PLEC DE PRESCRIPCIONS TÈCNIQUES

SUBMINISTRAMENT, INSTAL·LACIÓ I POSADA DE SISTEMA DE BACKUP PER LES DADES GENERADES PER LA RECERCA QUANTUM MITJANÇANT PROCEDIMIENT OBERT NO SUBJECTE A REGULACIÓ HARMONITZADA

NÚMERO D'EXPEDIENT: 2025.SU.024

Continguts

CLÀUSULA 1. Objecte del contracte

El present contracte té com a objectiu el Subministrament, instal·lació i posada en marxa d'un dispositiu per assegurar el backup de les dades obtingudes de la recerca en relació amb les comunicacions Quàntiques portada a terme a l'ICFO.

CLÀUSULA 2. Necessitats a satisfer amb la contractació

Les necessitats d'emmagatzematge de dades provinents de la recerca en els darrers anys han augmentat de manera considerable, de l'ordre d'un 15% continuat des de fa 6 anys.

D'altra banda, la normativa legal, ens demana tenir la informació correctament arxivada i assegurada amb el sistema de backups adient.

Actualment s'estan emmagatzemant de l'ordre de 260 TB en diversos repositoris que no podran absorbir el volum de dades que s'espera generar amb el projecte definit al "Plan de Trabajo para la ejecución de un programa de I+D+I en el marco de los planes complementarios con cargo a fondos del plan de recuperación, transformación y resiliencia" en relació amb la Comunicació Quàntica. Tenint en compte que la capacitat total d'emmagatzematge és 460 TB i les dades abans esmentades més els snapshots necessaris per sortir d'una situació crítica suposen 380 TB, això ens deixa amb una capacitat lliure de 80 TB per nous grups i projectes de recerca.

Pel que fa a la capacitat de backups actualment es disposa de dos repositoris: un intern a l'ICFO (63 TB) i un extern (100 TB), per si el primer es veiés afectat. Davant d'un increment en la necessitat de backups, la gestió d'aquests dos sistemes per poder abastir-les, donat que no es disposa de la capacitat suficient, resulta en una intervenció continuada per part del departament d'IT, donat que s'han d'alliberar dades manualment per tal d'afrontar els nous backups complets una vegada al mes. D'altra banda, la copia de les dades des del repositori de backup intern cap a l'extern és excessivament lenta, ja que les dades s'han de rehidratar abans de poder enviar cap a l'exterior, consumint molt de temps en aquesta fase, i afegint una dificultat addicional.

Aleshores, un cop presentada la situació actual de l'ICFO quant emmagatzematge de dades i situació de backup d'aquestes, cal tenir en compte els següents requeriments derivats de la recerca i desenvolupament de sistemes de comunicació quàntica:

- Els sistemes de comunicació quàntica, tant siguin xarxes quàntiques com dispositius Quantum Key Distribution, generen un volum important de dades experimentals derivades, per exemple, dels registres de sincronització temporal, dades de calibratge de dispositius fotònics i òptics, etc. Cal un sistema d'emmagatzematge d'alta capacitat i velocitat que pugui registrar, processar i analitzar aquestes dades sense pèrdua d'integritat ni endarreriments.

- Els experiments quàntics necessaris per desenvolupar els sistemes de comunicació quàntica poden requerir condicions de laboratori exigents tant en economia com en temps i que puguin ser reproduïts. Per aquesta raó és important portar a terme un programa de backups de dades que permetin recuperar qualsevol experiment en cas de pèrdua de dades, ja sigui per ciberatacs, errors humans o corrupció de dades.

- Les comunicacions quàntiques estan suportades per una infraestructura "clàssica", en el sentit que depèn de controladores, sistemes de registre, nodes intermitjos, etc, de manera que que és necessari implementar sistemes "convencionals" de protecció de dades. En aquest sentit les cabines d'emmagatzematge i la seva

possibilitat d'encriptació de dades, i redundància, permeten garantir la confidencialitat, la integritat i la disponibilitat de la informació.

- D'altra banda, un dels objectius del programa és l'escalat dels sistemes de comunicació quàntica desenvolupat en l'àmbit del laboratori a la xarxa física i real actual. Per tant, cal sistemes tant d'emmagatzematge de dades com de backup que siguin fàcilment escalables, donat que l'augment de dades també augmentarà en la mateixa proporció.

