existent al cloud públic *Amazon Web Services*. Inicialment es requerirà, com a base, la primera de les següents arquitectures següents:

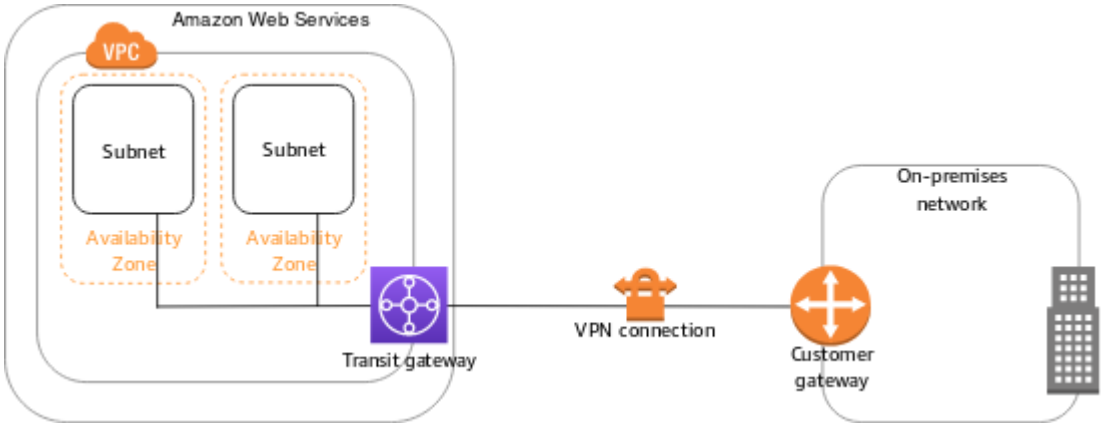
Connexió única de Site-to-Site VPN

La VPC disposa d'un gateway privat virtual associat i la xarxa local (remota) conté un dispositiu de gateway de client que haureu de configurar per activar la connexió de Site-to-Site VPN. Configuració de l'encaminament perquè el trànsit procedent de la VPC vinculada a la xarxa s'adreci al gateway privat virtual.



Connexió de Site-to-Site VPN amb un gateway de trànsit

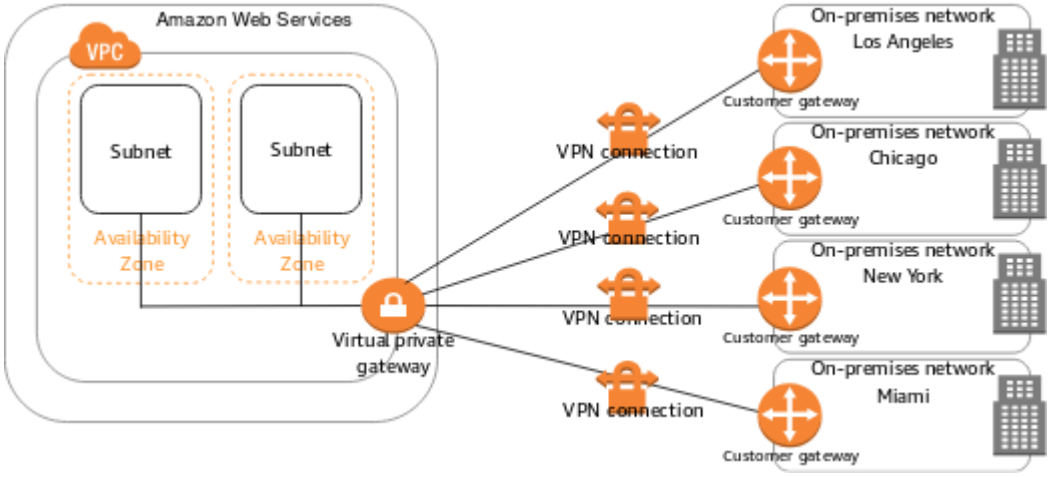
La VPC disposa d'un gateway de trànsit i la xarxa local (remota) conté un dispositiu de gateway de client que s¡haurà de configurar per activar la connexió de Site-to-Site VPN. S'haurà de configurar l'encaminament perquè el trànsit procedent de la VPC vinculada a la xarxa s'encamini al gateway de trànsit.



Connexions múltiples de Site-to-Site VPN

La VPC té associada un gateway privada virtual i hi ha diverses connexions de Site-to-Site VPN amb diferents ubicacions locals. S'hauria de configurar l'encaminament per a què el trànsit procedent de la VPC vinculada a xarxa s'adreci al gateway privat virtual.

