



ANNEX 1 – REQUERIMENTS TÈCNICS ESPECÍFICS

SERVEI DE CIBERSEGURETAT PER AL CONSORCI SANITARI INTEGRAL

EXPEDIENT CSI2026003



CatSalut

Servei Català
de la Salut



Generalitat de Catalunya
Departament de Salut

Índex

1	Requeriments del servei.....	3
1.1	Requeriments Fortinet.....	3
1.1.1	Fortigate 1800F	3
1.1.2	FortiMail	3
1.1.3	FortiSandbox.....	3
1.1.4	FortiAnalyzer	3
1.1.5	FortiSIEM	4
1.2	Requeriments Trend Micro.....	4
1.2.1	Trend Micro Vision ONE	4
1.2.2	Trend Micro Email Security	4
1.2.3	Trend Micro Security Expert.....	4
1.3	Millores als requeriments.....	4
1.3.1	FortiPAM.....	5
1.3.2	FortiDeceptor	5
1.3.3	Trend Micro Security Expert.....	5
1.3.4	Trend Micro CREM.....	5
2	Oficina tècnica de seguretat de la informació (OTSI).....	6
2.1	Governança i Compliment Normatiu.....	6
2.2	Gestió de Riscos i Consultoria Estratègica	7
2.3	Operacions i Suport Tècnic Especialitzat	7
2.4	Formació i Conscienciació.....	8
2.5	Perfil professional i Certificacions.....	8
3	Serveis de suport.....	9
3.1	Suport i garantia del fabricant	9
3.2	Suport de l'adjudicatari	9
3.2.1	Tipus de suport.....	9
3.2.2	Acords de nivell de servei (SLA).....	10
3.3	Monitorització.....	10
3.4	Firmware i upgrades	10
3.4.1	Upgrade anual	11
3.4.2	Upgrade firmware i software d'emergència	11
3.4.3	Consideracions generals.....	11
4	Service Manager.....	12

5	Formació.....	13
---	---------------	----

1 Requeriments del servei

Els requeriments descrits a continuació han de renovar-se i estar suportats al llarg de tota la durada del contracte.

Si no s'indica el contrari, s'ha de prendre com a base l'inventari de serveis i tecnologies del quadre del punt 2.

1.1 Requeriments Fortinet

1.1.1 Fortigate 1800F

El CSI disposa de dos tallafocs perimetral que treballen en alta disponibilitat (actiu-passiu), cadascun instal·lat a un datacenter diferent, tots dos ubicats a HSJDMB.

Es requereix la renovació del suport hardware, llicenciamnt i subscripció dels equips:

- Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium).

Si el licitador ho considera es poden oferir equipaments nous del mateix fabricant, amb llicències de la mateixa durada requerida, sempre que les característiques siguin iguals o superiors a les dels equips actuals.

1.1.2 FortiMail

Es requereix el subministrament i la instal·lació d'un segon node que permeti l'alta disponibilitat (HA) amb la infraestructura existent. El llicenciamnt ha de ser l'equivalent, permetent 2 x vCPU cores i la resta de característiques. El suport al llicenciamnt dels equips ha de ser:

- FortiCare Premium and FortiGuard Base.

1.1.3 FortiSandbox

El canvi recent de llicenciamnt per part del fabricant obliga a subministrar i instal·lar nova infraestructura amb el següent llicenciamnt:

- Advanced AI Sandbox subscription
- 3 x FortiSandbox Windows Licenses Expands FSA license of Windows 11 for FSA VM Appliance
- 1 x FortiSandbox Office Licenses Expands FSA (Appliance/VM) licenses of Microsoft Office 2021
- 1 x FortiSandbox Windows Licenses Addon FortiSandbox license of Microsoft Windows 11 by 1

1.1.4 FortiAnalyzer

Renovació del suport al llicenciamnt de l'equips:

- FortiAnalyzer-VM FortiCare Premium Support FortiCare Premium Support (for 1- 101 GB/Day of Logs)
- FortiAnalyzer-VM Upgrade license for adding 25 GB/Day of Logs

1.1.5 FortiSIEM

Actualment el CSI té un servei de SIEM ubicat en el cloud de l'actual adjudicatari, basat en FORTISIEM.

Es requereix d'un servei de SIEM ubicat a la infraestructura externa (cloud públic o privat) proposada per l'adjudicatari, amb les capacitats de ingesta i retenció que tenim actualment a CSI, que són uns 1500 events per segon (EPS) i un mínim de 150 dispositius. El cost d'aquest servei estarà inclòs dintre del servei.

