

PLEC DE PRESCRIPCIONS TÈCNIQUES PER AL CONCURS
OBERT:

SUBMINISTRAMENT EN MODALITAT D'ARRENDAMENT AMB
OPCIÓ DE COMPRA DEL MAQUINARI I PROGRAMARI BASE
DEL CPD DE L'INSTITUT D'ASSISTÈNCIA SANITÀRIA

CONTR20250000000100

1 OBJECTE I ABAST DE L'EXPEDIENT ADMINISTRATIU

1.1 OBJECTE DEL CONTRACTE

L'objectiu del present contracte es el subministrament, en modalitat d'arrendament amb opció de compra, del maquinari i programari base, i el seu manteniment, del centre de processament de dades de l'Institut d'Assistència Sanitària (IAS).

1.2 ABAST DEL SERVEI

L'abast del subministrament és el següent:

- El subministrament per a la renovació de la infraestructura TIC de l'IAS considerada com a equips de còmput, emmagatzematge i llicenciament de programari de virtualització.
- La provisió d'un sistema d'emmagatzematge replicat per a backups que millori el rendiment d'aquest, la seguretat i la disponibilitat de les dades. Així mateix, la renovació de les del software de còpies emprat pel IAS, (Veeam Backup).
- La substitució de la infraestructura de firewall perimetral per un model més avançat i modern que permeti tenir suport del fabricant a més llarg termini.
- Subministrament de sistema NAS per a emmagatzematge secundari de dades.
- La renovació d'un conjunt de llicències i manteniments de maquinari que seran detallats més endavant que permetran la continuïtat dels serveis TI.
- Els serveis de posada en marxa i adequació dels sistemes segons un disseny que es definirà més endavant en aquest document.

Com a norma general, tots els suports, manteniments, i llicències objecte d'aquesta licitació, tindran una data de coterminació a 31/12/2030, llevat de dues excepcions:

- Llicenciament de Hypervisor Vmware VSphere, que serà a dos anys.
- Manteniment de cabina HPE Nimble existent, que només s'ampliarà per garantir la migració fins al 31/12/2026.

1.3 TERMINI I IMPORT DE LICITACIÓ

El termini d'execució del contracte serà per cinc anualitats contractuals (arrendament de 60 mesos) i que afecta a cinc exercicis pressupostaris.

L'import màxim de licitació serà de **727.532,36 €** (IVA no inclòs); PVP de l'iva (21%) 152.781,80 €.

L'import del subministrament i els mòduls i conceptes relatius a les hores, consten desglossats a la Taula de Determinació del Preu en arxiu adjunt a aquest Plec de Prescripcions Tècniques.

El subministrament en modalitat d'arrendament inclou l'opció de compra per import màxim de 100 €.

En cas que l'empresa contractista vulgui transmetre els drets de cobrament, haurà d'actuar d'acord amb el que diu l'article 200 de la LCSP.

2 CONDICIONS GENERALS

El present plec de prescripcions tècniques particulars és d'aplicació conjunta amb el plec de clàusules administratives. **De manera complementària i subsidiària, i en tant no s'oposi al present plec serà d'aplicació el contingut de l'oferta dels licitadors.**

3 ESPECIFICACIONS TÈCNIQUES DEL SUBMINISTRAMENT

3.1 DESCRIPCIÓ DE LA INFRAESTRUCTURA ACTUAL

L'IAS a Salt, utilitza per a l'exercici i compliment de les seves funcions, un conjunt d'aplicacions i sistemes d'informació que estan suportats sobre una infraestructura TIC pròpia, gestionada mitjançant virtualització basada en **VMware vSphere**. Aquesta infraestructura està protegida mitjançant l'alta disponibilitat pròpia (per a hipervisor, servidors i emmagatzematge) i per les còpies de seguretat que es realitzen periòdicament sobre una altra infraestructura físicament diferent a la de producció.

Aquesta infraestructura TIC està suportada en l'actualitat en dos "clúster" de virtualització diferenciats i de fabricants diferents.

Cada clúster està format per quatre nodes ESXi respectivament, governats per un servidor vCenter. L'emmagatzematge d'ambdós clúster procedeix d'una cabina Nimble AF-40 connectada per FC, en aquest emmagatzematge resideixen totes les màquines virtuals de l'entorn de producció amb una ocupació del 60% de l'espai.

La connectivitat FC es realitza mitjançant tres switch fabric. Dos d'aquest switch donen servei a la connexió SAN del CPD de producció per accés a la cabina existent. El tercer switch es troba a un segon CPD, proporcionant connectivitat FC a tota la infraestructura de backup, amb connexió cap al CPD principal per a l'execució de còpies de seguretat més àgils. Els switchs de producció tenen llicenciades tots els ports, el tercer dedicat al CPD de Backup, té 8 ports llicenciats.

Quant a la infraestructura de backup, consta d'un servidor físic dedicat per al programa de còpies Veeam Backup & Replication, el qual realitza les còpies de totes les màquines virtuals de la infraestructura a diferents destinacions de còpia que són, dues cabines d'emmagatzematge addicionals (MSA); la primera de repositori principal de còpia i la segona de backup copy; aquestes últimes envien les dades a una unitat de cintes MSL amb dues unitats LTO; cadascú amb una retenció configurada diferent per complir amb els punts de recuperació. Tots els sistemes d'emmagatzematge dedicats a backup es connecten pel protocol FC.

Per necessitats d'augment de la capacitat i actualització dels seus sistemes i seguint la seva planificació de gestió de la capacitat, l'IAS **precisa renovar les capacitats de la seva infraestructura TIC actual**, actualitzant-la i dotant-la de noves i més segures funcionalitats i, així, donar resposta al creixement orgànic dels serveis i sistemes suportats per l'organització. La infraestructura proporcionada seguirà allotjada físicament en les seves pròpies instal·lacions tècniques o CPDs per motius de criticitat dels serveis, de seguretat i de protecció de dades.

Es busca, per tant, una plataforma de virtualització, que permeti a l'Hospital disposar d'alta disponibilitat reduint la complexitat tant tècnica com administrativa, amb un únic fabricant i períodes de garantia comuns.

A més, es necessita l'adquisició d'un dispositiu d'emmagatzematge dedicat com a destinació de backup per tal de garantir la disponibilitat, protecció i recuperació de les dades hospitalàries. És fonamental comptar amb una solució d'emmagatzematge dedicada que ofereixi capacitats avançades de suport i eficiència en el maneig de grans volums d'informació.

Adicionalment, es pretén renovar la infraestructura de seguretat perimetral que actualment està en producció.

En l'actualitat, el client disposa de diversos firewalls del fabricant FGT, cadascun dels quals compleix un rol en l'arquitectura del client:

- **Firewall de segmentació interna:** Format per un clúster en HA actiu-passiu de dos FGT600E, amb llicències UTP fins el 03/12/2025.
- **Firewall perimetral:** Format per un clúster en HA actiu-passiu de dos FGT100F, amb llicències UTP fins 03/12/2025 (membre 1) i 14/02/2027 (membre 2).
- **Firewall terminador de VPN:** Format per tres firewalls 100F en standalone balancejats que donen servei VPNSSL via web per a usuaris interns i túnel per a proveïdors, amb llicències FortiCare fins a 08/12/2025.

Tot el parc de firewall es gestiona per una consola de gestió **FortiManager** on-premise amb llicències perpètuas per a 10 dispositius fins a 03/05/2026.

A més dels firewalls, IAS disposa dels següents serveis addicionals de Fortinet:

- **FortiAnalyzer:** On s'emmagatzemen els logs de tots els firewalls, amb una llicència en subscripció per a 25 GB/dia i data de vigència fins a 03/12/2026.
- **FortiAuthenticator:** Que actua com a servidor RADIUS per al servei VPNSSL proporcionant doble factor (via mail o token mobile) i una llicència perpètua per a 4200 usuaris i data de suport FortiCare fins a 09/10/2028.
- **FortiToken Mobile:** Configurats al FAC per dotar de doble factor via token en les autenticacions VPNSSL dels usuaris amb mòbil corporatiu, en total es disposa de 200 FortiToken.
- **FortiClient EMS:** Per comprovar la postura dels usuaris amb PC corporatiu en les connexions VPNSSL, aquest llicenciat en la modalitat SaaS per subscripció amb una llicència per a 25 usuaris i vigències fins a 22/05/2027.

En aquest context s'inicia un expedient de licitació per treure a concurs públic el subministrament (en modalitat d'arrendament), posada en marxa d'una nova infraestructura TIC per a l'Hospital, els serveis de migració dels aplicatius a la nova infraestructura, així com el suport de la mateixa durant el període de vida del contracte.

Els objectius que es pretenen amb la present licitació són per tant els següents:

- **Infraestructura de Còmput:** Disposar d'una nova plataforma de virtualització a través d'una solució de nova generació, amb l'última tecnologia disponible en el mercat, que proporcioni a IAS les capacitats de computació suficients per a execució dels servidors virtuals de l'hospital en alta disponibilitat, a més de simplificar l'aprovisionament i la gestió del cicle de vida de la infraestructura i els servidors virtuals.
- **Infraestructura SAN d'emmagatzematge de dades::** Disposar de capacitats d'emmagatzematge de dades per a l'entorn de virtualització suficients, amb escalabilitat i funcions d'eficiència de consum d'espai en disc, a més de

funcionalitats que permetin garantir la seguretat, la integritat i la disponibilitat de les dades.

- **Dispositiu d'emmagatzematge per a còpies de seguretat:** La solució ha de ser capaç de proporcionar una deduplicació i compressions òptimes per maximitzar la utilització de l'emmagatzematge, alhora que minimitza els costos operatius i els temps de recuperació. Així mateix, s'espera que ofereixi resiliència, alta disponibilitat i opcions d'escalabilitat per satisfer tant necessitats actuals com el creixement futur de l'organització.
- **Dispositius NAS per a emmagatzematge d'imatges i vídeo:** Actualment, aquestes dades són emmagatzemades en discs locals i es persegueix millorar la redundància, integritat i seguretat de les dades.
- **Equipament de seguretat perimetral:** Mantenir el rol actual de cadascun dels firewalls, però dotant de majors recursos al core de la infraestructura per seguir cobrint les necessitats actuals i possible creixement futur.
- **Llicenciament de programari:**
 - Renovació de llicències de Veeam Backup and Replication
 - Adquisició de llicències de Hypervisor VMware
 - Renovació de llicències de RedHat Enterprise
- **Manteniments de Maquinari:**
 - Es demana la renovació del manteniment maquinari del fabricant de divers material que serà detallat a l'apartat corresponent
- **Serveis d'instal·lació**
 - Instal·lació de tota la infraestructura ofertada
 - Serveis de migració cap a la nova infraestructura proposada tant en la part de còmput emmagatzematge, backup i seguretat perimetral.