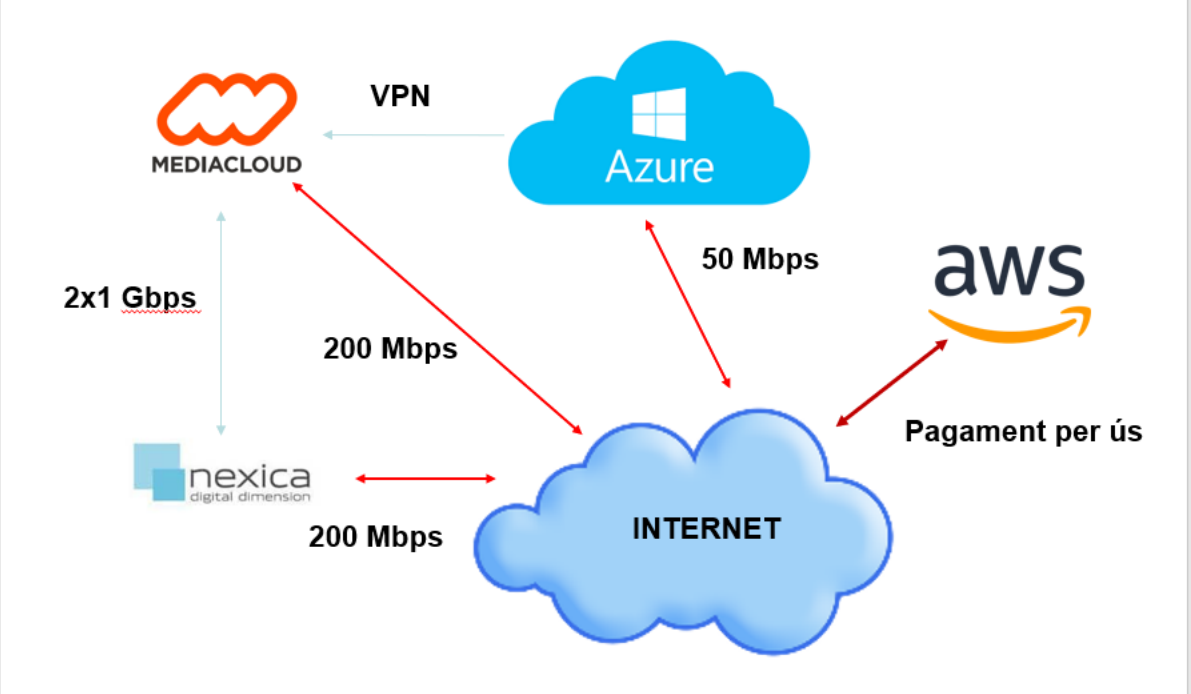
També es podria utilitzar aquesta solució per crear connexions de Site-to-Site VPN amb els diferents Centres d'Operació i proporcionar una comunicació segura entre ells.



3.3 Descripció de l'entorn actual

En aquests moments els servis de negoci i aplicacions del Consorci AOC es troben ubicats en diferents Centres d'Operació, ja siguin Centre de dades on-premise, cloud privat o cloud públic. Al Centre de dades on-premise es troben diferents serveis que són consultats o són peça essencial d'altres serveis ubicats fora del mateix. Per tal d'enfortir la seguretat d'aquestes comunicacions es considera inprescindible que aquestes viatgin per mitjà de xarxes privades virtuals, ja que no es considera suficient l'encapsulament de les dades per protocols d'aplicació encriptats i restriccions d'accés als tallafocs perimetrals. Es troben a disposició uns elements tallafocs, diferents dels que

permeten la securització perimetral, que permetrien l'establiment d'aquestes xarxes privades virtuals amb els requeriments tècnics dels serveis de cloud públic actualment operatius. Aquests dispositius es troben ja disponibles per a la seva utilització.



Els elements tallafocs destinats al desplegament d'aquestes xarxes privades virtuals són equips físics del fabricant Cisco Systems model Firepower 2100. Les característiques principals, segons taula d'especificacions del fabricant (https://www.cisco.com/c/en/us/products/collateral/security/firepower-2100-series/datasheet-c78-742473.html) , d'aquests dispositius són les següents:

Característiques	2110
Throughput: FW + AVC (1024B)	2.6 Gbps
Throughput: FW + AVC + IPS (1024B)	2.6 Gbps
Maximum concurrent sessions, with AVC	1 million
Maximum new connections per second, with AVC	14K
TLS	365 Mbps
Throughput: IPS (1024B)	2.6 Gbps
IPSec VPN Throughput (1024B TCP w/Fastpath)	950 Mbps
Maximum VPN Peers	1,500

Característiques	2110
Cisco Firepower Device Manager (local management)	Yes
Centralized management	
Application Visibility and Control (AVC)	
AVC: OpenAppID support for custom, open source, application detectors	
Cisco Security Intelligence	
Cisco Firepower NGIPS	
Cisco AMP for Networks	
Cisco AMP Threat Grid sandboxing	
URL Filtering: number of categories	
URL Filtering: number of URLs categorized	
Automated threat feed and IPS signature updates	
Third-party and open-source ecosystem	
High availability and clustering	
Cisco Trust Anchor Technologies	

3.4 Descripció dels serveis

Els serveis requerits globals són els següents:

- Serveis de configuració i posada en marxa
- Serveis d'operació i suport
- Serveis basat ens bossa d'hores

3.4.1 Serveis de configuració i posada en marxa

Els serveis de configuració i posada en marxa hauran de ser tractats com a projecte, respectant les bones pràctiques de la gestió i execució de projectes. El proveïdor podrà presentar la seva proposta que haurà de incloure una estructura de projecte que inclogui es següents fases o similars:

Fase de disseny i proposta

En aquesta fase, l'adjudicatari farà una revisió de la infraestructura actual per definir la estratègia de desplegament de la solució amb les màximes garanties considerant l'objectiu i els requeriments esmentats. Les tasques a realitzar són les següents:

- Auditoria i inventari dels nous equips
- Disseny i proposta de solució
- Revisió i preparació del disseny de la solució;
- Flight-plan de la intervenció

Al final d'aquesta fase, l'adjudicatari haurà d'entregar un document amb la estratègia de la intervenció de desplegament de la solució consensuada amb l'AOC.

Fase de implementació

En aquesta fase, l'adjudicatari haurà d'executar la proposta de configuració i posada en marxa acordada a la fase anterior seguint la planificació proposada al document de disseny i posada en marxa. El Consorci AOC validarà la consecució dels objectius i el bon funcionament de la solució segons els criteris establerts i la proposta acordada.