El servei de SIEM haurà de tenir una integració nativa amb la actual infraestructura de seguretat del CSI, mitjançant connectors certificats pel fabricant dels dispositius, sense necessitat de desenvolupaments addicionals, SDL o agents personalitzats.

1.2 Requeriments Trend Micro

1.2.1 Trend Micro Vision ONE

Es mantindrà i renovarà el llicenciament actual tan per la part d'endpoint (Endpoint Security Essentials) com per els servidors (Endpoint Security PRO).

1.2.2 Trend Micro Email Security

El CSI es troba actualment en un procés de migració de les bústies de correu a Microsoft 365. Per tant, el llicenciament pel número de bústies indicades al quadre anterior, s'anirà migrant al llarg de la durada del contracte, i de manera progressiva, cap a:

- Trend Vision One Email and Collaboration Security – Core

Cal tenir en compte que, durant el període de migració, serà necessari un sistema híbrid on hauran de conviure les dues plataformes alhora (Trend Micro Email Security i Trend Vision One Email and Collaboration Security – Core).

La proposta haurà de detallar el procés d'implantació via API en l'entorn M365, assegurant una configuració amb impacte mínim per l'usuari final i garantint la continuïtat del servei. Haurà de ser integrable amb les plataformes actuals de CSI sense requerir desenvolupaments ni adaptacions pròpies.

La solució proposada haurà de generar informes periòdics que garanteixin la continuïtat del servei i permetin el registre i la gestió de logs d'incidents.

La instal·lació i configuració de l'eina aniran a càrrec de l'adjudicatari.

1.2.3 Trend Micro Security Expert

No es requereix de la renovació de servei de Trend Micro Security Expert. Tot i això, la inclusió d'aquest servei a l'oferta és una característica que es podrà valorar.

1.3 Millores als requeriments

Sense perjudici del compliment obligatori de tots els requeriments del servei establerts en aquest plec, es valorarà la inclusió d'una sèrie de serveis addicionals o millores opcionals. Aquests serveis no són requerits per la prestació essencial del contracte, però l'aportació d'un o diversos d'ells, en els termes que el licitador determini a la seva Proposta Tècnica, es valorarà d'acord amb la puntuació detallada en els criteris d'adjudicació. S'estableixen un màxim de

quatre possibles millores, i cada una d'elles serà avaluada de manera independent i assignada la puntuació corresponent només si compleix íntegrament la seva especificació.

Aquestes millores només podran optar a puntuar als criteris objectius en cas de que s'ofereixin per tot el període del contracte.

1.3.1 FortiPAM

A CSI disposem de comptes amb privilegis elevats que requereixen una gestió segura i controlada. Per garantir la protecció, el control i la supervisió d'aquests accessos, es proposa la implantació de la solució Privileged Acces Management (PAM) del fabricant Fortinet. Aquesta solució permetrà gestionar de manera segura les credencials i els accessos dels diferents usuaris a la infraestructura de CSI.

Es valorarà la incorporació de la solució FortiPAM a CSI, amb un llicenciamient per a 25 usuaris concurrents.

1.3.2 FortiDeceptor

Per millorar la detecció d'atacs avançats dins la infraestructura del CSI, especialment en les fases inicials de reconeixement i moviment lateral, es proposa la incorporació de la solució FortiDeceptor. Aquesta eina permetrà reduir el temps de detecció i augmentar la capacitat de resposta davant d' incidents de seguretat.

Es valorarà la integració de FortiDeceptor dins la infraestructura actual del CSI amb un llicenciamient per 3 vlans.

1.3.3 Trend Micro Security Expert

Es valorarà la inclusió del servei Trend Micro Security Expert, aportant assessorament especialitzat, revisió proactiva de les configuracions de l'eina, detecció avançada de vulnerabilitats i recomanacions alineades amb millors practiques i normatives (ISO 27001, ENS, NIS2, RGPD).

1.3.4 Trend Micro CREM

La solució Trend Micro CREM (Cyber Risk Exposure Management) permet descobrir, avaluar, prioritzar, predir i mitigar els riscos de una manera proactiva dins del entorn del CSI.

Actualment no es disposa de crèdits dedicats a aquesta solució, per tant, es valorarà la inclusió dels crèdits necessaris per garantir la disponibilitat permanent de la solució **Trend Micro CREM Core** per a la totalitat dels Endpoints (equips clients i servidors) llicenciats.