- Com a darrera condició, podem dir que un projecte com aquest, recolzat per fons públics exigirà, com a mínim, la realització de còpies de seguretat periòdiques i la conservació de les dades durant un període no inferior a cinc anys.

Per tant, tenint en compte els requeriments a nivell d'emmagatzematge de dades requerit i la capacitat en la gestió i creació de backups actualment a l'ICFO, es considera estratègica la incorporació d'un sistema de backup robust de darrera generació, que permeti garantir la seguretat, integritat i disponibilitat de les dades experimentals i dels entorns de simulació crítica. S'ha de considerar un equip d'arquitectura escalable i resistent a ciberatacs que pugui garantir la continuïtat operativa dels experiments i la protecció de dades. Cal tenir en compte que el backup de les dades són un suport per mesuraments presents i futurs.

CLÀUSULA 3. Requeriments tècnics

A grans trets, els requeriments a satisfer són:

- Preservar Veeam com a únic programari de còpia de seguretat, per tal de poder conviure amb els sistemes de backup actuals de l'ICFO.

- Possibilitat d'introduir CommVault a l'arquitectura en mode de coexistència o com a substitució de Veeam: Opcions d'evolució il·limitades i sense dependència de proveïdor (*vendor lock-in*).

- Incorporar un repositori immutable que garanteixi:
  Recuperació davant ciberatacs mitjançant protecció *air-gapped* i objectes immutables.
  Còpies de seguretat i restauracions ultraràpides, incloent-hi l'arrencada instantània de màquines virtuals.

- Suport prèmium especialitzat en entorns de còpia de seguretat amb tècnic assignat
- El dispositiu de backup no pot ser un equip obsolet, hauria de pertànyer a una generació amb menys d'un any d'antiguitat i amb el suport garantit pel fabricant en un mínim de 5 anys.

Més específicament:

Factor de Forma 2U: Dissenyat per optimitzar l'espai en armaris de rack.

Capacitat: La solució ha de dimensionar-se per a satisfer les necessitats actuals definides anteriorment i el creixement estimat en 5 anys

  o L'emmagatzematge mínim requerit és de 370 TB, considerant com a tal l'emmagatzematge total net utilitzable real.

- El sistema ofertat tindrà una escalabilitat mínima de 5.000 TB de capacitat neta utilitzable real.
- Per calcular l'emmagatzematge net no es poden considerar els estalvis en l'eficiència obtinguts per deduplicació, es considerarà únicament la capacitat neta en disc després de les tasques bàsiques: donar format als discs, definició del RAID, etc.

Deduplicació i rendiment: La solució proposta ha d'incloure capacitat de deduplicació global per reduir l'espai d'emmagatzematge.

La solució serà un únic sistema hardware, amb deduplicació global basat en tecnologia de disc d'extrem a extrem, però contemplarà dues zones (tiers) diferenciades:

- **Landing Zone d'alt rendiment**: permet còpies de seguretat més ràpides i restauracions instantànies gràcies a la integració nativa amb Veeam mitjançant el *Data Mover* virtual, la qual cosa redueix la càrrega sobre els servidors *proxy* i millora l'eficiència global de l'entorn. Aquest fet resulta especialment útil per a les còpies cap a l'exterior, fent innecessària la rehidratació de les dades abans de ser enviades cap enfora, reduint les finestres temporals de backup. Idealment, les dades es guarden en aquesta zona en format nadiu de Veeam, per agilitar l'enviament cap a l'exterior, o la recuperació de dades per tornar a posar en producció.

- **Retention Zone immutable i *air-gapped***: les dades s'emmagatzemaran deduplicades i comprimides en un repositori no accessible per la xarxa, amb objectes immutables protegits contra *ransomware* i una política d'esborrat retardat (RTL) per un nombre de dies parametritzable, reforçant la ciberresiliència i assegurant el compliment de normatives com la NIS2. Això s'aconsegueix amb l'existència d'una air-gap entre ambdues zones, que permet aïllar l'entorn de retenció a llarg termini de possibles atacs realitzats des de la xarxa (dades no exposades a la xarxa).

Rendiment: Rendiment mínim de 16 TB/h per unitat donant uns 384 TB/h en total amb 24 unitats.