El Consorci AOC podrà demanar canvis necessaris que afectin a la seguretat de la solució o a la de la infraestructura pròpia relacionada amb el projecte, en funció de l'anàlisi de riscos que es faci, sempre i quan els riscos vinguin derivats de l'execució del projecte.

Les tasques a realitzar són les següents:

- Execució de les tasques de la proposta
- Integració de la solució a la infraestructura de l'AOC
- QA, revisió i proves

Fase d'entrega i supervisió

Una vegada el Consorci AOC hagi donat el vist i plau a la solució desplegada, s'hauran de fer les tasques necessàries per tal de realitzar la monitorització i control dels equips i els paràmetres afectats per l'execució de les tasques del projecte. Així i com la transferència dels accessos i control dels equips i la solució integral.

La transferència de la informació s'haurà de fer seguint les directrius de seguretat del Consorci AOC.

Les tasques a realitzar són les següents:

- Preparació per l'explotació i administració de la solució
- Coordinació amb tercers per integració de la monitorització i supervisió
- Entrega de documentació

3.4.2 Serveis d'operació i suport de la solució i equips

Els serveis que s'engloben dins aquesta classe en quant a la infraestructura desplegada o a desplegar al llarg del cicle de vida del contracte són els de Manteniment, Administració, Desplegament de solucions d'infraestructura, Explotació i Monitoratge, dels equips i serveis objecte del contracte.

Aquí descriurem les tasques necessàries que el proveïdor dels serveis haurà de garantir per mantenir la solució amb les màximes garanties de capacitat i disponibilitat, així com mantenir els equips actualitzats en les versions més recents i òptimes per als citats serveis.

S'entén com **Manteniment** dels equips totes aquelles tasques necessàries per garantir la correcta operativitat de tots els elements físics o lògics i funcionalitats tècniques associades als equips i la solució en global.

La tipologia del servei de Manteniment requerit es pot dividir en tres tipus independents:

- **Manteniment preventiu**. El manteniment preventiu correspon a aquelles actuacions destinades a solucionar potencials successos que podrien esdevenir com incidents que afectessin al correcte funcionament dels elements que conformen la solució o una degradació del seu rendiment o funcionament.

- **Manteniment correctiu**. El manteniment correctiu correspon a aquelles actuacions destinades a la resolució de qualsevol succés amb afectació al funcionament i disponibilitat del servei que ofereixi amb indiferència de la seva afectació a la disponibilitat i continuació de negoci i serveis oferts per qualsevol dels elements que conformen la solució.

- **Manteniment evolutiu.** El manteniment evolutiu correspon a aquelles actuacions destinades a actualitzar components de la infraestructura de la solució per qualsevol necessitat operativa del Consorci AOC i que afecti als elements que la componen.

S'entén com **Administració** totes les tasques necessàries per tal de configurar, adaptar, consolidar i extreure informació del comportament de tots els elements de la plataforma que figuren en aquest plec. L'objectiu d'aquest servei és el garantir el bon funcionament dels elements i de la plataforma en general per tal de garantir el compliment de l'Acord de Nivell de Servei (ANS) del Consorci AOC.

Aquest acord es troba publicat i accessible al portal corporatiu existent a Internet.

L'**Administració** dels elements de la plataforma implica, entre altres, les tasques de modificació fina d'alguns components d'elements a administrar per tal de millorar el rendiment del mateix, la configuració dels elements en funció de la resta, realitzar les actualitzacions de versió possibles i necessàries en matèria de seguretat, canvis de versió informats per part del fabricant i modificacions de les versions existents.

S'entén també que dins de l'administració dels diferents sistemes es realitzaran els processos periòdics de còpies de seguretat segons la configuració acordada i l'accessibilitat amb l'agilitat necessària per tal de realitzar les tasques de recuperació i importació d'aquests còpies en cas d'incidència.

S'entén per **Explotació** qualsevol actuació que s'hagi de realitzar sobre qualsevol element de la solució sota petició prèvia del personal del Consorci AOC habilitat a tal efecte, o personal de terceres empreses als que s'hagi donat permís previ per realitzar aquesta petició. L'objecte d'aquest servei ve donat pel dinamisme propi del negoci del Consorci AOC i necessitats d'operació associades sobre la plataforma.

En aquesta modalitat del servei es poden entendre totes les actuacions que vulgarment s'entén com "el dia a dia" i donarà resposta a requeriments propis de l'Àrea de Tecnologia del Consorci AOC..

Dins d'aquesta modalitat del servei també es podran incloure peticions associades a afectacions a la continuïtat de negoci o degradació en el rendiment o funcionament de qualsevol element de la solució que, per qualsevol motiu, no estiguin cobertes pels elements de monitoratge i procediments de manteniment correctiu establerts.

S'entén per **Monitoratge** com la capacitat de recepció de successos davant d'un canvi de comportament, disponibilitat o accessibilitat de tots els elements de la plataforma o dels seus components individuals susceptibles de modificar la capacitat i funcionament del mateix. El licitador haurà d'utilitzar l'eina o solució que el Consorci AOC determini, i de la seva propietat o subscripció, per tal de garantir, la detecció, recepció i tractament dels esdeveniments informatius que es configurin per tal de garantir l'observabilitat global de la infraestructura i serveis associats.

El licitador haurà de garantir en tot moment l'accessibilitat a la solució, segons el model i procediments que siguin acordats, al personal de Consorci AOC i terceres parts que es considerin necessàries, tot implementant les mesures de seguretat i control adients.

