B:SM Barcelona de Serveis Municipals

Ajuntament de Barcelona

PLEC DE PRESCRIPCIONS TÈCNIQUES

SERVEIS DE CONTINGÈNCIA I DISASTER RECOVERY CLOUD EN ENTORNS CRÍTICS PER A BARCELONA DE SERVEIS MUNICIPALS S.A.

Sinopsi: El present document defineix els requisits i característiques tècniques pels serveis de contingència i disaster recovery cloud en entorns crítics per a Barcelona de Serveis Municipals S.A. (BSM).

En línia amb el compromís de salvaguardar les dades dels usuaris i empreses terceres amb els que interactuen en el seu model empresarial actual, BSM dins de les polítiques internes desenvolupades a la millora continuada de l'estat de ciberseguretat, seguretat, disponibilitat i contingència s'ha plantejat la contractació de serveis en cloud per minimitzar els riscos que puguin derivar de les incidències i deficiències dels sistemes, manca de disponibilitat i possibilitar una resposta àgil per a realitzar evolucions sobre els sistemes i aplicacions actuals.

En definitiva, amb aquests serveis es vol millorar la seguretat, disponibilitat i contingència dels diferents sistemes i aplicacions de BSM consolidant un marc de treball en el qual es coordinin les mesures necessàries per prevenir i augmentar la resiliència envers riscos tals com ciberamenaces, fallades en comunicacions, incidents, accidents, o desastres.

Realitzat: 15/09/2023

1 Introducció

1.1 Objecte del contracte

Aquest document constitueix el plec de requeriments tècnics que ha de regir el contracte dels serveis de contingència i disaster recovery cloud (DR) en entorns crítics de Barcelona de Serveis Municipals S.A. (BSM).

BSM es una empresa de l'Ajuntament de Barcelona que, en virtut del seu objecte social, te encarregades la gestió de diferents equipaments i instal·lacions municipals.

La contractació d'aquests serveis és necessària per poder disposar en la Divisió Corporativa de Tecnologies de la Informació, Comunicacions i Estratègia Digital de BSM dels mecanismes per satisfer les necessitats actuals i futures, i en aquest sentit es imprescindible cobrir els subministraments de serveis corporatius de contingència, disaster recovery i seguretat en la organització. Ja que BSM desenvolupa la seva activitat en un entorn altament regulat que, juntament amb els riscos intrínsecs a la seva activitat i aquells exògens a la mateixa, fan que resulti imprescindible disposar d'una estratègia de seguretat, ciberseguretat, contingència, disaster recovery, protecció de dades i privacitat.

En línia amb el compromís de salvaguardar les dades dels usuaris i empreses terceres amb els que interactuen en el seu model empresarial actual, BSM dins de les polítiques internes desenvolupades a la millora continuada de l'estat de ciberseguretat, seguretat, disponibilitat i contingència s'ha plantejat la contractació de serveis en cloud per minimitzar els riscos que puguin derivar de les incidències i deficiències dels sistemes, i possibilitar una resposta àgil per a realitzar evolucions sobre els sistemes i aplicacions actuals.

Degut la digitalització de serveis i amb la incorporació de nous serveis cada vegada mes crítics en els darrers anys, amb mes impacte especial per als ciutadans, clients, proveïdors i empleats de BSM, cada vegada s'ha anat incrementant les exigències i necessitats de disponibilitat d'aquests serveis mes crítics de BSM. Es requereix d'una contingència de serveis amb un bon temps de recuperació i posada en contingència en entorn ja redundat i securitzat, que no depengui de la infraestructura pròpia de BSM i sigui fàcilment mantenible amb els anys.

En definitiva, amb aquests serveis es vol millorar la seguretat, disponibilitat i contingència dels diferents sistemes i aplicacions de BSM consolidant un marc de treball en el qual es coordinin les mesures necessàries per prevenir i augmentar la resiliència envers riscos tals com ciberamenaces, fallades en comunicacions, incidents, accidents, o desastres.

1.2 Situació actual

Actualment, BSM disposa i te en funcionament una plataforma de sistemes corporatius amb serveis molt crítics en el centres de procés de dades en Tecnocampus de Mataró i oficines centrals del carrer Calabria, que donen servei a diferents sistemes i aplicacions per a empleats, clients, proveïdors, visitants i ciutadans de Barcelona, on es planteja la necessitat de minimitzar

els riscos que puguin derivar de les deficiències i incidències dels sistemes actuals i possibilitar una resposta àgil per a realitzar evolucions sobre els sistemes i proveir a l'organització de serveis, sistemes i eines d'alta qualitat, i mes segurs.

Degut la digitalització i amb la incorporació de nous serveis cada vegada mes crítics en els darrers anys, amb mes impacte especial per als ciutadans, visitants, clients, proveïdors i empleats de BSM, cada vegada s'han anat incrementant les exigències i necessitats de disponibilitat d'aquests serveis mes crítics en BSM, i es per tot això que és requereix d'una contingència de serveis amb un bon temps de recuperació i amb la posada en marxa d'un entorn ja redundat i securitzat, que no depengui de la infraestructura pròpia de BSM i sigui de fàcil d'aprovisionar i mantenir amb els anys.

La recuperació davant de desastres com a servei en Cloud (DRaaS) és un model de servei de computació al núvol que permet a una organització recolzar les seves dades i infraestructura de TI en un entorn de computació al núvol d'un tercer i proporcionar tota l'orquestració de recuperació davant desastres, tot a través d'una solució en Cloud, per recuperar l'accés i la funcionalitat a la infraestructura de TI en Cloud després d'un desastre. El model com a servei significa que l'organització en si mateixa no ha de tenir tots els recursos o manejar tota l'administració per a la recuperació davant de desastres, sinó que depèn del proveïdor del servei.

La planificació de la recuperació davant de desastres és fonamental per a la continuïtat del negoci de BSM, ja que molts tipus de desastres que tenen el potencial de causar estralls en una organització de TI s'han tornat més freqüents en els darrers anys:

- ✓ Desastres naturals com huracans, inundacions, incendis forestals i terratrèmols.
- ✓ Falles d'equips i talls d'energia.
- ✓ Atacs cibernètics.

Disaster Recovery en Cloud (DR) funciona mitjançant la replicació i l'allotjament de servidors a les instal·lacions d'un proveïdor extern en lloc de la ubicació física de l'organització propietària de la càrrega de treball. El pla de recuperació davant de desastres per a BSM s'haurà de executar a les instal·lacions del proveïdor extern en cloud, en cas d'un desastre que tanqui el lloc d'un client.

Les organitzacions poden comprar plans de contingència en Cloud mitjançant un model de subscripció tradicional o un model de pagament per ús que els permet pagar només quan passa un desastre. Identifiquem els serveis crítics de negoci actuals que seran candidats a la replicació i allotjament en un entorn Disaster Recovery (DR) en Cloud, i ubicats en origen en els CPD's de Tecnocampus de Mataró i Oficines Calabria en BSM. La següent taula es una aproximació a les necessitats de servidors virtuals que podran ser necessaris, en tot cas haurà de servir de referencia aproximada inicialment:

Servei	VM
SMOU	12
SPRO	6

SGD (Dipòsit de Grues)	5
WSO2 (Gestió apis)	10
Serveis Centrals IIS (SMOU)	3
Serveis Centrals IIS (Àrea)	3
ADFS (Autentificació de usuaris)	2
DC (Gestió d'usuaris/equips de BSM)	1
NetScaler (Balancejador de serveis)	2
GIVI-Dispatching	3
Euromus (Gestió compra entrades)	1
WEB Park Güell / Zoo / Tibidabo	4
Venda Online Park Güell / Zoo / Tibidabo	4
Control Accés Park Güell	1
Control d'Accés Anella	2
Altres	3
Total	**62 VM**

Com a referencia, també identifiquem els següents serveis no tant crítics, que en un futur es podria plantejar la necessitat de tenir una contingència, però sense estar previst la seva inclusió en la plataforma de Disaster Recovery (DR) inicialment en aquesta adjudicació o amb recursos lliures:

Servei	**VM**
SmartKiosks Restauració	1
Codyshop Restauració	2
Altres Webs (15)	15
Denúncies Àrea	1
Lince / Lince Cloud / Synapse	5
Plataforma RDS	13
Total	**37 VM**

1.3 Prestacions Objecte del Contracte

Els serveis a prestar per l'adjudicatari són:

- ✓ Totes les càrregues de treball virtuals necessàries, sense dependències dels entorns físics.
- ✓ Estimacions realitzades en base a escenari de DR de 62 VM i 250vCPU,
- ✓ Estimació de recursos sobre la base de la infraestructura VMware existents a Tecnocampus, on es disposa actualment de 7 Hosts ESXi, 164 Cores, i 3,5 TB RAM.
- ✓ S'estimen host de la mida i4 a AWS. Cada host disposa de 36Cores, 512GB RAM, i 10,37TiB RAW.
- ✓ 6 Host : 216 Cors, 3TB RAM i 62,22TiB (68TB) emmagatzematge NVME RAW
- ✓ 8 Host: 288 Cors, 4TB RAM, i 82,96 TiB (92,2TB) d'emmagatzematge NVME RAW.
- ✓ RTO màxim de 4h
- ✓ S'estima la següent política de protecció, amb una ocupació de 40TiB a l'scale out file System proporcionat sobre AWS.

En la següent taula es mostra el RTO i RPO dels entorns a protegir, així com els detalls de cadascun dels escenaris. L'adjudicatari haurà de complir necessàriament amb aquestes especificacions:

Solució	RTO (Hores)	RPO (Hores)	Notes
Entorn virtual	4	4	Desplegament SDDC i automatitzacions en base a la política de retenció proposada.
Servidors SQL	2	0	Còpia quasi síncrona.
Palo Alto + versionat S3	1	24	1 Versió diària de la configuració.
NetScaler + versionat S3	1	24	1 Versió diària de la configuració.

Estimacions i assumpcions entorn virtual:

- ✓ L'estimació del cost del servei VCDR es realitza a partir de les dades obtingudes del top 62 de màquines virtuals existents a TCM, excloent-ne el resource pool de Test.
  Els recursos obtinguts són els següents:

VM	vCPU Totals	Memòria Total (GB)	Emmagatzematge Aprovisionat (TiB)	Emmagatzematge en Ús (TiB)
62	**250**	**1.709,57**	**40**	**30,94**

- ✓ Es considera la següent política de protecció i retenció de punts de restauració al servei VCDR, permetent diversos punts de restauració.

La politica de protecció i retenció de punts de restauració en el servei VCDR que s'haurà de complir es presenta en la següent taula:

Snapshot	Franja	Retenció	Rati canvis
Cada 4 hores	12 AM – 4AM – 8AM...	2 dies	0,5 %
Diàries	12 AM	7 dies	1,0 %
Setmanals	Diumenge	4 setmanes	2,5 %

- ✓ D'acord amb les estimacions anteriors i tenint en compte la política de retenció aplicada, s'estimen els recursos necessaris d'emmagatzematge i còmput següents a AWS.

Talla Calculada	
Capacitat Protegida	40 TiB
VMs Protegides	580.000 VM-hores/Any (62 VMs)
DR Test Hosts	336xi4i Host-hores/Any (4xi4i hosts)

Es consideren necessaris els següents recursos en el clúster SQL, objecte de DR de serveis crítics:

Ubicació	Entorn	Clúster	Servers	Instancia	vCPUs	RAM (GB)	Disc (GB)	Notes
TCM	PRO	Clúster TCMS SQLSERVER 2016	CLSQL2K16TCMN1	PROCORE	24	256	2Tb Dades 200Gb Temp 300Gb Tlog	Unitats de Dades, Temporals i Translog
TCM	PRO	Clúster TCMS SQLSERVER 2016	CLSQL2K16TCMN2	PROINTERNA	24	256	300Gb Dades 200Gb Temp 200Gb Tlog	Unitats de Dades, Temporals i Translog

Item	Total Emmagatzematge (GB)
Clúster SQLServer TCM	3.248

Estimacions i assumpcions NetScaler/Palo Alto:

- ✓ A les instàncies virtuals NetScaler, es considera que l'adjudicatari proporcionarà les llicències necessàries per poder realitzar un DR.

- ✓ A nivell NetScaler/Palo Alto es consideren els següents equips per realitzar el DR d'origen:

Sistemes	Unitats
Clúster Firewalls Palo Alto PA-3220	2
Clúster ADCs NetScaler VPX-1000	2

1.4 Marc Temporal del Contracte

El termini del contracte s'estableix en un total de (1) any i 2 mesos des de la signatura del contracte, amb TRES prorrogues d'UN (1) any.
BSM es reserva el dret de poder cancel·lar el contracte, i per tant no existiria cap compromís per continuar amb la contractació del serveis de contingència o disaster recovery amb l'adjudicatari, en el cas que es consideri que no s'ha superat satisfactòriament les dues proves de concepte(PoC) plantejades en la fase inicial del projecte.

El termini de lliurament dels serveis de la PoC serà de com a màxim de 1 mes natural des de la signatura del contracte, mes 1 mes addicional per la realització de les validacions, comprovacions i proves necessàries per part de BSM.

2 Condicions d'execució

A continuació s'estableixen les condicions generals d'execució que regiran aquest contracte i que l'adjudicatari estarà obligat a complir durant la seva consecució.

2.1 Prova de concepte (PoC) en fase inicial

En aquest contracte es requereix la realització de una prova de concepte (PoC) de com a mínim dos serveis crítics. Amb aquesta prova de concepte es vol validar el correcte funcionament de la plataforma de Disaster Recovery i del servei de contingència. Aquesta prova de concepte s'haurà d'implantar i de posar a disposició de BSM com a màxim en 1 mes i haurà de estar a disposició per a fer les proves durant un mínim de 1 mes addicional, en el qual es realitzaran les proves i comprovacions necessàries per tal de validar els entorns.