3.2 DESCRIPCIÓ DE LA INFRAESTRUCTURA A INCORPORAR I IMPLANTAR

Es demana el subministrament, instal·lació i configuració d'una plataforma de virtualització per a l'IAS, que permeti executar els servidors virtuals allotjats al centre de dades de producció i concentri les càrregues de les dues granges de virtualització que actualment les allotgen.

Per a això, la solució proposada haurà d'estar basada en una **plataforma de virtualització, emmagatzematge i backup d'un únic fabricant** i que haurà de ser compatible amb VMware VSphere, que és el hypervisor emprat per l'AS.

Haurà de comptar també amb funcionalitats avançades d'optimització de la dada i oferir alta resiliència, alta disponibilitat i escalabilitat.

Adicionalment, de cara la modernització i evolució dels serveis TI de l'IAS, es subministraran nous equips de seguretat perimetral, sistemes d'emmagatzematge NAS per arxivat d'imatges i vídeos per a diagnòstic a més de renovació de llicenciament i suport que es detallarà més endavant.

A continuació, es detallen els **requisits mínims d'obligat compliment** que han de complir les solucions proposades. Aquestes solucions hauran d'abordar de forma integral l'objecte de la licitació a través d'infraestructures maquinari i programari que proporcionin al IAS les característiques i funcionalitats mínimes requerides. Tot

l'equipament que s'inclogui amb les propostes ha de ser nou de fàbrica i en cap cas s'inclouran components remanufacturats o sense garantia directa del fabricant.

3.2.1 Requeriments mínims de còmput

Subministrament de **sis servidors** en format rack d'1U, compatibles amb fins a 8 discos SFF (Small Form Factor), per instal·lar en centre de dades. Les característiques tècniques mínimes requerides per a cada equip són:

- Característiques generals del servidor
 - Factor de forma: Rack 1U, capacitat d'allotjar mínim 8 discos SFF (2,5").
 - Tots els components y accessoris necessaris per a la integració física en rack estàndard (kit de rails inclòs).
 - Bezel o sistema de bloqueig davanter inclòs.
- Processador
 - Dos processadors d'arquitectura x86 compatibles amb instruccions Intel Xeon d'última generació.
 - Cada processador ha de disposar d'almenys 16 nuclis físics, freqüència base de 3,20 GHz, mínim 72 MB de caché L3 y un TDP màxim de 190W.
- Memòria RAM
 - 768 GB de memòria RAM, tecnologia DDR5 RDIMM, arquitectura de doble canal (2R), velocitat mínima de 6400 MT/s.
 - Configuració: 8 mòduls de 96 GB cadascun.
- Emmagatzematge primari (arrencada del sistema operatiu)
 - Controladora interna compatible amb RAID per a dispositius NVMe PCIe.
 - Dos dispositius SSD NVMe de mínim 480 GB cadascun, configurats en RAID 1 (mirall) per a l'arrencada del sistema operatiu.
- Comunicacions i connectivitat
 - Targeta de xarxa Ethernet que proporcionï almenys 2 ports SFP+ compatibles amb 10 GbE (mínim estàndard IEEE 802.3ae).
 - Adaptador Fibre Channel amb almenys 2 ports de 32 Gb/s, compatible amb estàndard FC-NVMe
- Gestió remota i administració
 - Cada servidor ha d'oferir un sistema/controladora de gestió remota del sistema integrada a l'equip amb redirecció gràfica independent de les CPU de producció. S'haurà d'incloure el corresponent programari de consola de KVM virtual, amb les funcionalitats següents:
 - Gestió mitjançant interfície web HTML5
 - Seguretat basada en rols, amb accés que suporti two-factor authentication
 - Llistat dels components del servidor i descripció de l'estat dels mateixos
 - Accés remot a l'estat i logs integrats del servidor
 - Regulació dinàmica d'energia de servidor i gràfics 3D de temperatura

- Apagada i encesa remota, independentment del sistema operatiu
- Muntar remotament carpetes, CDs, DVDs, floppy, USBs, etc
- Suportar monitorització SNMP sense necessitat d'agents al sistema operatiu
- Enviament d'esdeveniments a servidor syslog y sincronització NTP
- Suportar automatització mitjançant una API Rest conforme amb Redfish
- Pantalla de nivell de desgast NVMe
- Llicència de gestió avançada inclosa per a la solució d' administració remota compatible amb el maquinari ofert.
- La targeta de gestió (i SW associat) haurà de venir activada i totalment operativa per a cada node, tenint el servidor un port dedicat 1GbT RJ45 per a aquest fi.
- Serveis i programari de gestió
 - Els servidors proposats han de tenir accés a una consola nativa Cloud (SaaS) per a la gestió d'un nombre il·limitat de servidors, amb un dashboard comú per la gestió de múltiples servidors
 - Aquesta eina ha de ser verdaderament nativa Cloud (SaaS), i per tant no en caldrà configuració, actualització i aplicació de pegats durant tot el cicle de vida del contracte, i ofert com a servei.
 - L'eina haurà de poder tenir accés de forma orgànica tant a la gestió dels servidors proposats com a la gestió de la plataforma de cabines, de forma que es pugui passar de la gestió d'una part a l'altra des de la mateixa consola. Això també aplica per a la gestió d'usuaris/permisos d'ambdós plans.
 - Les funcionalitats que ha d'oferir a nivell de gestió de cicle de vida dels servidors són:
 - Actualitzacions de micro-codi intel·ligents, només pels deltes entre versions
 - Gestió de micro-codi per grups de servidors sota demanda o de forma programada
 - Actualització de micro-codi dels servidors en sèrie o paral·lel, amb opció de parar en cas d'error
 - Actualització automàtica dels servidors a una base definida de micro-codi
 - Actualització del micro-codi del sistema/controladora de gestió dedicat, de forma automàtica o sota demanda
 - Validació de compliment de nivell de micro-codi, en base a nivells base definibles de forma grupal
 - Desplegament d'imatges de sistema operatiu.
 - Informació en temps real de consum energètic així com el càlcul estimatiu de les emissions en CO2

- A nivell de suport:
 - Creació automàtica de casos de suport al fabricant per les falles crítiques, així com notificació de les mateixes tant per correu electrònic com en in-app
 - Informes sota demanda de compliment dels nivells de micro-codi
 - Capacitat de fer seguiment dels registres d'auditoria en servidors individuals
 - Consola al sistema/controladora de gestió dedicat de cada servidor, via HTML5
 - Suport per exportar el llistat inventari dels servidors
 - Generació d'informes agregats de consum energètic, així com petjada de CO2
 - Integració amb eines d'agregació d'incidències i ticketing, com ServiceNow
- Alimentació i refrigeració
 - Doble font d'alimentació redundant, intercanviable en calent, de mínim 1000W cadascuna i certificació energètica Titanium (ha de complir la normativa EU ERP Lot9)
 - Ha d'incloure tots els ventiladors i dissipadors necessaris per a funcionament en condicions de càrrega màxima i entorns de centre de dades.
- Altres elements
 - Ha d'incloure kit de rails per a integració en rack estàndard de centre de dades.
 - Sistema de bloqueig físic frontal (bezel lock o equivalent).
 - Tots els elements i cables necessaris per a la connexió i ús dels equips.
- Garantia i suport
 - Garantia estesa del fabricant de 5 anys, que cobreixi peces, mà d'obra i desplaçament in situ amb temps de resposta al següent dia laborable (NBD), cobertura mínima 9x5.
- Altres:
 - El servidor haurà de proporcionar una arrel de confiança de silici a nivell maquinari, creant una empremta digital immutable que permeti garantir que el servidor no arrencarà amb nivells de firmware que no coincideixin amb aquesta empremta.
 - El sistema, durant la seva operació, haurà de realitzar una validació periòdica dels nivells de firmware en recerca de codi compromès. En cas que es produeixi una infracció, es durà a terme una restauració automàtica a un estat de confiança conegut. Aquesta capacitat de restauració automàtica haurà d'incloure com a mínim els components essencials de firmware del servidor: xip

de gestió, UEFI, CPLD (system programmable logic) i SPS (server Platform services).

- S' hauran d' incloure els transceiver i cables necessaris per connectar tant a la xarxa de producció com al sistema d' emmagatzematge SAN.

Les referències a marques, noms comercials i models concrets de components s' han d'entendre únicament com a referència de nivell de prestacions. S'acceptarà qualsevol proposta que compleixi igual o superior nivell tècnic i funcional.

Tots els equips hauran d' estar homologats per al seu funcionament en entorns de centre de dades professional i ser compatibles amb Vmware Vsphere en les seves últimes versions.

3.2.2 Requisits mínims del sistema d'emmagatzematge.

La cabina d' emmagatzematge principal tindrà les següents característiques:

- **Elements bàsics**

- Haurà d' estar totalment redundada i no disposarà de punts únics de fallada. Haurà d' estar configurada segons les millors pràctiques del fabricant.
- Haurà de disposar almenys de dues controladores o elements de processament de la dada independents, que no faran ús de bateries ni elements tipus supercapacitadors per protegir la informació en cas de fallida elèctrica. El licitador haurà de justificar documentalment com realitza la protecció de les dades escrites mantenint la seva integritat en cas de pèrdua d'alimentació elèctrica.
- Disposarà almenys 32 cores de procés i 512GB de memòria entre ambdues controladores o elements de processament de la dada.
- El sistema ha d'incorporar com a mínim la següent connectivitat per controladora, 4 ports FC de 32Gbps amb un mínim de 2 SFPs per controladora.
- La tecnologia de disc utilitzada haurà de ser SSD NVME, i no hauran de suportar cap altre tipus de disc.
- Atesa la criticitat de les aplicacions que s' executaran, la solució d' emmagatzematge proposada haurà de disposar d' una certificació de disponibilitat del 100%. Aquesta certificació haurà d'estar disponible i accessible en el lloc web públic del fabricant de la solució i haurà d'incloure's juntament amb la proposta.
- El llicenciament serà de tipus "tot inclòs", per la qual cosa no hauran d'existir funcionalitats pròpies de la solució d'emmagatzematge que no estiguin incloses amb la proposta.
- Haurà de ser compatible amb els sistemes operatius estàndard de mercat. Com a mínim amb VMware ESXi 7/8, Windows Server 2019/2022, Red Hat Enterprise Linux i Suse Linux Enterprise Server (SLES).

- Certificació i integració amb la darrera versió de Veeam. Detallar el grau d'integració.

