	ANNEX 12	Data: febrer 2025
	SISTEMA DE CONTROL DE LA QUALITAT DE NETEJA	Pàgina 1 de 5

I si es presenta la millora d'un sistema de control de qualitat, en el termini de 10 mesos a comptar des del dia de l'inici del servei haurà de posar en marxa el sistema de control de la qualitat de neteja i servei que permeti un seguiment de les tasques de cada lloc de treball definit, de la supervisió feta per l'empresa i el seu resultat.

El sistema proposat ha d'implicar a tot el personal de neteja en la recollida de dades de manera que cada treballador formi part activa del sistema.

El sistema ha de permetre:

- Definir els llocs de treball del centre i relacionar cada un amb el metratge de neteja.
- Determinar les càrregues de treball de cada lloc de treball definit.
- Relacionar els llocs de treball amb les persones que l'ocupen.
- Registrar per cada lloc de treball les tasques efectuades per jornada diària
- Diferenciar entre neteges generals, neteges a fons, neteges ordinàries, aïllaments,... Es a dir ha de permetre flexibilitat en els ítems a seguir.
- Definir quins elements es controlen a cada tipus de neteja
- El sistema ha de donar dades en temps real
- L'Hospital ha de tenir accés al sistema en temps real. Aquest accés ha de ser fent servir tecnologies que impliquin nul·la modificació de les estacions de treball estàndard en producció a la nostra organització, sense necessitat de programari client dedicat (accés web "https" des d'un navegador).
- Ha de permetre flexibilitat en la seva configuració per tal de poder demanar dades addicionals per part de l'Hospital relacionades amb el sistema .

L'empresa adjudicatària ha de presentar mensualment un informe derivat del sistema que permeti saber:

Nº de llocs de treball del centre

Nº de persones en el centre dia a dia

Dades agregades d'altres realitzades

Dades agregades d'altres realitzades al centre i per franja horària


Seguiment de neteges a fons, dades de terminis i temps dedicat

Dades agregades de neteges rutinàries, de fons, aïllaments,

Seguiment de la supervisió pròpia de l'empresa de neteja

Dades agregades de les diferents supervisions

Els sistemes proposats s'hauran de poder fer efectius a l'Hospital i l'empresa haurà de comptar amb la despesa de proveir els equips que siguin precisos pels diferents llocs de treball de l'Hospital, així com dels elements i tecnologies necessaris per l'adequat desenvolupament de les seves funcions. Si els operaris de la neteja han de portar equipament per enregistrar les seves tasques, aquest equipament no ha de dependre dels serveis de comunicacions de l'Hospital. L'empresa ha de proporcionar el mecanisme de connectivitat d'aquest equipament amb el sistema central de gestió per tal d'enviar les dades que ha enregistrat i que quedin emmagatzemades en aquest sistema (ja sigui de forma síncrona o asíncrona).

	ANNEX 12	Data: febrer 2025
	SISTEMA DE CONTROL DE LA QUALITAT DE NETEJA	Pàgina 2 de 5

Les dades obtingudes amb aquest sistema seran propietat de l'Hospital i per tant exportats totalment al sistema informàtic de l'Hospital mensualment, en un format que no impliqui l'ús de programari no estàndard a la nostra organització, i que permeti un tractament àgil i eficaç de les dades contingudes.

El sistema proposat haurà de complir amb els principis bàsics de la seguretat de la informació :

- Confidencialitat : assegurant l'accés a la informació només a aquelles persones amb la deguda autorització.
- Integritat : el sistema ha de mantenir la informació tal qual sigui generada, minimitzant al màxim la possibilitat de manipulació o alteració per part de persones o processos no autoritzats. A efectes d'assegurar aquesta integritat, ha de comptar amb un mecanisme de traçabilitat de les accions sobre el sistema que puguin alterar o manipular les dades.
- Disponibilitat : el sistema ha d'estar disponible en tot moment en que sigui requerit, a fi de no entorpir les tasques del personal que en fa ús.
- Autenticació : el sistema ha de permetre identificar a qui genera la informació, a través dels mecanismes de programari o maquinari implementats per l'empresa licitadora.

El sistema proposat ha de permetre definir diferents permisos per als usuaris que l'utilitzin, ja siguin de visualització, modificació o administració sobre la plataforma, podent arribar a una major granularitat en la seva aplicació.

El sistema ha de permetre el registre de les actuacions realitzades per usuari sobre la plataforma per a poder tenir una traçabilitat de les tasques realitzades, en cas de ser requerides en algun moment. En aquest cas, l'HCB proporciona el sistema ADFS (Active Directory Federation Services) per a poder interconnectar el sistema via SAML amb el nostre AD (Active Directory) i així simplificar l'alta, baixa o modificació dels usuaris, com l'autenticació dels mateixos al sistema.

En el cas de que no sigui possible utilitzar aquesta solució, l'empresa ens haurà d'indicar com es realitzaran aquestes tasques administratives al sistema, que hauran de ser el més simple possible i no provocar una càrrega de treball a l'HCB per acometre aquesta tasca.

Les empreses hauran de fer una demostració del sistema en funcionament que es valorarà.


En cas de que fos necessari, s'adjunten els requeriments de connectivitat, Hardware i Software:

CONNECTIVITAT

En cas de que l'equip es requerís connectivitat a la xarxa de l'Hospital aplicarà el següent:

Xarxa cablejada

- Interfície Ethernet amb conector RJ45
- Velocitat: autonegociació 10/100/1000 Mbps
- Mode dúplex: autonegociació half/full

	ANNEX 12	Data: febrer 2025
	SISTEMA DE CONTROL DE LA QUALITAT DE NETEJA	Pàgina 3 de 5

Xarxa sense fils

- Interfície inalàmbrica recomanada basada en estàndar 802.11ac. En el cas de que no es suporti, hauria de suportar els estàndars A i/o B/G/N
- Protocols de roaming: 802.11k, 802.11r i 802.11v

Xarxa cablejada i sense fils

- Suport 802.1x utilitzant usuari i contrasenya i certificat.