Un dels serveis de la prova de concepte haurà d'accedir a dades de base de dades SQLServer proporcionats en el mateix entorn VCDR o està ubicats del servidors d'aplicació, i per tant l'adjudicatari haurà de proporcionar també l'entorn o servei SQLServer en la PoC, i l'altra prova de concepte haurà d'accedir a dades Oracle que es trobaran ubicats en l'actual entorn Cloud Oracle que proporcionarà BSM.

Es planteja una primera fase de pilot inicial on es contempla el DR dels entorns següents:

- Servei GIVI-DISPATXING de les Grues: (No hi ha balancejador Citrix Netscaler en aquest servei)
  - ✓ BD SQLServer (3 Bd's de la mateixa aplicació però per a diferents serveis de l'aplicació).

    2 Gb BD CALLEJERO

    105Gb BD DISPATXING

    100Gb BD GRUES
  - ✓ Es faran les proves des d'un dispositiu intern de BSM, sense publicació a internet.
  - ✓ 3 Servidors (2 Windows Server y 1 Server Redhat):

    VMWEBAPPS04 (4vCPU's, 8GB RAM, 70GB HDD)

    VMGRUCENTRAL (4vCPU's, 10GB RAM, 45GB+30GB HDD)

    VMINFORMMOBPRO (2vCPU's, 8GB RAM, 75GB HDD)

- Servei SPRO per a aparcament professional a les zones de càrrega i descàrrega:
  - ✓ BD Oracle (1 Bd's) de 90Gb de dades a la BD. Aquesta base de dades es externa en el Cloud Oracle i per tant no ocuparà espai a Amazon. L'adjudicatari haurà de configurar les connexions necessàries per arribar a aquesta BD.
  - ✓ 4 servidors Linux Redhat.

    VMSPROPRO01-04 => 6vCPU, 12GB RAM, 50 GB HDD

(Tots 4 d'iguals característiques)

- ✓ Citrix Netscaler
- ✓ Certificat SSL públic
- ✓ IP Publica d'accés
- ✓ Es faran les proves des d'una APK de proves amb un telèfon Android o Iphone.

L'entorn desplegat a AWS durant el pilot sí que es podrà portar i aprofitar a producció, i s'haurà de contemplar una durada màxima per al desplegament de 1 mes dels dos entorns o sistemes contemplats en la prova de concepte. S'haurà de contemplar durant la prova de concepte (PoC) un mínim de 1 mes de test en període de DR per realitzar les proves necessàries de validació del funcionament del serveis crítics en Disaster Recovery per BSM.

2.1.1 Condicions de validació de la Prova de concepte (PoC) referents als dos serveis DR en Cloud

La computació al núvol és un model de prestació i consum de serveis que ofereix molts avantatges a les empreses (alta disponibilitat, elasticitat, màxim aprofitament de recursos, ect.) que s'han de traduir en requisits de qualitat que han de ser complerts per la valoració dels serveis.

Per la correcta valoració dels serveis per part de BSM, l'adjudicatari haurà de garantir temps de latència dels serveis suficients per la correcta experiència d'usuari, i els temps de RTO/RPO per sota dels mínims requerits en aquesta licitació. L'organització BSM, representada en les persones designades a tal efecte per la mateixa, serà exclusivament qui haurà de validar, acceptar, i donar el vist i plau als resultats de les proves realitzades, i sempre tindrà la ultima paraula en la consideració dels resultats de les proves de concepte com a satisfactoris o no satisfactoris.

BSM prepararà amb antelació una bateria de proves per a cadascun dels dos serveis en cloud, recollint el resultats respecte al atributs proposats i realitzant comparació amb l'entorn on premise actual, i prenent com a guia de validació les mètriques i valors definides en el quadre de sota.

Es realitzarà una prova real per cadascun dels dos serveis, es mesuraran els temps de passi a DR des del moment en què es decideix per a cadascun d'aquest serveis productius passar el servei a DR en AWS. Aquest temps ha de ser igual o menor al SLA requerit al plec, de 4h. Si se sobrepassa aquest temps en un 10% en algun dels dos serveis es donarà per invalida la prova de contingència.

També es realitzarà una validació del servei per part de BSM a nivell funcional i de rendiment. Pel que fa a la validació funcional, el sistema en l'entorn DR haurà de superar el 100% de les proves funcionals definides, es a dir, els sistema en DR s'haurà de comportat de manera exactament igual al sistema productiu, des d'un punt de vista funcional. Pel que fa al rendiment, els temps de resposta al servei cloud han de superar com a màxim en un 25% els temps de resposta del servei on-premise. La latència mitjana del servei cloud haurà de estar per sota de 40 mil.lisegons.

En la següent taula es mostra el RTO i RPO dels entorns de la prova de concepte. L'adjudicatari haurà de complir necessàriament amb aquestes especificacions:

Solució	RTO (Hores)	RPO (Hores)	Notes
Entorn virtual dels dos serveis PoC	4	4	Desplegament SDDC i automatitzacions en base a la política de retenció proposada.
Servidors SQL i BBDD PoC	2	0	Còpia quasi síncrona.
Palo Alto + versionat S3	1	24	1 Versió diària de la configuració.
NetScaler + versionat S3	1	24	1 Versió diària de la configuració.

La valoració dels dos serveis PoC es realitzaran amb les següents mètriques:

Atribut	Significat	Mètrica	Valoració
Temps per passar els serveis a DR en AWS	Es mesuraran els temps de passi a DR des del moment en què es decideix per a cadascun d'aquest serveis productius passar el servei a DR en AWS	RTO (Recovery Time Objective) - Determina la quantitat màxima de temps tolerable necessari perquè el servei torni a estar en línia	RTO < 4h
Latència del servei cloud	Representa el temps necessari perquè la sol·licitud d'un usuari pugui ser manejada pel servei competent.	Temps d'anada i tornada (RTT) en mil.lisegons	Latència mitjana < 40ms
Temps de resposta del servei cloud	Representa la diferència entre el temps de sol·licitud de servei i el temps quan el servei està disponible.	Temps mitjà de resposta	Com a màxim <25% respecte al servei on premise
Qualitat percebuda del Servei Cloud	Representa la puntuació de l'usuari pel que fa a la qualitat percebuda	Escala ordinal ACR-9 de la puntuació d'opinió mitjana (MOS, Mean Opinion Score)	Com a màxim <25% respecte al servei on premise

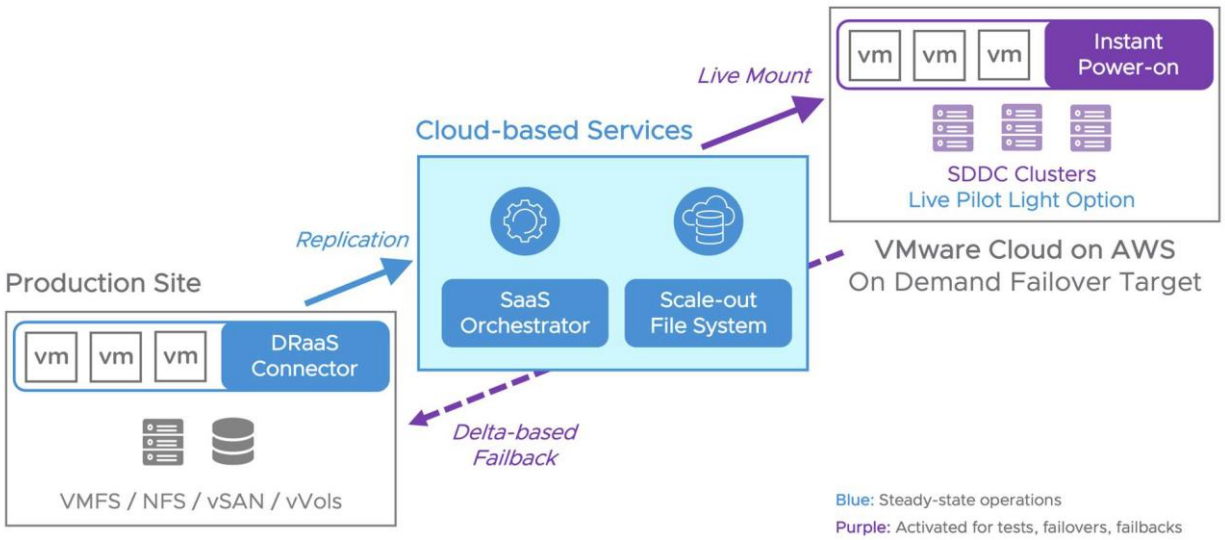
Si després d'aquest període de validacions el resultat del mateix no fora satisfactori, BSM es reserva el dret de poder cancel·lar el contracte de forma unilateral, i per tant no existiria cap compromís per continuar amb la contractació del serveis de contingència o disaster recovery amb l'adjudicatari.

2.2 Serveis

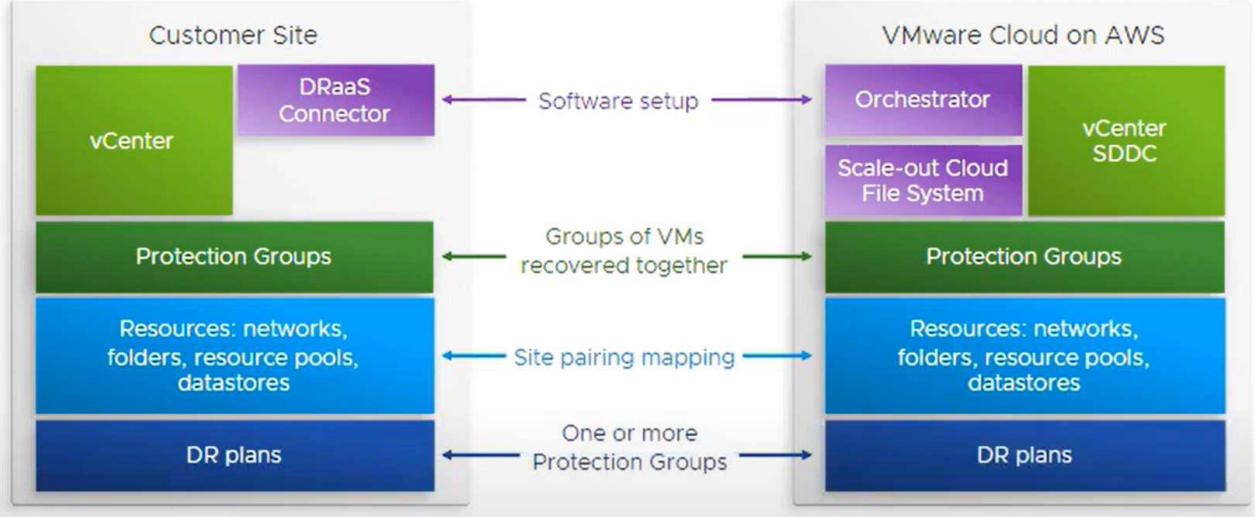
Els serveis recurrents que s'hauran proveir per par de l'empresa adjudicatària son:

- ✓ VMware Cloud Disaster Recovery és un servei de recuperació de desastres baix demanda de VMware que s'ofereix com una solució SaaS fàcil d'usar i que permet la recuperació en el cas d'un desastre.
- ✓ Revisió de capacitats i pro activitat per pre avisar en la manca de capacitat.
- ✓ Servei SaaS, sobre AWS. Es disposa d'un panell de control i orquestració juntament amb un file System on s'emmagatzemen les còpies de les VM protegides.
- ✓ Permetre l'encesa instantània de les VM sense necessitat de rehidratació de la dada, a infraestructura VMware sobre AWS.
- ✓ Comprovació automàticament de l'estat de recuperació cada 30 minuts.
- ✓ Escenaris disponibles per a Site DR sobre AWS:
  - ✓ On-Demand : RTO :120 Aprox, més temps necessari per finalitzar configuració.
  - ✓ Pilot Light: Infraestructura mínima disponible de forma permanent

L'adjudicatari haurà de proporcionar la següent arquitectura:

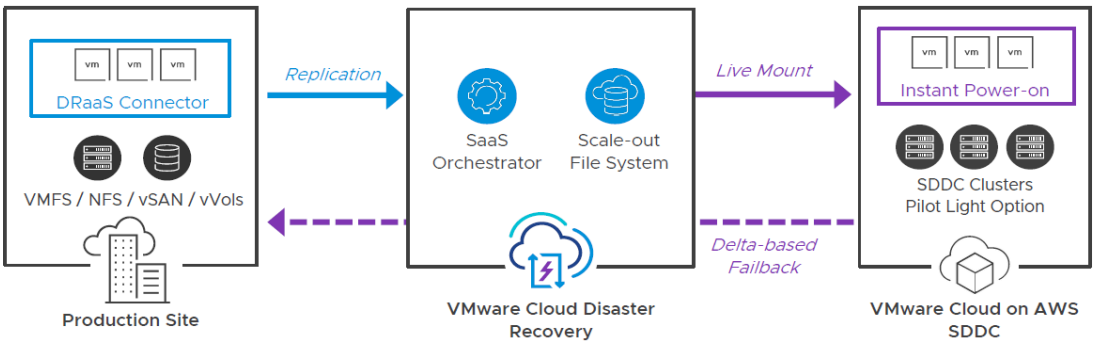


Relacions entre elements on-premise i Vmware Cloud on AWS i VCDR:

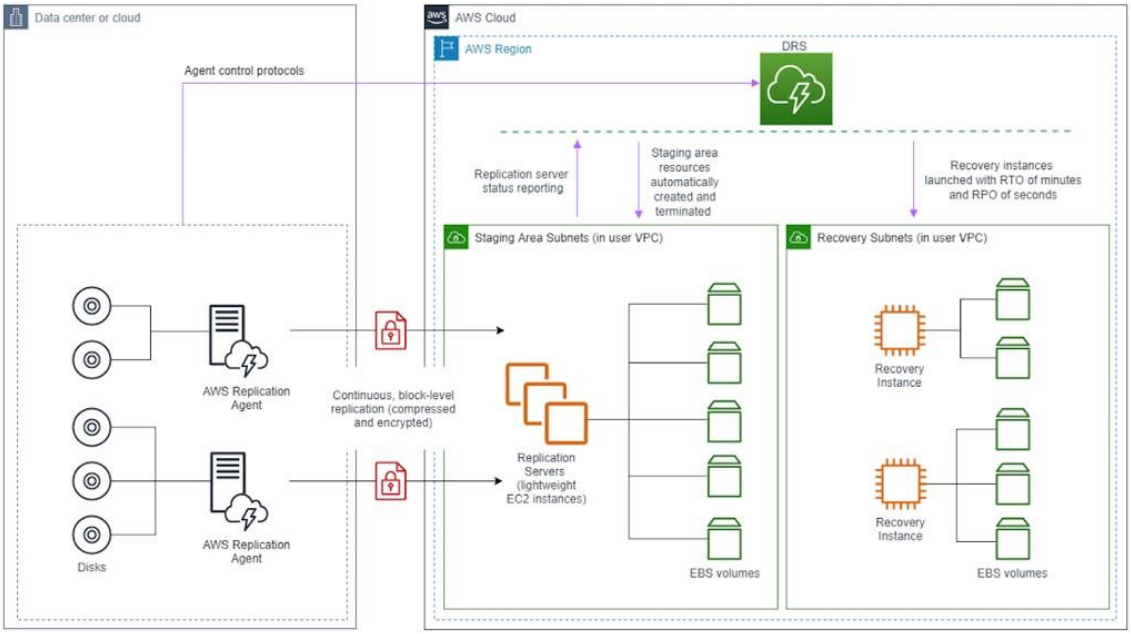


A continuació es detallen les característiques clau que ha de tenir el servei VCDR:

Solució requerida Vmware amb VCDR:



Solució requerida SQL amb AWS Elastic Disaster Recovery:



En resum la solució global requerida haurà de complir amb els següents requisits:

- ✓ Amazon Direct Connect per estendre línia de nivell 2 a AWS (1VPC).
- ✓ Es configurarà NSX per estendre la xarxa a nivell 2 entre l'entorn VMware i l'entorn VMware Cloud on AWS.
- ✓ Direct Connect AWS 1Gb. No s'hi inclou interconnexió física amb AWS (operació entre BSM i el seu operador de comunicacions). Aquesta connectivitat la proporcionarà BSM amb el seu proveïdor de comunicacions. Una vegada BSM proporcioni aquesta línia de comunicacions l'adjudicatari proporcionarà tot el material, elements i treballs necessaris per completar la connexió i per tal de complir.
- ✓ VMware Cloud Disaster Recovery en modalitat servei SaaS, com a solució de replicació de l'entorn VMware. L'adjudicatari haurà de contemplar un escenari de SDDC (Centre de Dades Definit per Software), en modalitat "On Demand" amb RTO de 4 hores per al desplegament del SDDC més el temps de les automatitzacions.
- ✓ En la automatització s'haurà d'utilitzar com a eina Terraform, per la automatització de la configuració del SDDC, una vegada desplegat.
- ✓ Instàncies Amazon EC per a balancejadors Netscaler i firewall Palo Alto.
    - ✓ Dimensionament 1 a 1 per a equips amb DR.
    - ✓ Repositori de configuració contra bucket S3 i amb versionat diari.

- ✓ Per als entorns SQLServer s'haurà d'utilitzar el servei AWS Elastic Disaster Recovery.

- ✓ AWS EDR haurà de realitzar la replicació a nivell de bloc, a través d'un agent instal·lat a cada màquina de origen protegida. L'agent s'haurà de executar en memòria i reconèixer les operacions d'escriptura dels discos connectats localment. Les escriptures capturades es replicaran de forma asíncrona en una àrea de preparació dins del compte d'AWS, mantenint l'ordre d'escriptura entre tots els discos del mateix servidor d'origen.

- ✓ AWS Elastic Disaster Recovery utilitza snapshots d'Amazon Elastic Block Store (EBS) per prendre snapshots puntuals de les dades replicades a l'àrea de preparació. D'aquesta manera, proporcionarà opcions de recuperació puntuals que s'utilitzaran en cas de desastre o simulacre de DR.

- ✓ En cas que es produeixi un esdeveniment o simulacre de DR. s'executaran de forma nativa dins de Amazon Elastic Compute Cloud (EC2), amb el següent sizing mínim estimat de les instàncies, en base als recursos indicats per BSM:

Element	Comentaris
Instancia EC2 CLSQL2K16TCMN1	1 Instancia EC2 (r6i.8xlarge). Aquesta instancia amb 32vCPU, 256GB RAM, 2.500Gb de disc.
Instancia EC2 CLSQL2K16TCMN2	1 Instancia EC2 (r6i.8xlarge). Aquesta instancia amb 32vCPU, 256GB RAM, 2.700Gb de disc.

- ✓ Per als entorns Tallafocs Palo Alto i Citrix ADC Netscaler l'adjudicatari haurà de proporcionar les instancies AWS amb el llicenciament necessari inclòs, i amb el següent dimensionament mínim estimat:

Instancia	Throughput Mínim
Palo Alto VM-Series Virtual NextGen Firewall w/ Threat Prevention – Bundle1 AWS Instancia EC2: m5.2xlarge:8vCPU, 32GB.	10Gbps
Citrix ADC VPX Enterprise Edition-3Gbps Instancia EC2: m5.xlarge:4vCPU, 16GB.	3Gbps

- ✓ Per a l'entorn de connexió a internet de les instancies AWS l'adjudicatari haurà de proporciona com a mínim 200Mbps d'amplada de banda, amb un 20% d'ocupació mitjana, les 24x7 hores x dia, i amb una estimació de 3TBytes de dades.

RTO/RPO de la solució requerida:

En la següent taula es mostra el RTO i RPO dels entorns a protegir, així com els detalls de cadascun dels escenaris. L'adjudicatari haurà de complir necessàriament amb aquestes especificacions:

Solució	RTO (Hores)	RPO (Hores)	Notes
Entorn virtual	4	4	Desplegament SDDC i automatitzacions en base a la política de retenció indicada.
Servidors SQL	2	~0	Còpia quasi síncrona.
Palo Alto + versionat S3	1	24	1 Versió diària de la configuració.
NetScaler + versionat S3	1	24	1 Versió diària de la configuració.

Serveis professionals requerits:

La proposta presentada per l'adjudicatari, es basarà en una implementació de tipus "claus en mà" amb el següent abast:

- Consultoria prèvia de l'entorn per al disseny definitiu de l'arquitectura.
- Implementació de l'entorn de DR per a l'entorn virtual, SQLServer / Oracle / NetScaler / Palo Alto.
- Automatitzacions als entorns de DR protegits.
- Proves pilot de DR.
- Documentació de l'entorn.
- Sessió de traspàs de coneixements a l'equip tècnic de BSM.

Servei Gestionat d'administració/monitorització de l'entorn de Disaster Recovery (DR):

- Desplegament del sistema de monitorització.
- Checklist amb caràcter diari.
- Health check de la plataforma amb periodicitat de 6 mesos.
- Proves de DR parcials.

- Configuració de l'entorn de DR sobre la base de canvis produïts a l'entorn productiu.
- Elaboració d'informes mensuals sobre l'entorn i el servei gestionat.

2.3 Condicions de servei

La gestió dels serveis s'haurà d'adequar als processos establerts per BSM, vigents en el moment de l'execució del servei.

Estimacions del servei sobre la base dels recursos necessaris per cobrir l'escenari de 62 VM, 250vCPU, 3,5TB RAM i 40TB d'emmagatzematge.

Estimació de serveis addicionals AWS per a DR.

L'abast de les tasques dels serveis professionals proposats és la següent:

Anàlisi de serveis crítics:

- ✓ Anàlisi i identificació de càrregues de treball que componen els serveis crítics, recursos necessaris, interaccions i entesa dels processos.
- ✓ Anàlisi i identificació de requeriments de connectivitat, networking i serveis associats com ara balancejos de càrrega, regles de firewall, autenticació, per a cada un dels serveis
- ✓ Identificació de RPO i RTO per a cadascun dels serveis. Definició de grups de protecció i polítiques de protecció associades.
- ✓ Anàlisi i identificació de configuració necessària a automatitzar en entorn SDDC sobre AWS.
- ✓ Documentació de solució i processos.

Implementació solució

- ✓ Desplegament i implementació de solució Vmware Cloud Disaster Recovery.
- ✓ Configuració grups de protecció i polítiques de VM's en base als requeriments definits durant la fase d'anàlisi. Seguiment estat protecció.
- ✓ Disseny, i preparació de workflows per a automatització de tasques en desplegament SDDC.
- ✓ Proves d'aprovisionament i d'automatització VMware Cloud on AWS.
- ✓ Proves de connectivitat entre site on-prem i site DR a AWS.
- ✓ Prova pilot DR parcial
- ✓ Formació i traspàs de coneixements

Actualment, els processos que es consideren dins l'àmbit de gestió del servei són:

- ✓ Procés de gestió de peticions.
- ✓ Procés de gestió d'incidències.

- ✓ Procés de gestió del coneixement.
- ✓ Procés de gestió de problemes.
- ✓ Procés de gestió d'esdeveniments i monitoratge.
- ✓ Procés de gestió de canvis.
- ✓ Procés de gestió de la configuració i inventari.
- ✓ Procés de gestió d'entregues i desplegaments.
- ✓ Procés de gestió de la capacitat i disponibilitat.

Abast inicial

- ✓ Elaboració de documentació i processos.
- ✓ Manteniment tasques d'automatització aprovisionament (2 cops l'any)
- ✓ Health check i actualitzacions versió plataforma en cas necessari (2 cops l'any)
- ✓ Informes periòdics estat plataforma (mensuals)
- ✓ Dues (2) Proves de DR parcials anuals
- ✓ Suport incidències
- ✓ Seguiment del servei

Aquests processos estableixen els mecanismes adients per mantenir un nivell de qualitat idoni dels serveis. Dins d'aquests processos, l'adjudicatari haurà de fer focus específic en les activitats de gestió dels diferents serveis:

- ✓ Assegurament dels mecanismes adients de monitoratge continu dels serveis.
- ✓ Registre, anàlisi i resolució de les incidències, peticions, canvis, problemes.
- ✓ Assegurament de la correcta gestió del coneixement relacionat amb aquests serveis i manteniment de la documentació relacionada.

Dintre de la millora continua, l'adjudicatari pot realitzar propostes relacionades amb la gestió dels processos, sempre enfocades a l'optimització i eficiència del procés/procediments extrem a extrem.

Procediments Failback:

Preparació Failback VCDR

- ✓ Com a primer pas s'ha de crear un Pla de Recuperació del tipus Failback, el qual es basa en un Pla de recuperació del tipus Failover, ja finalitzat (commited).

- ✓ El pla de recuperació per a Failback es pot crear de dos formes:
  - ➢ Quan s'executa i confirma un failover, es mostra la opció que ens permeti crear un pla duplicat amb els passos en ordre invers. Aquesta operació fa una còpia del pla original i afegeix [FAILOVER] al nom del pla.
  - ➢ Duplicar i invertir l'ordre dels passos del pla original de manera manual.

- ✓ Un cop creat un pla de recuperació del tipus Failback, es pot editar com qualsevol altre pla de recuperació. Per exemple, si el lloc protegit original no es pot recuperar després d'un desastre, es pot ajustar el pla de Failback per utilitzar un altre site com a objectiu.

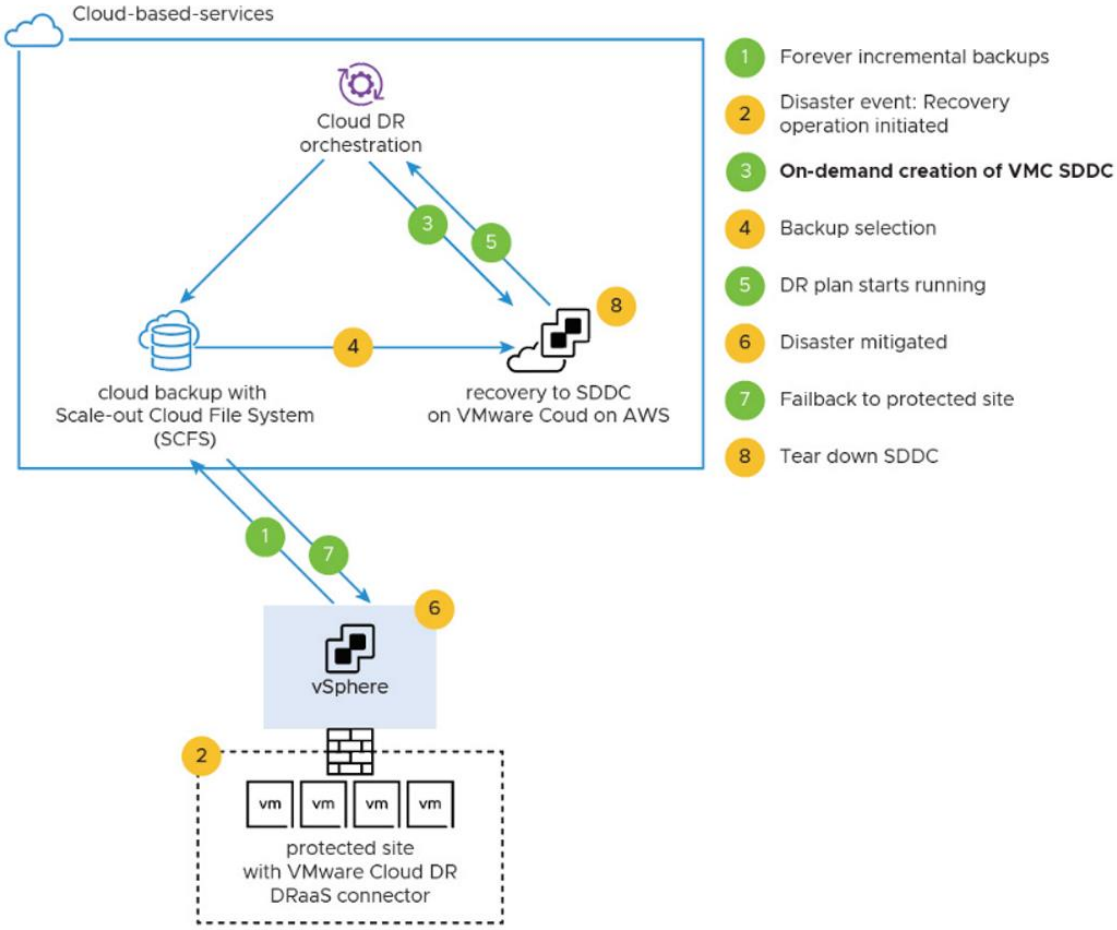
Procediment Failback VCDR:

- ✓ Les VM s'apaguen al SDDC desplegat a Vmware Cloud a AWS.
- ✓ Es pren una darrera instantània de la VM després de l'apagat. Les diferències entre l'estat de la màquina virtual al moment de failover i el Failback s'apliquen a la instantània utilitzada per a la recuperació per construir una còpia de seguretat de la màquina virtual al sistema de fitxers de el núvol per a la posterior recuperació.
- ✓ Aquesta còpia de seguretat es recupera a l'entorn OnPremise de forma incremental, aplicant els canvis a la màquina existent en entorn origen.
- ✓ La màquina virtual es recupera al lloc protegit.
- ✓ Un cop la recuperació és satisfactòria, la màquina virtual s'elimina automàticament del SDDC de VMware Cloud on AWS.