- **Capacitat, escalabilitat, rendiment, protecció de la informació i connectivitat**

- Es requereixen almenys 33,96TiB nets usables a nivell d'infraestructura, en una configuració de doble paritat i espai spare igual a la capacitat d'un disc. Aquesta mesura mínima ha de ser abans d'aplicar eficiències. L'emmagatzematge haurà d'utilitzar tecnologies d'eficiència de la dada (Compressió i deduplicació) que assegurin un mínim de 2.0:1
- Tots els discs del sistema d'emmagatzematge han de ser de tecnologia SSD i comptar amb connectivitat NVMe. Tots els discs proposats seran iguals i de la mateixa mida, els discs han de ser TLC o equivalent i no s'acceptaran discs QLC o equivalent.
- Almenys 163.000 IOPS en lectures/escriptures (60/40) en blocs de 16k aleatòria. 415.000 IOPS en lectures en blocs de 16k i 85.000 IOPS en escriptura en blocs de 16k.
- Per maximitzar el rendiment de la solució proposada i la durabilitat dels discs SSD NVMe, cada sistema d'emmagatzematge haurà de ser capaç de distribuir tots els volums entre tots els discs que componguin la solució. És a dir, qualsevol volum creat a cada cabina haurà d'estar distribuït entre tots els discs que la conformen. No s'acceptaran solucions basades en pools diferenciats de discs, per exemple, per a aprovisionament de volums i snapshots.
- La informació haurà d'estar protegida per un sistema RAID de doble paritat (RAID6) o superior, que permeti almenys la fallida simultània de dos discs. Igualment haurà de comptar amb un espai de spare equivalent almenys a la mida total d'un dels discs. Aquest espai de spare estarà distribuït entre tots els discs que conformen la solució i en cap cas no haurà de ser un disc dedicat.
- Addicionalment, s'haurà d'incorporar un sistema per evitar les corrupcions silencioses de les dades basat en el càlcul de hashs criptogràfics, que permetrà protegir dels següents escenaris: escriptures perdudes (no consolidades a disc), escriptures redirigides (consolidades però en una posició errònia) i lectures redirigides (lectures d'una posició incorrecta).
- El sistema d'emmagatzematge proposat haurà de disposar d'almenys 10 slots destinats a disc lliures i podrà escalar fins a un mínim de 72 discos en un màxim de 6U en total en cas d'emprar safates de discs addicionals (JBOF).
- En cas d'haver d'ampliar espai usant safates addicionals tipus JBOF, s'haurà d'implementar mitjançant protocol NVMeoF/RoCE natiu, de forma que es garantirà que la solució sigui nativa NVMe en backend. Aquestes connexions hauran de ser redundades i amb un mínim ample de banda de 100Gbps, tant per les safates JBOF com per les controladores.
- El creixement del sistema haurà de ser modular i sense requerir interrupció del servei. Les actualitzacions de firmware o sistema operatiu i canvis o ampliacions

de components hardware o software s'han de poder dur a terme sense interrupció del servei i sense pèrdua de rendiment.

- La totalitat dels discs físics instal·lats en les cabines conformaran un espai únic on es crearan els volums o LUNs que es presentaran als host. En cas d'ampliació de capacitat d'aquest espai únic, aquesta es farà de manera dinàmica a la capacitat disponible de manera que pugui ser utilitzada per les LUNs ja existents.
- El sistema ha de permetre l'addició de noves targetes de xarxa 10/25Gb iSCSI o 32/64Gb FC per a futures necessitats que puguin aparèixer en l'entorn. També haurà de suportar la incorporació d'interfases 100Gb NVMeoF/RoCE per tal d'afegir elements JBOF d'ampliació de discs.
- Les cabines hauran de tenir la certificació per SAP Hana. S'haurà d'indicar el número de nodes SAP Hana certificats per a cada cabina proposada. El número mínim haurà de ser de 25 nodes per cabina. Aportar documentació acreditativa.

- **Funcionalitat**

- El sistema d' emmagatzematge proposat haurà de suportar i incloure l'encryptació de la informació emmagatzemada. Aquesta funcionalitat haurà d' estar implementada en el maquinari dels discs per no afectar el rendiment global de la solució, per la qual cosa no s'acceptaran solucions que implementin aquesta encryptació com a procés programari en els elements de processament de la dada.
- Haurà de disposar de capacitat de realitzar còpies tipus clone i tipus snapshot. Haurà de suportar un mínim de 1024 còpies tipus snapshot per volum mitjançant estratègia RoW (redirect-on-write). S'han de poder marcar polítiques d'immutabilitat pels snapshots realitzats.
- Per disposar de còpies lògiques immutables de només lectura i una major protecció contra atacs tipus Ransomware, en les còpies tipus snapshot, haurà de ser possible establir individualment un període de retenció durant el qual no serà possible eliminar aquesta còpia sota cap concepte (ja sigui de forma intencionada o no intencionada). El període d' immutabilitat podrà anar des d' 1 minut fins a diversos anys.
- Haurà de disposar d' un motor d' eficiència de la dada inline, suportant les funcionalitats de detecció de zeros Thin, reclamació d' espai Thin, deduplicació i compressió. Haurà de ser possible habilitar o deshabilitar les funcions de compressió i deduplicació granularment a nivell volum.
- La solució d' emmagatzematge proposada ha de disposar de funcionalitat orientada a la qualitat de servei, de manera que es puguin prioritzar certes càrregues de treball en cas de congestió de recursos. Aquest sistema de qualitat de servei haurà d'estar basat en intel·ligència artificial, de tal manera que s'establirà un nivell de prioritat per a cada volum o grup de volums (per exemple: baix, mitjà, alt). El sistema d' emmagatzematge monitoritzarà de forma contínua

els recursos i només prioritzarà uns volums respecte a d' altres en cas de congestió.

- Addicionalment també s' ha de suportar la funcionalitat de qualitat de servei clàssica, podent establir límits d' IOPS i rendiment, així com establir objectius de latència d' accés.
- De cara a possibles futures necessitats, la solució d' emmagatzematge proposada haurà de suportar replicació de dades nativa tant síncrona com asíncrona, basada en maquinari a nivell de la controladora i entre tots els models de la família oferta, sense elements o appliances addicionals.
- En el cas de necessitar replicació síncrona, haurà de ser possible configurar dos sistemes d'emmagatzematge en mode d'alta disponibilitat tipus "actiu/actiu" amb RPO = 0 i RTO proper a 0. És a dir, ambdós sistemes puguin ser capaços de replicar la seva informació de forma síncrona i oferir els volums replicats als hosts com una única unitat. La solució haurà de suportar que els hosts de cada centre de dades treballin de forma local (lectura i escriptura) amb el sistema que resideixi en el seu mateix centre de dades.
- Addicionalment, s'ha de suportar replicació incremental en el cas de recuperar-se d'una fallada dels enllaços de rèplica o d'operacions de failback, de forma que no es forci a una re-sincronització completa de totes les dades originals.

- **Suport, Gestió i Monitorització**

- La plataforma proposada ha de disposar d'una consola nativa Cloud (SaaS) per a la gestió d'un nombre il·limitat de cabines. Aquesta consola ha d'oferir les següents funcionalitats:
 - Dashboard comú per la gestió de múltiples cabines, oferint informació del nombre total de cabines, volums, hosts i capacitat. Ha d'oferir també informació de rendiment dels principals volums i cabines.
 - Sistema de control d'accés basat en rols (RBAC) per la gestió centralitzada de múltiples cabines, enlloc d'haver de crear rols i usuaris per a cada cabina.
 - Sistema d'auditoria comú per a totes les cabines.
 - Capacitat de marcar els volums en funció de l'aplicació, de forma que es puguin tenir informes de rendiment en funció de divers aplicacions.
 - Sistema recomanació de la cabina més adequada per absorbir una càrrega de treball específica definida per l'usuari.
 - Ha de poder opcions d'actualització de firmware per a cada cabina, en funció del context.
 - Oferirà gestió i configuració as-a-service, evitant les tasques de mantenir, instal·lar pegats/actualitzar les eines de gestió.

- Aquesta eina de gestió ha de ser verdaderament nativa Cloud, i per tant no en caldrà configuració, actualització i aplicació de pegats durant tot el cicle de vida del contracte, i ofert com a servei.
- El fabricant haurà de poder executar un servei d'assessment basat en Cloud de l'entorn VMware, en periodicitat trimestral. Aquest servei ha de poder oferir analítiques detallades de: utilització RAM i CPU dels hosts VMware, analítiques de l'emmagatzematge i detecció de màquines virtuals que puguin generar contencions. L'anàlisi també haurà de poder avaluar l'estat de llicenciat dels host en rol d'hipervisor.
- S'han d'incloure també monitorització en el Cloud, suport per AI/ML i un motor d'analítica per la gestió proactiva de l'emmagatzematge i minimització de riscos. Les llicències necessàries per aquestes funcionalitats han d'estar incloses en l'oferta.
- El motor Cloud de monitorització ha de oferir les següents funcionalitats:
 - Oferir una guia per l'actualització del microcodi de cada cabina, amb informació del camí d'actualització, versió prèvia, validacions prèvies i nivell de severitat de cada actualització.
 - El dashboard ha de mostrar de forma clara i detallada els possibles problemes existents en cada cabina de l'entorn sota gestió.
 - Ha de aportar analítiques de rendiment en quasi temps real (interval de mínim 5 minuts). S'han de poder generar informes a mida en format CSV i/o PDF sense la necessitat d'habilitar logging addicional, ni sense instal·lar cap tipus de software o appliance (física o virtual).
 - Donar informació sobre l'ús general de la cabina, tot combinant diversos paràmetres com IOPS, MB/s i tamany de bloc, entre altres.
 - La informació d'ús es podrà separar per volum i per tipus d'aplicació marcades en les cabines.
 - Oferir detall sobre els 5 volums que pateixin latències més altes, també amb funcionalitats avançades per poder marcar els punts crítics en rendiment.

3.2.3 Requisits mínims dispositius per a còpies de Seguretat.

Almenys **dues cabines per a emmagatzematge de còpia de seguretat (Backup)**. Aquestes cabines es configuraran perquè una d'elles sigui una còpia remota de l'altra, garantint l'externalització de la còpia del datacenter principal. Han de complir amb les característiques següents:

- **Requeriments generals**

- El sistema proposat ha d'oferir una controladora base amb les característiques següents:
 - Mínim de dos (2) CPU AMD con 8 cores cadascun.

