Localret

INFORME TÈCNIC DE VALORACIÓ DELS CRITERIS D'ADJUDICACIÓ LA QUANTIFICACIÓ DELS QUALS DEPÈN D'UN JUDICI DE VALOR – LOT 4 SERVEIS DE CENTRE D'OPERACIONS DE SEGURETAT (SOC) CORRESPONENT A L'ACORD MARC DE SUBMINISTRAMENT DE SOLUCIONS I SERVEIS GESTIONATS DE SEGURETAT TIC (Exp. 1431-0003/2025)

1 Proposicions

El passat 14 de d'abril de 2025 la mesa de contractació va procedir a obrir el sobre 1 de les proposicions de les empreses licitadores, que conté la documentació acreditativa de la capacitat i solvència.

Dins del termini han presentat les seves proposicions les empreses següents:

	Data de presentació
1. SEMICONDUCTORES Y SISTEMAS SA	10/04/2025 a les 11:27:31 h.
2. SISTEMAS INFORMÁTICOS ABIERTOS SAU	11/04/2025 a les 09:19:54 h.
3. VODAFONE ESPAÑA SAU	11/04/2025 a les 09:52:47 h.
4. SISTEMAS AVANZADOS DE TECNOLOGÍA SA	11/04/2025 a les 10:59:24 h.
5. SEIDOR SOLUTIONS SL	11/04/2025 a les 11:29:39 h.
6. GMV SOLUCIONES GLOBALES INTERNET SAU	11/04/2025 a les 11:31:04 h.
7. APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA	11/04/2025 a les 11:44:11 h.
8. CLARANET SAU	11/04/2025 a les 11:52:10 h.
9. ORANGE ESPAGNE SAU	11/04/2025 a les 12:03:18 h.
10. CONNECTIS ICT SERVICES SAU	11/04/2025 a les 12:28:37 h.
11. S2 GRUPO SOLUCIONES DE SEGURIDAD SLU	11/04/2025 a les 12:31:59 h.
12. SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL	11/04/2025 a les 12:44:21 h.
13. ATECH ADVANCED SOLUTIONS SA	11/04/2025 a les 13:06:45 h.
14. OMEGA PERIPHERALS SL	11/04/2025 a les 13:23:59 h.
15. TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU	11/04/2025 a les 13:31:00 h.
16. EVOLUTIO CLOUD ENABLER SAU	11/04/2025 a les 13:41:19 h.
17. INETUM ESPAÑA SA	11/04/2025 a les 13:42:47 h.
18. ITGLOBAL SL	11/04/2025 a les 13:48:53 h.
19. CAPGEMINI ESPAÑA SL	11/04/2025 a les 10:07:05 h.
20. EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL	11/04/2025 a les 09:14:26 h.
21. A2SECURE TECNOLOGÍAS INFORMÁTICA SL	11/04/2025 a les 12:27:03 h.
22. SOTHIS SERVICIOS TECNOLÓGICOS SLU	11/04/2025 a les 13:12:49 h.
23. KPMG ASESORES SL	11/04/2025 a les 13:17:00 h.

24. SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS SAU (SERMICRO) — 11/04/2025 a les 09:14:26 h.

El passat 24 d'abril de 2025 la mesa de contractació va procedir a l'obertura del sobre 2 de les proposicions de les empreses licitadores, que conté la proposta tècnica i la documentació relativa als criteris d'adjudicació la quantificació dels quals depèn d'un judici de valor (lot 4).

2 Admissió d'ofertes

A la clàusula vint-i-sisena del PCAP s'especifica quina documentació havien de presentar les empreses licitadores; en concret, pel que fa al lot 4:

> "**1. Funcions i capacitats del SOC**:
>
> 1.1. Capacitats de prevenció: Proposta detallada que descrigui els processos i eines que utilitzarà l'empresa per complir i mitigació d'aspectes identificats a la superfície d'exposició externa.
> 1.2. Capacitats de detecció: Descripció detallada de les eines i tecnologies de protecció que es desplegaran, incloent-hi funcionalitats d'automatització.
> 1.3. Resposta a incidents: Procediments i protocols per a la resposta a incidents, incloent-hi el procés de notificació i erradicació.
>
> **2. Prestacions tècniques del SIEM**:
>
> Memòria descriptiva del/s SIEM proposat/s, que inclogui l'arquitectura, incloent els elements de recol·lecció amb la seva ubicació, agregació i processat d'esdeveniments, el dimensionament i mètriques de llicenciament, automatitzacions i correlacions, així com de registres
> d'activitat i els elements a incloure de cara a la integració amb el Centre Criptogràfic Nacional.
>
> **3. Implantació del SOC**:
>
> Proposta de processos, procediments i estratègia d'implantació."

Aquesta informació és necessària perquè l'òrgan de contractació pugui verificar que l'oferta és admissible d'acord amb els criteris que figuren en els plecs.

La mateixa clàusula vint-i-sisena del PCAP advertia el següent:

> "Incloure en el sobre 2 qualsevol informació de l'oferta de caràcter rellevant avaluable de forma automàtica (sobre 3), comportarà l'exclusió de l'empresa licitadora quan es vulneri el secret de les ofertes o el deure de no tenir coneixement del contingut de la documentació relativa als criteris de valoració "fórmula matemàtica" abans d'avaluar les ofertes de conformitat amb els criteris "judici de valor"."

Els criteris avaluables de forma automàtica són:

1. Temps d'instal·lació i gestió d'un SIEM: ... dies naturals (temps mínim, 5 dies naturals / temps màxim 15 dies naturals).
2. Generació d'informes d'incidències: sí / no.
3. Generació d'informes post-incident: sí / no.
4. Temps de resposta i resolució d'incidències no crítiques: ... hores (temps mínim, 1 hora / temps màxim, 24 hores).

Doncs, bé, l'empresa SEMICONDUCTORES Y SISTEMAS SA (SEYS) ha inclòs dins del sobre 2 informació rellevant que hauria d'estar inclosa en el sobre 3; en concret, el temps d'implantació d'un SIEM (a la pàgina 11 de la seva proposta indica els dies que trigaria a implantar un SIEM, 7 dies), la generació d'informes d'incidències (a la pàgina 13 indica que generarà informes d'incidents, i quin contingut tindran), la generació d'informes post-incident (a la pàgina 14 de la seva proposta assenyala que es compromet a elaborar un informe port-incident complet i detallat, amb indicació del seu contingut) i el temps de resposta i resolució d'incidències no crítiques (a la pàgina 15 de la seva proposta explica quin temps aplicarà per atendre aquestes incidències no crítiques).

Igualment, l'empresa KPMG ASESORES SL inclòs dins del sobre 2 informació rellevant que hauria d'estar inclosa al sobre 3; en concret, el temps d'instal·lació d'un SIEM (a la pàgina 16 de la seva proposta indica en una taula les jornades de treball de cada fase), la generació d'informes post-incident (a la pàgina 17 indica com presentarà l'informe post-incident) i el temps de resposta i resolució d'incidències no crítiques (a la pàgina 21 de la seva proposta presenta un apartat complert, on parla d'aquests temps de resposta i resolució d'incidències no crítiques)

Les ofertes de les empreses SEMICONDUCTORES Y SISTEMAS SA (SEYS) i KPMG ASESORES SL han de ser excloses de la licitació.

A criteri de la sotasignada, la resta d'ofertes de les empreses presentades són admissibles d'acord amb els criteris que figuren en els plecs:

1. SISTEMAS INFORMÁTICOS ABIERTOS SAU
2. VODAFONE ESPAÑA SAU
3. SISTEMAS AVANZADOS DE TECNOLOGÍA SA
4. SEIDOR SOLUTIONS SL
5. GMV SOLUCIONES GLOBALES INTERNET SAU
6. APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA
7. CLARANET SAU
8. ORANGE ESPAGNE SAU
9. CONNECTIS ICT SERVICES SAU
10. S2 GRUPO SOLUCIONES DE SEGURIDAD SLU
11. SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL
12. ATECH ADVANCED SOLUTIONS SA
13. OMEGA PERIPHERALS SL
14. TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU
15. EVOLUTIO CLOUD ENABLER SAU
16. INETUM ESPAÑA SA
17. ITGLOBAL SL
18. CAPGEMINI ESPAÑA SL
19. EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL
20. A2SECURE TECNOLOGÍAS INFORMÁTICA SL
21. SOTHIS SERVICIOS TECNOLÓGICOS SLU

22. SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS SAU (SERMICRO)

3 Avaluació dels criteris d'adjudicació dels quals depèn d'un judici de valor

Criteris d'adjudicació la quantificació dels quals depèn d'un judici de valor, fins a un màxim de 45 punts:

"**1. <u>Funcions i capacitats del SOC</u>, fins a un màxim de 30 punts**:

Es valoraran les funcions del servei SOC proposat: prevenció, detecció, protecció i resposta a incidents:

1.1. <u>Capacitats de prevenció</u>, fins a un màxim de 10 punts:

Es valorarà la millor idoneïtat de la solució per anticipar amenaces, gestionar vulnerabilitats i analitzar la superfície d'exposició de l'entitat, segons els següents paràmetres:

- Informes d'inventari i classificació d'actius segons la seva criticitat.
- Eines utilitzades per a l'anàlisi i gestió de vulnerabilitats, amb especial èmfasi en els escanejos de vulnerabilitats, proves tècniques com pentests i tests de phishing.
- Propostes concretes per al seguiment i mitigació d'aspectes identificats a la superfície d'exposició externa.

Les empreses licitadores presentaran una proposta detallada que descrigui els processos i eines que utilitzarà per complir aquestes funcions, així com evidències de l'ús d'eines homologades (per exemple CVE, CVSS 3.1) per al *scoring* de vulnerabilitats."

S'han agrupat les ofertes en diferents grups per rang de puntuació:

<u>Grup A – Alt nivell (10-8 punts)</u>:

Aquestes ofertes mostren una maduresa alta en ciberseguretat i una visió estratègica clara.

Característiques destacades:

- Presenten informes d'inventari complets, amb classificació de sistemes segons la seva criticitat.
- Utilitzen eines avançades d'anàlisi de vulnerabilitats, com escanejadors automàtics amb integració de bases de dades CVE.
- Demostren una capacitat proactiva per anticipar amenaces i gestionar vulnerabilitats.
- Inclouen propostes concretes i detallades per al seguiment, mitigació i millora contínua de l'exposició externa.

Les empreses incloses en aquest grup són: EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL, SISTEMAS INFORMÁTICOS ABIERTOS SAU, EVOLUTIO CLOUD ENABLER SAU, A2SECURE TECNOLOGÍAS INFORMÁTICA SL, SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL, S2 GRUPO SOLUCIONES DE SEGURIDAD SLU, SEIDOR SOLUTIONS SL, INETUM ESPAÑA SA, SISTEMAS AVANZADOS DE TECNOLOGÍA S.A, SOTHIS SERVICIOS TECNOLÓGICOS SLU i GMV SOLUCIONES GLOBALES INTERNET SAU.

- **EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL**:

  La seva oferta detalla un procés complet d'inventari i classificació d'actius, amb integració automàtica a la CMDB.
  La gestió de vulnerabilitats inclou escanejos automatitzats (Nessus), pentesting (OWASP, OSSTMM), simulacions BAS (PICUS), i reporting periòdic. Utilitzen estàndards reconeguts (CVE, CVSS 3.1) per a la classificació i priorització.
  L'anàlisi de la superfície d'exposició externa és exhaustiva: escanejos, pentesting, anàlisi de codi, proves de phishing i plans de mitigació amb seguiment actiu.
  S'evidencia l'ús d'eines homologades i metodologies avançades, amb exemples d'informes i dashboards.
  La proposta és proactiva, modular i adaptable cobrint de manera excel·lent la prevenció, amb processos i eines homologades, automatització i adaptabilitat, garantint la màxima anticipació i gestió de riscos.

  Es proposa assignar a l'oferta de l'empresa EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL 10 punts.