El Failback des d'un SDDC només retorna les dades modificades. No hi ha rehidratació, i les dades romanen en la seva forma nativa comprimida i de duplicada. Procediment gestionat des d'orquestrador del servei en modalitat SaaS.

Consideracions Failback VCDR:

- ✓ VMware Cloud Disaster Recovery no permet fer Failback d'una VM, on s'han realitzat canvis a la geometria de discos, després de realitzar el procés de failover.
- ✓ No es pot afegir un pas de recuperació individual d'una VM als plans de Failback. No obstant això, es pot restaurar VM's individualment des d'una instantània de grup de protecció.
- ✓ VMware Cloud DR no permet realitzar Failback de cap VM creada després de la recuperació al SDDC que coincideixi amb el patró de noms del grup de VM protegides o els criteris de carpetes definits en un Pla de recuperació.
- ✓ Qualsevol VM nova que s'hagi creat després de la recuperació i que coincideixi amb els patrons de nom del grup de protecció al Pla de Recuperació no quedarà inclosa quan es faci una operació de Failback a un nou site nou.



Preparació Failback EDR:

- ✓ Mitjançant EDR, un cop finalitzat el procediment de failover, permet fer un Failback a el vostre servidor d'origen original o qualsevol altre servidor que compleixi els requisits previs.

- ✓ Mitjançant EDR, caldrà configurar els Settings de Failback a les instàncies recuperades.

- ✓ Per a la utilització del client Elastic Disaster Recovery Failback, cal generar les credencials de AWS necessàries, per la qual cosa es requerirà almenys un rol d'AWS Identity and Access Management (IAM), i assignar la política de permisos adequada a aquest rol. S'obtindrà un ID de clau d'accés i una clau d'accés secreta, que caldrà introduir a la sol·licitud d'instal·lació de l'agent per començar la instal·lació.

- ✓ Un cop completat el Failback, es pot optar per acabar, eliminar o desconnectar la instància de recuperació d'AWS EDR.

Procediment Failback SQL:

- ✓ El Failback consisteix a redirigir el trànsit des del sistema en DR al sistema origen. Aquesta operació es fa fora d'Elastic Disaster Recovery. Elastic Disaster Recovery ajuda

a fer el Failback assegurant que l'estat del vostre sistema primari estigui actualitzat amb l'estat del sistema de recuperació.

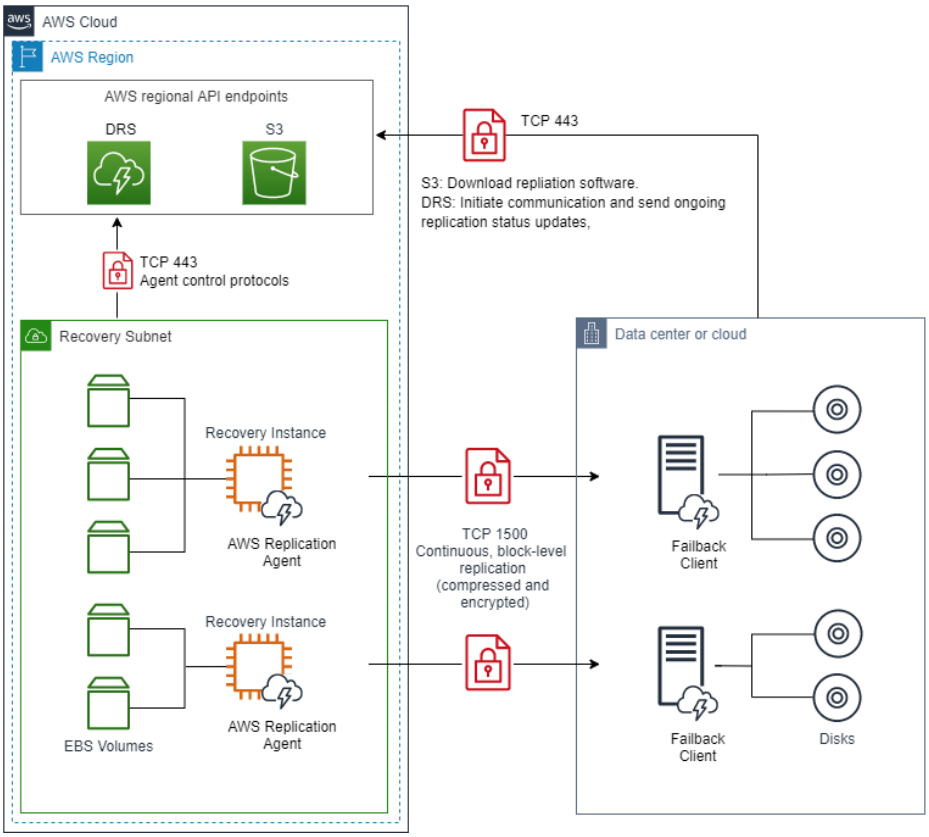
- ✓ La replicació de Failback es realitza arrencant el client de Failback mitjançant una imatge ISO al servidor d'origen al que voleu replicar les dades des d'AWS. Per utilitzar el Client Failback seran necessaris complir els requisits previs de Failback i generar les credencials d'AWS necessàries.

- ✓ Un cop realitzada la connexió amb AWS i el mapeig de la instància a DR amb el servidor origen, la replicació començarà entre tots dos. Un cop es mostri l'estat "Healthy" a l'estat de replicació podrà iniciar-se el procés de Failback i marcar com "Terminated" la instància de DR.

El servidor on es realitzarà l'operació de Failback ha de disposar del mateix nombre de volums i mida, o superiors, que la instància de recuperació executant-se a AWS.

Cal tenir en compte els requisits de connectivitat del servidor en què es vol realitzar el procediment de Failback. (connectivitat S3, ports i adreces IP publiques requerides).

AWS Elastic Disaster Recovery (AWS DRS) failback replication – architecture and networking



- ✓ Suposa activació de l'entorn DR durant un període de 7 dies x 24 hores:

2.3.1 Horaris i Ubicacions

Horari

La realització de les tasques del servei que no tinguin cap impacte, i per tant sense afectació als entorns productiu o de normal activitat es farà d'acord amb les especificitats que als efectes indiqui BSM. Es tracta d'un servei 24x7x365 dies a l'any.

Les tasques del servei que necessitin una parada planificada dels serveis productius o puguin produir inconvenients, i per tant amb afectació en la normal activitat dels serveis productius de BSM es desenvoluparan en horari Festiu/Nocturn de la seu i/o dintre del horari acordat amb BSM.

Processos	Horari Servei	Observacions
Gestió d'Incidències Crítiques	24x7	Es considera disponibilitat 24x7 mitjançant un mecanisme de guàrdies que garanteixi l'accés telefònic al personal tècnic de la unitat
Gestió de Peticions Gestió de Problemes Gestió de Canvis Resta de Processos	De dilluns a divendres, de 9h a 18h excepte els festius a tot Catalunya o 24x7x365 segons determini l'organització BSM per necessitat o criticitat.	L'adjudicatari haurà de realitzar fora de l'horari laboral definit totes les peticions i canvis amb risc d'afectació als serveis

Ubicació

Tota la activitat necessària per la realització de tasques relacionades amb el servei es realitzaran a petició de BSM, en la ubicació i en l'horari que aquesta indiqui, i de la forma que es determini, presencial o remota.

Les reunions d'anàlisi, requeriments, seguiment i coordinació del servei i altres que BSM determini es realitzaran a les instal·lacions de BSM, i en l'horari que es determini.

2.3.2 Estructura organitzativa per prestar el servei

Equip de treball

L'adjudicatari haurà de disposar i assignar per l'execució del contracte de personal tècnic qualificat que compleixi amb els següents perfils:

Es requereix un equip integrat per recursos especialitzats amb els diferents perfils necessaris per cobrir l'abast de les tasques sol·licitades, amb coneixement al sector dels serveis de Disaster Recovery (DR) en Cloud amb experiència al servei en referències similars.

El dimensionament de l'equip és responsabilitat de l'adjudicatari. Com a mínim ha d'estar compost pels perfils següents:

1 Cap de Servei	Enginyer de Telecomunicacions i/o informàtica (grau+màster), amb mes de 8 anys d'experiència professional en la realització de projectes de consultoria i serveis de gestió de contractes als àmbits de la present licitació. Caldrà demostrar experiència.
1 Enginyer en Sistemes Cloud – Consultor assignat al Servei	Enginyer de Telecomunicacions i/o Informàtica (grau+master), amb mes de 4 anys d'experiència professional en la realització de serveis de consultoria de sistemes cloud i/o sistemes de Disaster Recovery (DR) als àmbits de la present licitació. Caldrà demostrar experiència.
1 Tècnic en Processos / Comunicacions Cloud	Enginyer tècnic de Telecomunicacions i/o Informàtica i/o FP grau superior, amb mes de 2 anys d'experiència professional en consultoria especialitzada en sistemes cloud i/o sistemes de Disaster Recovery (DR). Caldrà demostrar experiència.

L'adjudicatari haurà d'acreditat el currículum vitae dels recursos proposats, i es requereix que almenys que 1 dels recursos assignats al projecte disposen de la **certificació ITIL v3/4 o similar**.

Per acreditar aquests extrems, s'adjuntarà còpia de les titulacions de les persones que s'assignen a aquest projecte, així com una relació dels projectes de serveis en què han participat i funcions exercides en els darrers anys. Als requisits de solvència tècnica i professional es defineixen les titulacions i experiència necessària per a cada membre de l'equip de treball. Així mateix es valorarà la experiència addicional.

L'adjudicatari es compromet a proveir els recursos humans i tècnics oferts en la seva proposta. En cas de que s'hagi de reemplaçar un dels recursos, haurà d'informar amb una setmana d'antelació d'aquest fet, i contrastar i acordar amb el comitè de seguiment del projecte les circumstancies del canvi i del nou recurs, i BSM haurà d'acceptar explícitament aquest canvi.

BSM es reserva el dret de demanar un canvi de recurs si aquest no compleix amb els requisits de qualitat, coneixements tècnics o d'entrega de tasques a temps.

Qualsevol comunicació o petició, especialment si pot implicar una despesa econòmica posterior, haurà de ser aprovada pel comitè de seguiment del servei, i BSM no acceptarà cap mena de càrrec econòmic per actuacions no hagin estat expressament demanades per part dels seus interlocutors i, en aquest sentit, es responsabilitat de l'adjudicatari no acceptar altres demandes que no siguin les d'aquests referents.

L'adjudicatari ha d' oferir un servei en general amb un nivell d'excel·lència i qualitat màxims. Per això, l'adjudicatari s'obliga a tenir implantada una sèrie de mecanismes que permeten a BSM, valorar la qualitat de servei així com reportar qualsevol dubte o incidència en la gestió del mateix.

Durant el procés de resolució d'una incidència, l'adjudicatari ha de facilitar una comunicació amb el consultor assignat al servei, de manera que es faciliti la comunicació primera de qualsevol inquietud o dubte respecte a l'atenció que s'estigui rebent.

2.3.3 Servei d'operació i suport

El servei d'operació i suport que haurà de prestar l'adjudicatari comprèn la realització d'activitats destinades a la gestió i resolució de qualsevol procés TIC objecte del present procediment de Disaster Recovery (DR) en Cloud (migració del serveis crítics, gestió d'incidències, peticions, canvis, problemes, configuració, capacitat, etc.) i, en general, qualsevol tasca addicional que contribueixi a assolir els objectius de BSM dins de la gestió dels serveis de contingència necessaris per l'organització.

L'adjudicatari serà responsable de definir, implementar i executar el servei, d'acord amb els requisits establerts que es detallen a continuació:

Monitorització i gestió d'esdeveniments

L'adjudicatari haurà de prestar un Servei de Monitorització que garanteixi la qualitat, disponibilitat i rendiment dels serveis oferts per a BSM, disposant de tots els mitjans tècnics i materials necessaris (hardware, software, comunicacions, etc.) per a la prestació efectiva del servei. Aquest servei no ha de tenir cap cost addicional per a BSM, en qüestió d'equipament, software, llicenciament o ma d'obra.