2 Oficina tècnica de seguretat de la informació (OTSI)

L'Oficina Tècnica de Seguretat de la Informació (en endavant OTSI) es constituirà com el punt central de referència i el principal òrgan d'assessorament i consultoria en matèria de ciberseguretat per al CSI. La seva missió serà ajudar en garantir la confidencialitat, la integritat i la disponibilitat de la informació i els sistemes, així com acompanyar en el compliment del marc normatiu vigent, amb una atenció especial a l'Esquema Nacional de Seguretat (ENS), al Reglament General de Protecció de Dades (RGPD) i la Directiva NIS2, assegurant l'alineació amb les millors pràctiques i estàndards internacionals.

La prestació del servei inclourà, com a mínim, una sessió mensual on es tractaran els diferents temes que gestiona l'oficina. A més, es poden incloure una quantitat no establerta de sessions específiques de treball per tecnologia i amb diferents àmbits i departaments de l'hospital o organitzacions i agències externes.

L'OTSI actuarà com una extensió de l'equip de l'hospital, proporcionant el coneixement expert i el suport tant de manera continuada com sota demanda, per a la correcta governança de la seguretat de la informació. Les seves funcions principals es poden agrupar en les àrees següents:

2.1 Governança i Compliment Normatiu

Aquesta és la pedra angular del servei per a una entitat pública. L'OTSI s'encarregarà que l'organització compleixi totes les seves obligacions legals i normatives en matèria de seguretat.

- **Assessorament i adequació a l'ENS/NIS2:** Fer l'avaluació inicial, definir la Declaració d'Aplicabilitat, elaborar el Pla d'Adequació i mantenir tota la documentació exigida per l'Esquema Nacional de Seguretat. S'inclou el suport continu per superar les auditories de certificació.
- **Suport en Protecció de Dades (RGPD i LOPDGDD):** Col·laborar estretament amb el Delegat de Protecció de Dades (DPD) de l'hospital. Això inclou la realització d'Anàlisis de Riscos per als tractaments de dades, l'execució d'Avaluacions d'Impacte (AIPD) quan sigui necessari i la definició de mesures de seguretat tècniques i organitzatives.
- **Supervisió de la normativa sectorial:** Garantir el compliment de normatives específiques del sector salut, com la Llei 41/2002 d'autonomia del pacient, i altres regulacions que afectin la seguretat de la informació clínica i els sistemes d'informació sanitària.
- **Elaboració i manteniment del cos normatiu:** Desenvolupar, revisar i actualitzar el conjunt de polítiques, normatives i procediments de seguretat de la informació de l'hospital, assegurant que estiguin alineats amb la legislació i les millors pràctiques.

El servei haurà d'incloure:

- Un **perfil Sènior en Ciberseguretat (OTSI)** per desenvolupar tots els punts citats anteriorment, que haurà de liderar la definició, la implantació i el seguiment del model de seguretat de la informació.

2.2 Gestió de Riscos i Consultoria Estratègica

L'OTSI ha de proporcionar una visió estratègica i anticipar-se a les amenaces, ajudant l'hospital a prendre decisions informades.

- **Anàlisi i gestió de riscos tecnològics:** Realitzar anàlisis de riscos periòdiques sobre la infraestructura tecnològica, les aplicacions (incloent-hi sistemes d'informació hospitalària com HIS/RIS/PACS) i els dispositius mèdics connectats. Els anàlisis hauran de contemplar la identificació de vulnerabilitats, l'avaluació de l'impacte i la definició de plans de mitigació. A més, s'hauran de proposar accions orientades a la millora continua dels processos de protecció, detecció i resposta davant incidents de seguretat.
- **Assessorament en projectes i noves adquisicions:** Actuar com a consultor de seguretat en qualsevol nou projecte tecnològic o en l'adquisició de nou equipament (programari, maquinari, dispositius mèdics). La seva funció serà emetre informes de seguretat que garanteixin que les noves incorporacions no introdueixen riscos inacceptables i compleixen les polítiques de l'hospital.
- **Elaboració del Pla Director de Seguretat:** Definir el full de ruta estratègic en matèria de ciberseguretat a mitjà i llarg termini, alineat amb els objectius de l'hospital.
- **Informes i Quadres de Comandament (Reporting):** Generar informes periòdics per a la direcció sobre l'estat de la seguretat, el nivell de compliment normatiu, els riscos identificats i el progrés del Pla Director. Aquests informes han de ser clars i executius.

2.3 Operacions i Suport Tècnic Especialitzat

Aquesta àrea se centra en el dia a dia de la ciberseguretat, donant suport directe als equips tècnics de l'hospital.