- **SISTEMAS INFORMÁTICOS ABIERTOS SAU**:

  SISTEMAS INFORMÁTICOS ABIERTOS SAU planteja una estratègia de prevenció molt completa, basada en la gestió i classificació d'actius a través de Proactivanet ITAM i altres solucions (com Nessus, Tenable, Rapid7 o scripts propis), a més d'informes detallats i una gestió acurada de llicències.
  La detecció i gestió de vulnerabilitats es fonamenta en escanejos actius i sistemes d'alerta primerenca (com Achilles), utilitzant estàndards reconeguts com CVE i CVSS 3.1, i generant informes periòdics per fer-ne el seguiment.
  L'anàlisi de la superfície d'exposició contempla escanejos, proves de penetració, revisió de codi, simulacions de phishing (amb GoPhish) i l'elaboració de plans de mitigació amb un seguiment actiu de les accions.
  A més, la proposta incorpora metodologies de referència (OWASP, OSSTMM, MITRE ATT&CK), informes d'auditoria i dashboards per monitoritzar l'estat de la seguretat.
  En definitiva, la prevenció de SIA destaca per l'ús d'eines homologades, processos ben definits, fet que la converteix en una de les opcions més robustes en aquest àmbit.

  Es proposa assignar a l'oferta de l'empresa SISTEMAS INFORMÁTICOS ABIERTOS SAU 10 punts.

- **EVOLUTIO CLOUD ENABLER SAU**:

  EVOLUTIO aposta per una prevenció sòlida, amb una gestió contínua de vulnerabilitats (TVM), inventari i classificació d'actius segons la seva criticitat (tant amb CMDB pròpia com del client), i escanejos mensuals de vulnerabilitats mitjançant Tenable, amb informes detallats (CVE/CVSS 3.1) i reunions de seguiment regulars.
  La seva proposta inclou l'anàlisi de la superfície d'exposició externa, proves tècniques com pentests, revisió de codi i campanyes de phishing, així com informes de risc, monitoratge de filtracions de dades, dark web i accions de conscienciació per als usuaris.
  La metodologia d'EVOLUTIO segueix estàndards reconeguts (CVE, CVSS, NIST, MITRE ATT&CK) i demostra capacitat d'adaptació, reporting i millora contínua.
  En resum, EVOLUTIO cobreix tot el cicle preventiu amb eines homologades, processos detallats, informes automatitzats i simulacions, assegurant una anticipació eficaç i una gestió proactiva de vulnerabilitats i exposició.

  Es proposa assignar a l'oferta de l'empresa EVOLUTIO CLOUD ENABLER SAU 10 punts.

- **A2SECURE TECNOLOGÍAS INFORMÁTICA SL:**

  L'empresa A2SECURE TECNOLOGÍAS INFORMÁTICA SL proposa la realització d'inventari i classificació d'actius per criticitat, així com la composició del mapa de xarxa i mapa d'arquitectura.
  Utilitza eines reconegudes com Qualys, Acunetix, Burp Suite, Metasploit, Nmap, Nessus. Inclou la realització d'escaneigs de vulnerabilitats, auditories tècniques i proves d'intrusió (pentests, anàlisi de codi font, tests de phishing) aplicant metodologies OWASP, PCI-DSS, OSSTMM. Gestiona el cicle de vida de les vulnerabilitats (Descobriment, Priorització, Compensació) i utilitza CVE i CVSS 3.1 per a la classificació d'aquestes vulnerabilitats i *scoring,*. Analitza la superfície d'exposició externa per identificar debilitats des de la perspectiva d'un atacant.
  Compleix tots els requeriments, però amb menys detall que les ofertes anteriorment avaluades, menys integració i menys capacitat de personalització i seguiment continu.

  Es proposa assignar a l'oferta de l'empresa A2SECURE TECNOLOGÍAS INFORMÁTICAS SL 9 punts.

- **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL (SIRT)**:

  La proposta de SIRT presenta un servei preventiu molt complet, amb gestió contínua de vulnerabilitats, inventari i classificació d'actius segons criticitat (integració amb SIEM Splunk, Asset & Risk Intelligence, CMDB, etc.), ús d'eines homologades (Nessus, Rapid7, OpenVAS, FortiRecon, SOC Radar), escanejos autenticats i no autenticats, informes automatitzats i quadres de comandament.
  Inclou proves tècniques periòdiques (pentests, phishing, simulacions d'engany), seguiment de la superfície d'exposició externa, detecció de malware, monitoratge de leaks i dark web, i campanyes de conscienciació.
  La metodologia està alineada amb estàndards reconeguts (CVE, CVSSv4, EPSS, NIST, OWASP, MITRE ATT&CK) i es demostra una clara capacitat d'adaptació i coordinació amb el SOC Tàctic i la Xarxa Nacional de SOC.
  Es troben a faltar plataformes de simulació BAS, que SIRT no ofereix, per a l'avaluació continua dels controls de prevenció.

  Es proposa assignar a l'oferta de l'empresa SIRT 9 punts.

- **S2GRUPO SOLUCIONES DE SEGURIDAD SLU**:

  La proposta de S2GRUPO es distingeix per un sòlid enfocament en la prevenció, amb una gestió de vulnerabilitats robusta i una estreta coordinació amb el SOC Tàctic de l'Agència. Aquesta col·laboració permet una personalització i adaptació a les necessitats específiques del sector públic local, oferint una visió molt alineada amb la realitat de l'entorn.
  L'oferta es fonamenta en la plataforma GLORIA, que opera com a SIEM, i utilitza l'eina Tenable Nessus Professional Vulnerability Scanner per a l'anàlisi de vulnerabilitats internes i externes, incloent el descobriment d'actius i la classificació basada en el risc. La seva metodologia per a pentesting i enginyeria social es basa en estàndards reconeguts com OSSTMM, OWASP i GIAC, demostrant una maduresa estratègica significativa.
  Li manca l'avaluació continua dels controls de prevenció.

  Es proposa assignar a l'oferta de l'empresa S2GRUPO SOLUCIONES DE SEGURIDAD SLU 9 punts.

- **SEIDOR SOLUTIONS SL**:

  Implementa un procés d'Inventari i classificació d'actius continu (descobriment inicial i manteniment) tenint en compte les particularitats de cada organització. Utilitza Qualys Asset Inventory, Tenable.SC, Nmap, Shodan.

Excel·lència en Proves Tècniques ja que realitza escanejos (autenticats/no autenticats) amb ús d'eines estàndard com Tenable Nessus, Metasploit i Burp Suite Pro i també realitza Pentests (caixa negra, grisa, blanca) usant metodologies reconegudes PTES, OSSTMM, OWASP. Inclou Tests de phishing per a la sensibilització.
El *scoring* utilitza CVE i el sistema CVSS v4.0 (la versió més recent). Fa seguiment i mitigació de la superfície d'exposició externa amb escaneig actiu (Nmap, Masscan) i monitoratge de reputació (MISP, IBM, OTX, X-Force)
Li manca l'avaluació continua dels controls de prevenció.

Es proposa assignar a l'oferta de l'empresa SEIDOR SOLUTIONS SL 9 punts.

- **INETUM ESPAÑA SA**:

L'oferta cobreix de manera àmplia tots els requeriments establerts, incloent l'inventari i classificació d'actius amb eines com Forescout i Flexxible, aplicant metodologies com ISO 27001 i NIST, així com la gestió de vulnerabilitats amb Tenable Nessus, utilitzant CVE i CVSS 3.1, alertes primerenques, informes periòdics, integració amb SIEM i suport a l'aplicació de pegats. També s'hi inclouen auditories tècniques (pentesting) i de seguretat perimetral basades en OSSTMM i OWASP, exercicis de phishing regulars, informes detallats i plans de formació, a més de propostes concretes per al seguiment i mitigació de la superfície d'exposició mitjançant accions coordinades. La descripció presentada és detallada i aporta evidències clares de l'ús d'eines i metodologies reconegudes.
Tot i això, no s'hi aporta tant de detall com en les propostes anteriors pel que fa a la automatització d'esdeveniments, fet que justifica una puntuació inferior. Més específicament, la proposta no detalla l'automatització dels *workflows* de gestió i tancament del cicle de vida de les vulnerabilitats (detecció, assignació i mitigació), que permetrien un tractament més ràpid i precís dels pegats i correccions. També es penalitza lleugerament la manca d'ús de l'última versió de l'estàndard CVSS v4.0

Es proposa assignar a l'oferta de l'empresa INETUM ESPAÑA SA 8,5 punts.

- **SISTEMAS AVANZADOS DE TECNOLOGÍA SA**:

SATEC presenta una proposta molt sòlida pel que fa a l'inventari i classificació d'actius, utilitzant la plataforma Qualys VMDR per fer un inventari automàtic i classificació segons la criticitat, amb etiquetes dinàmiques i informes personalitzats. La gestió de vulnerabilitats es basa en escanejos periòdics automàtics i comprovacions manuals, integrant estàndards com CVE i CVSS 3.1. S'inclouen proves de pentesting (intern i extern) amb metodologies reconegudes (OSSTMM, OWASP, PTES), i campanyes de phishing personalitzades.
Tanmateix, hi ha alguns aspectes on la proposta podria ser més exhaustiva: No queda clar si la gestió de vulnerabilitats cobreix tot el cicle de vida (detecció, assignació, seguiment i tancament) amb *workflows* automatitzats. No s'explicita la integració directa amb una CMDB (Base de Dades de Configuració) corporativa ni si l'inventari es manté sincronitzat amb altres sistemes. La periodicitat i abast de les proves de *phishing* i *pentesting* no es detallen tant com en altres ofertes. Aquestes mancances en la formalització del cicle de vida de la vulnerabilitat justifiquen una puntuació de 8 punts.

Es proposa assignar a l'oferta de l'empresa SISTEMAS AVANZADOS DE TECNOLOGÍA SA 8 punts.

- **SOTHIS SERVICIOS TECNOLÓGICOS SLU**:

La proposta de SOTHIS desplega una estratègia de prevenció que va molt més enllà del simple compliment normatiu. Amb una combinació d'eines com Tenable Nessus i Outpost24, la vigilància dels actius digitals es converteix en una autèntica xarxa de sensors que anticipen les amenaces. Tot i que no detalla la classificació de actius, si detalla l'escoring de vulnerabilitats amb CVS i CVSS v3.1. Proposa un servei de pentesting

semestral per posar a prova els sistemes de l'organització. Podria millorar la seva proposta amb més exemples de simulacres reals i formació pràctica per als equips interns, li manca també l'avaluació continua dels processos de detecció per millorar la qualitat del servei.

Es proposa assignar a l'oferta de l'empresa SOTHIS SERVICIOS TECNOLÓGICOS SLU 8 punts.

- **GMV SOLUCIONES GLOBALES INTERNET SAU**:

L'empresa presenta un enfocament molt complet per anticipar amenaces, gestionar vulnerabilitats i analitzar la superfície d'exposició de l'entitat. Disposen d'una eina pròpia, GestVul®, que permet inventariar i classificar els actius segons la seva criticitat, i que facilita la generació d'informes detallats i quadres de comandament avançats. Aquesta eina integra escanejos actius (amb Nessus i Qualys), escanejos passius, i permet la importació de resultats de pentests i altres eines homologades, sempre utilitzant estàndards com CVE i CVSS v3 per al scoring de vulnerabilitats.
Encara que GMV utilitza l'eina pròpia GestVul®, les ofertes amb major puntuació (com EY i SIA) han detallat de manera més exhaustiva la integració i automatització dels *workflows* per a la gestió i tancament del cicle de vida de les vulnerabilitats (detecció, assignació de responsables, seguiment i mitigació)
A més, GMV inclou en la seva metodologia la realització de pentests, tests de phishing (tant automatitzats com manuals) i fins i tot exercicis de *vishing* amb IA generativa, la qual cosa demostra una aposta clara per la conscienciació i la detecció proactiva de vulnerabilitats humanes. També es posa èmfasi en el seguiment i la mitigació d'aspectes identificats a la superfície d'exposició externa, amb propostes concretes i processos de validació de solucions.
La proposta de GMV no obté la màxima puntuació perquè li manca incloure l'avaluació contínua dels controls de prevenció mitjançant plataformes de simulació d'atacs com BAS/CTEM (Breach and Attack Simulation / Continuous Threat Exposure Management)

Es proposa assignar a l'oferta de l'empresa GMV SOLUCIONES GLOBALES INTERNET SAU 8 punts.