Amb caràcter general, les característiques mínimes han de respondre a les següents necessitats:

- ✓ Definició i configuració de paràmetres i llindars a les eines de monitorització, i construcció de mapes de monitorització i detecció d'alarmes o esdeveniments.
- ✓ Vigilància contínua i detecció de les alarmes, per detectar les incidències que es puguin produir en els sistemes o serveis, a el cas del qual, seran escalades al primer nivell d'operació segons es descriu a l'apartat Service Desk, i es realitzarà el registre de la incidència i comunicació als responsables o contactes autoritzats de BSM.
- ✓ L'abast el servei, comprèn les 24 hores, els 7 dies de la setmana i els 365 dies a l'any (d'ara endavant 24x7x365).
- ✓ L'activitat es realitzarà de forma remota des de les instal·lacions del adjudicatari excepte si, a criteri del Responsable del Contracte designat per BSM, es requereixi una assistència in-situ puntual.
- ✓ L'adjudicatari serà responsable de definir, implementar i executar el procés de gestió d'esdeveniments i monitorització dels serveis, d'acord amb els requisits establerts en aquest procediment amb les necessitats de l'organització BSM, responsabilitzant-se del mateix i de reportar la informació i mètriques associades.

A més de les característiques globals enunciades amb caràcter general, es distingeixen diversos

àmbits de monitorització integrats al servei, com la monitorització de sistemes , comunicacions de l'entorn de DR, monitorització d'usuari i el suport a la monitorització de seguretat.

Monitorització de sistemes i comunicacions de l'entorn Disaster Recovery (DR)

L'adjudicatari haurà de prestar un servei de monitorització al àmbit dels sistemes i les comunicacions, destinat a determinar el estat de tots els equips que componen, la infraestructura de sistemes i comunicacions de l'entitat, i de les funcionalitats configurades a aquests equips, en termes de disponibilitat, rendiment i capacitat.

Amb caràcter general, les característiques mínimes han de respondre a les següents necessitats:

- ✓ Definició i implantació de la solució tecnològica que es farà servir per accedir, recollir i analitzar les dades a monitoritzar.

- ✓ El sistema ha de permetre com a mínim els següents requisits:

- ➢ Monitorització distribuïda.
- ➢ Monitorització web integrada.
- ➢ Autodescobriment de sistemes.
- ➢ Eina de predicció de tendències.
- ➢ Monitorització IPv4 i IPv6.
- ➢ Possibilitat d´invocar agents/clients d´altres eines.
- ➢ Execució d'accions remotes sobre nodes diferents de l'origen de l'alarma.
- ➢ Estadístiques SNMP.
- ➢ Funcionalitat syslog.

Monitorització d'usuari

L'adjudicatari haurà de prestar un servei de monitorització al àmbit de l'experiència d'usuari real, destinat a determinar el rendiment i la qualitat en la percepció de l'usuari dels serveis crítics en Disaster Recovery (DR) que es presten. Es pretén disposar, en cas d'entrada en contingència DR, d'una monitorització que confirmi el bon funcionament dels serveis i els seus temps de resposta.

Les característiques mínimes del servei són les següents:

- ✓ Definició i implantació de la solució tecnològica que es implementarà per accedir, recollir i analitzar les dades a monitoritzar.

- ✓ El sistema ha de permetre com a mínim els següents requisits de monitorització:

- ➢ Monitorització activa d'accions d'usuari final.
- ➢ Monitorització de temps de resposta per sistema crític.
- ➢ Verificació de contingut per text, enllaços o objectes.
- ➢ Captura de pantalla en cas d'error.

- Descàrrega de fitxers.
- Consum de CPU i Memòria.

✓ Cada node o sonda de monitorització, ha de tenir la capacitat de poder ser configurada en funció de les necessitats de l'organització BSM, amb el major nombre d'opcions possibles de cadascun dels següents elements:

- Sistema operatiu.
- Navegadors web.
- Tipus de Dispositiu.

✓ L'adjudicatari implementarà la monitorització d'experiència de usuari real, en base als criteris següents:

- Monitorització bàsica:

✓ El sistema haurà de descarregar-se la pàgina del servei principal o funcionalitat principal, i avaluar-ne el rendiment en base a mètriques.

S'implementarà necessàriament per a tots els serveis i aplicatius en explotació Crítics.

✓ La freqüència màxima de les mètriques serà d'una hora, i es realitzarà el monitoratge des d'almenys un node:

- Sonda de monitorització.
- Monitorització avançada:

✓ El sistema haurà de poder configurar un escenari de transacció complet sobre els serveis de Disaster Recovery (DR) en Cloud, les característiques en funció dels sistemes, seran definides en col·laboració amb BSM.

✓ S'implementarà per defecte per els sistemes categoritzats com a crítics, segons el que determini l'organització BSM.

La freqüència màxima de les mètriques, serà de 15 minuts, i es realitzarà el monitoratge des d'almenys dos nodes o sondes de monitorització.

Suport a la monitorització de seguretat

BSM podrà disposar d'altres sistemes o serveis de monitorització en l'àmbit de la seguretat (SOC, CEX, etc...), i en aquest cas el adjudicatari haurà de donar suport i col·laborar en l'operativa de la seva activitat, incloent l'autorització i la implementació de les eines o configuracions tècniques necessàries a la seva infraestructura per obtenir la informació necessària, a fi de garantir el correcte estat dels actius de BSM i generar les alertes corresponents en cas de esdeveniments que poden afectar la seguretat de la informació, amb les següents característiques mínimes:

- ✓ Facilitar i proporcionar l'accés a la informació necessària pel sistema de monitorització de seguretat que BSM determini, així com emmagatzemar i resguardar els esdeveniments recol·lectats per, en cas de necessitat, realitzar una anàlisi forense i obtenir dades relatives al origen, destinació i traça dels incidents de seguretat.

- ✓ Configurar els elements de sistemes d'informació per permetre el funcionament correcte del sistema de monitorització.

- ✓ Col·laborar a discernir entre falsos positius o negatius analitzant les diferents alertes detectades, amb els grups de suport o monitorització de seguretat de BSM.

- ✓ Considerar els requisits tècnics necessaris per permetre la monitorització efectiva de seguretat.

Service Desk: Centre d'atenció d'usuaris i primer nivell d'operació i suport

L'adjudicatari haurà de proporcionar un punt de contacte tècnic centralitzat per a la gestió de tots els esdeveniments (incidències, peticions, consultes, canvis i qualsevol altre procés estimat per BSM), així com aquells que apliquin a tot allò referent a l'àmbit TIC dels sistemes i serveis de contingència i Disaster Recovery (DR), des de la recepció del servei, fins a la resolució si és possible mitjançant procediments d'operació i suport pel Service Desk o l'escalat, la coordinació i el seguiment de l'esdeveniment fins al tancament.

El Service Desk, no ha de limitar-se a ser un centre de recepció de incidències, ha de ser capaç de donar suport de primer nivell als processos del servei, coordinant i fent seguiment de tots els esdeveniments relacionats amb el servei de Disaster Recovery (DR).

Les característiques del servei a implementar són les següents:

- ✓ Definició i implantació del servei d'atenció i dels procediments de primer nivell d'operació i suport.

- ✓ L'activitat es podrà realitzar de forma remota, excepte si a criteri del responsable del contracte de BSM es considera adequada una modalitat de servei in situ en determinats casos puntuals. L'abast del servei, comprèn les 24 hores, els 7 dies de la setmana i els 365 dies a l'any (d'ara endavant 24x7x365), per al següent àmbit:

- ➢ Serveis de prioritat alta o crítica.
- ➢ Incidències relatives a la seguretat dels serveis TIC allotjats en l'entorn de Disaster Recovery (DR) en Cloud, relatives a les vulnerabilitats i atacs a la mateixa que comprometin el funcionament dels serveis que presta per l'organització com a contingència.
- ➢ Aquells que BSM consideri com a causa justificada pel impacte o context aplicable.

La classificació i determinació dels serveis per prioritat correspon a BSM, i seran comunicats a l'adjudicatari a l'inici. La classificació i prioritat podrà estar subjecta a modificació en funció de

les necessitats de l'organització BSM, dites canvis seran comunicats a l'adjudicatari amb la suficient antelació.

- ✓ El servei es prestarà en idioma Català o Castellà.
- ✓ BSM podrà integrar al servei, en funció de les seves necessitats, altres Centres d'Atenció d'Usuaris, CEX, SOC, Service Desk, o serveis de suport i operació específics. A qualsevol cas, l'adjudicatari haurà d'integrar-se de manera operativa de acord als requisits que li seran comunicats per part de l'organització BSM.
- ✓ L'adjudicatari serà responsable de definir, implementar i executar el procés de gestió de Service Desk, d'acord amb els requisits establerts i amb les necessitats de l'organització BSM responsabilitzant-se del procés i de reportar la informació i mètriques del mateix.

Gestió i suport de segon nivell d'operació i suport

L'adjudicatari haurà de fer totes les tasques de gestió, operació i administració tècnica de tota la infraestructura tecnològica de sistemes, comunicacions, seguretat de l'entorn de Disaster Recovery (DR) en Cloud, a fi de garantir la qualitat dels serveis de contingència i per donar resposta als objectius estratègics de l'organització BSM.

Amb caràcter general, les característiques mínimes han de respondre a les següents necessitats:

- ✓ Definició i implantació del servei de gestió i segon nivell de operació i suport del Disaster Recovery (DR).
- ✓ L'activitat es podrà realitzar de forma mixta, excepte si a criteri del Responsable del contracte de BSM es considera adequada una modalitat de servei remot o in-situ en casos puntuals. Per a la realització del servei, l'adjudicatari haurà d'assegurar el compliment dels requisits de servei de contingència a través dels tècnics dedicats que permetin assegurar una gestió i suport àgil i eficaç de les funcions objecte de contracte (especialment les que puguin dependre de l'actuació sobre elements físics per incapacitat de activitats remotes). Igualment, si així es determinés i sempre baix supervisió de BSM, aquelles activitats que es poden realitzar a remot, es realitzarien d'aquesta manera sense perjudici de la qualitat del servei i del compliment dels acords de nivell de servei que es determinin.
- ✓ El servei s'haurà de prestar 24x7x365.
- ✓ De manera addicional, per aquells canvis que siguin planificats en finestres d'actuació que s'han de fer fora de l'horari establert de manera preliminar, podent fer-se fins i tot en horari nocturn, fins de setmana o festius. Aquestes activitats no suposaran cap cost addicional per a BSM.
- ✓ L'adjudicatari prestarà assessorament tecnològic i de qualsevol procés actual o futur relatiu al servei de Disaster Recovery (DR) en Cloud i contingència de BSM.

- ✓ Enfocament del servei de contingència basat en bones practiques ITIL, per la qual cosa es prestaran serveis destinats a la gestió de qualsevol procés i activitat que BSM determini en l'àmbit del servei de Disaster Recovery (DR) en Cloud.

Gestió d'accessos, incidències, peticions i problemes

- ✓ L'adjudicatari serà el responsable d'executar la gestió efectiva i control dels incidents i peticions del servei de DR, ajustant-se als procediments establerts a aquest efecte, proposant i implantant si és el cas, les modificacions, necessitats i millores possibles del procés, a fi d'assegurar el correcte funcionament dels serveis.

- ✓ El servei, haurà de prestar especial suport a les incidències relacionades amb la seguretat de la informació, reaccionant davant qualsevol alerta i incidència i proporcionant un nivell d'alerta primera davant d'amenaces emergents, encara que aquestes encara no s'hagin materialitzat als actius de BSM en l'entorn DR.

- ✓ Davant de riscos motivats per un aprofitament d'una vulnerabilitat emergent o existent en els sistemes de BSM, el adjudicatari s'encarregarà de proposar plans d'actuació per a minimitzar l'impacte d'aquest risc, així com implementar els canvis necessaris en els actius protegits afectats, si BSM ho sol·licita.

- ✓ L'adjudicatari haurà d'utilitzar canals de comunicació segurs per a l'intercanvi d'informació que garanteixin la confidencialitat, integritat i origen legítim de les notificacions.

- ✓ L'adjudicatari serà responsable del procés de Gestió de Incidències i Peticions, i per tant del seu cicle de vida des de la seva obertura fins al tancament, així com proveir la informació i les mètriques del procés.

- ✓ L'adjudicatari reportarà en el cas d'incidències que causin interrupció del servei de DR, les relatives a la seguretat o que per la seva impacte, l'entitat consideri la seva justificació detallada, un informe justificatiu del detall de la incidència i de l'actuació del servei.

- ✓ Com a complement del procés de gestió d'incidents, el adjudicatari serà el responsable de definir, implementar i executar el procés de gestió de Problemes.

- ✓ L'adjudicatari serà responsable d'executar la gestió efectiva i operació de l'accés dels usuaris als serveis de Disaster recovery (DR) en Cloud, assegurant la confidencialitat, disponibilitat i integritat de la informació.

Gestió de canvis, capacitat, actius i configuració

- ✓ L'adjudicatari serà el responsable d'executar la gestió i el control dels canvis del servei de contingència, ajustant-se als procediments establerts a aquest efecte, proposant i implantant si és el cas, les modificacions, necessitats i millores possibles del procés, amb el objecte de minimitzar els riscos en els canvis, i en conseqüència assegurar la qualitat dels serveis de Disaster Recovery (DR) en Cloud.

- ✓ L'adjudicatari serà el responsable d'executar la gestió efectiva i control de la capacitat dels actius, i de la configuració dels elements de configuració, ajustant-se als procediments establerts a aquest efecte, proposant i implantant si és el cas, les modificacions, necessitats i millores possibles dels processos per controlar la qualitat dels serveis de contingència. L'adjudicatari haurà de fer ús i administrar si escau, la Base de dades de gestió de la configuració (CMDB) proposada per l'organització BSM per a la gestió efectiva dels elements de configuració de l'entitat.

- ✓ L'adjudicatari haurà de proposar requeriments de seguretat en quant a la gestió de canvis a la infraestructura de Disaster Recovery (DR) en Cloud de BSM.

- ✓ L'adjudicatari serà responsable dels processos de Gestió de canvis i configuració, i per tant del cicle de vida de qualsevol canvi i de la configuració dels components, així com de proveir la informació i mètriques dels processos.

- ✓ L'adjudicatari amb l'organització BSM, amb periodicitat setmanal, liderarà els Comitès de canvis, i en aquests reportarà l'estat dels canvis realitzats la setmana anterior al comitè, així com la planificació dels canvis proposats per a la setmana en curs. Aquests Comitès, podran exigir la presència in situ a les dependències de BSM de l'adjudicatari.