Altres

Cal que el licitador proporcioni informació precisa d'altres mitjants de connectivitat que incorporin els equips, com Bluetooth, NFC o altres tecnologies basades en transmissió radioelèctrica. I complir:

- Encriptació: Tota transmissió inalàmbrica ha de ser xifrada.
- Freqüències: No s'utilitzen bandes de freqüència ja utilitzades a l'Hospital per altres solucions (WiFi, RFID, lectors temperatura)

Protocols de comunicació

Les comunicacions entre diferents elements es realitzaran amb protocol TCP/IP de manera segura, utilitzant sempre rangs de ports acotats que caldrà comunicar per tal que es puguin definir regles d'accés en els tallafocs corporatius.

Adreçament IP i nom d'equip

Qualsevol dispositiu, a excepció dels servidors, ha de poder obtenir IP de forma automàtica mitjançant el servidor DHCP corporatiu.


Tots els dispositius hauran de ser configurats amb un nom d'equip previament pactat amb la DSI, el servidor DHCP registrarà de forma automàtica en el DNS aquest nom.

Les comunicacions entre diferents elements hauran de realitzar-se sempre a través dels noms d'equip en format FQDN, permetent així que els canvis de IP no suposin indidents de comunicacions.

Gestió

- Consola de gestió central

Per a desplegament de gran nombre d'elements caldrà incloure, en cas de que no existeixi ja, una consola central de gestió que permeti realitzar operacions a múltiples dispositius amb una sola acció (evitant la mateixa operació equip a equip).

	ANNEX 12	Data: febrer 2025
	SISTEMA DE CONTROL DE LA QUALITAT DE NETEJA	Pàgina 4 de 5

Accés remot

- Equips d'usuari

Si fos necessari l'accés remot a un equip d'usuari, aquest haurà de ser autoritzat cada vegada que sigui necessari i supervisat per personal intern.

- Servidors

L'accés remot als servidors es realitzarà amb un client VPN proporcionat per la DSI. Aquests accessos són de caràcter nominal i hauran de ser sol·licitats per personal de l'Hospital.

Cloud

- Solucions basades en cloud

Caldrà definir quin tipus de dades son emmagatzemades en clouds públics.

Les comunicacions per aquest tipus d'entorn caldrà que siguin autoritzades pels responsables de tractament de dades de l'Hospital.

L'accés a les dades en clouds públics s'ha de realitzar de manera segura i s'ha d'enregistrar l'accés i les tasques realitzades mitjançant un usuari nominal.

En cas de ser necessari, el servei cloud es pot autenticar amb el nostre Directori Actiu mitjançant SAML.

Hardware

- Servidors

Per norma general la implantació de nous servidors es realitzarà sota la plataforma de virtualització corporativa. Qualsevol excepció haurà de tenir el vist i plau de la DSI i complir les especificacions de hardware establertes internament.


- PCs

Per norma general s'intentarà no incloure PCs, aprofitant sempre que sigui possible i no hi hagi disconformitat per part de la DSI els PCs que hi ha desplegats a l'hospital.

En cas de requerir nous PCs, la DSI donarà les especificacions del hardware a incloure en el PPT. En alguns casos, si es considera convenient, es podria optar per modalitat virtual. En aquest cas caldria incloure en el PPT els costos de llicenciament.

- SO

No s'admeten SO obsolets o no suportats pels fabricants. En el cas dels servidors les plataformes suportades són Microsoft Windows Server 2016 o SuSE Linux 15.

	ANNEX 12	Data: febrer 2025
	SISTEMA DE CONTROL DE LA QUALITAT DE NETEJA	Pàgina 5 de 5

Els equips han de poder estar protegits per l'antivirus corporatiu de l'HCB (Symantec) i han de poder instal·lar-se els mecanismes de còpies de seguretat i recuperació corporatius.

La solució ha de permetre que s'instal·lin els pegats de seguretat que cregui convenient l'HCB per a la seguretat de la plataforma.

En el cas dels PCs la plataforma suportada és Windows 10.

Qualsevol excepció haurà de tenir el vist i plau de la DSI, i en el cas de tenir cost de llicenciament caldria incloure'l al PPT.

- Base de dades

Per norma general la utilització de Bases de dades ha d'utilitzar els motors homologats per l'Hospital: MSSQL Server, MySQL, MariaDB. Qualsevol excepció haurà de tenir el vist i plau de la DSI, i en el cas de tenir cost de llicenciament caldria incloure'l al PPT.

-CIBERSEGURETAT

L'empresa adjudicatària s'ha de responsabilitzar del compliment de les mesures en ciberseguretat que, d'acord amb el Reial Decret 311/2022 de 3 de maig pel qual es regula l'Esquema Nacional de Seguridad (ENS), ha establert l'HCB relacionades amb els equips i/o serveis objecte del contracte. Per acreditar aquest compliment l'adjudicatari ha de presentar la documentació indicada a l'annex del PPT "Seguretat TI i OT". El serveis corresponents, requeriran aquesta documentació a l'empresa que hagi presentat la millor oferta en el tràmit de requeriment establert a l'article 150.2 de la LCSP. En cas de no complir adequadament el requeriment, o no complir amb els requeriments sol·licitats, s'aplicarà allò establert en el mateix article 150.2.