Grup B – Bon nivell (75–6 punts):

Aquestes ofertes són sòlides, però amb marge de millora pel que fa la integració i seguiment continuat.

Característiques destacades:

- Disposen d'un inventari funcional, tot i que pot no estar completament classificat per criticitat.
- Utilitzen eines d'anàlisi de vulnerabilitats, però amb menor grau d'automatització o cobertura.
- Inclouen algunes propostes de seguiment, però no sempre són sistemàtiques ni detallades.
- Mostren una bona capacitat reactiva, amb iniciatives per millorar la postura de seguretat.

Les empreses incloses en aquest grup són: CAPGEMINI ESPAÑA SL, OMEGA PERIPHERALS SL, ORANGE ESPAGNE SAU, CONNECTIS ICT SERVICES SAU i ITGLOBAL SL.

- **CAPGEMINI ESPAÑA SL**:

La proposta indica que es realitza un inventariat al principi del projecte per detectar possibles vulnerabilitats. El procés inclou l'execució de *Discovery Scan* per identificar actius, ports oberts i serveis en execució, així com actius exposats fora de l'organització.
La classificació d'actius crítics depèn de si el client ja disposa d'una CMDB (Base de Dades de Configuració). Aquesta dependència de la CMDB existent es considera una manca de concreció en la proposta.

Proporcionen un servei de gestió de vulnerabilitats continu i *pentesting*, processos de Discovery Scan i verificació. Utilitza el *scoring* de vulnerabilitats (implícit) i genera un informe de gestió mensual amb l'estat de vulnerabilitat. No obstant això, la proposta no detalla les eines específiques utilitzades per a l'escaneig ni s'explica l'ús d'escàners de tercers homologat.
Sobre l'avaluació de les mesures de detecció i la seva implementació no fa referencia, per tant no podem dir que hi ha avaluació continua i proactiva
Així doncs, la proposta de CAPGEMINI ESPAÑA SL és robusta i metodològica, però la falta de detall en la formalització de les eines i en el procés continu d'avaluació de controls justifica la seva puntuació.

Es proposa assignar a l'oferta de l'empresa CAPGEMINI ESPAÑA SL 7,5 punts.

- **OMEGA PERIPHERALS SL**:

La proposta implica l'existència d'un inventari d'actius a través del seu servei d'escaneig de vulnerabilitats, però no descriu una metodologia per a la descoberta d'actius o la seva classificació per criticitat.
La proposta descriu capacitats d'escaneig de vulnerabilitats però omet la menció a les proves de penetració i les proves de phishing.
Per a la gestió de la superfície d'exposició externa realitzen monitoratge continu mitjançant eines especialitzades com Kaspersky Digital Footprint Intelligence (DFI) i Kartos. La modalitat CYBEROO esmenta "Continuous Scanning" i la modalitat BULHOST cita una "gestió contínua de vulnerabilitats (VMaaS)" basada en Tenable One, però cap de les dues modalitats esmenta explícitament proves de penetració o tests de phishing ni seguiment proactiu de les mesures de detecció implementades.

Es proposa assignar a l'oferta de l'empresa OMEGA PERIPHERAL SL 7 punts.

- **ORANGE ESPAGNE SAU**:

ORANGE se centra principalment en el descobriment d'actius exposats a Internet (EASM - External Attack Surface Management). La seva capacitat de Threat Intelligence inclou la gestió constant d'amenaces des del punt de vista extern o de la superfície d'exposició a possibles atacants. Utilitza FortiRecon o Kartos per a la vigilància de la superfície externa, també monitoritza fugues de credencials a la Dark Web i xarxes socials.
Orange utilitza el scoring de vulnerabilitats (implícit) i genera informes. No obstant això, la proposta no detalla les eines o processos per a l'ús d'estàndards com CVE o CVSS 3.1 de manera explícita
L'oferta fa referència a la simulació de comportaments d'Amenaces Persistents Avançades (APT), així com a la metodologia d'Incident Response. Per una altra banda la proposta d'Orange no detalla els escanejos de vulnerabilitats o pentests com a part del servei continu de prevenció. Tampoc es detallen els tests de phishing dins d'aquest servei de prevenció continu.
La proposta compleix amb els requisits generals d'ús d'eines homologades per a l'*scoring* (encara que sigui de manera implícita) i amb l'anàlisi de la superfície d'exposició externa, però es puntua amb 7 punts perquè l'inventari i la classificació d'actius es centren majoritàriament en la superfície externa, sense detallar la metodologia per a la classificació per criticitat dels actius interns i perquè no es detallen els processos, eines o compromís de periodicitat per a la realització d'escanejos de vulnerabilitats, *pentests* o tests de *phishing* com a part del servei continu de prevenció (només es fa referència a la simulació d'APT).

Es proposa assignar a l'oferta de l'empresa ORANGE ESPAGNE SAU 7 punts.

- **ITGLOBAL SL**:

  L'oferta d'ITGLOBAL destaca per la integració d'una plataforma pròpia (ASIP) que permet la gestió centralitzada d'actius, la importació i classificació automàtica des de la CMDB i la priorització d'incidents segons el risc i la criticitat. La gestió de vulnerabilitats és contínua, amb escanejos periòdics, informes històrics i dashboards evolutius. Es fa servir la metodologia OWASP i OSSTMM per a l'anàlisi de vulnerabilitats i es realitzen proves tant automàtiques com manuals. La proposta inclou la detecció proactiva de phishing (amb tecnologies pròpies com Trapcode), accés a un laboratori de malware, i integració amb fonts de Threat Intelligence (Delfos, MISP, feeds STIX/TAXII).
  La plataforma permet la gestió de tot el cicle de vida de la vulnerabilitat, des de la detecció fins al tancament, amb assignació de responsables i seguiment de la mitigació. S'inclouen informes periòdics, inventari d'actius i integració amb el SIEM i altres eines de seguretat.
  La principal deficiència de la proposta és el caràcter genèric de les seves descripcions. Tot i que es parla de la gestió de vulnerabilitats, no es detallen les eines específiques que s'utilitzaran ni la metodologia concreta per a la realització de proves d'intrusió (*pentesting*) per a l'avaluació del grau d'exposició de l'entitat, ni com reduiran l'exposició. Només anomenen que faran servir metodologia OSSTTMM.

  Es proposa assignar a l'oferta de l'empresa ITGLOBAL SL 6 punts.

- **CONNECTIS ICT SERVICES SAU**:

  Tot i que la proposta fa referència a l'inventari d'actius i a la classificació segons criticitat, no concreta en cap moment com es farà aquest inventari, ni quins processos o eines s'utilitzaran per etiquetar els actius segons la seva importància, ni tampoc com es garantirà el manteniment i l'actualització d'aquest inventari al llarg del temps. Aquesta manca de detall és una carència rellevant, ja que la gestió d'actius és fonamental per a la prevenció i la gestió de vulnerabilitats. En canvi, sí que ofereixen una gamma amplia de pentests (caixa negra, gris i blanca) i un servei de Firewall Assurance per revisar i optimitzar les regles del firewall, aspectes que aporten valor però que no compensen la manca de concreció en la gestió d'actius.
  Comparat amb altres licitadors, la proposta queda per sota en aquest apartat, ja que altres empreses descriuen processos més detallats i automatitzats per a la gestió d'actius i la seva classificació per criticitat, així com metodologies més clares per al manteniment i la revisió contínua.

  Es proposa assignar a l'oferta de l'empresa CONNECTIS ICT SERVICES SAU 5,5 punts.

Grup C – Nivell acceptable (1-4 punts):

Ofertes que mostren un servei sense una estructura robusta ni capacitat proactiva clara.

Característiques destacades:

- Presenten un inventari parcial o genèric, sense classificació clara per criticitat.
- Les eines d'anàlisi són bàsiques o manuals, amb poca cobertura de CVE.
- Les propostes de seguiment són limitades o genèriques, sense accions concretes.
- La gestió de vulnerabilitats és reactiva, amb poca anticipació.

Les empreses que presenten aquestes ofertes són: CLARANET SAU, APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA, ATECH ADVANCED SOLUTIONS S.A, SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS, TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU i VODAFONE ESPAÑA SAU.

- **CLARANET SAU**:

  La proposta és força genèrica, tot i que CLARANET SAU fa una exposició extensa de les eines que utilitzarà (SIEM, EDR/XDR, SOAR, TIP, IDS/IPS), la descripció del procés d'inventari d'actius és pràcticament inexistent: només es fa referència a la necessitat d'identificar i gestionar logs, però no s'explica com es farà l'inventari, la classificació ni la priorització dels actius segons la seva criticitat. Això és una mancança rellevant, ja que la gestió d'actius és la base de qualsevol estratègia de prevenció.
  Pel que fa a la gestió de vulnerabilitats, la proposta es limita a dir que s'identificaran, analitzaran i corregiran vulnerabilitats, però no concreta quines eines homologades s'utilitzaran per a l'escaneig ni com es farà el scoring (CVE/CVSS), ni tampoc es detalla el seguiment ni la mitigació de vulnerabilitats detectades. Les referències a pentests, tests de phishing o altres proves tècniques són molt superficials.

  Es proposa assignar a l'oferta de l'empresa CLARANET SAU 3 punts.

- **APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA**:

  La proposta de l'empresa APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA es presenta com una solució agnòstica, amb integració de múltiples fabricants i serveis MDR, però la descripció de la prevenció és molt genèrica. No es detalla cap procés específic d'inventari d'actius ni de classificació segons criticitat, ni tampoc es concreta l'ús d'eines homologades per a l'anàlisi i scoring de vulnerabilitats (CVE, CVSS). Es fa referència a la fase inicial de "discovery" i anàlisi de la infraestructura del client, però sense explicar com es genera l'inventari ni com es fa el seguiment i la mitigació de vulnerabilitats o exposició externa. La proposta es limita a garantir la cobertura 24x7 i la integració amb diferents plataformes, però sense aportar evidències de processos concrets ni informes d'inventari o seguiment.

  Es proposa assignar a l'oferta de l'empresa APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA 3 punts.

- **TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU**:

  Manca d'evidència de l'ús d'eines homologades o metodologies d'anàlisi de vulnerabilitats (escanejos, pentests, phishing). No s'esmenten estratègies de mitigació o seguiment d'exposició externa, ni cap sistema de priorització de vulnerabilitats.
  La proposta presenta el compliment mínim i assumeix el compliment normatiu.

  Es proposa assignar a l'oferta de l'empresa TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU 3 punts.

- **VODAFONE ESPAÑA SAU:**

  Presenta una eina de SOC que no està al CPSTIC. Tot i que Vodafone presenta una visió avançada de la gestió de la superfície d'exposició i la prevenció, la manca de detall sobre el procés d'inventari d'actius, la seva caracterització i la metodologia d'anàlisi del grau d'exposició redueix la solidesa de la proposta.
  Ofereix una visió avançada de la gestió de la superfície d'exposició i la detecció de vulnerabilitats externes, però la proposta no aporta detalls sobre les eines específiques d'escaneig ni sobre l'aplicació de scoring de CVE/CVSS, ni tampoc sobre el seguiment detallat de la mitigació de vulnerabilitats.
  Aquesta manca de concreció i la manca d'eines homologades i processos de scoring i seguiment ens porta a una baixa valoració de l'oferta en aquest apartat.

  Es proposa assignar a l'oferta de l'empresa VODAFONE ESPAÑA SAU 3 punts.