- ✓ L'adjudicatari serà el responsable d'executar la gestió i el control dels actius i configuració dels serveis de Disaster Recovery (DR) en Cloud, ajustant-se als procediments establerts a aquest efecte, proposant i implantant si és el cas, les modificacions, necessitats i millores possibles del procés, a fi de gestionar la informació i el control sobre actius dels serveis, i en conseqüència assegurar la qualitat dels serveis de contingència.

Gestió del coneixement

- ✓ L'adjudicatari serà el responsable d'executar la gestió de coneixement dels serveis de contingència, ajustant-se als procediments establerts a aquest efecte, proposant i implantant si és el cas, les modificacions, necessitats i millores possibles del procés, a fi de compartir la informació i que estigui disponible per permetre l'anàlisi i facilitar la presa de decisions.

Suport tècnic de tercer nivell

L'adjudicatari prestarà serveis destinats a la realització de suport tècnic per a incidències dels serveis operats, amb especial èmfasi a les incidències de serveis crítics i de seguretat, amb l'objecte de garantir la disponibilitat, continuïtat, seguretat i qualitat dels serveis de contingència.

Amb caràcter general, les característiques mínimes han de respondre a les següents necessitats:

- ✓ Definició i implantació del servei de suport tècnic de tercer nivell.

- ✓ L'activitat es podrà realitzar de forma remota, excepte si a criteri de l'organització BSM es considera adequada una modalitat de servei in situ en determinats casos puntuals.

- ✓ L'abast el servei, comprèn les 24 hores, els 7 dies de la setmana i els 365 dies a l'any (d'ara endavant 24x7x365).

- ✓ L'adjudicatari haurà de definir i implementar un procediment de gestió i actuació d'incidències per a tots els serveis crítics i els relacionats amb la seguretat dels sistemes de la informació en Disaster Recovery (DR) en Cloud de BSM, en què es reflecteixi detalladament els passos i mecanismes de contingència a realitzar, el flux i mitjans de comunicació, escalats, i qualsevol altre aspecte que es consideri interessant.

Suport especialitzat i recolzament a nous projectes

L'adjudicatari prestarà serveis addicionals de suport especialitzat per a nous projectes de Disaster Recovery (DR) en Cloud, tasques d'enginyeria o consultoria tècnica de contingència, que per la seva complexitat, criticitat, magnitud, relació amb el negoci o tecnologia, necessiteu un suport d'alt nivell especialitzat o de recursos addicionals, o que no es trobi contemplat a la resta de requisits objecte del present procediment, i sempre que tingui relació amb l'objecte del servei de contingència.

L'activitat es podrà realitzar in situ (en casos puntuals), de forma remota o mixta, depenent de les necessitats o naturalesa del projecte o suport, i s'haurà de prestar sempre conforme amb les condicions establertes.

2.4 Formació i transferència de coneixements

Per completar l'abast dels servei presentat i fer una formació i transferència de coneixement completa als responsables tècnics de BSM, l'adjudicatari ha de posar a disposició de BSM un expert o experts amb coneixements dels serveis i configuracions desenvolupades a BSM per realitzar la formació i transferència de coneixements. El servei es realitzarà dintre del horari laboral de BSM al llarg de com a màxim 2 jornades laborables de 4 hores com a màxim.

L'adjudicatari haurà de prestar la formació i transferència de coneixements a les instal·lacions de BSM.

L'adjudicatari haurà de proporcionar la documentació completa d'aquesta formació i transferència de coneixements. Tota la documentació s'entregarà en format digital.

La documentació es lliurarà en Català i/o Castellà.

2.5 Equip de treball

L'adjudicatari haurà d'aportar un equip tècnic amb la categoria professional i el nivell d'especialització més adient a les necessitats objecte del contracte i que acompleixi amb els criteris de solvència tècnica i professional detallats en el plec administratiu que regeix aquesta licitació.

Qualsevol modificació de l'equip assignat haurà de ser comunicat prèviament a BSM amb una antelació mínima de 10 dies laborables i la substitució s'haurà de fer per un perfil que, com a mínim, tingui les mateixes característiques professionals i tècniques que les exigides el contracte. En cas de substitució l'adjudicatari haurà de realitzar obligatòriament un procés de transferència de coneixements.

BSM es reserva el dret de verificar les capacitats del personal que participa en el projecte o servei en qualsevol moment, rebutjar-lo i/o aplicar les penalitzacions corresponents en cas que no compleixin amb els requisits exigits. Les despeses que es derivin com a conseqüència de canvis en l'equip de projecte aniran a càrrec de l'adjudicatari.

BSM es reserva el dret a sol·licitar el canvi d'un o més dels recursos assignats en el cas d'identificar que la qualitat del servei prestat no és la mínima requerida. Aquest canvi s'haurà de produir en un període màxim de 15 dies laborables a partir de la comunicació al adjudicatari.

2.6 Acords del nivell de Servei (ANS)

Es requereixen acords de nivells de servei de tots els serveis exposats en el plec. Aquests serveis poden ser de dos tipus diferents: els que responen a una petició i els que ofereixen un servei en línia (via extranet-entorn web). En els que responen a una petició, el nivell de servei exigible es mesurarà segons un temps de resolució màxima (que s'estableix a continuació), mentre que en els serveis en línia el que s'establirà és la disponibilitat que han de tenir aquests serveis. S'estableix en cadascun dels supòsits el percentatge de casos en que s'han de complir els temps establerts.

En caràcter general, els ANS a respectar en aquest contracte són els estipulats al plec de clàusules administratives que regula aquesta licitació.

S'estableixen dos tipus de petició: normal o crítica. L'organització client serà qui decidirà, en funció de la urgència de l'acció a dur a terme, si una petició és normal o crítica. Les peticions normals s'enviaran a l'interlocutor de l'empresa adjudicatària via correu electrònic, mentre que les peticions crítiques, una vegada s'hagin enviat per correu electrònic, es comunicaran també per via telefònica.

Processos	Horari Servei	Observacions
Gestió d'Incidències Crítiques	24x7x365	Es considera disponibilitat 24x7 mitjançant un mecanisme de guàrdies que garanteixi l'accés

		telefònic al personal tècnic de la unitat
Gestió de Peticions Gestió de Problemes Gestió de Canvis Resta de Processos	De dilluns a divendres, de 9h a 18h excepte els festius a tot Catalunya o 24x7x365 segons determini l'organització BSM per necessitat o criticitat.	L'adjudicatari haurà de realitzar fora de l'horari laboral definit totes les peticions i canvis amb risc d'afectació als serveis

2.6.1 Penalitzacions pels subministraments del servei

ANS associat de servei:

L'adjudicatari haurà de complir els acords de nivell de servei (ANS) de l'apartat següent.

Descripció	Valor Objectiu
POSADA EN MARXA I DISPONIBILITAT DE LA PLATAFORMA DR EN CLOUD	
Data compromesa per a la finalització de la posada en marxa de la plataforma de Servei de Disaster Recovery (DR) o Contingència des de la sol·licitud formal per correu electrònic	6 mesos
Disponibilitat de la plataforma de Servei de Disaster Recovery (DR) o Contingència	>= 99% (No es tindran en compte les finestres pactades de manteniment).
Data compromesa per la finalització de la posada en marxa de la prova de concepte (PoC) o maqueta del servei crític Disaster Recovery o Contingència a implementar en fase inicial per sol·licitud formal per correu electrònic	2 mesos

BSM aplicarà una penalització per a l'incompliment del termini, imputable a l'adjudicatari, per al no compliment dels cadascun dels subministraments i serveis associats especificades en el plec tècnic, i definits en l'acord de nivell de servei (ANS).

Descripció	Fórmula de càlcul	Penalització associada
POSADA EN MARXA I DISPONIBILITAT DE LA PLATAFORMA DR EN CLOUD		
Data compromesa per a la finalització de la posada en marxa de la plataforma de Servei de Disaster Recovery (DR) o Contingència des de la sol·licitud formal per correu electrònic	Per setmana hàbil de retard	2% de pressupost de anual de licitació
Disponibilitat de la plataforma de Servei de Disaster Recovery (DR) o Contingència	Hores totals disponibilitat (mes) / Hores totals (mes	2% de pressupost de anual de licitació per cada 1% de desviació de la disponibilitat de la plataforma de servei DR. (No es tindran en compte les finestres pactades de manteniment)

Temps de posta en marxa dels serveis indicats a la licitació en la plataforma de DR en AWS	Temps objectiu: Crític: 4 hores Greu: 8 hores Lleu: 32 hores	10% de pressupost de anual de licitació per cada 1h de desviació.
Data compromesa per la finalització de la posada en marxa de la prova de concepte (PoC) o maqueta del servei crític Disaster Recovery o Contingència a implementar en fase inicial per sol·licitud formal per correu electrònic	Per setmana hàbil de retard	2% de pressupost de anual de licitació

- ✓ BSM aplicarà una penalització per a l'incompliment del termini, imputable a l'adjudicatari, per al no compliment dels cadascun dels subministraments i serveis associats especificades en el plec tècnic.
- ✓ Per a cada setmana d'endarreriment en el lliurament dels equips, material o subscripció o d'una part es penalitzarà amb un import del 2% del pressupost anual de licitació.
- ✓ Els retards de més de quatre setmanes donarà lloc a la pèrdua total de la fiança i si BSM ho considera adient, a la rescissió d'aquest contracte. En qualsevol cas, el contractista està obligat a respondre dels danys i perjudicis que BSM haurien de suportar a causa de l'incompliment del termini contractual.

2.6.2 Penalitzacions associades al nivell de servei (ANS)

ANS associat de servei:

Incidència critica	Temps màxim de resposta de 15 minuts Temps màxim de resolució de 4 hores en horari 24x7x365
Incidència Greu	Temps màxim de resposta de 45 minuts Temps màxim de resolució de 8 hores en horari 24x7x365
Incidència Lleu	Temps màxim de resposta de 8 hores Temps màxim de resolució de 32 hores en horari 8x5 en la franja de 9h a 19:00h
Vulnerabilitat crítica	Temps màxim de resposta de 1 hora Temps màxim de resolució/mitigació de 48 hores en horari 24x7x365
Vulnerabilitat greu	Temps màxim de resposta de 4 hores Temps màxim de resolució/mitigació de 48 hores en horari 8x5 en la franja de 9h a 19:00h
Vulnerabilitat lleu	Temps màxim de resposta de 8 hores

	Temps màxim de resolució/mitigació de 72 hores en horari 8x5 en la franja de 9h a 19:00h

Les penalitzacions seran acumulables. Per a una mateixa incidència o vulnerabilitat es podrà penalitzar pel temps de resposta i per el temps de resolució.

BSM es reserva el dret de modificar una incidència o vulnerabilitat i classificar-la segons la seva urgència i criticitat.

En cas de concurrència d'incidències o vulnerabilitats, l'adjudicatari haurà de destinar els recursos disponibles a la incidència més crítica i ha de ser capaç de resoldre dues incidències simultànies.

La resolució d'una incidència o vulnerabilitat haurà de ser acceptada pel corresponent responsable dins de l'estructura organitzativa de BSM.

Qualsevol incompliment del pla de suport tècnic o del temps de resolució d'incidències pot donar peu a les penalitzacions establertes entre BSM i l'adjudicatari.

L'aplicació de penalitzacions comporta obrir un expedient contradictori en què es dona audiència a l'adjudicatari. L'aplicació dels ANS comporta l'aplicació automàtica en factura sense tràmit contradictori.

Penalitzacions per al temps de resposta:

- Incidències i vulnerabilitats Crítiques: Cada cop que se superi el temps de resposta estipulat (15 minuts Critiques i 45 minuts per Greus), s'aplicarà una penalització del 2,5% del import anual adjudicat del servei per cada 15 minuts de retard addicional en donar resposta.

- Resta d'incidències i vulnerabilitats: Es farà revisió trimestral. Si el >20% per incidències del període mesurat, supera el temps de resposta, s'aplicarà una penalització del 2,5% del import anual adjudicat.

Penalitzacions per al temps de resolució d'incidències i vulnerabilitats:

Per a les incidències i vulnerabilitats de prioritat Crítica:

✓ En cas de superar el temps màxim de resolució es realitzarà una penalització del 10% del import anual adjudicat del servei per a cada hora d'excés en el cas d'una incidència.

Per a les incidències i vulnerabilitats de prioritat Greu:

✓ En cas de superar el temps màxim de resolució es realitzarà una única penalització per incidència del 10% del import anual adjudicat del servei per a cada hora d'excés en el cas d'una incidència.

Per a les incidències i vulnerabilitats de prioritat Lleu:

- ✓ Es farà una revisió trimestral. Si el >20% per incidències lleus del període mesurat supera el temps de resolució, s'aplicarà una penalització del 2,5% del import anual adjudicat del servei.

En cas de repetició d'incidències greus o crítiques BSM es reserva el dret de discontinuar el contracte o penalitzar amb l'import total de la quota de dret d'ús establert.

2.6.3 Penalitzacions complementaries

COMPLIMENT DE GDPR I NOTIFICACIONS DE BRETXES DE SEGURETAT

La Regulació General de Protecció de dades (GDPR), és vinculant per a qualsevol corporació que processi les dades de ciutadans de la UE, i estarà sota la jurisdicció a l'autoritat de supervisió de dades o els tribunals de l'estat membre que tinguin la relació més estreta amb les persones o entitats que manegen aquestes dades personals.

GDPR s'aplica al tractament de dades personals en el context de les activitats d'un establiment a la UE/EEE d'un controlador o processador, independentment de si el processament es duu a terme a la UE/EEE o no.