- Mínim de 512GB RAM, de tipo DDR4-3200.
- Mínim de dos (2) ports de 10/25Gb Ethernet (PCIe)
- Mínim de dos (2) puerts de 1/10GBase-T Ethernet (integrades en placa)
- Mínim de dos (2) discs dedicats per allotjar el sistema operatiu.
- Ha d'admetre l'etiquetatge de VLAN. Els ports IP que s'ofereixen del mateix tipus també admetran agregacions de ports (port bonding).
- El sistema proposat ha d'oferir un mínim de 80TB d'espai local brut (RAW) a nivell d'infraestructura, distribuït en discos de 8TB.
- Ha de poder escalar fins com a mínim 250 TB d'espai local brut (RAW) a nivell d'infraestructura.
- Ha de ser escalable també fins almenys 200 TB de capacitat neta local, i uns 400TB addicionals de capacitat neta usant emmagatzematge al núvol com AWS, Azure o sobre un object storage S3.
- Es considera la capacitat neta local com: el resultat de restar la capacitat bruta local del sistema (RAW) l'espai necessari per a la implementació de la protecció de la informació (grups de RAID, discos de hot spare) sense aplicar cap tècnica d'estalvi en disc com a deduplicació, i/o compressió. Tampoc es considerarà pel càlcul d'espai local la capacitat externa que pugui consumir-se en el núvol públic o privat.
- Ha de tenir una única capa d'emmagatzematge local activa per operar amb les dades. No es permetran configuracions amb moviment intern o arxivat de la informació en una capa secundària de disc dins de l'emmagatzematge local del mateix repositori.
- Ha de poder oferir un rendiment sostingut d'escriptura d'almenys 25TB/hr.
- Ha d'incorporar totes les llicències necessàries per implementar les funcionalitats de deduplicació/compressió i rèplica optimitzada (permetent la transmissió de blocs únics no duplicats)

- **Eficiència de l'emmagatzematge de còpies de seguretat**

- El sistema ha d'integrar un motor de deduplicació obligatòriament in-line, fent l'optimització d'espai abans de l'escriptura en els discos físics. No es permetran dispositius que utilitzin deduplicació post procés.
- L'algoritme de la deduplicació ha de poder treballar obligatòriament mides de bloc variable sobre les dades de backup, per reconèixer un major nombre de patrons repetits i garantir la màxima eficiència en l'enviament i emmagatzematge de dades en el mateix repositori.
- Addicionalment a la deduplicació, ha d'integrar obligatòriament la compressió in-line de les dades, és a dir, abans de l'escriptura sobre els discos físics. No es permetran dispositius que utilitzin compressió post procés.

- **Protecció de la informació i seguretat**

- El sistema proposat ha de protegir les dades mitjançant un RAID 6 hardware, que vindrà configurat de fàbrica i no requerirà manipulacions addicionals durant la fase d'instal·lació. En cas d'haver d'escalar la mida, s'incorporarien discs en grups RAID 6 addicionals.
- Addicionalment, ha d'incorporar com a mínim un (1) disc en rol de hot spare per cada RAID grup.
- Ha de disposar de mecanismes de revisió i verificació continus durant la ingesta de la informació, i periòdicament, sobre les dades ja emmagatzemades per assegurar la consistència de la informació.
- Ha de suportar la funcionalitat d' encriptació data-at-rest, que compleixin la validació FIPS140-2. El xifrat de les dades s' ha de realitzar després del procediment de deduplicació, i es pot executar sobre la totalitat del repositori, així com sobre volums parcials..
- Addicionalment, també haurà de suportar la funcionalitat de Secure Erase, per tal de garantir que no es pugui recuperar dades de forma no autoritzada. Cal que compleixi NIST SP800-88, realitzant un mínim de set (7) sobre escriptures aleatòries.
- Ha d' incloure mecanismes de seguretat per garantir la protecció total enfront d' atacs de ransomware i altres malware.
 - Autorització dual: el sistema requerirà d'un sistema d'autorització dual mitjançant un usuari específic de seguretat per validar l'execució o no de les operacions crítiques sobre el sistema (modificar i/o esborrar un volum/tot l'emmagatzematge, canvi en la data/hora, desactivació de la funcionalitat d'autorització dual).
 - Immutabilitat: el sistema podrà configurar un període d' immutabilitat com a mínim a nivell de volum.

- **Tipus d' accés**

- El sistema proposat ha de suportar accés VTL FC, VTL ISCSI, NFS exports i SMB shares com a repositori de backup, amb accés concurrent per a cadascun d' ells.
- Haurà de poder emular, com a mínim, els formats de cintes LTO-5, LTO-6 y LTO-7.
- Ha de tenir la capacitat de configurar almenys una combinació de 64 biblioteques de cintes i objectius NAS juntament amb 100.000 o més ranures de cartutxos en un únic dispositiu.
- Ha de tenir intel·ligència per entendre tant la deduplicació basada en origen com en destinació i s'ha d'integrar amb el programari de backup en producció de l'IAS, en aquest cas Veeam Backup.

- Addicionalment, ha d'estar certificat per poder treballar amb la resta de principals proveïdors del mercat (CommVault, Zerto , entre d'altres), a banda de l'actual programari de backup d'IAS.
- El dispositiu proposat serà capaç d' oferir el seu emmagatzematge de forma directa i integrada en les aplicacions de backup, de manera que s' optimitzin les transferències de dades i no sigui necessari utilitzar els modes VTL ni NAS. Es requereix integració d' aquesta funcionalitat pel programari de backup actualment en producció IAS, com a mínim. Aquesta capacitat permet realitzar les tasques de deduplicació en origen utilitzant el mateix algoritme que implementa el dispositiu de disc.
- Per al cas particular de l' actual programari de backup implantat a l' IAS, tecnologia Veeam Backup, s'hauran d'incorporar les següents integracions:
 - Capacitat de realitzar còpies full virtuals sintètiques integrades amb la cabina. D'aquesta manera, a l'hora de realitzar un backup sintètic, no serà necessari que el media server torni a llegir el backup full i els seus incrementals per consolidar-lo i tornar a escriure'l, delegant directament aquesta capacitat al sistema proposat.
 - Per a una recuperació més ràpida i eficient, es requereix la integració del dispositiu de còpies amb les funcionalitats Instant Recovery, file-level recovery i application items recovery a través de Veeam Explorers.
 - Possibilitat de configurar una tasca tipus "Backup Copy Job" que els dispositius de còpies entendran i realitzaran de forma autònoma (amb compressió, deduplicació, sense haver de llegir de nou el backup per replicar-lo per part dels mitjans i amb control per part de l'ISV).

- **Monitorització i gestió remota**

- El sistema proposat ha de suportar monitoratge local, que mostri:
 - Llicenciament.
 - Configuració detallada del maquinari instal·lat.
 - Informació global i parcial sobre la capacitat actual, l' eficiència de l' emmagatzematge per volum de dades i la predicció automàtica de la capacitat futura del sistema.
- Ha de ser integrable en una plataforma de monitoratge basada en protocol SNMP.
- Ha d'incloure d'una eina de gestió, monitoratge i report integrada en un processador dedicat (ASIC) dins de la placa base de l'equip.
 - L'accés es realitzarà mitjançant un port 1GBase-T dedicat (OOBM, fora de banda).
 - Proporcionarà una API REST de gestió d' acord amb l' especificació Redfish DMTF.

- Compliment de: FIPS 140-2, CNSA, SSL/TLS 256 bits, i autenticació en 2FA
- Suport d' alertes de components maquinari crítics: CPU, memòria i disc.
- Funcionalitat d' actualització del firmware.

3.2.4 Requisits mínims dels dispositius de seguretat perimetral

Tal com es descriu en la introducció, IAS disposa de tres infraestructures de tallafocs en diferents capes de la xarxa:

- **Firewall de segmentació interna:** Format per un clúster en HA actiu-passiu de dos FGT600E, amb llicències UTP fins el 03/12/2025.
- **Firewall perimetral:** Format per un clúster en HA actiu-passiu de dos FGT100F, amb llicències UTP fins 03/12/2025 (membre 1) y 14/02/2027 (membre 2).
- **Firewall terminador de VPN:** Format por tres firewalls 100F en standalone balancejats que donen servei VPNSSL via web per a usuaris interns i túnel per a proveïdors amb llicències FortiCare fins a 08/12/2025.

Tots aquests sistemes estan integrats en un ecosistema del fabricant Fortinet per als quals IAS té llicències en vigor, com es detallen en la introducció: FortiAnalyzer, FortiManager, FortiAuthenticator, FortiToken i

FortiClient. A causa d' aquesta integració i dependències de serveis actualment existents, es requereix la substitució de l' equipament de seguretat perimetral per dispositius del mateix fabricant.

• Requisits firewall de segmentació interna

El firewall de segmentació interna estarà compost per dos dispositius que hauran de complir amb els següents requisits:

Característica	Valor
Firewall Throughput	Fins a 164Gbps
IPS Throughput	Fins a 42Gbps
NGFW Throughput	Fins a 36Gbps
Threat Protection Throughput	Fins a 30Gbps
Concurrent Sessions (TCP)	16,000,000
New Sessions/s (TCP)	720,000
SSL Inspection Throughput	12Gbps
SSL VPN Throughput	10Gbps
Concurrent SSL-VPN Users	10,000
Firewall Policies	10,000
VPN Gateway-to-Gateway Tunnels	2,000

Interfície GE RJ45	16 (Switch Ports) + 1 MGMT
GE SFP	8
SFP+/SFP28	4 x SFP+ (10GE) + 4 x SFP28 (25GE/10GE)
HA Port (Alta disponibilitat)	1 x 2.5GE
USB Ports	2
Console Port	1
Format	Rack 1U
Dimensions (Al x An x Prof)	44.45x432x380mm
Peso	7.25kg
Font d'alimentació	100–240VAC, 50/60Hz (2 PSU hot swap)
Consum màxim	252W
Temperatura operativa	0°C a 45°C
Humitat operativa	10–90% sense condensació
Capacitat màxima FortiAPs Tunnel/Total	1,024 / 2,048
Gestió	Centralitzada via FortiManager, FG-Cloud
Seguretat inclosa	IPS, Antivirus, AppControl, WebFilter, ZTNA, SD-WAN
Acceleració hardware	ASIC Fortinet SPU

Ambdós dispositius hauran de disposar de llicència del bundle ATP (Advance Threat Protection) i FortiCare Premium a 5 anys.