- **ATECH ADVANCED SOLUTIONS SA**:

  La proposta d'ATECH, tot i presentar una infraestructura amb cinc SOC distribuïts i destacar la seva pertinença a fòrums internacionals com FIRST, TF-CSIRT i CSIRT és un document molt genèric, amb referències constants a normatives i estàndards (NIST, DFIR, ISO 27035), però sense desenvolupar ni adaptar els processos a la realitat i l'exposició específica de l'entitat. No es presenta cap anàlisi de la superfície d'exposició ni es detalla cap metodologia pròpia per a la gestió de vulnerabilitats més enllà de la menció a la cobertura de llicència EPS i la retenció de logs. L'inventari i la classificació d'actius no s'especifiquen, i tampoc es concreten eines homologades ni processos de *scoring* de vulnerabilitats.

  Es proposa assignar a l'oferta de l'empresa ATECH ADVANCED SOLUTIONS SA 1 punts.

- **SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS (SERMICRO)**:

  La proposta, tot i presentar una estructura de servei SOC i amb certificacions rellevants, no explicita ni el procés d'inventari d'actius ni les eines concretes que s'utilitzen per a l'anàlisi i gestió de vulnerabilitats. La documentació fa èmfasi en la capacitat d'implementar alertes ràpides i en el coneixement acumulat, però no detalla el procediment ni la tecnologia emprada per anticipar amenaces, ni tampoc la gestió proactiva de vulnerabilitats abans d'un incident.

  Es proposa assignar a l'oferta de l'empresa SEMICRO 1 punt.

"**1.2. <u>Capacitats de detecció</u>, fins a un màxim de 10 punts:**

Es valorarà la millor idoneïtat per a la detecció d'amenaces mitjançant monitorització 24x7 i ús de tecnologies avançades com SIEM/XDR, segons els següents paràmetres:

- Regles de detecció desenvolupades per mitigar amenaces concretes.
- Implementar anàlisi proactiu d'amenaces amb pràctiques de Threat Hunting.
- Creació de quadres de comandament en temps real que ofereixin visibilitat de les amenaces i indicadors de compromís.

Les empreses licitadores presentaran una descripció tècnica de la monitorització proposada, incloent-hi les funcionalitats de configuració, actualització i integració de fonts."

S'han agrupat les ofertes en diferents grups per rang de puntuació:

<u>Grup A – Alta capacitat (8–10 punts)</u>:

Aquestes ofertes demostren una maduresa elevada en detecció d'amenaces i capacitat d'adaptació a entorns complexos.

Característiques destacades:

- Disposen de monitorització 24x7 amb cobertura completa i resposta immediata.
- Utilitzen tecnologies avançades com SIEM i XDR, amb integració de múltiples fonts de dades.
- Han desenvolupat regles específiques de detecció per a amenaces concretes, adaptades al context de l'entitat.

- Implementen pràctiques de Threat Hunting proactives, amb equips dedicats a la recerca d'indicadors de compromís.
- Ofereixen quadres de comandament en temps real, amb visibilitat clara i detallada de l'estat de seguretat.

Les empreses incloses en aquest grup són: EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL, SISTEMAS INFORMÁTICOS ABIERTOS SAU, SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL, EVOLUTIO CLOUD ENABLER SAU, S2 GRUPO SOLUCIONES DE SEGURIDAD SLU, INETUM ESPAÑA SA, A2SECURE TECNOLOGÍAS INFORMÁTICA SL, VODAFONE ESPAÑA SAU, SISTEMAS AVANZADOS DE TECNOLOGÍA SA, ITGLOBAL SL, CAPGEMINI ESPAÑA SL i ORANGE ESPAGNE SAU.

- **EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL**:

  La proposta de l'empresa EY TRANSFORMA SERVICIOS DE CONSULTORÍA SAL destaca com una de les millors opcions pel que fa a la detecció d'amenaces. Ofereix una solució molt robusta i avançada, amb tecnologia de primer nivell i una clara orientació a la millora contínua. La monitorització 24x7x365 des de Barcelona, amb el suport d'altres centres d'EY, garanteix una vigilància constant i una resposta ràpida davant qualsevol incident. L'ús del SIEM Splunk, líder de mercat, permet integrar múltiples fonts d'informació, aplicar correlació avançada i desplegar regles personalitzades alineades amb el marc MITRE ATT&CK, tot amb quadres de comandament en temps real.
  A més, la proposta inclou la implementació de regles de detecció adaptades, activitats proactives de threat hunting i la generació de runbooks i playbooks per a la gestió eficient dels incidents. També es detalla de manera exhaustiva la gestió d'alertes, l'escalat, la documentació i el reporting, així com la integració d'indicadors de compromís (IoC) i la coordinació amb el SOC Tàctic. Finalment, es posa especial èmfasi en la integració de fonts, l'actualització i ajust de regles, i la millora contínua dels casos d'ús, fet que consolida la proposta d'EY com una de les més sòlides i completes en aquest àmbit. És una oferta molt complerta i detallada.

  Es proposa assignar a l'oferta de l'empresa EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL 10 punts.

- **SISTEMAS INFORMÁTICOS ABIERTOS SAU**:

  La detecció de l'empresa SISTEMAS INFORMÁTICOS ABIERTOS SAU es presenta com una de les més avançades, amb una cobertura tecnològica àmplia, monitorització contínua i una gran capacitat de personalització i evolució constant. El servei ofereix monitorització 24x7x365 mitjançant SIEM de referència com MONICA NGSIEM, IBM QRadar i Microsoft Sentinel, així com solucions XDR/EDR de diversos fabricants i la integració amb la Xarxa Nacional de SOC. Es despleguen regles de detecció avançades, amb més de 800 casos d'ús, que permeten la correlació d'esdeveniments, la detecció d'indicadors de compromís (IoC) i la visualització de quadres de comandament en temps real. A més, s'inclou el threat hunting proactiu, basat en una metodologia pròpia i l'ús del marc MITRE ATT&CK, amb informes periòdics i notificacions immediates d'amenaces. Finalment, la descripció tècnica és molt detallada pel que fa a la monitorització, configuració, actualització i integració de fonts, així com el manteniment i l'evolució de les eines utilitzades.

  Es proposa assignar a l'oferta de l'empresa SISTEMAS INFORMÁTICOS ABIERTOS SAU 10 punts.

- **EVOLUTIO CLOUD ENABLER SAU**:

  EVOLUTIO presenta una proposta de detecció altament robusta i sofisticada, que combina una monitorització contínua amb regles adaptades a cada entorn, capacitats avançades de threat hunting i quadres de comandament en temps real, tot assegurant una resposta ràpida,

precisa i personalitzada davant qualsevol amenaça. El servei es fonamenta en una monitorització 24x7x365 mitjançant SIEM Google SecOps, una solució nativa cloud amb ENS Alt, i integra tecnologies de primer nivell com EDR/XDR, NDR, IDS/IPS, UEBA, Threat Intelligence i honeypots. A més, incorpora fonts OSINT, privades i comercials, i desenvolupa regles de detecció pròpies i adaptades, basades en marcs com MITRE ATT&CK, PowerBI i YARA-L, amb una base de coneixement de casos d'ús i workbooks personalitzats per a cada client. El servei inclou threat hunting proactiu, dashboards dinàmics en temps real, reporting periòdic, i una integració fluida amb MISP i SOAR.
Tot plegat configura una solució flexible, escalable i altament personalitzable, amb connexió directa i informes regulars al SOC Tàctic.

Es proposa assignar a l'oferta de l'empresa EVOLUTIO CLOUD ENABLER SAU 10 punts.

- **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL (SIRT)**:

SIRT destaca per la seva detecció avançada, amb una monitorització contínua i l'aplicació de regles adaptades a cada entitat, fet que permet una resposta ràpida i ajustada davant qualsevol amenaça. El servei es basa en una monitorització 24x7x365 amb SIEM Splunk (amb Enterprise Security i SOAR), i integra tecnologies com EDR/XDR, NDR, IDS/IPS, UEBA, Threat Intelligence i honeypots.
SIRT incorpora més de 2.000 connectors i desenvolupa regles de detecció pròpies, basades en marcs com MITRE ATT&CK, KillChain i MaGMa, a més de realitzar threat hunting proactiu mitjançant consultes ad hoc, hipòtesis, IOC/TTP i anàlisi d'anomalies, però la seva proposta li manca explicitar el nivell d'integració metodològica de priorització de TH basada en el mapeig continu de vulnerabilitats explotables a la matriu MITRE de l'entitat, que sí es detalla en l'oferta d'EY.
També disposa d'una base de coneixement de casos d'ús i workbooks personalitzats per a cada client. Els quadres de comandament són dinàmics i en temps real, aportant visibilitat sobre compromisos, incidents, tendències i la gestió d'alertes.
En definitiva, es tracta d'un servei flexible, escalable i altament personalitzable, amb integració i reporting periòdic al SOC Tàctic, però la seva descripció dels quadres de comandament i informes no posa el mateix èmfasi en les mètriques de rendiment per regla o font orientades a la millora del *Fine-Tuning* tal com ho fa l'oferta de l'empresa EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL.

Es proposa assignar a l'oferta de l'empresa SIRT 9 punts.

- **S2GRUPO SOLUCIONES DE SEGURIDAD SLU**:

En l'apartat de detecció, S2GRUPO presenta una bona capacitat de monitorització i correlació d'esdeveniments, amb una integració clara amb el SOC Tàctic. Destaquen per la seva plataforma SIEM pròpia, GLORIA, que inclou una base de més de 200 casos d'ús i 600 regles de correlació predefinides. Pel que fa a la implementació d'anàlisi proactiu d'amenaces amb pràctiques de *threat hunting*, cal ser crític i realista: S2 Grupo inclou el concepte de *threat hunting* dins la seva metodologia de detecció, però la seva aposta no és tan avançada ni tan estructurada com la d'altres competidors.
Els quadres de comandament de S2grupo compleixen amb els requisits bàsics de visibilitat, reporting i personalització, i són adequats per a un entorn públic que necessita coordinació amb el SOC Tàctic.
Comparant aquesta oferta amb la resta de propostes podem dir que són menys avançats en automatització, explotació de dades i capacitat d'integració multinivell.

Es proposa assignar a l'oferta de l'empresa S2GRUPO SOLUCIONES DE SEGURIDAD SLU 9 punts.

- **A2SECURE TECNOLOGÍAS INFORMÁTICA SL**:

  Presenta una monitorització i detecció automàtica 24x7 amb eines SIEM/XDR. Implementa regles de detecció d'amenaces, incloent-hi les indicades pel SOC Tàctic. Utilitza una nodrida biblioteca de recursos, casos d'ús i alertes que amplien l'espectre de visibilitat.
  Realitza execució de missions de Threat Hunting (TH) basades en indicadors d'intel·ligència i utilitza monitorització d'indicadors de compromís (IoC) per a la recerca contínua d'activitat. Pel que fa als quadres de comandament, presenta l'elaboració i monitorització de quadres d'activitat en temps real i accessibles. Donarà visibilitat de l'activitat gestionada al SOC Tàctic amb exportacions de les eines que s'integraran en un repositori del SOC Tàctic.
  A2SECURE obté 9 punts pel seu rigor metodològic en la definició de casos d'ús, la garantia de lliurament de registres d'activitat complets en format interoperable i la integració amb eines de l'ecosistema del CCN.
  La pèrdua d'1 punt es deu a la manca de quantificació i formalitat en la pràctica de *Threat Hunting* i en la definició d'un catàleg mínim de regles de detecció en la fase inicial del desplegament.

  Es proposa assignar a l'oferta de l'empresa A2SECURE TECNOLOGÍAS INFORMÁTICA SL 9 punts.