Per complir amb la normativa de protecció de dades GDPR cal que es compleixin els següents apartats:

- ✓ Prohibida la transferència de dades personals fora de la UE/EEE a països que no ofereixen un nivell similar de protecció de dades personals i drets de privadesa.
- ✓ Quan l'adjudicatari hagi patit una bretxa de la seguretat que pugui afectar a dades propietat de BSM, haurà de notificar amb informes basats en el risc i dels diferents requisits necessaris per informar l'incompliment a l'Autoritat de Supervisió de les dades afectades per la bretxa. Les infraccions han de ser reportades dins de les 24 hores posteriors a què la companyia conegui l'ocurrència de l'incident.
- ✓ L'adjudicatari serà el controlador de les dades que se'ls han confiat. Com es va veure anteriorment, nombroses lleis, regulacions i contractes prohibeixen, restringeixen i limiten la revelació i transferència de dades a un tercer.

L'incompliment dels requeriments de GDPR o dels temps de notificació requerits per BSM, pot donar peu a les penalitzacions establertes entre BSM i l'adjudicatari. En concret:

- ✓ En cas de transferència de dades personals fora de la UE/EEE o països amb nivell de protecció similar es realitzarà una única penalització per incidència del 2,5% del import anual del pressupost adjudicat del servei.

- ✓ En cas de superar el temps màxim de notificació de bretxes de seguretat es realitzarà una penalització del 2,5% del import anual del pressupost adjudicat del servei per a **cada hora d'excés** en la notificació.

En cas de repetició d'incidències d'incompliment de GDPR o notificacions de bretxes, BSM es reserva el dret de discontinuar el contracte o penalitzar amb l'import total de la quota de dret d'ús establert.

DEVOLUCIÓ DEL SERVEI

BSM es reserva el dret de no retornar la garantia dipositada per l'adjudicatari, en cas de que l'adjudicatari no retorni les dades complertes i estructurades a BSM 30 dies abans de finalitzar el contracte, o no realitzi l'acompanyament en la transició del servei segons els requeriments descrits al plec tècnic.

CAPACITACIÓ PERFILS EQUIP

BSM es reserva el dret de a partir de la 2 vegada que es rebutgi un perfil proposat (com a substitut), per manca de compliment de requisits del plec administratiu, la possibilitat de rescissió el contracte.

ROTACIÓ EQUIP

BSM es reserva el dret de, a partir que durant l'últim any hi hagi una rotació del equip superior a 1/3 del equip, la possibilitat de rescissió del contracte.

Resolució de contracte: En cas de reiterades penalitzacions, BSM es reserva el dret d'extingir el contracte.

En la tramitació de l'expedient, es donarà audiència a l'Adjudicatari perquè pugui formular al·legacions que estimi pertinents, i l'òrgan de contractació de BSM resoldrà.

Independentment de les penalitzacions aplicables, periòdicament la Direcció General de BSM el seu Comitè del Qualitat analitzaran les no conformitats als proveïdors, així com les corresponents respostes.

L'aplicació de les penalitzacions es realitzarà mitjançant el descompte a la factura.

2.7 Compliment Estàndards i Polítiques de BSM

BSM es regeix per un seguit de polítiques i procediments en l'àmbit de tecnologia orientats a garantir tant la qualitat com la correcta consecució i evolució dels projectes i serveis que governa.

Amb aquesta orientació, en els següents apartats es detallen els aspectes més rellevants a tenir en compte per a la correcta execució del contracte que l'adjudicatari haurà de respectar i s'obligarà a aplicar per alinear-se amb les bones practiques referides.

Si es considera necessari, durant l'execució del contracte, BSM posarà a disposició del adjudicatari aquells procediments complementaris que consideri rellevants.

L'adjudicatari ha de presentar en l'oferta com proposa aplicar aquestes polítiques i com s'alinearà amb els requeriments metodològics i tècnics de BSM, especificant amb claredat l'abast de les mateixes.

2.7.1 Gestió del Contracte

L'adjudicatari nomenarà un únic responsable del contracte com interlocutor per a la gestió del contracte; alhora BSM nomenarà un interlocutor únic.

Periòdicament, i a sol·licitud de BSM, es realitzaran reunions de seguiment i coordinació de l'objecte del contracte en el que és obligatòria la participació de l'adjudicatari.

2.7.2 Certificacions per proveïdors de serveis al núvol

BSM necessita la garantia que el licitador compleix amb les seves obligacions contractuals i regulatòries, i els licitadors han de proporcionar certificacions de tercers rigoroses per demostrar que compleixen amb les seves obligacions, especialment quan el proveïdor no permet avaluacions directes del client. Aquests han de basar-se en els estàndards de la indústria, amb àmbits clarament definits i la llista de controls específics avaluats. La publicació de certificacions i atestats (en la mesura permesa legalment) ajudarà molt a BSM a avaluar els proveïdors.

Les certificacions són activitats puntuals i per això els proveïdors han de mantenir actualitzat qualsevol resultat publicat o s'arrisquin a exposar riscos d'incompliment legal.

Els proveïdors del núvol hauran de:

- ✓ Comunicar clarament els resultats d'auditoria, certificacions prestant especial atenció a l'abast de les avaluacions.
- ✓ Quines característiques/serveis específics estan coberts en quines ubicacions i jurisdiccions.
- ✓ Com els clients poden implementar aplicacions i serveis que compleixin el marc legal i regulatori al núvol.
- ✓ Qualsevol responsabilitat i limitacions addicionals del client.
- ✓ Els proveïdors del núvol han de mantenir les seves certificacions / testimonis al llarg del temps i comunicar de manera proactiva qualsevol canvi a l'estat.
- ✓ Els proveïdors del núvol s'haurien d'involucrar en iniciatives contínues de compliment legal per evitar la creació de zones no cobertes i, per tant, riscos per a BSM.
- ✓ Proporcionar a BSM evidència i instruments comunament requerits de compliment legal, com ara registres d'activitat administrativa que el client no pot recol·lectar per si mateix.

2.7.3 Eines de suport al servei

BSM disposa d'eines corporatives per donar suport a la gestió i operació dels diferents serveis i projectes. En el cas d'identificar que per a portar a terme l'execució d'aquest contracte l'adjudicatari necessita accés a alguna d'elles, BSM donarà accés sense cost al adjudicatari als sistemes requerits.

L'adjudicatari haurà de fer us obligatòriament de les eines de suport que BSM consideri necessàries per a portar a terme l'execució d'aquest contracte.

B:SM, quan l'adjudicatari es trobi en les instal·lacions del BSM, proveirà a les persones que prestin els serveis:

- ✓ Ubicació física adequada per al desenvolupament i prestació dels serveis ubicats a les instal·lacions de BSM.
- ✓ Infraestructura per al suport de les eines corporatives i xarxa de comunicacions necessàries per la prestació del servei a les instal·lacions escollides per BSM.
- ✓ Telefonia fixa a les instal·lacions del servei.
- ✓ Accés a Internet a través de la xarxa d'àrea local, restringit als llocs de treball que ho requereixin així com a les adreces o pàgines web que siguin necessàries per al desenvolupament del servei.
- ✓ Connexió VPN, restringida a les necessitats del servei, per als casos en els que es consideri necessari (suport remot, etc).

BSM, quan l'adjudicatari presti el servei de forma remota, proveirà a les persones que prestin els serveis:

- ✓ Connexió VPN, restringida a les necessitats del servei, per als casos en els que es consideri necessari (suport remot, etc).
- ✓ Infraestructura per al suport de les eines corporatives i xarxa de comunicacions necessàries per la prestació del servei a les instal·lacions escollides per BSM.

B:SM no proveirà:

- ✓ Ordinadors de sobretaula, portàtils o ordinadors de mà (PDAs) amb sistema operatiu i programari habitual d'oficina, si no són requerits per a donar el servei contractat.
- ✓ Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de BSM, si se'n requereixen.
- ✓ Accés a Internet via GPRS, UMTS.
- ✓ Cap altre recurs no especificat explícitament.

En conseqüència, els adjudicataris hauran de:

- ✓ Subministrar tots elements de maquinari, programari i serveis i el seu manteniment durant la durada del contracte, que siguin necessaris per complir amb els requeriments del servei.
- ✓ Disposar d'un entorn (virtual) aïllat i d'us exclusiu pels serveis prestats a BSM i es requerirà l'esborrat complet dels mateixos quan es deixi de prestar el servei de manera individual o de part de l'adjudicatari a la finalització del contracte.
- ✓ Acceptar i respectar les polítiques de seguretat establertes per l'Àrea de Seguretat de la Informació de BSM.

- ✓ Permetre la supervisió dels equips per part de l'equip de Sistemes de BSM, si es consideres necessari.

B:SM es troba en procés de revisió i millora contínua que pot implicar la realització de canvis importants en el referent a les eines que s'hauran d'utilitzar per dur a terme l'execució del servei.

Per aquest motiu és imprescindible que l'adjudicatari tingui presents les següents consideracions en el referent a les eines de gestió i suport durant l'execució del contracte:

- ✓ BSM pot decidir la utilització de qualsevol tecnologia nova o evolució de les existents, relacionades amb la prestació del servei.
- ✓ Els adjudicataris es comprometen a assumir i adaptar-se a aquestes noves tecnologies i sistemes per donar el servei de suport, així com a participar activament en el procés de transició, formant i preparant el seu personal en aquestes noves tecnologies i sistemes implantats sense cost addicional pel BSM.

2.7.4 Gestió d'entorns

La implantació d'una nova aplicació requereix que aquesta romangui correctament configurada i provada en tots ens entorns operatius de BSM.

En termes generals, l'arquitectura de BSM disposa dels següents entorns:

Entorn de Desenvolupament o Test. És l'entorn que servirà per que els desenvolupadors desenvolupin i provin les noves funcionalitats.
Entorn d'Integració. Entorn comú on tots els desenvolupaments fan "commits" dels canvis del codi. L'objectiu d'aquest entorn es combinar i validar el treball de l'equip complet del projecte perquè pugui ser testejar abans de ser promogut.
Entorn de Preproducció. Es l'entorn que servirà per a provar les noves versions de codis desenvolupats en un entorn de codi i dades idèntic al de Producció i que ha de poder-se replicar tantes vegades com calgui a partir de l'entorn de producció, poder detectar errors abans de fer un canvi de versió a l'entorn de Producció i fer-lo quan es tinguin les garanties que s'han superat les proves necessàries. Aquest entorn serà un clònic de producció on desplegar tots els elements que formen el sistema.
Entorn de Producció. Correspon amb l'entorn productiu de les aplicacions de BMS on es troben les aplicacions que donen serveis als processos de negoci de l'organització. Aquest entorn, per sistemes crítics es troba distribuït en més d'un CPD.

BSM es reserva la potestat de modificar el número d'entorns operatius requerit en cas de necessitat i si el servei ho exigeix, quan això sigui requeriment crític per l'objecte del contracte.

L'adjudicatari es compromet a complir amb aquest estàndard i contribuir a que les aplicacions del seu àmbit estiguin implantades correctament als entorns operatius requerits.

2.7.5 Seguretat de la Informació de BSM

Tant l'empresa adjudicatària com el personal de l'adjudicatari s'haurà de sotmetre a les polítiques i regulacions internes que estableix l'Àrea de Seguretat de la Informació de BSM en matèria de seguretat de la informació, com a mínim, i no limitant-se a:

- ✓ Permetre i facilitar la realització d'auditories de compliment de les normatives establertes per Seguretat, internes o externes, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les accions fetes per l'auditor per facilitar el seguiment d'aquestes i els seus possibles impactes no desitjats.
- ✓ Permetre a BSM l'execució de revisions tècniques de seguretat (és a dir, les avaluacions de vulnerabilitat i/o proves de penetració) sobre els sistemes d'informació vinculats a la prestació del servei.
- ✓ Facilitar l'accés en qualsevol moment als equips i mitjans tècnics emprats pel personal de l'adjudicatari en les oficines del B:SM (sigui o no per l'exercici de la seva funció).
- ✓ Acceptar les normes i polítiques que estableix l'Àrea de Seguretat de la Informació de BSM tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions.
- ✓ Els equips, així com la informació resident dels mateixos serà sempre custodiada per BSM.
- ✓ Garantir l'estabilitat dels equips (reduint al mínim la rotació de personal)
- ✓ Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte (RGPD, ENS, CSA, ISO 27001;27017;27018, NIST).

A la finalització del contracte, l'adjudicatari quedarà obligat a la entrega o destrucció en cas de ser sol·licitada, de qualsevol informació obtinguda o generada com a conseqüència de la prestació del servei.

2.8 Garantia

L'adjudicatari haurà de garantir els productes i serveis derivats o inclosos en la present contractació per un període o termini de garantia de, com a mínim, un any, a partir de la data de recepció dels mateixos i acceptació de l'entrega –a través de l'acta de recepció del sistema– per part de BSM, obligant-se a fer els canvis necessaris per solucionar les deficiències detectades imputables a l'adjudicatari si així ho sol·licita BSM.

Aquesta garantia inclourà l'esmena d'errors o fallades ocults que es posin de manifest en el funcionament dels desenvolupaments o que es descobreixin mitjançant proves o qualsevol altre mitja. Els productes originats com a conseqüència de l'esmena d'errades s'hauran de lliurar a conformitat amb el que exigeix aquest plec.

Durant el període de garantia, totes les tasques de suport tècnic i consultoria necessàries per diagnosticar i resoldre els defectes ocorreguts aniran a càrrec de l'adjudicatari a cost zero.

En l'oferta s'adjuntaran les condicions específiques de la garantia proporcionada per l'empresa adjudicatària pel que fa als productes derivats o inclosos en la present proposta, especificant amb claredat l'abast de les mateixes.

2.9 Contingència i resiliència a fallades en entorns al núvol

Els licitadors hauran de proveir un pla de contingència, en cas de desastre de les instal·lacions principals, en unes instal·lacions alternatives (centre de gestió secundari) propietat del licitador, que inclouran:

- ✓ Estacions de treball amb el programari adequat per realitzar les tasques descrites.

- ✓ Comunicacions d'accés a les aplicacions informàtiques.
- ✓ Telefonia fixa a les instal·lacions del servei.
- ✓ Accés a Internet a través de la xarxa d'àrea local.
- ✓ Espai suficient per allotjar en condicions de treball òptimes:
  - ➢ El personal necessari de l'adjudicatari per realitzar el servei i
  - ➢ Personal de BSM, o de terceres parts determinades per aquest.