- **Requisits firewall perimetral**

Els dos Fortigate 100F actuals hauran de ser substituïts per dos dispositius que compleixin amb els següents requisits tècnics:

Característica	Valor segons datasheet
Firewall Throughput (1518/512/64B UDP)	39 / 39 / 28Gbps
Firewall Latency (64B UDP)	3.17µs
Firewall Throughput (pps)	42Mpps
Connexions concurrents (TCP)	3,000,000
Noves sessions TCP/s	140,000
Polítiques de firewall	10,000
Throughput IPS	5.3Gbps
Throughput NGFW	3.1Gbps

Throughput Protecció d'amenaçes	2.8Gbps
Throughput IPsec VPN (512B)	35Gbps
Túnel Gateway-to-Gateway IPsec VPN	2,000
Túnel Client-a-Gateway IPsec VPN	16,000
Throughput SSL-VPN	1.5Gbps
Usuaris SSL-VPN concurrents	500
Throughput Inspecció SSL	3Gbps
Sessions concurrents inspecció SSL	315,000
Control Aplicacions (HTTP 64K)	6.7Gbps
Throughput CAPWAP (HTTP 64K)	35Gbps
Domini virtuals (VDMs)	10/10 (per defecte/màxim)
FortiSwitches suportats (màx.)	48*
FortiAPs suportats Total/Túnel	128 / 64
FortiTokens suportats (màx.)	5,000
Configuracions HA	Activa-Activa, Activa-Passiva, Clustering
Ports GE RJ45	16 switch + 1 MGMT + 1 HA (total 18)
Ports GE SFP	8
Ports 10GE SFP+	4
Ports USB	1
Port consola (RJ45)	1
Dimensions (Al x An x Prof)	44x432x254mm (1.73x17x10in)
Pes	5.52kg (12.17lb)
Format	Rack 1U
Font d'alimentació	100–240VAC, 50/60Hz, dual no intercanviable
Redundància PSU	Sí (no hot-swap)
Consum mitjà / màxim	38W / 40W
Dissipació calor	138BTU/h
Temperatura de funcionament	0°C a 40°C
Humitat operativa	20–90% no condensant
Nivell de soroll	49dBA
Altitud operativa màxima	3,048m (10,000ft)
Certificacions	FCC, CE, RCM, VCCI, UL/cUL, CB, BSMI, USGv6/IPv6

Ambdós dispositius hauran de disposar de llicència de bundle UTP (Unified Threat Protection) i FortiCare Premium a 5 anys.

- **Requisits Firewall terminador de VPN**

Els tres Fortigate 100F actuals hauran de ser substituïts per dos dispositius que compleixin amb els següents requisits tècnics:

Característica	Valor segons datasheet
Firewall Throughput (1518/512/64B UDP)	39 / 39 / 28Gbps
Firewall Latency (64B UDP)	3.17µs
Firewall Throughput (pps)	42Mpps
Connexions concurrents (TCP)	3,000,000
Noves sessions TCP/s	140,000
Polítiques de firewall	10,000
Throughput IPS	5.3Gbps
Throughput NGFW	3.1Gbps
Throughput Protección de amenazas	2.8Gbps
Throughput IPsec VPN (512B)	35Gbps
Túnel Gateway-to-Gateway IPsec VPN	2,000
Túnel Cliente-a-Gateway IPsec VPN	16,000
Throughput SSL-VPN	1.5Gbps
Usuaris SSL-VPN concurrents	500
Throughput Inspecció SSL	3Gbps
Sessions concurrents inspecció SSL	315,000
Control Aplicacions (HTTP 64K)	6.7Gbps
Throughput CAPWAP (HTTP 64K)	35Gbps
Domini virtuals (VDMs)	10/10 (por defecte/màxim)
FortiSwitches suportats (máx.)	48*
FortiAPs suportats Total/Túnel	128 / 64
FortiTokens suportats (máx.)	5,000
Configuracions HA	Activa-Activa, Activa-Passiva, Clustering
Ports GE RJ45	16 switch + 1 MGMT + 1 HA (total 18)
Ports GE SFP	8
Ports 10GE SFP+	4
Ports USB	1
Port consola (RJ45)	1
Dimensions (Al x An x Prof)	44x432x254mm (1.73x17x10in)
Pes	5.52kg (12.17lb)

Format	Rack 1U
Font d'alimentació	100–240VAC, 50/60Hz, dual no intercanviable
Redundància PSU	Sí (no hot-swap)
Consum mitjà / màxim	38W / 40W
Dissipació calor	138BTU/h
Temperatura operativa	0°C a 40°C
Humitat operativa	20–90% no condensant
Nivell de soroll	49dBA
Altitud operativa màxima	3,048m (10,000ft)
Certificacions	FCC, CE, RCM, VCCI, UL/cUL, CB, BSMI, USGv6/IPv6

Ambdós dispositius hauran de disposar de FortiCare Premium a 5 anys.

3.2.5 Requisits mínims dels dispositius d'emmagatzematge NAS

A l'IAS, disposem d'una unitat de son que genera un gran volum d'imatges i vídeos que ocupen una gran quantitat d'emmagatzematge. Actualment, aquesta informació s'emmagatzema en discs locals i es fa necessari centralitzar aquestes dades i dotar-les d'una capa de seguretat i redundància. Per a això, demanem el subministrament de dos dispositius NAS. Un d'ells serà el principal en el qual l'equip allotjarà les imatges i vídeos i un segon, que estarà allotjat en una altra ubicació, que únicament serà rèplica del principal i no compartirà emmagatzematge amb cap usuari.

• Característiques generals

- Unitat NAS per a muntatge en rack de 2U, compatible amb armaris estàndard de 19".
- Capacitat mínima de 8 slots per a discs durs de 3,5"/2,5", interfície SATA III (6 Gb/s), compatibles amb intercanvi en calent (hot swap).
- Processador
 - Processador d'arquitectura x86 de 64 bits, 4 nuclis físics i 8 fils, freqüència base mínima de 2,2 GHz.
 - Suport per a xifrat accelerat per maquinari (AES-NI o equivalent) i unitat de coma flotant.
- Memòria
 - 16 GB de memòria RAM DDR4 instal·lada, ampliable, en format SODIMM o DIMM.
 - 5 GB de memòria flash per a la protecció del sistema operatiu
- Memòria CAU SSD i expansió

- 2 ranures M.2 2280 PCIe Gen3 x1 (o superior), compatibles amb unitats SSD NVMe d'almenys 500 GB cadascuna per a ús de memòria CAU.
- Almenys 1 ranura d'expansió PCI Express Gen3 x8 o superior, per a targetes de xarxa/emmagatzematge addicionals.
- Emmagatzematge i RAID
 - Ha d'incloure instal·lats 8 discos durs de 4 TB cadascun, tecnologia NAS optimitzada, velocitat mínima 5400 rpm, compatibles amb operació 24x7 (nivell empresarial o destinat a NAS).
 - Capacitat de configuració de nivells RAID 0, 1, 5, 6, 10, 50, 60 i JBOD per hardware.
 - Ha d'incloure controlador SATA III (6 Gb/s) amb suport complet de gestió i monitoratge SMART.
- Connectivitat de xarxa
 - 2 ports Ethernet RJ-45 amb velocitat mínima de 2,5 Gbps, compatibles amb 1 GbE/100M.
 - Ha d'incloure 1 targeta de xarxa d'expansió amb 2 ports SFP+ (10 GbE), estàndard 10GBase-SR, distàncies de fins a 300 metres sobre fibra òptica multimode (850 nm).
 - Ha d'incloure un mínim de un transceptor SFP+ SR (multimode 850 nm, 10 GbE).
- Alimentació y Refrigeració
 - Doble font d'alimentació redundat, intercanviable en calent, amb potència suficient per a operació contínua (mínim 300W cadascuna).
 - Sistema de ventilació actiu amb ventiladors redundants i reemplaçables en calent.
- Sistema i programari
 - Ha d'incloure sistema operatiu propietari especialitzat en emmagatzematge NAS, basat en arquitectura ZFS, amb suport per a snapshots, deduplicació, compressió, protecció de dades i recuperació davant desastres.
 - Totes les llicències d'ús necessàries per a l'operació indicada.
- Garantia i servei
 - Garantia del fabricant d'almenys 5 anys, amb servei de substitució avançada i suport tècnic telefònic, incloent reemplaçament de maquinari al següent dia laborable (NBD).
- Altres requeriments
 - Compatible amb administració web i monitorització avançada (ús, esdeveniments, alertes).
 - Ha d'incloure kit de muntatge en rack i tots els accessoris i cables necessaris per a possibilitat d'ús immediat.

3.2.6 Relació de llicències i manteniments a oferir

Amb l'execució d'aquesta licitació, l'IAS vol unificar les dates en què s'ha de renovar tot el llicenciament i manteniment de la seva infraestructura, unificant aquesta data al 31/12/2030, llevat d'un sistema d'emmagatzematge HPE Nimble, al qual només se li ampliarà el suport per al període de migració dels sistemes a la nova infraestructura i les llicències de Hypervisor VMware, que, a conseqüència dels moviments al mercat, només es demanarà a dos anys.

3.2.6.1 Llicències Hypervisor

Per mantenir la compatibilitat amb la infraestructura existent, es demana la provisió de les llicències de VMware Estàndard per al nombre de cores adequats per a la plataforma ofertada i per a 2 anys de llicenciament. A diferència de la resta de les llicències, aquesta únicament es demanarà per a aquest termini, donat les incerteses en el mercat i que el propi fabricant està generant.

3.2.6.2 Veeam Backup and Replicaton

Actualment, l'IAS té tota la seva infraestructura de backup basada en Veeam Data Platform Foundation Universal Subscription License (Enterprise Plus Features) per a un total de 140 VUL i té un contracte vigent fins al 23/01/2027.

Amb aquesta licitació, es pretén unificar els terminis de venciment de tot el programari i manteniment de les infraestructures. Així doncs, es demana l'ampliació del contracte amb Veeam nº **02626572 fins al 31/12/2030**.

3.2.6.3 Red Hat Enterprise Linux

Actualment, l'IAS disposa de llicències de RHEL for SAP Applications. Es requereix la renovació dels següents suports amb una coterminació a 31/12/2030:

- Red Hat Enterprise Linux Server, Standard (Physical or Virtual Nodes)
 - SN:12555990 De:01/01/2026 a 31/12/2030 (2 unidades)
- Red Hat Enterprise Linux for SAP Solutions, Standard (Physical or Virtual Nodes)
 - SN:12915786 De:01/01/2026 a 31/12/2030
- Red Hat Enterprise Linux for SAP Solutions, Premium (Physical or Virtual Nodes)
 - SN:12915786 De:01/01/2026 a 31/12/2030

Adicionalment, es requereix una nova llicència:

- Red Hat Enterprise Linux Server, Standard (Physical or Virtual Nodes)
De:01/01/2026 al 31/12/2030

3.2.6.4 Renovació de manteniments d'equips HPE

Part del maquinari actualment en producció en IAS, serà mantingut en funcionament i, per a això, es requereix del licitador que ofereixi la renovació del suport oficial del fabricant, HPE Tech Care Basic dels següents dispositius fins al 31/12/2030:

P/N	Descripció	S/N
Q1J03B	HPE MSA 2052 SAN DC SFF Storage	ACM035T54M
AK380A	HP MSL4048 2 LTO-4 Ultr 1760 SAS Library	DEC00308HP
Q6Q67A	HPE MSL LTO-8 FC Drive Upgrade Kit	CZ20410DJ9
Q6Q67A	HPE MSL LTO-8 FC Drive Upgrade Kit	CZ20410DJB
Q1H70B	HPE SN3600B 32 Gb 24/8 FC Switch	CZC036W3G4
Q1H70B	HPE SN3600B 32 Gb 24/8 FC Switch	CZC036W3GP
R4G55B	HPE SN3600B 24/8 8p 16Gb SW SFP+ FC Swch	CZC3438MLR

Adicionalment, per disposar de suport sobre la cabina d'emmagatzematge actual durant el procés de migració de tots els serveis, es demana la renovació del suport oficial del fabricant HPE Tech Care Basic de la següent cabina d'emmagatzematge HPE Nimble fins al **31/12/2026**:

P/N	Descripció	S/N
5UM041005V	HPE NS AF40 All Flash CTO Base Array	Q8H41A

3.2.6.5 Renovació de IMC Aruba

Es requereix la renovació del contracte IMC Aruba amb referència: 2002248918, fins al 31/12/2030.