- **VODAFONE ESPAÑA SAU**:

  VODAFONE presenta una arquitectura de detecció avançada, basada en SIEM Elastic, XSOAR de Palo Alto i una plataforma pròpia de detecció d'anomalies amb ML. La monitorització 24x7 es complementa amb la creació i manteniment de casos d'ús alineats amb MITRE ATT&CK, i la generació de playbooks automatitzats per a la resposta immediata. El servei de Threat Hunting es desplega en diferents graus de maduresa, des de la cerca d'IOC i TTP fins a la simulació d'APT i l'automatització de playbooks, amb una clara orientació a la millora contínua i la reducció de falsos positius. Els quadres de comandament i indicadors de servei són detallats i permeten un seguiment exhaustiu de l'eficàcia de la detecció.
  Vodafone sobresurt per la integració real de ML i automatització, així com per la maduresa del seu model de detecció i la capacitat d'adaptació a l'entorn del client. També presenta una àmplia cobertura de casos d'ús i la gestió proactiva. Com a punt negatiu s'observa que els seus Dashboards, no estan orientats a KPI específics de l'Administració pública.

  Es proposa assignar a l'oferta de l'empresa VODAFONE ESPAÑA SAU 9 punts.

- **SISTEMAS AVANZADOS DE TECNOLOGÍA SA**:

  La proposta de SISTEMAS AVANZADOS DE TECNOLOGÍA SA destaca per la monitorització 24x7 de tots els esdeveniments i registres de seguretat, integrant-los en SIEM líders (IBM QRadar i Splunk). Ofereix regles de detecció avançades, correlació d'esdeveniments en temps real, integració d'intel·ligència d'amenaces i marcs com MITRE ATT&CK. Inclou activitats de threat hunting proactiu i dashboards interactius que donen visibilitat en temps real de les amenaces i indicadors de compromís. El sistema permet configurar, actualitzar i integrar noves fonts i regles de detecció de manera contínua.
  L'oferta no deixa clars alguns punts com el grau de personalització de les regles de detecció per a cada entitat. El threat hunting es menciona, però no s'explica si és periòdic, sota demanda o reactiu. Tampoc no s'explicita si hi ha informes d'eficàcia de les regles ni si es revisen periòdicament amb el client.

  Es proposa assignar a l'oferta de l'empresa SISTEMAS AVANZADOS DE TECNOLOGÍA SA 8 punts.

- **INETUM ESPAÑA SA**:

  La proposta de l'empresa INETUM ESPAÑA SA presenta un servei de detecció molt complet, amb monitorització contínua, regles de detecció pròpies i adaptables, integració d'intel·ligència d'amenaces i pràctiques avançades de threat hunting. La descripció tècnica és exhaustiva i cobreix tots els punts demanats, incloent la monitorització 24x7x365 amb SIEM Microsoft Sentinel, la integració de fonts, quadres de comandament en temps real i informes periòdics. Les regles de detecció es desenvolupen i milloren de forma contínua, amb integració de feeds d'intel·ligència i IOC, però no es basen en marcs de referència com MITRE ATT&CK, fet que limita la traçabilitat i l'estandardització. Tot i que s'inclouen pràctiques de *threat hunting* proactiu i la participació en xarxes de col·laboració com RNS, CSIRT.es i FIRST, el plantejament de les regles per a la mitigació d'amenaces no mostra el mateix grau d'enfoc metodològic ni de maduresa que les propostes més destacades. Així i tot, el servei ofereix una descripció tècnica detallada pel que fa a la configuració, actualització i integració de fonts, així com el reporting i la visualització mitjançant dashboards.

  Es proposa assignar a l'oferta de l'empresa INETUM ESPAÑA SA 8 punts.

- **ITGLOBAL SL**:

  La detecció es basa en una arquitectura SIEM Cloud multi-client, amb ingestió massiva de logs, normalització, enriquiment amb Threat Intelligence i correlació avançada. Disposa de centenars de casos d'ús adaptables, dashboards en temps real, i monitorització 24x7x365.
  La detecció d'amenaces es basa en marcs com MITRE ATT&CK, CAPEC i NIST, i es fa threat hunting proactiu (basat en hipòtesis, IOC i analítica avançada).
  La plataforma permet la creació i validació de regles de correlació, la gestió de falsos positius, i la priorització automàtica segons la criticitat dels actius. S'inclouen informes periòdics, quadres de comandament i integració amb altres eines de seguretat.
  En el threat hunting no queda clar si es fa revisió periòdica de l'eficàcia de les regles amb el client. La personalització de dashboards i informes és bona, però potser menys flexible que per exemple en EVOLUTIO.
  La proposta d'ITGLOBAL destaca per la seva arquitectura avançada en el núvol i la seva aproximació metodològica a la detecció d'amenaces, però manca el detall en la formalització de compromisos i la integració específica amb l'ecosistema del CCN-CERT

  Es proposa assignar a l'oferta de l'empresa ITGLOBAL SL 8 punts.

- **CAPGEMINI ESPAÑA SL**:

  Presenta una oferta de detecció basada en la plataforma ICDP (Devo/Sentinel). Llibreria de casos d'ús (Use Case Factory). Activa 50 casos d'ús inicials. Les regles s'alineen amb el marc Mitre ATT&CK.
  Implementa anàlisi proactiu d'amenaces amb pràctiques de Threat Hunting. Metodologia de TH de 5 etapes (Petició del SOC Tàctic, Perfilat de comportament, Generació d'hipòtesis/casos d'ús, Exercici de hunting, Informe).
  Proporciona quadres de comandament en temps real de l'estatus del servei (KPI/SLA) i incidents en temps real que inclouen amenaces i indicadors de compromís. Informes avançats per facilitar la presa de decisions.
  Tot i que es descriu una metodologia clara de *Threat Hunting* i s'utilitzen plataformes SIEM/SOAR avançades, s'aprecia la manca de quantificació del catàleg de regles de detecció inicial, l'absència de detall sobre l'avaluació contínua i la implementació de les regles de detecció i la seva validació (*fine-tuning* avançat), limitant la confiança en l'eficàcia real de la detecció.
  Addicionalment la proposta d'inventariat de regles i casos d'ús no proporciona un detall tècnic exhaustiu de les funcionalitats de configuració i actualització de les regles especifiques de detecció.

Es proposa assignar a l'oferta de l'empresa CAPGEMINI ESPAÑA SL 8 punts.

- **ORANGE ESPAGNE SAU**:

  ORANGE ESPAGNE SAU ofereix una monitorització 24x7 utilitzant una plataforma SIEM basada en la tecnologia Elastic. La seva arquitectura està orientada a l'automatització i s'integra amb l'orquestrador XSOAR de Palo Alto Networks. L'ús d'XSOAR, una plataforma líder, permet l'automatització completa de l'atenció d'alertes. Tot i utilitzar XSOAR (SOAR d'alt nivell), Orange no proporciona un catàleg específic o quantificat de *playbooks* d'automatització de resposta per a accions de protecció (com bloquejos en tallafocs o aïllament d'endpoints).
  El SOC d'Orange disposa de més de 800 regles de correlació desenvolupades i ajustades per la seva experiència, que estan a disposició per ser adaptades al projecte. A més, utilitza el *framework* MITRE ATT&CK per a la identificació i caracterització dels casos d'ús i incidents.
  Malgrat que Orange presenta el *Threat Hunting* com a servei permanent i en diferents graus de maduresa (4 graus), la proposta omet la descripció d'un compromís ferm i mesurable en la seva execució periòdica. Aquesta manca de detall sobre els processos de *threat hunting* periòdics i la seva aplicació pràctica pot limitar la percepció de la seva pro activitat.
  Els quadres de comandament per a KPIS i incidents son en temps real, reflectint l'estat d'alertes i indicadors de compromís, però els KPI no són específics de l'Administració
  En resum, Orange ofereix una arquitectura de detecció tecnològicament molt avançada, amb un fort enfocament en l'automatització (XSOAR) i la intel·ligència (ML, CTI del CCN), la qual cosa justifica la seva alta puntuació. Les seves febleses se centren en la manca de formalització i la quantificació de la seva metodologia de *Threat Hunting* i la documentació detallada de tots els elements del *pipeline* de detecció/resposta.

  Es proposa assignar a l'oferta de l'empresa ORANGE ESPAGNE SAU 8 punts.

Grup B – Capacitat mitjana (5–7 punts):

Ofertes funcionals, amb capacitat de detecció raonable però amb marge de millora en proactivitat i personalització.

Característiques destacades:

- Disposen de monitorització activa, tot i que pot no ser 24x7 o amb cobertura total.
- Utilitzen SIEM o XDR, però amb funcionalitats limitades o no totalment integrades.
- Presenten algunes regles de detecció, però no sempre adaptades a l'entorn específic.
- Inclouen iniciatives de Threat Hunting, però de manera puntual o reactiva.
- Els quadres de comandament ofereixen visibilitat parcial, amb indicadors bàsics.

Les empreses incloses en aquest grup són: SOTHIS SERVICIOS TECNOLÓGICOS SLU, SEIDOR SOLUTIONS SL, GMV SOLUCIONES GLOBALES INTERNET SAU, CONNECTIS ICT SERVICES SAU i OMEGA PERIPHERALS SL.

- **SOTHIS SERVICIOS TECNOLÓGICOS SLU**:

  La integració de tecnologies com IBM QRadar, juntament amb metodologies inspirades en MITRE ATT&CK i la Cyber Kill Chain, permeten identificar patrons anòmals i amenaces emergents amb molta precisió. El quadre de comandament en temps real ofereix una visió panoràmica i detallada, facilitant la presa de decisions estratègiques a tots els nivells.
  Respecta a les altres ofertes, mostren un nivell mes baix d'expertesa en la automatització de la resposta davant deteccions crítiques.

Es proposa assignar a l'oferta de l'empresa SOTHIS SERVICIOS TECNOLÓGICOS 7 punts.

- **SEIDOR SOLUTIONS SL**:

L'oferta de SEIDOR es basa en la plataforma SIEM DEVO, que és nativa al núvol, escalable i multi-client. Utilitza anàlisi de comportament d'usuaris i entitats (UEBA) i casos d'ús adaptats. La intel·ligència (IoC, TTP) s'integra al SIEM per a la detecció anticipada.
La proposta ofereix accés a la plataforma de consulta i visualització avançada (Devo) i generació d'informes forenses exhaustius. Els informes són útils per al compliment de requeriments normatius com els de l'Agència de Ciberseguretat de Catalunya.
En conclusió, la proposta de SEIDOR, malgrat complir amb tots els elements conceptuals (SIEM, UEBA, Threat Hunting, CTI, Dashboards), no ofereix la quantificació d'actius (casos d'ús inicials) ni la formalitat dels compromisos (periodicitat del Threat Hunting), que es troba en altres ofertes avaluades.

Es proposa assignar a l'oferta de l'empresa SEIDOR SOLUTIONS SL 7 punts.

- **GMV SOLUCIONES GLOBALES INTERNET SAU**:

En l'àmbit de la detecció, GMV proposa una arquitectura de monitorització 24x7 basada en Splunk (SIEM líder de mercat), complementada amb NSM, EDR, NDR i integració amb múltiples fonts de dades. La proposta inclou una biblioteca pròpia de més de 500 casos d'ús i regles de detecció, desenvolupades i documentades segons estàndards com MITRE ATT&CK i SIGMA, i adaptables a les necessitats específiques de cada client.
El servei de Threat Hunting es basa en una metodologia pròpia, alineada amb frameworks reconeguts, i incorpora la generació d'informes detallats, la integració amb el CSIRT i la creació de playbooks de resposta, però la proposta omet la descripció de processos de threat hunting periòdics i la seva aplicació pràctica, limitant-se a la detecció basada en regles estàtiques i escanejos programats.
Els quadres de comandament són avançats i personalitzables, i la proposta inclou un procés de millora contínua per a la integració de noves fonts i l'actualització de regles. Però aquesta capacitat d'adaptació i evolució constant, juntament amb la riquesa de casos d'ús i la proactivitat en la detecció, no s'explicita en la capacitat de crear quadres de comandament en temps real amb visibilitat d'indicadors de compromís.
GMV presenta un motor de detecció potent basat en Splunk i una metodologia ben estructurada, però manca detall en les seves capacitats de Threat Hunting periòdic i proactiu, en la integració i visualització d' IoC i mètriques avançades orientades a la millora de la qualitat del servei de detecció.

Es proposa assignar a l'oferta de l'empresa GMV SOLUCIONES GLOBALES INTERNET SAU 6,5 punts.