Els serveis definits en aquest punt s'hauran d'executar des de la signatura del contracte fins el 31 de Desembre de 2022.

3.4.3 Bossa d'hores per reconfiguracions o ampliacions de les taques de configuració i explotació de nous equips

Al llarg del cicle de vida del contracte es podran produir situacions que requereixin, per necessitats del servei o del negoci de l'AOC, la reconfiguració, ampliació o canvi d'arquitectura de la solució desplegada o elements de la infraestructura relacionats. Aquests canvis i tasques sobrevingudes implicarien també la revisió dels serveis de suport i operació associats. Per tal de contemplar aquestes situacions potencialment factibles, es requereix que el proveïdor ofereixi aquest serveis en la modalitat bossa d'hores.

Les peticions derivades d'aquestes necessitats seran avaluades per les dues parts i un cop acordada la volumetria d'hores es procediria a l'execució de les tasques i la seva posterior facturació. Donades les tasques potencialment necessàries es considera que aquest servei deu contemplar un mínim d'hores amb els mateixos perfils professionals dels que han executat les tasques dels serveis anteriors, Serveis de configuració i posada en marxa i Serveis d'operació i suport. Els requeriments mínims d'aquesta bossa d'hores són:

- Nombre mínim: 40 hores
    - Hores en horari laboral
    - Hores fora d'horari laboral

La bossa d'hores està calculada dins l'horari laboral. El proveïdor podrà proposar una equivalència o permuta entre hores dins horari laboral i fora d'horari laboral però el còmput global en quant al servei i, per tant, a la seva facturació es realitzarà considerant el resultat en hores dins horari laboral dels càlculs finals i la proposta del proveïdor per aquesta permuta.

4. Acords de Nivell de Servei

En aquest apartat es descriu el marc contextual d'aplicació dels Acords de Nivell de Servei per al contracte. Per solucionar aquestes incidències s'estableix el següent procediment de treball i Acord de Nivell de Servei (ANS). Les possibles penalitzacions que es derivin de l'incompliment dels ANS, s'aplicaran sobre descompte en la següent factura emesa després de la penalitat. L'aplicació de penalitats serà acumulativa.

Els Acords de Nivell de Servei es podran revisar i modificar sempre i quan hi hagi acord mutu entre l'adjudicatari i el Consorci AOC.

Requeriments de nivell de servei

Resolució d'incidències sense errors:

- Percentatge de la resolució d'incidències sense errors en el termini.
  - Càlcul: (A/B)*100
    A: Número total d'incidències resoltes sense error en el termini
    B: Total d'incidències resoltes en el termini
- Periodicitat: Diària
- El percentatge d'incidències sense error en el termini establert haurà de ser com a mínim del 90%.
- El nivell ofert per qui resulti adjudicatari del lot constituirà un Acord de Nivell de Servei (ANS), el compliment del qual es mesurarà durant tota la durada de la prestació del servei.

ANS per a la gestió de les incidències

Aquest ANS aplica a la totalitat del servei contractat.

Definicions:

Nivell	Descripció
Bloquejant	Una incidència es catalogarà amb criticitat bloquejant si impedeix la utilització total del servei a tots els usuaris d'aquest.
Alta	Una incidència es catalogarà amb criticitat alta si impedeix la utilització d'una part concreta del servei, a tots o alguns usuaris, i l'afectació pel negoci és elevada.
Mitja	Una incidència es catalogarà amb criticitat mitja si impedeix la utilització d'una funcionalitat concreta d'algun dels serveis a tots o alguns usuaris externs a la plataforma i l'afectació pel negoci és relativament baixa.

Baixa	Una incidència es catalogarà amb criticitat baixa si no impedeix la utilització ni parcial ni total d'algun dels serveis a algun dels usuaris.

El temps de resposta i de resolució s'estableix segons el tipus d'incidència:

- **Temps de resposta**.

  Es defineix com a temps de resposta el temps que transcorre des de que la incidència es comunicada, i l'usuari rep el tiquet de la seva incidència. El temps de resposta es compta sobre l'horari de suport de recepció d'incidències.

- **Temps de resolució**.

  Es defineix el temps de resolució d'una incidència com el nombre d'hores que transcorren des de que l'usuari rep el tiquet de la incidència fins el moment en que la incidència està solucionada. En el càlcul del temps de resolució d'una incidència no es tenen en compte els possibles increments de temps provocats per la intervenció inevitable de tercers en el procés de resolució (per exemple, intervenció d'altres organismes).

El temps màxim permès per la resposta i resolució d'una incidència dependrà del nivell de criticitat de la incidència. En la següent taula es mostren els temps màxims permesos per la resolució d'una incidència en funció del nivell de criticitat:

Criticitat Incidència	Temps de resposta (hores)	Temps de resolució (hores)	% de resolució dins del temps compromès
0 Bloquejant	0,5	2	95 %
1 Alta	1	16	95 %
2 Mitja	1	40	95 %
3 Baixa	1	64	95 %

Pel càlcul del temps de resolució d'una incidència s'exclouran els possibles increments de temps provocats per la intervenció inevitable en el procés de resolució per part de tercers.