Còpies de Seguretat: Les còpies de seguretat i les restauracions s'han d'executar directament des del disc amb màxima velocitat, sense necessitat de rehidratar dades comprimides o deduplicades, és a dir, tant el backup com la recuperació de dades es faran des de la "landing zone" per tenir un rendiment òptim.

Compatibilitat amb VEEAM:

- El sistema ofertat respectarà la deduplicació nativa pròpia de VEEAM, proporcionant més eficiència i deduplicació addicional a la que ofereix el Veeam.
- La solució proposada permetrà que les funcionalitats avançades de VEEAM: *Sure Backup, Virtual Lab, Instant VM Recovery, Copy o Replicate,* utilitzin còpies de la informació en format natiu i sense deduplicació, per garantir la inmediatesa d'aquestes operacions
- La solució s'integrarà amb la funcionalitat '*Scale Out Backup Repositories'* (SOBR) de Veeam, permetent la federació de múltiples repositoris, per simplificar la gestió i l'automatització dels Jobs de backup i recuperació.
- La parametrització de les operacions de backup i recuperació s'ha de poder fer a través de la consola de VEEAM BR, sense passes addicionals.

Escalabilitat: Arquitectura escalable i resilient que permeti:

- Augmentar la capacitat de forma modular sense impactar el rendiment, sense migracions ni reconfiguracions.
- Garantir que el rendiment de l'equip podrà incrementar-se en paral·lel per tal que la finestra de backup no s'amplii malgrat el creixement del volum de dades.

Protecció i fiabilitat:

- Configuració RAID 6 amb almenys un disc hotspare.
- Opció de xifrat de dades en repòs (SEC basat en l'estàndard FIPS 140-2) fet en hardware, en els propis discos, per no impactar en el rendiment i la deduplicació del sistema.

Alimentació eléctrica: Subministrament monofàsic de 230 V amb endolls schucko EU / IEC C13

Connectivitat:

- Per xarxa, accessible mitjançant protocols estàndard, com a mínim NFS, CIFS i el propi de Veeam: Veeam Data Mover
- Mínim de 2 ports 1GbE + 4 ports 10 GbE
- Els ports 10 GbE haurien de ser compatibles RJ45 Base-T(10GbE), SFP+Twin Axial, SFP+Optical

Política de retenció: La solució proposada hauria de facilitar l'adopció de polítiques de gestió del cicle de vida de la informació (ILM), permetent la derivació de còpies històriques a núvols públics optimitzant costos segons l'SLA de retenció.

Verificació automatitzada de backups: La solució proposta ha de permetre la validació al 100% de la recuperabilitat de les còpies o aixecar serveis complets des del backup en entorns aïllats. D'aquesta manera es garanteix el compliment normatiu i la ciberresilència.

Retenció local ampliada: La deduplicació de la solució aportada ha de permetre estendre les retencions en local sense impacte econòmic, millorant el RTO, reduint la finestra de l'enviament de dades al núvol i assegurant el compliment de normatives com NIS2 o l'ENS.

Còpia segura i immutable de totes les dades: Cada còpia de seguretat s'emmagatzema com a objecte immutable. Cap dada pot ser alterada o esborrada, ni tan sols per un atacant intern o extern.

Air-gap físic real (sense accés extern): Les dades haurien de quedar completament aïllades de la xarxa. Sense ruta d'accés. Sense vector d'atac.

Protecció indeleble contra ransomware: La solució proposada ha de permetre l'emissió d'ordres d'esborrat retardades durant un mínim de 10 dies. Temps suficient per detectar, reaccionar i evitar la pèrdua de dades. Garantia de **disponibilitat total**.

Llicències: Incloure totes les llicències necessàries per la correcta activació de totes les funcionalitats descrites en el PPT, incloent la deduplicació, la protecció davant del ransomware, la replicació, la gestió remota, la integració amb Veeam, etc.

Redundància: El producte solució ha de ser fiable i redundant, i els discos i fonts d'alimentació han de ser reemplaçables en calent en cas de necessitar substituir-los.

Millores puntuables, d'acord amb el previst a l'Annex 2:

- Suport tècnic especialitzat per atendre incidències
- Actualitzacions i noves funcionalitats gratuïtes
- Manteniment preventiu i correctiu
- Disposar de Certificació d'aptitud en la integració dels productes, emès pel fabricant del dispositiu de backup.