- **CONNECTIS ICT SERVICES SAU**:

L'oferta de CONNECTIS es fonamenta en la robustesa de la seva plataforma tecnològica i la seva operació continuada. L'empresa proposa un servei de monitorització 24x7, utilitzant Microsoft Sentinel com a eina principal.
Un altre element a destacar és l'ús de múltiples tecnologies de suport en l'ecosistema de detecció i resposta, ja que la proposta esmenta l'ús de solucions de SOAR (Security Orchestration, Automation, and Response) i intel·ligència d'amenaces (Threat Intelligence - TI), citant Recorded Future, Swimlane, i Skybox, a més de les capacitats natives de Microsoft Sentinel. Addicionalment, l'empresa fa referència a un equip d'enginyeria de detecció responsable del desenvolupament i manteniment dels *playbooks* alineats amb el *framework* MITRE ATT&CK.
Les limitacions principals de la proposta de CONNECTIS radiquen en la manca de concreció en regles de detecció, en la manca de detall de l'anàlisi proactiu d'amenaces (Threat

Hunting) que es descriu de manera superficial (no concreta metodologia, freqüència o resultats esperats) i en la manca de coordinació amb el SOC Tàctic. L'oferta proporciona una solució funcional amb una capacitat de detecció raonable, però amb un marge de millora considerable en termes de proactivitat, detall metodològic i formalització.

Es proposa assignar a l'oferta de l'empresa CONNECTIS ICT SERVICES SAU 6 punts.

- **OMEGA PERIPHERALS SL**:

El punt fort de la proposta és la transparència (portal web personalitzat i informes exportables), però manca la concreció sobre la integració d'aquests dashboards amb un repositori del SOC Tàctic per assegurar la visibilitat directa des de l'Agència de Ciberseguretat de Catalunya.
Tot i mencionar l'ús de casos d'ús basats en ENISA i MITRE ATT&CK, l'oferta no proporciona la xifra del nombre de regles de correlació disponibles. L'oferta integra la capacitat de Threat Hunting, però no descriu la metodologia de TH per fases (generació d'hipòtesis, execució, informe) amb claredat.
OMEGA presenta una oferta funcional amb capacitats de detecció raonables, però amb un marge de millora en la proactivitat, la formalització de la seva metodologia i la visibilitat d'indicadors de seguretat específics.

Es proposa assignar a l'oferta de l'empresa OMEGA PERIPHERALS SL 5 punts.

Grup C – Capacitat limitada (0–4 punts):

Ofertes que no garanteixen una detecció eficaç ni una visibilitat adequada de les amenaces.

Característiques destacades:

- La monitorització és inexistent o molt limitada, sense cobertura continuada.
- Les tecnologies SIEM/XDR són molt bàsiques.
- No hi ha regles de detecció desenvolupades específicament.
- No s'apliquen pràctiques de Threat Hunting.
- No es disposa de quadres de comandament en temps real o són molt genèrics.

Les empreses incloses en aquest grup són: SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS, APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA, ATECH ADVANCED SOLUTIONS S.A, CLARANET SAU i TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU.

- **SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÍNICOS (SERMICRO)**:

Tot i que la proposta fa referència a una base de correlacions pròpia, no entra en el detall de casos d'ús i regles de detecció desenvolupades ni en la cobertura específica de la matriu MITRE ATT&CK. Aquesta absència de detall i quantificació redueix la capacitat de l'avaluador per determinar l'abast immediat de la detecció.
Sobre Threat Hunting la proposta es queda curta en la descripció de la gestió proactiva de la detecció. No es detallen les pràctiques d'anàlisi proactiu d'amenaces (*Threat Hunting*), més enllà de la funcionalitat bàsica del SIEM o l'ús d'intel·ligència.
Tot i que s'esmenta l'existència de *dashboards*, la proposta no aprofundeix en el nivell de personalització ni en com s'ofereix la visibilitat d'indicadors de compromís (IoC) o indicadors clau de rendiment (KPI) específics per a l'Administració Pública.
La puntuació es veu penalitzada principalment per la falta de concreció i detall en els paràmetres clau d' avaluació.

Es proposa assignar a l'oferta de l'empresa SERMICRO 3 punts.

- **APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA**:

  En detecció, la proposta aposta per una arquitectura híbrida basada en serveis MDR de fabricants líders (Barracuda, Sophos, SentinelOne, etc.), amb integració de dades de múltiples fonts (endpoint, xarxa, cloud, email, servidors) i cobertura 24x7. Es fa referència a la correlació d'esdeveniments, l'ús de XDR i la capacitat de threat hunting proactiu, però la descripció és força superficial: no es detallen regles de detecció concretes, ni es mostra cap metodologia pròpia de threat hunting més enllà de la funcionalitat estàndard dels fabricants. Tampoc es concreta la creació de quadres de comandament en temps real, més enllà de la capacitat de les plataformes utilitzades.

  Es proposa assignar a l'oferta de l'empresa APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA 3 punts.

- **ATECH ADVANCED SOLUTIONS SA**:

  Pel que fa a la detecció, la proposta es limita a descriure la monitorització 24x7 i la correlació d'esdeveniments, però sense aportar exemples de regles de detecció desenvolupades per a amenaces concretes ni pràctiques de threat hunting més enllà de la funcionalitat bàsica del SIEM. La creació de quadres de comandament es presenta com una funcionalitat genèrica de la plataforma, sense cap exemple ni personalització per a l'entitat ni cap detall sobre la integració de fonts o la configuració de casos d'ús.

  Es proposa assignar a l'oferta de l'empresa ATECH ADVANCED SOLUTIONS 3 punts.

- **CLARANET SAU**:

  Enumera les funcionalitats de les eines i presenta una llista de casos d'ús, però la descripció és força estàndard i no aporta exemples pràctics ni detalls sobre la configuració, l'actualització o la integració de fonts. No es concreta la metodologia de threat hunting més enllà de la integració de TIP i l'anàlisi de comportament. Parla dels quadres de comandament, però no profunditza en el seu contingut.

  Es proposa assignar a l'oferta de l'empresa CLARANET SAU 3 punts.

- **TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU**:

  No s'identifica el SIEM ni es detallen les regles de detecció, així com tampoc s'esmenta cap pràctica de Threat Hunting ni la integració d'indicadors d'intel·ligència d'amenaces.
  No hi ha referències a la creació o accés a quadres de comandament en temps real per al seguiment d'amenaces. La proposta és poc detallada.

  Es proposa assignar a l'oferta de l'empresa TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU 3 punts.

"**1.3. <u>Capacitats de protecció</u>, fins a un màxim de 5 punts:**

Es valorarà l'aplicació de contramesures i operació de les eines de protecció, mitjançant els següents punts:

- Desplegament de contramesures efectives en incidents simulats o reals.
- Nivell d'automatització de les tasques recurrents per evitar errors humans i millorar la rapidesa de resposta.

Les empreses licitadores presentaran una descripció detallada de les eines i tecnologies de protecció que es desplegaran, incloent-hi funcionalitats d'automatització."

S'agrupen les ofertes en diferents grups per rang de puntuació:

<u>Grup A – Alt nivell (5 punts)</u>:

Aquestes ofertes presenten una protecció excel·lent, amb alt nivell d'automatització, resposta ràpida i desplegament efectiu de contramesures

Característiques destacades:

- Automatització molt avançada: ús intensiu de plataformes SOAR amb playbooks personalitzats, scripts, i integració amb SIEM.
- Resposta immediata i efectiva: capacitat demostrada per actuar davant incidents simulats o reals amb accions com quarantena, bloqueig d'IP, reconfiguració de trànsit, etc.
- Desplegament complet de contramesures: amb exemples pràctics i detallats.
- Integració amb ecosistemes de seguretat: adaptació a entorns CCN i tercers.
- Descripció tècnica exhaustiva: detall de processos, manteniment, gestió de llicències i suport.

Les empreses incloses en aquest grup són: EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL, SISTEMAS INFORMÁTICOS ABIERTOS SAU i SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL.

- **EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL**:

  La protecció està molt ben resolta, amb alta automatització i capacitat de resposta ràpida davant qualsevol amenaça. L'oferta destaca per la imparcialitat en la selecció d'eines de protecció, ja que treballen amb múltiples fabricants i tecnologies, adaptant-se a l'entorn del client. Destaca la integració de plataformes SOAR (orquestració i resposta automatitzada), que permeten automatitzar la resposta a incidents, la gestió d'alertes i la remediació de vulnerabilitats, minimitzant l'error humà i accelerant la resposta.
  La fortalesa principal rau en l'estratègia d'automatització que garanteixen una resposta immediata, automatitzada i lliure d'errors humans davant de tasques recurrents i incidents crítics.
  La proposta d'EY en matèria de protecció destaca com una de les solucions millor resoltes, amb una alta automatització i capacitat de resposta ràpida davant qualsevol amenaça. El seu enfocament combina tecnologia líder del mercat, integració extensiva i una metodologia de resposta que prioritza l'eficiència i la minimització de l'error humà. La proposta compleix de manera excel·lent els requisits del criteri gràcies al seu focus en l'orquestració avançada, les contramesures efectives i el rigor en els processos d'operació.

  Es proposa assignar a l'oferta de l'empresa EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL 5 punts.

- **SISTEMAS INFORMÁTICOS ABIERTOS SAU**:

  La protecció està plenament optimitzada, amb un alt grau d'automatització, resposta immediata i capacitat d'integració tant amb l'ecosistema del CCN com amb eines de tercers. El desplegament i l'operació de les solucions de seguretat (firewalls, EDR/XDR, WAF, SIEM/SOAR, etc.) es duen a terme amb procediments detallats que garanteixen una gestió, manteniment i actualització eficients. En cas d'incidents reals o simulats s'apliquen contramesures efectives, recolzades en l'ús d'API per potenciar l'automatització i la rapidesa de la resposta.
  El sistema incorpora un nivell avançat d'automatització (SOAR natiu i integració amb TheHive/Cortex), amb playbooks i scripts personalitzats. A més, s'ofereix una descripció clara de la gestió de llicències, del manteniment i del suport, sempre en alineació amb les guies STIC del CCN.
  SIA obté la màxima puntuació perquè la seva proposta de protecció està plenament optimitzada amb un alt grau d'automatització i una resposta immediata, garantint que les eines de seguretat funcionin de la millor manera possible davant qualsevol amenaça.

  Es proposa assignar a l'oferta de l'empresa SISTEMAS INFORMÁTICOS ABIERTOS SAU 5 punts.

- **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL (SIRT)**:

  La seva oferta assegura una protecció sòlida gràcies a l'automatització avançada, la resposta immediata i la integració completa amb l'ecosistema de seguretat, reduint de manera significativa la superfície d'atac i els riscos associats.
  La protecció es basa en el desplegament i l'operació d'eines de seguretat (IAM, NAC, EDR/XDR, NGFW, WAF, DLP, SOAR, etc.), en l'aplicació de contramesures, en la implantació d'IOC i en l'automatització de tasques recurrents mitjançant playbooks, scripts i integració SIEM–SOAR. Tot plegat es combina amb una resposta ràpida i efectiva davant d'incidents, tant simulats com reals.
  El grau d'automatització és alt, amb casos pràctics que inclouen el bloqueig automàtic d'IP, la quarantena d'equips, la reconfiguració de trànsit o la desactivació immediata de comptes sospitosos.
  SIRT obté la màxima puntuació perquè la seva proposta ofereix una protecció extremadament sòlida mitjançant l'automatització avançada de tasques i una resposta immediata i efectiva davant d'incidents, utilitzant tecnologia d'última generació que redueix tant els errors humans com la capacitat de l'atacant per causar danys.

  Es proposa assignar a l'oferta de l'empresa SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL 5 punts.

Grup B – Puntuació mitja (4 - 4,5 punts):

Ofertes molt sòlides, amb automatització avançada i bona integració, però amb algun petit dèficit de detall o formalització.