En el cas que l'adjudicatari no compleixi l'acord de nivell de servei definit anteriorment almenys en el 95% de les d'incidències amb criticitat 0 i 1 que hagin ocorregut dins el mes se li aplicarà les següents penalitzacions:

Percentatge d'incidències amb criticitat 0 i 1 dins el mes que compleixen l'ANS	Penalització sobre la quota mensual de la factura
Superior al 95%	0%
Entre 95% i 80%	5%

Entre 80% i 70%	10%
Inferior al 70%	15%

Cas que l'adjudicatari no compleixi l'acord de nivell de servei definit anteriorment per almenys el 90% de les d'incidències amb criticitat 2 i 3 que hagin ocorregut al mes se li aplicarà les següents penalitzacions:

Percentatge d'incidències amb criticitat 2 i 3 dins el mes que compleixen l'ANS	Penalització sobre la quota mensual de la factura
Superior al 90%	0%
Entre 90% i 51%	5%
Inferior al 51%	10%

Requeriments de nivell de servei en la protecció de dades

Es considerarà incompliment del contracte la no aplicació de les mesures de seguretat imposades al contractista. A banda de les possibles responsabilitats que es puguin derivar de dit incompliment, i que en funció de la gravetat del mateix pugui comportar la resolució del contracte, es preveu la imposició de penalitats.

Les penalitats a imposar seran per cada incompliment que es produeixi i amb el topall màxim establert a l'article 192 de la Llei 9/2017, de Contractes del Sector Públic:

- Mesures de seguretat de nivell baix: 0,5% del preu d'adjudicació
- Mesures de seguretat de nivell mig: 0,75% del preu d'adjudicació
- Mesures de seguretat de nivell alt : 1% del preu d'adjudicació

5. Equip de treball

L'equip de treball serà el que l'adjudicatari cregui convenient, però com a mínim haurà d'aportar una persona amb el rol principal que estigui de forma estable durant tot i el projecte, i un cap de projecte i/o responsable del servei que gestioni les tasques associades als diferents.

El proveïdor proposarà els perfils del personal que consideri adequats per l'execució i garantia dels serveis professionals requerits i descrits en aquest document. De qualsevol manera, es considera necessària la participació mínima dels següents perfils, rols i la seva dedicació en tasques constructives, de desenvolupament de la infraestructura i operació de la mateixa:

- Networking Engineer. Perfil associat a tasques relatives a la configuració i suport permanent i la revisió de l'estat de les vulnerabilitats i incidències associades a la solució. La dedicació i

el nombre de persones necessàries per aconseguir els objectius acordats serà proposat pel proveïdor en funció dels requeriments del servei.

- On-premise Systems Engineer. Perfil associat a tasques relatives a la configuració i suport permanent i la revisió de l'estat de les vulnerabilitats i incidències associades a la solució. La dedicació i el nombre de persones necessàries per aconseguir els objectius acordats serà proposat pel proveïdor en funció dels requeriments del servei.

L'adjudicatari d'aquesta licitació haurà d'aportar la infraestructura tècnica, llicències, i qualsevol altre component o mitjà tècnic necessari per a la realització dels treballs. Els costos d'aquesta infraestructura tecnològica aniran a càrrec de l'adjudicatari. És important destacar que aquesta infraestructura tecnològica no podrà contenir en cap moment dades reals.

Les tasques s'hauran de dur a terme a les oficines de de l'empresa adjudicatària, tot i que de forma puntual és possible que en alguna ocasió sigui necessari el desplaçament d'algun dels membres de l'equip associat als serveis a les instal·lacions del Consorci AOC o de tercers. Per aquest motiu es recomana que tots els membres de l'equip disposin d'ordinadors portàtils.

Tots els treballs desenvolupats, i en particular els lliurables entregats, hauran de seguir les guies d'estil definides pel Consorci AOC. El Consorci AOC facilitarà a tots els adjudicataris aquestes guies d'estil i el seu compliment haurà de ser obligatori per a l'acceptació dels treballs.

6. Horari del servei

El servei s'executarà en horari laboral, de dilluns a divendres de 9 a 18h, exceptuant el servei de monitoratge i manteniment en cas de incidència que tindran un horari d'execució de 24x7.

En cas d'intervencions que impliquin aturada de servei, aquestes s'hauran de fer en finestres fora de l'horari laboral.

7. Gestió del servei i consum d'hores.

L'adjudicatari haurà de valorar el cost en hores de les tasques que li siguin assignades i el Consorci AOC, aprovarà, denegarà i prioritzarà les tasques en funció del seu cost.

L'adjudicatari haurà d'informar en tot moment del progrés de la tasca i en la seva finalització imputar el cost real en hores de la mateixa.

Les hores imputades es descomptaran de la bossa d'hores de manteniment contractada.

L'adjudicatari i el Consorci AOC faran una revisió mensual de les hores dedicades aprovades realitzades i les pendents.

8. Condicions d'execució dels serveis

8.1 Propietat intel·lectual.

L'adjudicatari accepta expressament que la propietat intel·lectual de tots els lliurables, independentment de la seva naturalesa i resultats dels treballs realitzats, i en particular els productes i serveis objectes del contracte, corresponen únicament al Consorci AOC amb exclusivitat i amb caràcter general, sense que els adjudicataris puguin conservar, ni obtenir còpia dels mateixos o facilitar-lo a tercers.

L'empresa adjudicatària no podran fer cap ús o divulgació dels estudis i documents utilitzats o elaborats com a resultat de la prestació del servei objecte del contracte, bé sigui en forma total o parcial, directament o extractada, original o reproduïda, sense autorització expressa del Consorci AOC, que la donaria, si escau, prèvia petició formal de l'adjudicatari amb expressió de la fi.

8.2 Garantia

Totes les tasques que són objecte del contracte i que formen part de l'abast del projecte tindran una garantia de 6 mesos. Durant aquest període, l'adjudicatari s'haurà de comprometre a resoldre satisfactòriament totes aquelles incidències o defectes detectats en qualsevol de les activitats dutes a terme pels seus equips de treball que li siguin imputables amb ell per acció o omissió.