3.2.6.6 Renovacions Fortinet

Actualment es disposen de les següents llicències amb FortiCare Premium i les dates de finalització del suport indicades:

Producte	S/N	Tipus de Llicència	Data fi
FortiAuthenticator	FAC-VMTM23006019	Perpètua	09/10/2028 (Premium Support)
Fortianalyzer FortiGuard IOC	FAZVMSTM23007169	Subscripció 25 Gb/día	03/12/2026
FortiClient EMS	FCTEMS8824004244	SaaS para 25 usuarios	22/05/2027
FortiManager	FMG-VMTM21005276	Perpètua on prem 10 dispositius	03/05/2026 (Premium Support)

Es demana l'ampliació d'aquests productes fins al 31/12/2030 i, així, fer coterminació de tots els períodes de llicències o suports.

3.2.7 Altres subministraments

Es forma addicional, el licitador haurà d' oferir:

- 1 Pack de 20 cintes LTO-8 Ultrium 30TB RW amb estoigs
- L'oferta haurà d'influir tots els transceiver i cables (d'alimentació, de xarxes, FC, DAC, etc..) necessaris per posar en producció l'equipament sol·licitat.

3.3 SERVEIS ASSOCIATS AL SUBMINISTRAMENT

IAS vol contractar els serveis integrats de disseny, implantació, migració i transferència de coneixements per a la modernització de la infraestructura TI d' IAS, assegurant l'explotació completa de les capacitats tècniques del nou equipament.

Aquests serveis han d' incloure:

- Serveis associats al còmput, emmagatzematge i backup:
 - Disseny del sistema, incloent-hi les estratègies per facilitar la migració des dels sistemes actuals.
 - Instal·lació de la nova granja de virtualització
 - Migració dels serveis a la nova granja.
 - Instal·lació dels sistemes físics per al backup
 - Instal·lació i configuració d'un nou servidor de backups.
 - Instal·lació d'un nou controlador de domini
 - Instal·lació i configuració dels dos sistemes NAS replicats.
- Serveis associats a la seguretat perimetral:
 - Instal·lació de nous clústers de Fortinet.
 - Migració dels serveis als nous clúster de Fortinet.

A continuació, es descriuen el detall dels serveis demanats.

3.3.1 Serveis associats al còmput, emmagatzematge i backup

S' hauran d' incloure obligatòriament els serveis professionals dividits en els apartats a continuació:

- **Disseny del sistema**
 - Anàlisi detallada de l'entorn actual i propostes d'arquitectura del nou sistema.
 - Disseny de la infraestructura de sistemes per optimitzar la migració.
 - Definició de les estratègies concretes per facilitar la migració des dels sistemes existents, minimitzant riscos i períodes d' interrupció.
 - Determinació d' adreçaments IP, ports, etc a usar per la nova infraestructura.

- **Instal·lació de la nova granja de virtualització**

Aquests serveis han d'incloure la instal·lació de tota la granja de virtualització, incloent-hi els equips de còmput i emmagatzematge, la connexió a la infraestructura de xarxa SAN, etc. Ha d'incloure:

- Revisió física i anàlisi previs a la instal·lació al CPD de l'IAS, per garantir que es disposa de tots els elements físics necessaris per realitzar el desplegament de la solució.
- Testeig del maquinari desplegat.
- Instal·lació dels equips en els racks assignats a les instal·lacions d'IAS, cablejat/connexió físic (incloent-hi tant de corrent com de connectivitat de dades), actualització a les últimes versions de programari (firmware, sistema operatiu) dels equips. Desplegament físic i lògic de la solució seleccionada (VMware).
- Configuració inicial de hosts, xarxes i emmagatzematge integrat.
- Serà obligació del contractista la recollida i retirada de tots els embalatges o residus que sorgeixin de la instal·lació, compromentent-se a dipositar aquests en llocs apropiats i destinats per a la recollida de residus d'aquesta índole.

- **Migració de serveis a la nova granja**

- Planificació i execució de la migració de màquines virtuals i serveis crítics existents cap a la nova infraestructura.
- Validació de funcionament correcte post-migració i resolució d'incidències.

- **Instal·lació de sistemes físics per al Backup**

- Instal·lació física dels sistemes d'emmagatzematge de còpia de Seguretat.
- Inicialització dels sistemes, configurant les mesures de seguretat d' accés necessàries per garantir la integritat de les còpies emmagatzemades.
- Configuració de repositoris per a Veeam Backup
- Verificació de la visibilitat entre ambdós equips, configuració de rèpliques de còpies entre els dispositius.

- **Instal·lació i configuració del nou servidor de Backups**

Durant el procés de migració seran alliberats servidors de la infraestructura de virtualització anterior. Un d'ells, a determinar per IAS, serà usat com a nou servidor de Veeam Backup. El licitador haurà de detallar els serveis per:

- Instal·lació d'un nou servidor de Veeam Backup amb els rols de Veeam backup Console i Veeam Backup Proxy.
- Configuració dels nous repositoris de backup sobre els nous dispositius destinats a l'emmagatzematge de còpies, seguint les bones practiques del fabricant.
- Disseny i configuració de la nova estratègia de backup, incloent-hi les noves capacitats dels nous repositoris (immutabilitat, rèplica, etc.)
- Tots aquests serveis s'han de realitzar garantint que les còpies de seguretat continuen funcionant durant les migracions.

- **Instal·lació d'un nou controlador de domini**

Durant el procés de migració seran alliberats servidors de la infraestructura de virtualització anterior. Un d'ells, a determinar per IAS, serà usat com a nou servidor controlador de domini. S'han d'incloure els serveis següents:

- Instal·lació d'un nou servidor físic per al rol de controlador de domini.
- Instal·lació de rols de controlador de domini i integració amb el domini existent.
- Distribució adequada dels rols FSMO i despromoció dels servidors reemplaçats.

- **Instal·lació i configuració de dos sistemes NAS replicats**

- Instal·lació i ajust de dues cabines NAS en ubicacions diferents a determinar per IAS, per a magatzem d'imatges i vídeos de la unitat del son, amb configuració de replicació (sincrònica/asíncrona) entre ambdues.
- Verificació de la replicació i proves de restauració de dades.

- **Readequació d'altres serveis existents**

Revisió i adaptació de serveis o dependències afectats per la migració (adreces IP, autoritzacions, accessos, monitoratge, etc.).

- **Transferència de coneixements**

- Sessions pràctiques i documentals per a la capacitat del personal de l'IAS sobre l'operació, administració, del nou entorn desplegat.
- Entrega de la documentació de fi de projecte.

- **Lliurables**

Hauran de ser lliurats pel licitador els següents documents després d'aquestes tasques:

- Document de disseny i pla de migració adaptat a IAS.
- Cronograma detallat de desplegament i migració.

- Informes de validació després de cada fase.
- Manuals d'usuari i administració, específics per a la solució implantada.
- Certificats de formació i transferència de coneixement.

3.3.2 Serveis associats a la seguretat perimetral

- **Migració de clústers Fortigate**

Els serveis requerits per a la migració dels 3 clústers de Fortigate ha de ser clara, detallada i estructurada conforme a bones pràctiques i recomanacions del fabricant. Els serveis d'instal·lació han d'incloure – com a mínim - de forma detallada les següents tasques:

- Anàlisi i planificació de la migració
 - Auditoria de l'estat actual de cada clúster Fortigate, incloent revisió de configuració, polítiques de seguretat, objectes i diagrames de xarxa.
 - Identificació de dependències, rutes, serveis crítics i possibles optimitzacions de configuració.
 - Elaboració d'un pla de migració detallat per a cada clúster, contemplant finestres d'intervenció, estratègies de contingència i proves d'acceptació.
- Preparació de l'entorn de destinació
 - Subministrament, instal·lació i configuració inicial dels nous clústers en alta disponibilitat (HA), assegurant paritat de versió de firmware, mòduls i llicències entre membres del clúster.
 - Adaptació d'interfícies, VLANs i configuracions de xarxa per correspondre amb l'arquitectura existent o facilitar millores.
 - Registre i incorporació dels nous clústers sota gestió centralitzada (FortiManager), amb adequada vinculació de polítiques i objectes comuns.
- Migració de configuració
 - Migrar i convertir la configuració dels clústers actuals als nous, minimitzant errors manuals i assegurant la compatibilitat.
 - Revisió i ajust de configuracions crítiques tals com interfícies, HA, rutes estàtiques, objectes, polítiques de seguretat i certificats.
 - Càrrega i sincronitzacions inicials en els nous clústers, evitant conflictes amb l'entorn productiu durant la fase prèvia al tall.
- Execució de la migració i posada en marxa
 - Coordinació de finestra de manteniment per al switchover als nous clústers, incloent-hi protocols de recolzament i rollback.
 - Execució de proves funcionals i de connectivitat a les diferents xarxes i serveis protegits abans i després del tall.

- Supervisió del funcionament de l'alta disponibilitat i verificació de sincronització entre els nodes de cada clúster.
- Validació i documentació
 - Realització de proves d'acceptació per part de l'equip tècnic del client.
 - Documentació dels nous clústers Fortigate, incloent diagrames actualitzats, configuració i procediments de recuperació davant desastres.
 - Generació d'informes finals sobre el resultat de la migració i recomanacions de millora de polítiques si es detecten oportunitats durant el procés.
- Transferència de Coneixements
 - Sessió formativa i transferència de coneixements clau sobre administració, operació i recuperació dels clústers migrats.
- Notes addicionals:
 - El procés ha de contemplar sempre una estratègia de backup i rollback en cas de contingència, així com proves de HA i failover després de la migració.
 - S'haurà de realitzar un test de laboratori previ per simular els canvis més crítics en un entorn controlat.

• Migració del servei VPNSSL

A causa de discontinuació dels serveis VPNSSL per part de Fortinet a partir de la vesprada 7.6, requerim la migració d'aquests serveis a una solució ZTNA que permetrà a 25 usuaris corporatius amb llicència de Fortiauthenticator i la resta d'usuaris (interns i externs) l'accés segur a la infraestructura d'IAS. Cal tenir en compte que els usuaris externs són equips no gestionats per IAS, amb la qual cosa cal garantir aquest accés sense aquesta capacitat de gestió.