Característiques destacades:

- Automatització robusta però amb alguna limitació: ús de SOAR (XSOAR, TheHive, etc.) però amb menys detall o formalització que el grup 1.
- Resposta ràpida i funcional: accions automatitzades com quarantena, bloqueig, gestió de trànsit.
- Desplegament d'eines avançades: IAM, NAC, EDR/XDR, NGFW, DLP, etc.
- Manca d'evidències concretes en alguns casos: absència de catàlegs de playbooks o simulacions BAS contínues.
- Integració sòlida però no sempre formalitzada: bona arquitectura però amb menys personalització.

Les empreses incloses en aquest grup són EVOLUTIO CLOUD ENABLER SAU, INETUM ESPAÑA SA, OMEGA PERIPHERALS SL, GMV SOLUCIONES GLOBALES INTERNET SAU, ORANGE ESPAGNE SAU, SISTEMAS AVANZADOS DE TECNOLOGÍA SA, ITGLOBAL SL, CAPGEMINI, SEIDOR SOLUTIONS SL i S2 GRUPO SOLUCIONES DE SEGURIDAD SLU.

- **EVOLUTIO CLOUD ENABLER SAU**:

  La proposta d'EVOLUTIO contempla el manteniment, l'evolució i la integració de totes les eines de seguretat, alhora que assegura visibilitat i reporting constants al SOC Tàctic.
  La protecció es basa en un elevat nivell d'automatització, amb casos d'ús com el bloqueig automàtic d'IP, la quarantena d'equips, la reconfiguració de trànsit o la desactivació immediata de comptes sospitosos.
  Aquesta protecció robusta combina l'operació i el desplegament d'eines avançades (IAM, NAC, EDR/XDR, NGFW, WAF, DLP, SOAR, etc.), l'aplicació de contramesures, la implantació d'IOC i l'automatització de tasques recurrents mitjançant playbooks, scripts i integració SIEM–SOAR.
  Tanmateix, s'ha detectat la manca d'exemples concrets d'automatització de tasques, la qual cosa ha comportat una lleugera reducció en la puntuació.

  Es proposa assignar a l'oferta de l'empresa EVOLUTIO CLOUD ENABLER SAU 4,5 punts.

- **INETUM ESPAÑA SA**:

  L'oferta cobreix la protecció mitjançant el desplegament de contramesures, l'automatització i una descripció clara de les eines i processos, detallant la gestió i operació de les plataformes i la coordinació amb altres serveis. Inclou l'operació de les eines de protecció de l'entitat, el desplegament de contramesures i l'automatització de tasques recurrents, amb un equip especialitzat en seguretat perimetral, endpoint i cloud, i un model d'operació flexible basat en la gestió centralitzada de peticions i tasques a través d'una eina de ticketing (ITSM), protocols d'escalat i documentació detallada**.**
  No obstant això, la proposta no detalla l'automatització dels workflows de gestió i tancament del cicle de vida de les vulnerabilitats (detecció, assignació i mitigació), la qual cosa permetria un tractament més ràpid i precís de les correccions.

  Es proposa assignar a l'oferta de l'empresa INETUM ESPAÑA SA 4,5 punts.

- **OMEGA PERIPHERALS SL**:

  El servei SOCaaS incorpora un sistema SIEM amb capacitats integrades d'automatització (SOAR) i l'equip SOC activa el *playbook* corresponent en cas d'amenaça confirmada, guiant la contenció i resolució. La contenció i aplicació de contramesures està inclosa en els *playbooks*, però manca detall tècnic sobre l'operació remota d'eines de protecció (EDR, FW, etc.) i la seva validació.
  Es valora positivament la incorporació de sistemes de resposta automatitzada (SOAR) amb *playbooks* estructurats, assegurant una contenció ràpida i eficient davant les amenaces, i reduint al mínim els errors humans. La penalització en la puntuació es deu a la manca de detall tècnic sobre la validació de les contramesures aplicades en eines de protecció remotes.

  Es proposa assignar a l'oferta de l'empresa OMEGA PERIPHERAL SL 4,5 punts.

- **GMV SOLUCIONES GLOBALES INTERNET SAU**:

  Pel que fa a la protecció, GMV aposta per una combinació de desplegament d'infraestructura de seguretat (firewalls, IPS, NAC, EDR, NDR, proxies, etc.) i una operació integrada amb el SOC. Un dels punts més diferencials de la proposta és la integració de

Splunk SOAR (Phantom), que permet l'orquestració i automatització de tasques recurrents, la gestió de casos i la resposta automàtica a incidents. Aquesta automatització, amb playbooks i integració amb múltiples eines, permet reduir el temps de resposta i minimitzar els errors humans.
El punt feble de l'oferta és que no detalla la gestió i tancament del cicle de vida de les vulnerabilitats ni es detalla clarament la documentació i les simulacions contínues de contramesures.

Es proposa assignar a l'oferta de l'empresa GMV SOLUCIONES GLOBALES INTERNET SAU 4,5 punts.

- **ORANGE ESPAGNE SAU**:

ORANGE posa l'accent en l'automatització eficaç que redueix els temps de detecció i aplicació de contramesures considerablement. S'esmenta que, si bé l'objectiu és automatitzar tota l'atenció d'alertes, en cas de fallada o no integració de les fonts, el SOC monitoritzarà directament. El servei MDR inclou la monitorització, supervisió, detecció i reacció.
Es proposa l'ús de Cortex XSOAR de Palo Alto Networks, que és una plataforma d'orquestració que crea fluxos de treball i accions de resposta immediata.
Per contra, la proposta no proporciona un catàleg específic o quantificat de *playbooks* d'automatització de resposta per a accions com bloquejos en *firewalls* o aïllament d'endpoints, fet que es valora negativament.

Es proposa assignar a l'oferta de l'empresa ORANGE ESPAGNE SAU 4,5 punts.

- **S2 GRUPO SOLUCIONES DE SEGURIDAD SLU**:

Ofereix proporcionar als seus clients recomanacions per optimitzar la capacitat de resposta automàtica de la infraestructura de seguretat de l'entitat. Utilitza eines com Tenable Nessus Professional per a l'anàlisi de vulnerabilitats, però l'èmfasi en la contenció (*Desplegament de contramesures efectives*) no està detallat. La plataforma GLORIA (tritón®) compta amb capacitats natives d'Automatització de la resposta a incidents, incloent anàlisi reputacional automàtic d'IoC, enriquiment contextual, i esmenta l'ús d'IA per a l'automatització. Es fa referència a que SOAR/Automatització és una capacitat nativa i permet reduir la dedicació del persona.
S2 Grupo demostra un fort component d'automatització nativa i anàlisi amb IA/SOAR. Tanmateix, per a obtenir la màxima puntuació, caldria una descripció més formalitzada del procés de desplegament de contramesures sobre les eines de protecció de l'entitat, més enllà de les recomanacions.

Es proposa assignar a l'oferta de l'empresa S2 GRUPO SOLUCIONES DE SEGURIDAD SLU 4,5 punts.

- **SISTEMAS AVANZADOS DE TECNOLOGÍA SA**:

SATEC desplega contramesures efectives tant en incidents simulats com reals, gestionant i aplicant canvis en firewalls, IDS/IPS, EDR/XDR i eines de gestió d'accessos. El nivell d'automatització és alt gràcies a la integració de la solució SOAR (Cortex XSOAR), que permet orquestrar i automatitzar respostes, reduir errors humans i millorar la rapidesa de reacció. Els fluxos de treball automatitzats asseguren consistència i eficiència, i la solució és compatible amb la majoria d'eines del mercat.
SATEC desplega contramesures eficients i utilitza una tecnologia d'automatització avançada per garantir una resposta ràpida davant els atacs. Tot i la seva solidesa, la proposta no aclareix si totes les tasques de defensa estan completament automatitzades ni si realitza simulacions periòdiques per provar l'eficàcia de les seves contramesures.

Es proposa assignar a l'oferta de l'empresa SISTEMAS AVANZADOS DE TECNOLOGÍA SA 4 punts.

- **ITGLOBAL SL**:

  La protecció es basa en la integració amb SOAR, permetent l'automatització de respostes (playbooks), gestió automàtica de canvis en firewalls, quarantena d'amenaces, restauració de backups, bloqueig d'usuaris i integració amb NAC. El servei inclou gestió proactiva, manteniment evolutiu, accés a un equip d'experts i documentació completa.
  La plataforma permet la gestió centralitzada de polítiques de seguretat, control d'inventari i configuracions, i la presentació d'informes i dashboards en temps real. Però la proposta no formalitza si totes les tasques rutinàries estan completament automatitzades ni si es realitzen simulacions periòdiques per validar les seves defenses.

  Es proposa assignar a l'oferta de l'empresa ITGLOBAL SL 4 punts.

- **CAPGEMINI ESPAÑA SL**:

  El SOC Operatiu s'encarrega de l'aplicació de contramesures i la gestió de casos, seguint les polítiques prescrites pel SOC Tàctic. Es menciona l'aplicació de mesures sobre eines EDR/XDR i la gestió de vulnerabilitats continua i/o pentesting. Es parla de l'automatització de tasques per a una resposta ràpida i l'ús de playbooks. No obstant això, no hi ha un detall exhaustiu de la plataforma SOAR dedicada o un catàleg de playbooks. La seva automatització sembla més task automation que orquestració avançada i manca detall en la validació continua de les defenses.

  Es proposa assignar a l'oferta de l'empresa CAPGEMINI ESPAÑA SL 4 punts.

- **SEIDOR SOLUTIONS SL**:

  L'oferta descriu l'aplicació de polítiques de configuració segura (*hardening*), la contenció remota i l'activació de mesures correctores immediates (bloqueig, canvi de contrasenyes, filtres). Aquestes accions es gestionen per personal qualificat sota criteris de proporcionalitat. SEIDOR no detalla de manera explícita l'ús d'una plataforma SOAR dedicada per orquestrar accions complexes, ni quantifica el nivell d'automatització assolit en tasques recurrents. L'èmfasi és en la "resposta ràpida" i la "contenció", suggerint una intervenció més manual/semiautomàtica a través de les consoles de seguretat o les capacitats natives de la seva plataforma (DEVO), sense detallar el catàleg de playbooks.
  No detalla ni formalitza el seu catàleg d'automatitzacions complexes, suggerint una dependència més gran de la intervenció manual en lloc d'una orquestració totalment automatitzada.

  Es proposa assignar a l'oferta de l'empresa SEIDOR SOLUTIONS SL 4 punts.

Grup C – Baix nivell (<3,5 punts):

Aquestes ofertes presenten una protecció justa, amb parcial o poc detallat nivell d'automatització, resposta ràpida i desplegament efectiu de contramesures.

Característiques destacades:

- Automatització parcial o poc detallada: es menciona SOAR o automatització però sense exemples pràctics ni catàlegs de playbooks.
- Resposta més manual o semiautomàtica: dependència de tècnics o consoles, sense protocols formalitzats.
- Desplegament genèric de contramesures: sense evidències de simulacions ni validació contínua.

- Descripció tècnica limitada: manca de concreció en processos, integració o adaptació a l'entorn del client.
- Compliment bàsic del criteri: però sense destacar en innovació, personalització ni maduresa.

Les empreses incloses en aquest grup són A2SECURE TECNOLOGÍAS INFORMÁTICA SL, SOTHIS SERVICIOS TECNOLÓGICOS SLU, CONNECTIS ICT SERVICES SAU, VODAFONE ESPAÑA SAU, CLARANET SAU, APLICACIONES Y TRATAMIENTOS, ATECH ADVANCED SOLUTIONS SA, SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS SAU (SERMICRO) i TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU.