8.3 Normativa aplicable

L'adjudicatari es compromet a complir els requeriments de seguretat i continuïtat aplicables a l'objecte del contracte especificats a:

- La legislació vigent en general i, en particular, quan es tractin dades de caràcter personal, el Reglament UE 2106/679 del Parlament europeu i del Consell , de 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que respecta al tractament de dades personals. A més de l'establert en el Plec de clàusules administratives particulars per cada evolutiu que impliqui el tractament de dades de caràcter personal caldrà aportar un informe justificatiu de l'anàlisi de l'impacte del mateix sobre les dades afectades i la justificació de les mesures implantades per donar compliment a la normativa vigent.

- L'***Annex Requeriments de seguretat (ENS) pels proveïdors*** basat en les mesures de seguretat de l'Annex II de l'Esquema Nacional de Seguridad.

8.4 Protecció de dades

L'adjudicatari haurà d'aportar un informe justificatiu de les mesures de privacitat des del disseny i per defecte implantades, incloses les mesures de seguretat de nivell alt previstes en l'Esquema Nacional

de Seguretat, per donar compliment a la normativa vigent en matèria de protecció de dades de caràcter personal i per remissió d'aquesta a l'Esquema Nacional de Seguretat.

En tots els lots caldrà complir amb l'establert en el PCAP pel que fa a protecció de dades de caràcter personal i seguretat de la informació.

A més a més, l'adjudicatari haurà de comprometre's en el contracte a mantenir la confidencialitat en el tractament de la informació del client, i a no divulgar o accedir indegudament a la informació sense l'autorització expressa del seu propietari. L'adjudicatari quedarà obligat a no accedir ni utilitzar la informació a la qual tingui accés per a fi algun que no estigui explicitat en el contracte o s'autoritzi expressament per escrit amb posterioritat a la signatura del contracte i a complir l'establert al respecte al PCAP.

El proveïdor haurà de complir amb l'establert en el PCAP i només podrà subcontractar empreses prèvia autorització expressa per escrit del Consorci AOC i que compleixin les obligacions en matèria de protecció de dades i adoptin les mesures de seguretat de nivell alt de l'ENS requerides a l'adjudicatari. Entre aquestes està l'obligació del proveïdor de garantir que les successives subcontractacions que facin els seus contractistes compleixin l'establert al PCAP i les obligacions en matèria de protecció de dades i adopti les mesures de seguretat de nivell alt de l'ENS i comunicar al Consorci AOC les subcontractacions que puguin fer els seus subcontractistes.

8.5 Seguretat del servei

L'adjudicatari es compromet a vetllar per la seguretat dels equips on es trobin instal·lats els programes, bases de dades i informació del Consorci AOC, així com per la seguretat en els canals de comunicació emprats. Per tant, prestarà els seus serveis guardant estrictament les mesures de seguretat necessàries, amb la finalitat d'evitar la pèrdua d'informació, així com danys, pèrdua o deteriorament dels programes i bases de dades utilitzades i que són propietat del Consorci AOC.

L'incompliment d'aquests requeriments relatius a la seguretat i la protecció de dades en general constitueix falta molt greu i motiu suficient per a la resolució unilateral del contracte.

L'adjudicatari, tant els seus propis sistemes d'informació com el seu personal, seran un actiu més del sistema i per tant també estaran obligats a complir les mesures de seguretat organitzatives, operacions i de protecció que marca l'ENS. L'adjudicatari haurà de complir amb les mesures indicades en el l'***Annex Requeriments de seguretat (ENS) pels proveïdors***.

El Consorci AOC auditarà en un termini no superior a 6 mesos, que l'adjudicatari compleix amb els requeriments de l'***Annex Requeriments de seguretat (ENS) pels proveïdors***. L'auditoria es farà mitjançant la entrega d'evidències indicades en l'annex al Consorci AOC per a que aquest determini el grau de compliment.

L'adjudicatari estarà exempt de l'auditoria si aporta una certificació vigent de l'Esquema Nacional de Seguridad de nivell baix o superior, expedit per una empresa certificadora independent i homologada.

En cas d'auditoria externa del sistema, l'adjudicatari haurà de participar en l'auditoria en les tasques que li corresponguin, entregant les evidències que l'auditor reclami i fent les adequacions necessàries que els hi pertoquin.

L'adjudicatari s'ha de comprometre a que els seus subcontractistes ofereixen les garanties equivalents en matèria de seguretat a les que ell mateix assumeixi.

Els tècnics que hagin d'accedir als serveis del Consorci AOC per realitzar qualsevol tasca, hauran d'accedir mitjançant una eina PAM (*Privileged Acces Management*) proporcionada pel Consorci AOC sempre amb usuaris nominals. L'autenticació del servidor es farà amb certificat o si no fos possible amb un multi factor d'autenticació. La informació que entri o surti de la plataforma es farà sempre per canals xifrats.

8.6 Responsabilitats i obligacions

L'adjudicatari haurà d'identificar clarament els rols de les persones involucrades en la prestació del servei (no cal que hi hagi una persona per cada rol). El Consorci AOC també definirà per la seva banda els interlocutors que proposa. Les dues parts hauran de definir als seus relatius interlocutors com a mínim per als següents rols:

- Responsable de la seguretat.
- Persona de contacte per a incidents de seguretat.
- Persona de contacte per a canvis i manteniment de sistemes.
- Persona de contacte per a incidències relatives als indicadors de servei (SLA).
- Persona de contacte per a aspectes contractuals.
- Persona de contacte per a temes jurídics i reguladors, en particular quant a dades de caràcter personal (si n'hi ha el DPD).