- **Suport en la gestió d'incidents de seguretat:** Liderar la resposta davant d'incidents de ciberseguretat. Això inclou l'anàlisi forense, la coordinació de les accions de contenció i erradicació, la coordinació amb tercers (fabricants, ISP, integradors), la comunicació a les parts afectades (inclosa la notificació de violacions de dades a l'AEPD) i l'elaboració d'informes postincident.
- **Gestió de vulnerabilitats:** Supervisar i coordinar el cicle de vida de la gestió de vulnerabilitats. L'OTSI no necessàriament executarà l'escaneig, però sí que n'analitzarà els resultats, prioritzarà la criticitat de les vulnerabilitats en el context de l'hospital i en farà un seguiment de la remediació amb els equips tècnics o tercers.
- **Arquitectura de seguretat:** Dissenyar i proposar arquitectures de seguretat robustes i resilients per a la xarxa, els sistemes i les aplicacions de l'hospital, incloent-hi la segmentació de xarxes (especialment per aïllar dispositius mèdics) i la configuració segura dels sistemes.
- **Intel·ligència de Ciberamenaces:** Mantenir una vigilància activa sobre les amenaces específiques del sector salut (grups de ransomware, campanyes de pesca electrònica o *phishing*, etc.) i informar proactivament l'hospital sobre els riscos emergents i les contramesures recomanades.

2.4 Formació i Conscienciació

El factor humà és crucial, especialment en un entorn amb personal molt divers com un hospital.

- **Pla de Formació i Conscienciació Anual:** Dissenyar i impartir un programa continu de sensibilització en ciberseguretat per a tot el personal de l'hospital (sanitari, administratiu, etc.). Aquest pla ha d'incloure formacions específiques segons el rol i el nivell de risc.
- **Campanyes de Simulació de Pesca Electrònica (*Phishing*):** Realitzar campanyes periòdiques de simulació d'atacs de *phishing* per avaluar el nivell de conscienciació dels empleats i reforçar l'aprenentatge.
- **Elaboració de Guies i Bones Pràctiques:** Crear i difondre material de fàcil comprensió, com ara guies, infografies o butlletins de seguretat, sobre temes rellevants (ús segur del correu electrònic, protecció de dispositius mòbils, etc.).

2.5 Perfil professional i Certificacions

L'Equip encarregat de l'OTSI haurà de complir, com a mínim, amb els requisits següents:

- **Certificacions professionals en Ciberseguretat:** CompTIA Security+, CISA, CISM o CISSP, sent obligatori disposar-ne almenys d'una.
- **Certificacions en metodologies d'auditoria i hacking ètic:** CEH, OSCP o equivalents.
- **Experiència demostrada** en OTSI, consultoria de Ciberseguretat, governança i gestió de riscos.
- **Coneixements acreditats** en la gestió de marcs de referència ENS, NIS2, NIST CSF, RGPD i ISO 27001.

3 Serveis de suport

3.1 Suport i garantia del fabricant

Tots els equipaments inclouran una garantia de maquinari al llarg de la durada del contracte 24x7 a partir de la data de l'acta de recepció de la licitació. Aquesta garantia haurà de tenir un temps de resposta per canvi de peces hardware de màxim 4 hores in-situ. Aquest suport haurà d'incloure tant el manteniment hardware dels equipaments com tot el software, llicències o subscripcions incloses en la proposta.

Si el fabricant no disposa de suport proactiu l'adjudicatari haurà de cobrir el suport de tots els elements, monitoratge, proves de contingència i upgrade mitjançant una bossa d'hores suficientment dimensionada per cobrir el suport durant la vigència del contracte, i amb personal certificat en la màxima qualificació disponible per cadascun dels diferents elements de la infraestructura oferta.

Tant en les incidències de la plataforma com en la reposició de peces, l'esforç en la seva resolució ha de ser continuat fins a la seva resolució.

3.2 Suport de l'adjudicatari

L'adjudicatari haurà de donar suport tant a les incidències com a les peticions de servei que es puguin obrir al llarg de la durada del contracte. L'adjudicatari proporcionarà una bossa d'hores de suport per a peticions de servei i capacitació en les diferents tecnologies suportades pels operadors i administradors del CSI. Aquesta bossa d'hores tindrà un volum mínim de 25 hores anuals. Les peticions de servei tindran un horari de recepció de 9 x 5, amb un temps de resposta de "Next Business Day" i un temps de resolució màxim d'una setmana. Aquestes peticions seran per a resoldre dubtes i/o aplicar modificacions sobre la infraestructura suportada. Les capacitacions es pactaran amb l'adjudicatari per tenir temps de preparació del temari i organització de les sessions.