CLÀUSULA 4. Distribució d'energia i seguretat

- El sistema ha d'estar configurat per a la xarxa elèctrica de la UE (Espanya) (tensió, endolls, etc.) i estar marcat CE.
- El sistema estarà totalment protegit contra talls de llum inesperats i, en aquest cas, serà totalment segur per als operaris. Un encès ràpid i fàcil del sistema ha de ser possible després d'un tall de corrent.

CLÀUSULA 5. Disseny del sistema i serveis

- La proposta inclourà un conjunt complet d'imatges, dibuixos i manuals del sistema, incloent dimensions, ubicació i detalls dels diferents components.
- La proposta inclourà els requisits complets d'instal·lació i posada en marxa, especificant clarament el tipus de connexió elèctrica, per a la configuració específica del sistema ofert.
- S'hauran d'especificar les característiques necessàries de l'entorn per garantir un funcionament eficient.

CLÀUSULA 6. Transport, instal·lació, encesa i formació

- La proposta inclourà el transport a les instal·lacions de l'ICFO, inclosa l'assegurança i tots els drets d'exportació/importació i de duana. **S'aplicarà l'incoterm DDP**.
- L'empresa adjudicatària col·locarà l'equip a la ubicació seleccionada per l'ICFO. L'adjudicatari/ària del contracte cobrirà tots els costos, l'organització i la coordinació de la col·locació de la cabina, inclòs qualsevol equip o vehicle especialitzat necessari, i qualsevol desmuntatge i muntatge de components necessaris per a la descàrrega del sistema i el transport dins de l'edifici fins a la ubicació de la sala tècnica objectiu.
- Inici del sistema in situ inclòs seguit de les proves d'acceptació especificades a continuació.
- Formació del sistema al personal de l'ICFO inclosa. El nombre de dies de formació i horari aproximat s'especificarà a la proposta

CLÀUSULA 7. Prova d'acceptació

7.1 Verificació de la instal·lació física i connexions:

Suport estructural

Verificar la instal·lació de rails específics del fabricant.
Respectar les clearances de disseny entre dispositius.
Verificació de pes i estabilitat.

Connexions d'alimentació i terra

Connexió dual PSU a circuits diferents.
Revisar indicadors LED: "Power OK" verd, absència d'alarmes / alertes.

Connexions de xarxa

Landing Zone / Backup traffic: 25 GbE (o 10GbE si no hi haguès disponibilitat de ports a 25 Gb en la ubicació del dispositiu).
Inter Appliance replication links: 10GbE dedicats.
VLANs i etiquetatge.
Port de gestió (directe o out-of-band).
Connexió a RADIUS o TACACS+ per autenticació.

Boot inicial:

Engegar l'appliance i capturar logs BMC/IPMI & event logs.
Verificar funcionalitat ventiladors, redundància, sensors.

7.2 Configuració inicial per CLI o GUI:

Accés a gestió

Accedir via IP de gestió o consola (ssh/serial).
Login: usuari per defecte → canviar contrasenya i OTP segons polítiques internes.

Paràmetres de xarxa i seguretat

Configurar DNS (lookup forwarding).
Configurar NTP (RFCs) segons polítiqu-es.
Establir rangs d'accés SSH/HTTPS.

Zones i capacitat

Landing Zone → buffer primari (configurar la seva mida d'acord amb la finestra de backup).
Retention Zone → dades guardades amb retenció d'acord a polítiques compliance. Configurar les polítiques de retenció dels diversos tipus de dades de l'ICFO.
Validar espai lliure i reserves per upgrade futurs.

Deduplicació i compressió

Confirmar que estan habilitades i definides variables com el chunk size, dedupe tables.
Documentar ratios teòrics i objectius segons especificacions del fabricant.

Immutabilitat i Security

Habilitar immutability / WORM amb temps mínim (ex. 90 dies).
Validar accés només per backups signats/automàtics.
Configurar alertes de manipulació mitjançant SIEM/log audit.

Seguretat addicional

Canviar certificats TLS per uns que porporcionarà l'ICFO, i si és possible, configurar ACME, perquè aquests es renovin automàticament abans de caducar.

Integrar en LDAP/AD.
Clau SSH pública / privada segons política.