9. Devolució del servei.

En cas de finalització del contracte, l'adjudicatari haurà d'entregar tota la documentació, llicències i contrasenyes relacionades amb el projecte.

L'adjudicatari es compromet ha eliminar tota la informació propietat del Consorci AOC.

Barcelona, 12 de Juliol de 2022.

Andreu Martinez de Pablo

Responsable de la Unitat de Sistemes

ANNEX Requeriments de seguretat (ENS) pels proveïdors

ID 1. Política de Seguretat

Es disposa d'una Política de Seguretat que inclou:

1- Objectius de l'organització

2- Marc legal i regulador

3- Rols relacionats amb la seguretat, així com les seves responsabilitats i procediment de designació.

4- Estructura del comitè de gestió i coordinació de seguretat.

5- Criteri per a la classificació de la documentació.

6- Referència a la legislació aplicable en matèria de tractaments de dades de caràcter personal.

7- La Política de Seguretat ha de ser un document en paper o suport electrònic.

8- La Política de Seguretat inclou l'especificació del termini i condicions de la seva revisió i que ha d'estar aprovada per un òrgan superior.

9- La Política de Seguretat inclou un apartat específic de gestió dels usuaris i els seus privilegis, així com la persona responsable.

10- La Política de Seguretat inclou un apartat específic indicant els responsables de la informació gestionada pel sistema.

ID 3. Procediment de revisió de la Política de Seguretat

Document contenint el Procediment de revisió i aprovació de la Política de Seguretat o en el seu defecte, apartat de la Política de Seguretat on s'especifiqui el període de revisió i aprovació.

ID 4. Evidència de la difusió de la Política de Seguretat

Evidència de què la Política de Seguretat és accessible pel personal afectat a la Intranet, pàgina web, portal, repositori o ha estat distribuïda a tots els usuaris dels quals són responsables mitjançant del correu electrònic.

ID 10. Evidència de la difusió de la Normativa de Seguretat

Evidència que la Normativa de Seguretat - ja sigui pròpia o s'empri el Marc Normatiu de l'Agència de Ciberseguretat de Catalunya - està disponible a la Intranet, pàgina web, portal, repositori, llibreria o a qualsevol altre mitjà accessible per a tots els usuaris implicats o bé que els ha estat distribuïda a través del correu electrònic.

ID 11. Procediments de Seguretat

Es disposa de Procediments de Seguretat per a la realització de les tasques rutinàries.

Aquests han d'incloure com a mínim:

1- Com portar a terme les tasques habituals.

2- Qui ha de fer cada tasca.

3- Com identificar i reportar comportaments anòmals.

ID 13. Evidència de la difusió dels Procediments de Seguretat o de la possibilitat d'accés per part dels usuaris.

Evidència de que els Procediments de Seguretat - siguin propis o s'emprin els del Marc Normatiu de l'Agència de Ciberseguretat de Catalunya - estan disponibles a la Intranet, pàgina web, portal, repositori, llibreria o a qualsevol altre mitjà accessible per a tots els usuaris implicats.

ID 40. Document d'Identificació del Control d'Accés al sistema

Es disposa d'un procediment formalitzat de gestió d'usuaris degudament aprovat i actualitzat que s'indiqui:

- Com es realitza la gestió dels usuaris i dels seus privilegis així com la persona responsable de la gestió dels usuaris.

- Que els identificadors dels usuaris han de ser nominals i no es poden compartir.

- El període de retenció dels usuaris.

ID 43. Procediment d'Autenticació del Sistema

Es disposa d'un procediment degudament aprovat i actualitzat on es descriuen els mecanismes d'autenticació dels usuaris o s'especifica dins del procediment formalitzat de gestió d'usuaris els següents punts:

1- Es detalla els sistemes d'autenticació dels usuaris amb l'obligació de tenir almenys un factor d'autenticació.

2- Es detalla i s'obté l'evidència de que l'usuari confirma la recepció de l'identificador, coneix i accepta les obligacions.

3- S'explica com gestionar les baixes d'usuaris i el lligam amb RRHH que permeti avisar als responsables de gestió d'usuaris del canvi en les relacions amb aquests.

4- S'indica que es facin servir almenys dos factors d'autenticació en els sistemes categoritzats com a nivell mig i alt.

5- En el cas que es facin servir tokens, que aquests utilitzen un algoritme autoritzat pel CCN, per exemple AES.

ID 46. Document de Requeriments d'Accés al sistema

Es disposa d'un procediment formalitzat de gestió d'usuaris degudament aprovat i actualitzat que s'indiqui:

- Com es realitza la gestió dels usuaris i dels seus privilegis així com la persona responsable de la gestió dels usuaris.

- Que els identificadors dels usuaris han de ser nominals i no es poden compartir.

- El període de retenció dels usuaris.

ID 50. Eina corporativa específica per a la gestió dels usuaris propis

Es disposa d'una eina corporativa específica per a la gestió dels usuaris.

ID 54. Procediment de Gestió de Drets d'Accés al Sistema

Es disposa d'un procediment o s'inclou dins del procediment formalitzat d'usuaris del sistema els següents punts:

- S'assignarà el rol adequat a cada usuari amb els mínims privilegis possibles i revisant-se els mateixos periòdicament.

- S'inclourà la relació entre els permisos que ha de tenir cada usuari en funció del seu rol.