Es requerirà el següent:

- Disseny de la solució
- Prova de concepte, tant per a equips corporatius amb llicència, usuaris sense llicència i externs.
- Implementació de les diferents solucions possibles
- Desplegament inicial per a un subconjunt d'usuaris.
- Transferència de coneixements i documentació

4 DOCUMENTACIÓ A APORTAR PEL LICITADOR

4.1 OFERTA ECONÒMICA I CRITERIS QUANTIFICABLES DE FORMA AUTOMÀTICA (SOBRE C)

El licitador haurà de realitzar l'oferta econòmica tot complimentant l'ANNEX 2 del PCAP, amb el detall que s'indica a continuació:

4.1.1 OFERTA ECONÒMICA

Proposta econòmica de la solució segons el següent quadre, indicant el preu base de cada concepte i el preu final en modalitat d'arrendament a 5 anys:

Concepte	Any	Import mensual (IVA exclòs)	Import mensual (IVA inclòs)	Import anual (IVA exclòs)	Import anual (IVA inclòs)
Servei de subministrament en modalitat d'arrendament, amb opció de compra, del maquinari i programari base del CPD de l'IAS	2026				
	2027				
	2028				
	2029				
	2030				
	Total	-	-		

4.1.2 MEMÒRIA DE CERTIFICACIONS DEL LICITADOR EN TECNOLOGIA DE FABRICANT

Caldrà adjuntar memòria justificativa de les diferents certificacions de fabricant aportades pel licitador, tal i com es descriuen en l'apartat 5.2.2.1.

4.1.3 MEMÒRIA DE CERTIFICACIONS OFICIALS DE QUALITAT O MEDIAMBIENTALS

Caldrà adjuntar memòria justificativa de les diferents certificacions de qualitat o mediambientals aportades pel licitador, tal i com es relacionen en l'apartat 5.2.2.2.

4.1.4 CERTIFICACIÓ EN L'ESQUEMA NACIONAL DE SEURETAT

Caldrà adjuntar, d'acord amb l'epígraf 6.3, la certificació de l'empresa licitadora en l'ENS (Esquema Nacional de Seguretat) amb una certificació mínima de nivell mig.

4.2 OFERTA TÈCNICA (SOBRE B)

L'oferta tècnica del licitador consistirà en l'aportació d'una memòria per tal d'acreditar cadascun dels apartats descrits en el punt d'especificacions tècniques del servei, segons es detalla seguidament:

- **A/Descripció tècnica dels diferents elements del subministrament.** El licitador elaborarà una Memòria de la descripció tècnica del disseny de l'arquitectura proposada (epígraf 3.2 i 3.3 d'aquest Plec). El licitador lliurará l'oferta amb una estructura que s'adeqüi els punts exposats anteriorment, tot aportant la informació que cregui adient en cada un d'ells, de manera que permeti la seva avaluació de forma clara, evitant possibles interpretacions subjectives de la solució a aportar en cada un dels punts exposats. El licitador haurà **d'indicar clarament** com els diferents components que proposa en la solució, **compleixen amb tots i cada un dels requeriments mínims indicats** en els punts 3.2 i 3.3 d'aquest Plec.
- **B/Descripció del pla d'instal·lació i migració** de l'arquitectura proposada a partir de l'arquitectura tecnològica actual de l'IAS.

Per tal que aquesta Unitat Tècnica de l'IAS pugui valorar ponderadament cadascuna de les ofertes presentades, serà necessari que les ofertes es presentin detallades i que els seus apartats siguin identificables, segons les denominacions i epígrafs, essent la valoració de cada un d'ells el que es descriu en els criteris d'adjudicació especificats en aquest plec.

Tanmateix, és necessari que les Memòries siguin concretes i concises amb la mínima extensió possible que permeti la clara comprensió de la proposta aportada. No s'ha d'incloure documentació o informació comercial genèrica si no aporta valor a l'oferta concreta.

5 CRITERIS D'ADJUDICACIÓ

5.1 OFERTA TÈCNICA (SOBRE B)

Es puntuarà l'oferta tècnica amb un total de 20 punts. Es valorarà segons els següents apartats:

5.1.1 Criteris de valoració sotmesos a judici de valor (màxim 20 punts)

S'estableixen els següents criteris de valoració no quantificables automàticament o sotmesos a judici de valor:

5.1.1.1 Disseny tècnic de la solució proposada (màxim 10 punts)

Criteri	Punts
Es valorarà el disseny tècnic de l'arquitectura proposada en els següents aspectes: - Justificació dels components triats pel maquinari - Avantatges de la solució proposada en base a criteris de disponibilitat - Avantatges de la solució proposada en termes de rendiment - Avantatges de la solució proposada en relació a la infraestructura existent actualment - Per les capacitats d'escalabilitat vertical i horitzontal. Es valorarà la descripció detallada de les diferents possibilitats d'escalabilitat tant vertical com horitzontal, i la identificació d'aquelles característiques que destaquen en aquest punt. - Per la integració amb els components de l'arquitectura actual als que s'allarga la seva garantia	10

5.1.1.2 Pla d'instal·lació i migració (màxim 10 punts)

Criteri	Punts
Es valorarà el pla d'instal·lació i migració en base als següents conceptes: - Pla d'instal·lació i configuració de la plataforma. Es valorarà la claredat i detall del pla d'instal·lació i configuració, amb la descripció de totes les tasques a fer, i la identificació de les diferents fites calendaritzades. - Que les tasques a realitzar per a la migració i posada en marxa tinguin compte l'objectiu de reduir al màxim possible l'impacte sobre els usuaris, funcionament i operativa dels sistemes, i preservar la informació existent. - CV dels tècnics assignats al projecte.	10

5.2 OFERTA ECONÒMICA (SOBRE C)

La valoració de les proposicions i la determinació de l'oferta econòmica més avantatjosa es durà a terme per l'aplicació dels següents criteris de valoració:

5.2.1 Preu (fins a 60 punts)

Es valorarà el preu de sortida de la següent manera:

L'oferta més econòmica, sempre i quan compleixi els requeriments tècnics mínims indicats en el plec de prescripcions tècniques, obtindrà 60 punts.

Les restants ofertes obtindran la puntuació que resulti de l'aplicació de la següent fórmula:

$P_v = \left[1 - \left(\frac{O_v - O_m}{IL} \right) \times \left(\frac{1}{M} \right) \right] \times P$	P_v = Puntuació de l'oferta a valorar P = Punts criteri econòmic = 60 O_m = Oferta millor O_v = Oferta a valorar IL = Import de licitació M = Factor de modulació = 1,6
---	--

5.2.2 Altres criteris de valoració objectius (màxim 20 punts)

5.2.2.1 Certificacions del licitador en tecnologia de fabricant (màxim 10 punts)

Es tindran en compte les certificacions de fabricant que porti el licitador, de manera que es valorarà positivament el coneixement del licitador en les diferents tecnologies que està utilitzant l'IAS en la seva plataforma actual de CPD. Aquest fet revertirà en una millor comprensió de la situació tecnològica actual de l'IAS i de les possibles estratègies de migració a la nova arquitectura.

La puntuació de les certificacions del licitador es faran en base a la següent taula:

Certificació de fabricant	Nivell de certificació	Puntuació parcial
HPE/Equivalent ofertada	<i>Platinum</i>	4
	<i>Gold</i>	3
	<i>Silver</i>	2
	<i>Authorized Reseller</i>	1
	<i>No disposa</i>	0
HPE Serveis/Equivalent ofertada	<i>HPE Contract Specialist</i>	2
	<i>No disposa</i>	0
HPE Aruba	<i>Platinum</i>	4
	<i>Gold</i>	3
	<i>Silver</i>	2
	<i>Authorized Reseller</i>	1
	<i>No disposa</i>	0
Broadcomm - VMware	<i>Pinnacle</i>	3
	<i>Premier</i>	2
	<i>Select</i>	1
	<i>No disposa</i>	0
Veeam Backup	<i>Veeam Platinum partner</i>	4
	<i>Veeam Gold partner</i>	3
	<i>Veeam Silver partner</i>	2
	<i>Veeam Registered Partner</i>	1
	<i>No disposa</i>	0
Fortinet/Equivalent ofertada	<i>Advanced</i>	4
	<i>Select</i>	3
	<i>Advocate</i>	2
	<i>Registered</i>	1
	<i>No disposa</i>	0

La puntuació parcial màxima de 21 punts equivaldrà a una puntuació de 10 punts en aquest apartat de certificacions. Per tant la puntuació de cada licitador s'obindrà amb la següent fórmula:

$$P = P_c * \left(\frac{10}{21}\right)$$

On:

- P: Puntuació total en l'apartat de certificacions
- Pc: Suma de puntuacions de les diferents certificacions en base a la taula anterior

5.2.2.2 Certificacions oficials de qualitat o mediambientals (màxim 4 punts)

Es valorarà que el licitador estigui certificat en diferents normes internacionals i estatals en l'àmbit de la qualitat i gestió mediambiental.

Certificació	Puntuació
Certificat ISO 14001 (gestió ambiental)	1
Certificació ISO 27001 (gestió de la seguretat de la informació)	1
Certificació ISO 9001 (gestió de qualitat)	1
Certificació/registre de l'Empremta de carboni	1

5.2.2.3 Millores en la formació al tancament del projecte (màxim 3 punts)

Es valoraran millores a la formació del personal de la UTIC al tancament del projecte. La formació haurà de ser presencial i haurà d'estar enfocada a la tecnologia subministrada en el servei. La formació estarà orientada a l'administració bàsica de la nova infraestructura desplegada, noves versions de software instal·lat, software de monitorització o qualsevol altre software entregat.

Formació ofertada al tancament del projecte	Puntuació
3 jornades a casa del client amb formació efectiva total de 9 hores	3
2 jornades a casa del client amb formació efectiva total de 6 hores	2
1 jornada a casa del client amb formació efectiva total de 3 hores	1
No s'ofereix formació	0

5.2.2.4 Proximitat del servei tècnic de suport autoritzat de la cabina d'emmagatzemament (màxim 3 punts)

Es valorarà que el licitador disposi d'una seu fixe (dependències del SAT) amb equip tècnic de suport on-site autoritzat pel fabricant a prop del centre de processament de dades de l'IAS. La valoració es farà segons la següent taula:

Distància (d) de la seu amb servei tècnic del licitador a l'IAS	Puntuació
d < 25 km	3
25 km < d < 75 km	2
75 km < d < 100 km	1
d > 100 km	0

6 REQUERIMENTS DE SEGURETAT

En matèria de seguretat de la informació, l'empresa adjudicatària té les següents obligacions:

6.1 Deure de confidencialitat

Tot el personal de l'empresa adjudicatària així com els possibles subcontractistes han de mantenir absoluta confidencialitat i estricte secret sobre la informació coneguda arrel de l'execució dels serveis contractats. Aquesta obligació de confidencialitat s'haurà de mantenir durant 10 anys, o el que s'especifiqui en el contracte, des de que es va tenir coneixement de la informació, excepte en relació a les dades personals a les que accedeixin respecte a les que caldrà mantenir el deure de confidencialitat de manera indefinida, subsistint inclús quan es finalitzi la relació contractual, segons estableix la Llei Orgànica 3/2018.