7.3 Integració amb client de backup i validació:

Execució de backups

Full backup d'un volum test (mínim 1 TB).
Validar velocitat (≈16 TB/h) i completitud.
Avaluació de espai utilitzat i efficiency ratio.

Proves de restauració

Instant VM Recovery, és a dir arrencar VM des del backup.
Extracció de fitxers individuals.
Mesurar temps TTR (target ≤ 15 min VM, ≤ 5 min fitxer).

Test de replicació

Si es planifica multi-site: configurar peer, iniciar rèplica.
Comprovar eficàcia, diferències, integritat checksum.

Simulacions de fallades

Simular fallada de disc → ver alert, reemplaçament, rebuild.
Simular error de PSU → canvi d'una font sense apagar.
Upgrade firmware → seguir el procediment especificat pel fabricant: verificar si hi ha actualitzacions disponibles i, en aquest cas, validar l'èxit / rollback.

7.4 Monitorització, alertes i reporting.

Sistema d'alarmes i logs

Syslog/SSH forwarding a SIEM (ELK, Splunk).
Alertes proactives des del sistema de backup via SNMP v3 o emails.
Regles: fallades de disc, temperatura >55 °C, latència alta, fallades de backup.

Revisions periòdiques

Generació diària de report: backups completes/incompletes, error codes.
Reunió setmanal amb stakeholders responsables.
Pràctiques mensuals de test de restauració aleatòria.

Política de backups i retenció

Èxitus full, diferencials, incrementals (segons cycle).
Retenció mínima obligatòria, hold manual si cal.
Augmentar retenció per auditoria/legal segons GDPR.

Informes d'eficiència

Ratio dedupe, compressió, savings vs capacitat nominal.

Cost evitats (espai / temps / xarxa).

7.5 Acceptació final i transferència:

Documentació a l'entrega

Informe complet incloent: set-up, config, IPs, VLANs, zones, versions firmware/software.
Logs de boot, backups, test fallida/disc/PSU.
Taxa de compressió/dedupe, rapids restores, replicació testada.

Procediments operatius

Manuals: onboarding de nous job de backup, escalat issues, aplicació updates.
Checklists diàries d'estat i alertes.
Runbooks per fallades comunes (disc, PSU, stuck HA).

Formació i Transferència

Sessió de training (1–2 h) amb sysadmins i backup team.
Simulació Falles → exercicis de resposta.

SLA / suport

Revisar contactes de suport del fabricant i SLA (ex. resposta < 2 h critical).
Registrar contracte de manteniment.
Confirmar que tots els contactes/escalats estan operatius.

7.6 Escenaris Adversos.

Les proves d'acceptació hauran d'incloure l'assaig i resolució de diversos escenaris adversos:

Fallada de disc: Simulació o extracció controlada d'un disc dur.

Procediment:

- Forçar (o simular via GUI) la fallida d'un dels 24 discos.
- Observar temps de detecció i notificació.
- Monitorar rebuild del RAID (RAID-6 amb hot spare).
- Avaluar impacte en l'escriptura i lectura durant la reconstrucció.

Criteris d'acceptació:

- Alarmes generades (GUI, SNMP, e-mail).
- No hi ha pèrdua de dades ni interrupció del servei.
- Rebuild dins temps estimat (4–8h segons mida).

Tall sobtat d'alimentació: Simulació de fallida elèctrica a una o ambdues fonts d'alimentació.

Procediment:

- Tallar una font redundant → validar failover automàtic.
- Tallar ambdues fonts (amb supervisió).
- Tornar a alimentar → verificar boot clean i coherència RAID.

Criteris d'acceptació:

- Registre dels errors al log.
- No corruptes dades en cap zona (landing ni retention).
- Reengegada controlada amb alertes posteriors.
- Cap backup programat fallit de forma permanent.

Pèrdua de connexió de xarxa: Desconnexió d'una interfície de xarxa (backup o gestió).

Procediment:

- Desconnectar físicament el port de dades (10/25GbE).
- Simular caiguda de VLAN o tall de ruta.
- Verificar que es manté la disponibilitat via gestió o IP secundària.

Criteris d'accepació:

- Backup en curs falla amb error controlat (timeout, no corrupció).
- Alertes de xarxa generades.
- Resta d'operacions no compromeses.

Simulació d'atac ransomware / malware: Simular accés no autoritzat i intent d'eliminar backups.