- S'especificarà quins son els responsables dels recursos dels sistemes (físics i lògics) i qui té la responsabilitat delegada de concedir, alterar o anul·lar l'accés als mateixos.

ID 62 Evidència de què l'usuari confirma la recepció de l'identificador, coneix i accepta les obligacions

Es disposa de l'evidència que demostra que els nous usuaris confirmen la recepció de l'identificador, coneixen i accepten les obligacions. Aquesta evidència pot prendre diverses formes:

1- Evidència de que en crear el seu identificador s'informa l'usuari per correu electrònic, i en accedir per primer cop ha d'acceptar els drets i deures d'accés a l'aplicatiu.

2- Que el personal d'un proveïdor signi un document d'obligacions el primer dia, així com un acord de confidencialitat i queda constància del lliurament de l'identificador.

3- Que en la part inferior de la pantalla d'accés s'indiquin els termes i condicions, pel que els usuaris estan implícitament acceptant-les per accedir al sistema.

ID 63. Acord de confidencialitat on es fa constar el lliurament de l'identificador

Es disposa del document contenint l'Acord de Confidencialitat signat per l'usuari fent constar la recepció del seu identificador. Ha d'existir un registre de cada usuari confirmant la recepció de l'identificador.

ID 64. Evidència de l'últim usuari propi donat de baixa

Es disposa de l'evidència mostrant la baixa d'un usuari amb la data efectiva de la baixa.

ID 67. Procediment d'Accés en Local

Es disposa d'un Procediment d'Accés en Local què especifiqui que:

1- Els sistemes abans d'entrar en explotació o els ja existents han estat configurats de forma que no revelin informació del sistema abans d'un accés autoritzat.

2- Els diàlegs d'accés (al lloc de treball, dins les pròpies instal·lacions de l'organització, al servidor, al domini de xarxa, etc.) no revelin informació sobre el sistema al qual s'està accedint.

3- Faci constar que s'ha d'informar sempre els usuaris de les seves obligacions un cop han accedit dins el sistema.

4- S'ha d'informar a l'usuari del seu darrer accés al sistema.

5- Defineixi uns horaris en què és possible la connexió al sistema i altres en què no ho és.

6- No es pot accedir al sistema fora de les hores autoritzades.

7- Indiqui punts de renovació d'autenticació durant la sessió d'un usuari.

ID 107. Evidència què es disposa d'antivirus als sistemes d'informació

Es disposa de l'evidència de l'ús de mecanismes de prevenció davant de codi perjudicial (antivirus) per a tots els equips (Servidors i llocs de treball) del sistema i també en les maquetes, així com de la seva configuració.

ID 111. Evidència de què el programa antivirus es troba actualitzat

Es disposa de l'evidència que les opcions de configuració aplicades als antivirus són les recomanades pels fabricants (p.ex. Anàlisi d'execució de programes, anàlisi de correu entrant i sortint, bloqueig automàtic de codi nociu, etc.), així com les referents a la freqüència d'actualització.

ID 172. Evidències de la difusió del contingut del Pla de Conscienciació

Es disposa d'evidència de la difusió del contingut del pla de conscienciació (en la intranet o per algun altre mitjà es llancen missatges de conscienciació (p.ex. correus, comunicats interns,…)).

ID 174. Evidències de la difusió del contingut del Pla de Formació

Es disposa d'evidència amb la difusió del contingut del pla de formació en els darrers 3 anys.

ID 241. Document on s'indica el mecanisme d'autenticació i identificació

Es disposa d'una política o normativa documentada respecte al disseny d'un sistema que contempli els mecanismes d'identificació i autenticació i a més contempla els mecanismes de protecció de la informació tractada.

Així mateix no ha de ser possible accedir a informació del sistema que pugui ser utilitzada per a l'escalada de privilegis, ni executar accions fent-se passar per un altre usuari, etc.

ID 244. Procediment per a l'elaboració i execució del pla de proves de l'aplicació

Es disposa d'un procediment d'Acceptació i Posada en Servei de Protecció de les Aplicacions Informàtiques. Abans de passar a producció s'ha de comprovar el funcionament correcte de l'aplicació. S'ha de comprovar que:

1- Es compleixen els criteris d'acceptació en matèria de seguretat.

2- No es deteriora la seguretat d'altres components del servei.

3- Les proves s'han de fer en un entorn aïllat (preproducció).

4- Les proves d'acceptació no s'han de fer amb dades reals, llevat que s'asseguri el nivell de seguretat corresponent.

5- Es realitzen anàlisis de vulnerabilitats.

6- Es realitzen anàlisis de coherència i codi font.

ID 273. Procediment de configuració segura del correu.

Es disposa d'un procediment el qual es detalla com es configura el correu per tal de disposar d'un sistema segur.

ID 276. Evidència de l'eina monitoratge dels elements de seguretat

Es disposa de l'evidència en la qual s'observa que es disposa d'una eina per monitoritzar els elements de seguretat com ara els virus o l'spam degudament configurat i mantingut.

ID 330. Normativa documentada que especifica els deures i obligacions del personal contractat a través d'un tercer.

Es disposa de normativa on s'especifiquen els deures i obligacions del personal contractat a través d'un tercer.

ID 460. Protocol d'actuació envers l'incompliment de les obligacions per part del personal tercer

Es disposa d'un procediment que defineix la resolució d'incidents relacionats amb l'incompliment de les obligacions per part del personal del tercer, a més d'identificar a la persona de contacte amb el tercer per a la resolució d'aquest tipus d'incidents.