La gestió d'incidències i peticions de servei es realitzarà utilitzant les eines pròpies de CSI per a la gestió d'incidències informàtiques (software "Atlassian Jira en el moment de publicar aquest expedient). L'adjudicatari rebrà les peticions i incidències via correu electrònic, però haurà d'informar directament als referents del servei al CSI dels canvis d'estat per poder fer seguiment. Eventualment, l'adjudicatari podrà rebre les incidències i peticions per telèfon pel que haurà de proporcionar la informació de comunicació a les diferents franges horàries per cobrir el servei. Les incidències **no descomptaran hores bossa d'hores**. L'horari de recepció d'incidències serà 24x7x365.

3.2.1 Tipus de suport

Es pot definir el suport en els següents grups:

- **Manteniment Preventiu:** Orientat a la revisió constant del estat de la infraestructura i serveis, mantenint-la estable respecte a les necessitats de CSI. Realitzant les següents tasques:
 - Revisió de logs, gràfiques, alertes periòdiques i estat dels serveis.
 - Comprovar l'estat de tots els clúster HA i de la resta d'equipaments i eines a CSI.
 - Revisió de les diferents configuracions i polítiques aplicades.
 - Upgrade de Firmware dels equips.

- Backups periòdics de la configuració d'equips/appliance a CSI.
- Revisió de l'estat dels agents de TMVO.
- Estat del risc per servei.
- **Manteniment proactiu:** Aquell que no està contemplat dintre del manteniment preventiu:
 - Revisió de vulnerabilitats i realització del Upgrade firmware per evitar la vulnerabilitat detectada.
 - Notificació de funcionalitats no aplicades dels productes instal·lats a CSI que puguin millorar el servei.
 - Anàlisi forense de logs per trobar fons d'atacs i vulnerabilitats.
- **Manteniment Correctiu:** Inclourà la gestió de totes les incidències i peticions realitzades per CSI. Aquest servei contempla l'assistència tècnica remota i in-situ quan sigui necessari, així com la gestió d'escalat al fabricant en cas de que es requereixi.

3.2.2 Acords de nivell de servei (SLA)

Per tal d'estandarditzar la gestió de la qualitat i disponibilitat del servei, els Acords de Nivell de Servei (SLA) aplicables es defineixen mitjançant la matriu de nivells establerta en l'epígraf 7.4 del plec de prescripcions tècniques. Aquesta matriu classifica la resposta, resolució i disponibilitat en tres nivells de servei, adaptats a la crítica de la nostra organització.

A continuació es presenta una taula amb el nivell de servei específic dels diferents elements que componen el servei integral de ciberseguretat:

ELEMENT	NIVELL DE CRITICITAT
Firewalls Fortigate	VITAL
FortiMail	ALT
FORTISANDBOX	MIG
FORTIANALYZER	MIG
FORTISIEM	MIG
TrendMicro Vision One	VITAL
TrendMicro Email Security / Collab	ALT

3.3 Monitorització

El CSI disposa d'una plataforma de monitorització basada en Centreon. Durant tota la durada del contracte de servei, l'adjudicatari haurà de donar suport a CSI en les tasques necessàries per monitoritzar tot el hardware i software instal·lat.

3.4 Firmware i upgrades

El licitador haurà d'incloure dins del cost dels diferents elements del model d'oferta econòmica els costos d'actualització i manteniment de firmware i software al llarg de la durada del suport dels equips. Aquesta actualització haurà de realitzar-se anualment com a mínim i com a upgrade de firmware d'emergència en casos necessaris.

3.4.1 Upgrade anual

L'adjudicatari es compromet a que de forma anual realitzarà una actualització, on apliqui, de tots els elements inclosos en el suport de la proposta. Aquesta actualització inclourà l'actualització de firmware de tots els equipaments.

3.4.2 Upgrade firmware i software d'emergència

En cas de que durant la vida del contracte hi hagi una fallada en els equipaments subministrats o un anunci de vulnerabilitat o possible fallada catalogat com a crític pel fabricant, el licitador haurà de realitzar una actualització de firmware d'emergència per tal de mantenir els equipaments subministrats en un nivell de firmware estable i suportat pel fabricant.

També es considerarà com a upgrade de firmware d'emergència el fet que el suport del fabricant demani una versió concreta de firmware per tal de poder donar aquest suport.