Procediment:

- Intentar esborrar dades des de client amb accés a share CIFS/NFS.
- Accedir via usuari de backup a dades immutables.
- Simular script de xifrat massiu.

Criteris:

- Les dades immutables no poden ser esborrades ni modificades.
- L'usuari no pot alterar retencions.
- Logs d'intent registrats i notificats.
- Confirmació que polítiques Time-lock estan operatives.

Intent de manipulació d'admin / usuari: Intent de canvi de polítiques per un usuari amb accés.

Procediment:

- Accedir amb compte administrador i intentar:
  - Modificar polítiques de retenció.
  - Deshabilitar immutability.
  - Borrar dades "a la força".

Criteris:

- Qualsevol canvi és loguejat i notificat.
- Si el sistema té *retention lock*, les polítiques no poden ser modificades.
- Confirmar que l'auditoria no es pot esborrar.

Fallada de replicació remota: Intent de canvi de polítiques per un usuari amb accés.

Procediment:

- Accedir amb compte administrador i intentar:
  - Modificar polítiques de retenció.
  - Deshabilitar immutability.
  - Borrar dades "a la força".

Criteris:

- Qualsevol canvi és loguejat i notificat.
- Si el sistema té *retention lock*, les polítiques no poden ser modificades.
- Confirmar que l'auditoria no es pot esborrar.

Error de firmware/software: Actualització amb error o rollback de versió.

Procediment:

- Aplicar una actualització amb defecte controlat.
- Forçar rollback.
- Validar consistència i funcionament post-rollback.

Criteris:

- Logs complets de l'error.
- No impacte en configuració ni en dades existents.
- Restauració possible a versió funcional anterior.

Atac per xarxa (DoS o accessos múltiples): Simulació de múltiples connexions simultànies o escaneig actiu.

Procediment:

- Llençar peticions múltiples (test de càrrega).
- Escaneig de ports des d'IP externa.
- Provar límits de sessions SMB/NFS.

Criteris:

- El sistema rebutja o limita connexions no autoritzades.
- Alertes en logs.
- No afecta processos de backup ja en marxa.

7.7 Documentació final

- Tota la configuració documentada.
- Planificació de suport, escalat i manteniment definida: Software per un mínim de 5 anys i Hardware 24x7 – 4h reposició de peces durant 5 anys.
- Validació de les proves amb signatura de client/responsable tècnic.

CLÀUSULA 8. Garantia i suport de seguiment

- **Garantia completa de 1 any** en totes les peces i components del sistema, independentment del fabricant. La garantia inclourà la substitució de qualsevol peça defectuosa o danyada durant l'ús normal del sistema, independentment del fabricant dels components. Cobrirà qualsevol cost relacionat amb el desmuntatge, el transport, la reparació i el muntatge dels components danyats, inclosos tots els costos de viatge i manutenció dels enginyers de servei requerits. Una reparació in situ, o una alternativa justificada per reduir el temps d'inactivitat del sistema al mínim, sempre serà la primera opció de servei. Caldrà disposar d'un equip d'enginyers de servei degudament qualificats i qualificats.
- Suport durant tota la vida del sistema:
  - Per telèfon, correu electrònic i videotrucada amb resposta en 2 dies hàbils.
  - Visita d'urgència després d'una avaria del sistema en un termini de 10 dies hàbils.
- L'equip de servei tècnic ha de tenir seu a Europa.

CLÀUSULA 9. Termini d'entrega i instal·lació

El sistema s'ha de lliurar i instal·lar a ICFO en un termini màxim de **5 setmanes.**

El termini de lliurament es defineix com el temps transcorregut des de la signatura del contracte fins al lliurament del sistema a les instal·lacions de l'ICFO. Inclou la fabricació del sistema, el transport, la instal·lació i la prova d'acceptació a les instal·lacions d'ICFO.

CLÀUSULA 10. Pressupost de licitació

- El preu objectiu del sistema és de 220.000€ (IVA exclòs).
- Condicions de pagament:

- 20% a la signatura del contracte,
- 30% quan el 80% dels materials principals estiguin disponibles i comenci el muntatge del sistema,
- 40% a l'entrega,
- 10% després de la formació i acceptació de la instal·lació.

Castelldefels, a data de la seva signatura digital

Carlos Dengra Tineo
Facilities Management Head