L'empresa adjudicatària ha de comunicar aquesta obligació de confidencialitat al seu personal ja sigui intern com extern, que estigui involucrat en l'execució del contracte i possibles subcontractistes i ha de controlar el seu compliment.

L'empresa adjudicatària ha de posar en coneixement de l'IAS, de forma immediata, qualsevol incidència que es produeixi durant l'execució del contracte que pugui afectar la integritat o la confidencialitat de la informació.

6.2 Dades de caràcter personal

En relació amb el tractament de dades de caràcter personal, l'empresa adjudicatària del contracte donarà compliment com a encarregat de tractament el que estableix el Reglament General de Protecció de Dades.

Pel que fa a la seguretat en el tractament d'aquestes, l'empresa adjudicatària implementarà les mesures de seguretat establertes per l'Agència de Ciberseguretat en el Marc de Ciberseguretat per a la Protecció de Dades. Aquesta implementació i nivell de compliment seran incorporats al model de compliment normatiu de la Generalitat de Catalunya.

L'empresa adjudicatària es compromet a prendre totes les mesures tècniques i organitzatives al seu abast per garantir l'objectiu de seguretat de la informació, que es basa en els tres principis següents:

- La confidencialitat de la informació, assegurant que només hi accedeixen les persones que han estat autoritzades a fer-ho.
- La integritat de la informació, assegurant que la informació i els mètodes que la processen són exactes i complets.
- La disponibilitat d'aquesta informació, assegurant que els usuaris autoritzats tenen accés a aquestes dades, mòduls i aplicacions quan ho necessitin.

Igualment, es compromet a prendre les mesures que preveu la normativa en vigor en matèria de seguretat de la informació i protecció de dades de caràcter personal.

Accés a dades personals, o de caràcter reservat:

L'empresa adjudicatària es compromet a no accedir innecessàriament a aquelles dades a les quals tingui accés per raó de la tasca que té encomanada.

Sempre que calgui manipular dades, es treballarà amb dades de proves, simulades o fictícies. Un cop acabat el desenvolupament o prova, s'esborraran totes les dades manipulades, tant si són fictícies com reals.

En cas que sigui necessari accedir a les dades reals, l'empresa i els seus treballadors es comprometen a mantenir la confidencialitat respecte a la informació coneguda, a no alterar-ne el contingut i a no revelar, comunicar, ni posar a disposició de tercers, per cap mitjà, escrit, electrònic, verbal o per qualsevol altre procediment, cap d'aquestes dades o part d'elles, o la informació que se n'hagi pogut extreure.

L'accés a aquestes dades reals haurà de ser autoritzat pel responsable del fitxer o pel responsable de seguretat de l'hospital.

Així mateix, l'empresa adjudicatària haurà de **signar un contracte d'encarregat de tractament** de dades personals amb IAS.

En el cas de que el tractament de dades personals es faci en infraestructura en el núvol o s'apliquin algorismes de IA en les dades, **l'adjudicatari haurà de fer una AIPD** (Avaluació d'Impacte relativa a la Protecció de Dades).

6.3 Compliment del marc legal de ciberseguretat i del marc normatiu intern

L'empresa adjudicatària del contracte haurà de complir amb tots els requeriments que siguin d'aplicació d'acord amb el marc legal en matèria de ciberseguretat i amb el marc normatiu intern que siguin aplicables.

En relació al marc legal en matèria de ciberseguretat, i, en concret, al compliment de l'Esquema Nacional de Seguretat (ENS), l'empresa adjudicatària del contracte haurà d'assegurar la conformitat dels sistemes d'informació que sustentin la prestació de serveis o de les solucions que pugui proveir, amb l'ENS durant tot el termini d'execució del contracte i, si escau, haurà d'estendre aquesta exigència a la cadena de subministrament. L'empresa adjudicatària del contracte basat haurà de designar, segons estableix l'ENS, un punt de contacte per a la seguretat (POC) que canalitzarà i supervisarà el compliment dels requisits de seguretat de la informació i la gestió dels incidents que es puguin produir durant l'execució del contracte.

A més de l'ENS i la normativa i guies tècniques que el desenvolupen, l'empresa adjudicatària del contracte haurà de conèixer i aplicar el marc normatiu intern, que inclourà el Marc Normatiu de Seguretat la Informació de la Generalitat de Catalunya i la normativa pròpia, les directrius o instruccions de l'IAS. Especialment haurà de complir amb la Política de seguretat aplicable i la normativa relativa a l'ús de les tecnologies de la informació i la comunicació, aprovada per Instrucció de la Secretaria d'Administració i Funció Pública i que es pot consultar al lloc web d'aquesta Secretaria. Si escau, l'empresa adjudicatària del contracte basat haurà de desenvolupar els procediments que siguin necessaris per a poder aplicar el marc normatiu.

6.4 Adquisició de productes/eines i productes o serveis de seguretat

Tant en el cas que es desenvolupin productes/eines, es facin integracions amb altres eines o s'adquireixin eines de mercat o qualsevol component de sistemes d'informació (hardware, software, etc.), aquests hauran de ser compatibles amb l'arquitectura de

seguretat de l'IAS i complir amb els requeriments de seguretat que estableixi el marc legal i el marc normatiu intern, sotmetre's a proves tècniques de seguretat i aplicar les correccions necessàries prèviament a la posada en producció del producte/solució/eina. Caldrà incorporar el producte/eina dins el procés de desenvolupament segur de l'IAS des de la fase de disseny fins a la posada en producció.

L'empresa adjudicatària del contracte basat haurà de garantir que disposa dels perfils amb la capacitat i la formació necessària per tal de poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició. A més, haurà de proporcionar formació i capacitat per al personal que designi l'IAS per tal que aquest personal adquireixi els coneixements necessaris per tal de poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició.

En cas que es contractin productes de seguretat o serveis de seguretat de les tecnologies de la informació i la comunicació que vagin a ser emprats en els sistemes d'informació de l'IAS, segons estableix l'ENS, hauran de tenir certificada la funcionalitat de seguretat relacionada amb el seu objecte d'adquisició. Els productes o serveis de seguretat hauran de constar al Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del Centre Criptològic Nacional o bé complir amb els criteris que estableixi l'Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centre Criptològic Nacional o, en el seu defecte, acreditar que el producte o servei disposa de requeriments equivalents.

6.5 Interconnexions

Segons preveu l'ENS, en el cas que sigui necessari realitzar interconnexions entre sistemes de l'empresa adjudicatària del contracte i l'IAS o amb d'altres entitats:

- No es podran dur a terme, tret que prèviament hagin estat autoritzades expressament per l'IAS.
- En cas que s'autoritzi una interconnexió, l'empresa adjudicatària del contracte haurà de garantir que es documentin com a mínim les característiques de la interfície, els requisits de seguretat i protecció de dades i la naturalesa de la informació intercanviada. Aquesta documentació l'haurà de facilitar a l'IAS.
- L'empresa adjudicatària del contracte haurà de participar en els mecanismes de coordinació que estableixi l'IAS i seguir els procediments establerts per aquest fi, per a poder atribuir i exercir de manera efectiva, les responsabilitats en relació a cada sistema interconnectat.

6.6 Verificació del compliment i auditoria

L'IAS es reserva el dret a verificar i auditar, amb mitjans propis o de tercers, el compliment de les mesures de seguretat requerides en base al marc legal de ciberseguretat i al marc intern per als sistemes d'informació emprats per a l'execució del contracte, en el moment i amb la periodicitat que s'estimi convenient. L'IAS podrà requerir el seguiment dels plans d'acció derivats d'aquestes verificacions i auditories. L'empresa adjudicatària del contracte haurà de disposar dels recursos adients per a dur terme l'execució de les tasques que li corresponguin en relació a aquest model de compliment, donant resposta en els terminis marcats per l'IAS. Si escau, la gestió del compliment es realitzarà amb les eines que determini l'IAS.

6.7 Incidents de seguretat

El POC haurà de notificar a l'IAS qualsevol incident de seguretat que pugui redundar, directament o indirectament, en la seguretat dels sistemes d'informació, en els terminis i per les vies que determini o els procediments establerts. L'empresa adjudicatària del contracte haurà d'aportar tota la informació necessària per a la seva gestió i notificació als organismes competents per part de l'IAS.

En cas que sigui necessari, l'empresa adjudicatària del contracte haurà de col·laborar amb qualsevol de les tasques que siguin requerides per part de l'IAS per a la identificació, contenció, erradicació, recuperació i recopilació de les evidències dels incidents de seguretat.

6.8 Accés a la informació

L'empresa adjudicatària del contracte haurà de garantir l'accés del personal autoritzat de l'IAS a la informació de seguretat (procediments, registre d'incidents, traces, etc.) per a poder desenvolupar l'objecte del contracte.

Tota la informació de seguretat haurà d'estar sempre disponible per a aquest personal, autoritzat i prèviament identificat. L'IAS i l'empresa adjudicatària establiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, establint els controls de seguretat mínims.

7 TERMINI D'EXECUCIÓ

El termini d'execució del contracte serà de 3 mesos màxim a contar des de la data de notificació de la adjudicació, segons el calendari que s'estipuli des de l'IAS.

8 TERMINI DE GARANTIA

Tot el hardware, software, llicències i funcionalitats incloses a la proposta tindran una **garantia mínima de 5 anys** per part del fabricant amb cobertura total pel hardware de peces, mà d'obra, i desplaçament.

9 DADES DE CONTACTE

Per a qualsevol dubte de caràcter tècnic relacionat amb aquest Plec de Prescripcions Tècniques, aclariment o visita tècnica es pot contactar amb la Direcció de sistemes d'informació al telèfon 972 18 90 25 o per correu electrònic: dgasquerda@gencat.cat.

Per a qualsevol dubte, aclariment de caràcter jurídic o administratiu, es podrà contactar amb la responsable de Contractació Administrativa Pública de l'IAS (M.Jesús Costa Serra) per telèfon 972 18 25 09 o per correu electrònic : mariajesus.costa@ias.cat.

Salt, a 31 de juliol de 2025

Daniel Garcia Asquerda

Director de Sistemes d'Informació de l'IAS