3.4.3 Consideracions generals

En qualsevol upgrade de firmware s'hauran de complir les següents consideracions generals:

- El upgrade l'haurà de realitzar el fabricant directament amb el suport, si fos necessari, de personal tècnic de l'adjudicatari emprant el contracte de suport i garantia del fabricant.
- Els upgrades es realitzaran per la nit o en cap de setmana, també en període nocturn, en funció de les diferents necessitats dels serveis assistencials.
- La planificació es realitzarà amb 15 dies d'antelació a l'aturada, per tal de planificar els impactes i riscos de la intervenció i plans de contingència en cas necessari.
- En cas d'upgrade d'emergència la planificació serà el més ajustada possible atenent la urgència del canvi i les necessitats assistencials del Consorci Sanitari Integral.

4 Service Manager

Es requereix la disponibilitat d'un Service Manager dedicat, aportat per el licitador, complint com a mínim amb les següents característiques i responsabilitats:

- **Interlocució fluida en català/castellà i capacitat de comunicació executiva**, garantint una comunicació clara i estructurada tant amb perfils tècnics com directius, assegurant la correcta traducció de necessitats, riscos i decisions.
- **Coneixement profund de l'entorn, les tecnologies implantades i l'estratègia de seguretat del client**, assegurant una visió completa i actualitzada per a la correcta gestió del servei.
- **Actuació com a trusted advisor del CSI**, oferint recomanacions objectives i alineades amb les bones pràctiques del sector, marcs normatius (ISO 27001, ENS, NIS2, NIST CSF, RGPD) i fulls de ruta tecnològics existents.
- **Assessorament proactiu i en temps real davant riscos, vulnerabilitats i amenaces emergents**, emetent alertes, recomanacions i accions preventives basades en intel·ligència de Ciberseguretat actualitzada, garantint sempre l'alineació amb les plataformes implantades i l'estat operatiu del servei.
- **Coordinació integral de tots els processos de canvi**, incloent migracions, actualitzacions, ampliacions i millores. El gestor de servei vetllarà perquè totes les intervencions es duguin a terme amb garanties, sense afectacions al servei, assegurant la correcta planificació, validació, supervisió i comunicació abans, durant i després del canvi.
- **Provisió d'informes regulars d'estat, evolució i compromís del servei**, com a mínim haurà de lliurar informes mensuals (o amb la periodicitat que el CSI determini) que incloguin: nivell de compliment SLA/KPI, incidències crítiques i recurrents, millores proposades, evolució de l'arquitectura, estat de les integracions, anàlisi de riscos i recomanacions estratègiques.
- **Punt únic de contacte (Single Point of Contact – SPOC) per a la gestió de casos crítics i escalaments**, sent el responsable de coordinar tots els equips del proveïdor i, si escau, terceres parts involucrades, garantint una resposta ràpida, coordinada i eficient en situacions d'alt impacte.
- **Planificació estratègica anual i revisió del servei**, incloent roadmap tecnològic, recomanacions d'optimització, identificació de possibles riscos operatius i proposta de millores contínues.
- **Seguiment i governança del contracte**, assegurant el compliment de totes les obligacions, el correcte consum de llicències i serveis, i la detecció de desviacions, riscos o necessitats futures.

5 Formació

L'adjudicatari farà una proposta de formació per al traspàs de coneixements de la solució. El CSI vol fer un refresc formatiu al personal tècnic de la solució un cop implantada. Aquesta formació inicial serà com a mínim de 12 hores, dividida en 3 sessions de 4 hores per a facilitar l'assistència de tot el personal necessari.

El contingut mínim d'aquesta formació serà:

- Descripció general de les tecnologies emprades en el servei de ciberseguretat
- Descripció dels diferents elements que componen la solució, tant hardware com software.
- Funcionament habitual de la solució
- Funcionalitats que es poden implementar en la solució, tot i que no hagin estat implementades en primera instància
- Passos habituals per a la diagnosi d'incidències
- Aprofundir a les eines de monitorització i gestió
- Registre d'errors

Al llarg de la durada del contracte es requereix una sessió de formació anual, típicament repartida en 3 jornades de 2 hores, per resoldre dubtes operatius i aprofundir en la gestió i administració de la solució.

Les sessions formatives les realitzarà un tècnic especialitzat i qualificat, coneixedor de la estructura de forma global que pot donar solucions a dubtes, explicació de noves funcionalitats per upgrade de versió o resposta a futures necessitats que es puguin plantejar.