Pla i execució de proves per validar la solució de contingència implementada, amb la periodicitat que el BSM determini.

Les instal·lacions i equipament haurà de ser suficient per garantir la continuïtat dels serveis de BSM durant l'existència de la causa que doni lloc a la contingència.

Per garantir la màxima resiliència del servei, el proveïdor del servei SaaS haurà d'habilitar múltiples "zones" on poder implementar màquines virtuals dins d'un grup auto-escalable, que abasti centres de dades físicament diferents, millorant la disponibilitat total del servei. O oferir a BSM un servei amb repartiment de càrrega entre les zones, de manera que, si una zona sencera es perd, el servei roman actiu.

2.10 Confidencialitat

L'Adjudicatari 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 BSM.

L'Adjudicatari serà responsable de les violacions del deure de secret que es puguin produir per part del personal 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 del personal participant en el desenvolupament del contracte.

L'adjudicatari no podrà fer ús de la informació que es subministra en la documentació d'aquest concurs per a altres fins que la seva utilització per l'elaboració de les corresponents ofertes, no podent traslladar el seu contingut o còpia dels mateixos a tercers.

Es prohibeix expressament la utilització d'anàlisi funcionals o de requeriments en benefici propi de les persones físiques o jurídiques que retirin tal documentació annexa als presents plecs, en cas que existís.

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

2.11 Codi Font i Propietat intel·lectual

La propietat intel·lectual dels treballs realitzats a l'empara d'aquest contracte pertany a BSM, de forma exclusiva respectivament. Els desenvolupaments, productes o subproductes derivats, no podran ser utilitzats sense la deguda autorització prèvia.

Per tant BSMSA, restarà com a propietari respectivament dels fonts realitzats, sense cap dret per part de l'Adjudicatari.

L'adjudicatari renuncia expressament a qualsevol dret que pugui correspondre-li sobre els treballs realitzats com a conseqüència de l'execució del present contracte i no podrà fer cap ús o divulgació dels estudis i documents utilitzats o elaborats sobre la base d'aquest plec de condicions, bé sigui en forma total o parcial, directament o extractada, original o reproduïda, sense autorització expressa de BSM respectivament.

L'accés a la informació i/o productes protegits per la propietat intel·lectual, propietat de BSM, necessaris per al desenvolupament del servei contractat, no pressuposa en cap cas la cessió de la mateixa.

L'Adjudicatari accepta expressament que els drets d'explotació dels productes derivats d'aquest plec correspon única i exclusivament a BSM. Així doncs, el contractat cedeix, amb caràcter d'exclusivitat, la totalitat dels drets d'explotació dels treballs objecte d'aquest plec, inclosos els drets de comunicació pública, reproducció, transformació o modificació i qualsevol d'altre dret susceptible de cessió en exclusiva, d'acord amb la legislació sobre drets de propietat intel·lectual.

No obstant, si se'n deriva algun dret d'autor o inalienable pel seu autor, l'adjudicatari s'obliga a fer una cessió/transmissió de drets en exclusiva a favor de BSM, per temps indefinit, sense que aquest fet li doni dret a reclamar cap import en concepte de compensació i/o indemnització per aquest concepte.

2.12 Devolució del servei

Les dades emmagatzemades en l'eina seran propietat exclusivament de BSM i aquest podrà sol·licitar copies de les dades en qualsevol moment.

Un cop es finalitzi el servei, l'adjudicatari estarà obligat a retornar tots els documents dels projectes i/o serveis degudament actualitzats i formatejats, com també a la realització de documentació addicional i sessions de formació o d'acompanyament necessàries al nou proveïdor o en el seu defecte a B:SM 30 dies abans de finalitzar el contracte.

Les tasques d'acompanyament a la transició descrites anteriorment seran realitzades entre els 3 mesos previs a la finalització del contracte i els 3 mesos posteriors a la finalització del contracte, sense càrrec addicional per a BSM.

En cas que BSM ho sol·liciti, l'adjudicatari quedarà obligat a eliminar de forma permanent les dades emmagatzemades als seus sistemes d'informació.

2.13 Compliment GDPR, ISO 27017 ISO 27018

La certificació ISO 27017, ratificada el 01 d'abril de 2021, és un codi de bones pràctiques en controls de seguretat de la informació basats en la norma ISO 27002 pels serveis en el núvol. Aquesta norma s'uneix a l'anterior ISO / IEC 27001 i ISO / IEC 27002 en l'àmbit de gestió de la seguretat de la informació i que es dirigeix específicament als proveïdors de serveis de núvol.

L'adjudicatari estarà obligat a respectar el caràcter confidencial de tota aquella informació a la qual tingui accés per a l'execució del contracte, incloent aquella qualificada com a confidencial en aquest contracte, o aquella en la que la seva confidencialitat sigui indicada per BSM o bé aquella que per la seva pròpia naturalesa hagi de ser tractada com a tal. Aquest deure de

confidencialitat es mantindrà durant un termini mínim de 5 anys després de la finalització del contracte.

L'adjudicatari declara conèixer, i s'obliga al compliment d'allò previst en la Regulació General de Protecció de Dades (RGPD), publicada el 25 de maig de 2018, i la norma ISO 27018, publicada el 29 de Juliol del 2014, en el que respecta a la Protecció de Dades de Caràcter Personal així com a les restriccions descrites en aquest apartat.

2.13.1 CPD cloud i la Protecció de Dades Personals

La Regulació General de Protecció de dades (GDPR), és vinculant per a qualsevol corporació que processi les dades de ciutadans de la UE, i estarà sota la jurisdicció a l'autoritat de supervisió de dades o els tribunals de l'estat membre que tinguin la relació més estreta amb les persones o entitats que manegen aquestes dades personals.

GDPR s'aplica al tractament de dades personals en el context de les activitats d'un establiment a la UE/EEE d'un controlador o processador, independentment de si el processament es duu a terme a la UE/EEE o no.

Per complir amb la normativa de protecció de dades GDPR cal que es compleixin els següents apartats:

- ✓ Prohibida la transferència de dades personals fora de la UE/EEE a països que no ofereixen un nivell similar de protecció de dades personals i drets de privadesa.

- ✓ Quan l'adjudicatari hagi patit una bretxa de la seguretat, haurà de notificar amb informes basats en el risc i dels diferents requisits necessaris per informar l'incompliment a l'Autoritat de Supervisió de les dades afectades per la bretxa. Les infraccions han de ser reportades dins de les 24 hores posteriors a què la companyia conegui l'ocurrència de l'incident.

- ✓ L'adjudicatari serà el controlador de les dades que se'ls han confiat. Com es va veure anteriorment, nombroses lleis, regulacions i contractes prohibeixen, restringeixen i limiten la revelació i transferència de dades a un tercer.

- ✓ Qualsevol incompliment de la normativa de GDPR i condicions descrites anteriorment poden donar peu a l'aplicació de les penalitzacions establertes entre B:SM i l'adjudicatari.

2.14 Compromís de compliment de l'ENS (Esquema Nacional de Seguretat) i ISO 27001

El Reial decret 311/2022, de 3 de maig, regula l'Esquema Nacional de Seguretat (ENS).

L'objectiu de l'ENS és establir la política de seguretat en la utilització de mitjans electrònics i està constituït per principis bàsics i requisits mínims que permetin una protecció adequada de la informació a través de mesures per a garantir la seguretat dels sistemes, les dades, les

comunicacions i els serveis electrònics, que permeti als ciutadans i a les administracions públiques, l'exercici de drets i el compliment de deures a través d'aquests mitjans.

BSM, sol·licitarà a tots els seus licitadors el compliment de l'ENS amb una certificació de categoria MITJA com a mínim en tots els serveis que prestin a BSM, per a garantir l'accés, integritat, disponibilitat, autenticitat, confidencialitat, traçabilitat i conservació de les dades, informacions i serveis utilitzats en mitjans electrònics que gestionin en l'exercici de les seves competències.

Tots els licitadors que vulguin presentar-se a les ofertes públiques de BSM, hauran d'acreditar l'obtenció del certificat de l'ENS de nivell MITJÀ com a mínim i estar vigent, per als serveis prestats a BSM. Tot i això, es consideraran les moratòries establertes per la legislació vigent en el moment de la licitació.

L'ISO/IEC 27001 és un estàndard per a la seguretat de la informació aprovat i publicat com a estàndard internacional l'octubre de 2005 per la "International Organization for Standardization" i per la "International Electrotechnical Commission".

El compliment de l'ISO/IEC 27001, estableix un Sistema de Gestió de la Seguretat de la Informació (SGSI), aquest estableix un mètode de com implementar, operar, monitorar, revisar, mantenir i millorar la seguretat de la informació de cadascuna de les organitzacions garantint la gestió i el control dels riscos de la seguretat de la informació sobre els actius crítics per al negoci.

BSM, valorarà molt positivament que els licitadors acreditin la certificació a la norma ISO 27001.

2.15 Revisions tècniques de seguretat

L'adjudicatari estarà obligat a incorporar les revisions tècniques de seguretat (és a dir, les avaluacions de vulnerabilitat i/o proves de penetració) per posar remei a les vulnerabilitats que puguin suposar un risc per al negoci o un risc per als clients, abans de la seva publicació.

L'adjudicatari haurà de posar remei mitjançant mesures tècniques i processos de negoci de suport per a la detecció primerenca de vulnerabilitats dins dels components dels sistemes i les xarxes de la infraestructura propietat de l'organització (físics o virtuals) o de les aplicacions gestionades, aplicant un model basat en riscos que prioritzi la mitigació mitjançant un control de canvis, pegats del fabricant, canvis en la configuració o desenvolupament segur de programari de la pròpia organització. Haurà d'informar, a petició de BSM d'aquestes polítiques i procediments, especialment si es fan servir dades de BSM.

Es valorarà positivament que la solució permeti detectar monitorització de qualsevol tipus de transferència de dades, podent implementar una solució de Cloud Access and Security Brokers (CASB), eina que permetrà a BSM descobrir l'ús intern de serveis de núvol utilitzant diversos mecanismes com ara monitoratge de xarxa, consultes DNS, activitat dels serveis permesos a través de connexions API (quan estiguin disponibles) i DLP per gestionar de millor manera l'ús de dades sensibles.

2.16 Política ambiental

L'Adjudicatari resta obligat a treballar d'acord amb la Política Ambiental de BSM fent un ús racional dels recursos naturals i gestionant, correctament, els residus.

Els residus, sòlids o líquids, s'hauran de separar per fraccions i gestionar, correctament, mitjançant un gestor autoritzat per la Generalitat de Catalunya. Caldrà comunicar a BSM els gestors escollits i aportar la documentació relativa a la gestió de residus: fulls de seguiment de residus, fitxa d'acceptació (en cas que sigui necessari), així com altra informació que BSM puguin demanar per tenir constància d'aquesta gestió.

2.17 Compromís de prevenció de riscos laborals

D'acord amb la Llei 54/2003, de 12 de desembre, de reforma del marc normatiu de la prevenció de Riscos Laborals i pel Real Decret 171/2004, de 30 de gener, que desenvolupa l'article 24 de la Llei 31/1995, de 8 de novembre, de prevenció de Riscos Laborals, l'adjudicatària està obligada al compliment de la normativa vigent en matèria de prevenció de riscos laborals i en aquest sentit, s'obliga a lliurar a BSM la documentació següent:

- ✓ Avaluació dels riscos relacionats amb l'activitat que tingui previst realitzar.
- ✓ Pla de prevenció pel control dels riscos detectats.
- ✓ Mesures de prevenció i protecció que el personal de BSM haurà de tenir en compte davant d'aquests riscos.
- ✓ Llistat de treballadors que accediran a les instal·lacions.
- ✓ Justificants de la formació dels treballadors conforme han estat informats dels riscos als quals estan exposats i de les mesures de protecció que han de tenir en compte.
- ✓ Informes d'aptitud d'aquests treballadors en relació a les tasques que han de realitzar. Contracte amb la Entitat Asseguradora d'Accidents de Treball i Malaltia Professional.
- ✓ Justificants de lliurament d'equips de protecció individual als treballadors.
- ✓ BSM s'obliga a lliurar a l'adjudicatari la documentació corresponent a la prevenció, en relació a la Instal·lació, i és la següent:
  - ➢ Avaluació dels riscos relacionats amb els llocs on tingui previst realitzar l'activitat.
  - ➢ Pla de prevenció per al control de riscos detectats.
  - ➢ Mesures de prevenció i protecció que el personal del Promotor haurà de tenir en compte davant d'aquests riscos.

2.18 Auditoria

Els adjudicataris hauran de reconèixer el dret de BSM per examinar per mitjà d'auditors, externs o propis, el fidel compliment dels treballs per ells prestats i el compliment de les condicions d'execució.

BSM tindrà dret a dur a terme auditories de les activitats dels adjudicataris per assegurar-se que l'execució dels treballs es porta d'acord amb el que estableix el present Plec.

Tot el material i informació requerida per aquestes inspeccions i auditories pels representants de BSM o els seus representants estarà disponible sense restriccions.

BSM notificarà a l'adjudicatari amb dues setmanes d'antelació l'auditoria i amb un dia d'antelació la inspecció a realitzar, i l'adjudicatari tindrà l'obligació de:

- ✓ Facilitar l'accés al material sol·licitat pel grup auditor.
- ✓ Designar persones responsables que acompanyin els auditors.
- ✓ Facilitar un entorn de treball adequat a la mateixa ubicació en què té lloc l'auditoria.
- ✓ Cooperar amb l'auditor.
- ✓ Participar en les reunions que convoqui l'auditor.
- ✓ Analitzar les dades trobades perquè l'informe sigui real.
- ✓ Emprendre ràpidament accions correctores i / o preventives.
- ✓ Emetre una resposta oficial als defectes dels que ha informat el grup d'auditors.