- **A2SECURE TECNOLOGÍAS INFORMÁTICA SL**:

  Es detalla que el SOC Operatiu s'encarregarà de l'operació de les eines de ciberseguretat de l'entitat, configurant-les segons les polítiques del SOC Tàctic. Es fa referència a l'ús de simulacions *Breach & Attack* (BAS) per avaluar el rendiment del sistema.
  La proposta destaca per l'automatització de les tasques més concurrents per a una resposta ràpida i per evitar errors a causa de l'acció humana. Proposen l'ús de solucions SOAR autònomes o integrades (Chronicle SOAR, Microsoft Sentinel, Splunk Enterprise, IBM QRadar). La metodologia de selecció d'automatització es basa en l'anàlisi de guanys d'eficiència i eficàcia, sent molt formal en l'enfocament.
  Tot i que la capacitat de contramesures és clara, no es concreta el nombre de playbooks ni es garanteix de forma contínua l'ús de simulacions BAS com a eina de validació de la contramesura.

  Es proposa assignar a l'oferta de l'empresa A2SECURETECNOLOGÍAS INFORMÁTICAS SL 3 punts.

- **SOTHIS SERVICIOS TECNOLÓGICOS SLU**:

  La proposta detalla la gestió i administració de les eines de protecció (antivirus, EDR, etc.) i la resposta davant incidents des de la consola, però no aporta evidències de simulacres reals ni de proves pràctiques de desplegament de contramesures.
  S'inclouen processos automatitzats per a la gestió d'actualitzacions, revisions d'estat de les eines i informes mensuals. No obstant, l'automatització depèn de la correcta integració amb l'entorn del client i, en alguns casos actualitzacions manuals, la responsabilitat recau en el client.

  Es proposa assignar a l'oferta de l'empresa SOTHIS SERVICIOS TECNOLÓGICOS SLU 2,5 punts.

- **CONNECTIS ICT SERVICES SAU**:

  En l'àmbit de la protecció, la proposta inclou el recolzament d'un CERT europeu (GTN-CERT) per a totes les tasques relacionades amb el SOC, així com un equip d'enginyeria de detecció responsable del desenvolupament i manteniment dels playbooks MITRE ATT&CK, i un equip d'intel·ligència d'amenaces. També es presenten múltiples eines SOAR (Microsoft Sentinel, Recorded Future, Swimlane, Skybox), però la proposta no aprofundeix en com s'integren aquestes eines ni en casos d'ús pràctics d'automatització.
  La proposta no explica amb prou detall i claredat com funcionaran les seves eines per bloquejar atacs automàticament ni com s'aplicaran les contramesures pràctiques davant d'un incident real.

  Es proposa assignar a l'oferta de l'empresa CONNECTIS ICT SERVICES SAU 2 punts.

- **VODAFONE ESPAÑA SAU**:

  VODAFONA aposta per una arquitectura molt automatitzada, basada en la plataforma XSOAR de Palo Alto per a l'orquestració i resposta, amb playbooks avançats que cobreixen des de la detecció fins a la recollida forense de memòria. La integració amb EDR/XDR i la capacitat d'executar accions automàtiques o manuals permeten una resposta ràpida i coordinada. La proposta destaca per la flexibilitat i escalabilitat de la seva arquitectura. Ara bé, l'oferta no concreta processos interns de validació ni detalla de com es garanteix la cobertura de tots els vectors d'atac.

  Es proposa assignar a l'oferta de l'empresa VODAFONE ESPAÑA SAU 2 punts.

- **CLARANET SAU**:

  Tot i que CLARANET proposa una arquitectura amb EDR/XDR, IDS/IPS i SOAR, la descripció de la protecció és genèrica i es limita a enumerar funcionalitats de les eines sense aportar exemples pràctics, casos d'ús reals ni protocols específics d'automatització o desplegament de contramesures. No es mostra una personalització avançada ni una adaptació als riscos concrets del client. La proposta no presenta gaire detall.

  Es proposa assignar a l'oferta de l'empresa CLARANET SAU 2 punts.

- **APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA**:

  La protecció es basa en la integració d'eines EDR/XDR, la resposta automàtica a incidents i la capacitat d'actuar directament sobre múltiples plataformes. Es fa referència a l'ús de playbooks i protocols d'actuació, però la descripció és genèrica i no s'aporten exemples pràctics de desplegament de contramesures ni d'automatització avançada. La proposta destaca per la flexibilitat i la cobertura global, però manca de personalització i detall en la gestió de la protecció.

  Es proposa assignar a l'oferta de l'empresa APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA 2 punts.

- **ATECH ADVANCED SOLUTIONS SA**:

  En l'àmbit de la protecció, la descripció de les contramesures i l'automatització és molt bàsica i no es concreta cap desplegament efectiu ni es mostren casos d'ús reals. La resposta a incidents segueix el marc NIST i ISO, però es queda en la descripció teòrica de les fases i no aporta protocols específics, exemples pràctics ni detalls sobre la coordinació amb el SOC tàctic o la cadena de custòdia.

  Es proposa assignar a l'oferta de l'empresa ATECH ADVANCED SOLUTIONS SA 2 punts.

- **SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS (SERMICRO)**:

  SEMICRO desplega contramesures automatitzades, integra solucions CCN-CERT i ofereix una bona capacitat d'automatització, però no concreta tecnologies avançades de segmentació ni detalla processos específics de protecció més enllà de l'automatització i la resposta.

  Es proposa assignar a l'oferta de l'empresa SERMICRO 2 punts.

- **TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU**:

  L'oferta no detalla les eines de protecció que s'operaran (EDR, FW, etc.) ni descriu els processos o procediments tècnics per a l'aplicació efectiva de contramesures. No s'esmenta si es realitzaran simulacions o si hi ha protocols de resposta formalitzats per incidents (aïllament, bloqueig, etc.). No fa menció de cap plataforma SOAR ni a la implementació de *playbooks*. No es detalla com s'automatitzaran les tasques recurrents (com el bloqueig d'IoC o l'aïllament) per reduir l'error humà i millorar la rapidesa de resposta.

  Es proposa assignar a l'oferta de l'empresa TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU 2 punts.

"**1.4. <u>Resposta a incidents</u>, fins a un màxim de 5 punts:**

Es valorarà la millor idoneïtat per a la resposta a incidents, segons els següents paràmetres:

- La implementació d'anàlisis forenses i coordinació amb el SOC Tàctic en incidents crítics.
- Seguiment de la cadena de custòdia de les evidències recopilades.

Les empreses licitadores presentaran els procediments i protocols per a la resposta a incidents, incloent-hi el procés de notificació i erradicació."

<u>Grup A – Alta idoneïtat (4–5 punts)</u>:

Ofertes que demostren una capacitat robusta i professional per gestionar incidents de seguretat amb garanties.

Característiques destacades:

- Presenten procediments detallats i protocols complets per a la gestió d'incidents, incloent notificació, contenció, erradicació i recuperació.
- Inclouen anàlisis forenses avançades, amb capacitat de reconstrucció d'esdeveniments i identificació de vectors d'atac.
- Estableixen una coordinació clara amb el SOC Tàctic, amb rols definits i temps de resposta garantits.
- Asseguren el seguiment rigorós de la cadena de custòdia, amb registre i protecció de les evidències.
- Disposen de plans de comunicació i escalat en cas d'incidents crítics.

Les empreses incloses en aquest grup són: EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL, SISTEMAS INFORMÁTICOS ABIERTOS SAU, SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL, EVOLUTIO CLOUD ENABLER SAU, VODAFONE ESPAÑA SAU, SISTEMAS AVANZADOS DE TECNOLOGÍA SA, ITGLOBAL SL, SOTHIS SERVICIOS TECNOLÓGICOS SLU, S2 GRUPO SOLUCIONES DE SEGURIDAD SLU, OMEGA PERIPHERALS SL, A2SECURE TECNOLOGÍAS INFORMÁTICA SL, SEIDOR SOLUTIONS SL, ORANGE ESPAGNE SAU, CAPGEMINI ESPAÑA SL, GMV SOLUCIONES GLOBALES INTERNET SAU i INETUM ESPAÑA SA.

- **EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL**:

  La resposta a incidents és completa i alineada amb les millors pràctiques, garantint traçabilitat, rapidesa i coordinació amb tots els actors implicats. Procediments detallats per a la gestió d'incidents, tan crítics com no crítics, amb coordinació directa amb el SOC Tàctic.

Implementació d'anàlisi forense, preservació de la cadena de custòdia, documentació exhaustiva i reporting adaptat a diferents nivells (operatiu, tàctic, estratègic).
Simulacions i exercicis de resposta, formació contínua de l'equip, i millora iterativa dels procediments.
Procés clar de notificació, escalat, erradicació i recuperació, amb suport a la presa de decisions estratègiques.

Es proposa assignar a l'oferta de l'empresa EY TRANSFORMA SERVICIOS DE CONSULTORÍA SAL 5 punts.

- **SISTEMAS INFORMÁTICOS ABIERTOS SAU**:

La resposta a incidents de SIA és molt completa, amb equip expert, protocols forenses, coordinació amb el SOC Tàctic i millora contínua. Procediments detallats per a la resposta a incidents, amb equip especialitzat, coordinació amb el SOC Tàctic, i anàlisi forense avançada. Seguiment rigorós de la cadena de custòdia, informes pericials i judicials, i protocols basats en ISO 27037:2012. Inclou notificació, escalat, erradicació, recuperació i lliçons apreses. La proposta inclou informes post-incident i suport legal.

Es proposa assignar a l'oferta de l'empresa SISTEMAS INFORMÁTICOS ABIERTOS SAU 5 punts.

- **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL (SIRT)**:

SIRT disposa d'un servei de resposta a incidents molt complet, amb equip expert, protocols forenses, cadena de custòdia garantida i millora contínua, assegurant una gestió eficaç i àgil de qualsevol incident.
El servei de resposta a incidents (CSIRT/DFIR), amb equip altament especialitzat, metodologia basada en SANS (6-step incident handling), MITRE ATT&CK i coordinació amb el SOC Tàctic i CCN.
Inclou anàlisi forense avançada, seguiment rigorós de la cadena de custòdia (NIST, ISO/IEC), documentació exhaustiva, playbooks automatitzats, ciberexercicis anuals, feedback i millora contínua.
Es cobreixen totes les fases: preparació, identificació, contenció, erradicació, recuperació i lliçons apreses, amb integració d'eines forenses, SIEM, EDR, MISP, etc.

Es proposa assignar a l'oferta de l'empresa SIRT 5 punts.

- **EVOLUTIO CLOUD ENABLER SAU**:

EVOLUTIO destaca en resposta a incidents, amb equip expert, protocols rigorosos i orientació clara a la gestió de crisis i la recuperació. El servei de resposta a incidents (CERT/CSIRT) compta amb un equip altament especialitzat, metodologia NIST SP 800-61, MITRE ATT&CK, coordinació amb el SOC Tàctic i CCN, anàlisi forense, cadena de custòdia, informes detallats i protocols de comunicació multicanal.
Inclou assignació d'Incident Handler i ciberexercicis anuals.

Es proposa assignar a l'oferta de l'empresa EVOLUTIO CLOUD ENABLER SAU 5 punts.

- **CAPGEMINI ESPAÑA SL**:

CAPGEMINI proposa l'ús d'Analistes SWAT dedicats per a la investigació d'incidents de seguretat. Aquests analistes utilitzen un kit forense (tant *hardware* com *software*) per a l'adquisició i anàlisi de dades. Es compromet a operar sota les directrius del SOC Tàctic. Aplica un procediment de cadena de custòdia rigorós i orientat a peritatges judicials. CAPGEMINI ofereix una capacitat DFIR (Digital Forensics and Incident Response) de

primer nivell, reforçada amb recursos SWAT dedicats i un compromís formal amb la integritat legal de les proves.
S'aprecia certa manca de detall sobre la metodologia forense de N3 (per exemple, alineament amb estàndards forenses específics com EnCase o Hashing Tools, tot i que l'ús del "kit forense" implica la seva existència).

Es proposa assignar a l'oferta de l'empresa CAPGEMINI ESPAÑA SAL 4,5 punts.

- **SOTHIS SERVICIOS TECNOLÓGICOS SLU**:

L'empresa disposa de procediments i protocols ben documentats per a la resposta a incidents, amb un flux estructurat: detecció, anàlisi, contenció, erradicació i "lliçons apreses". El model inclou informes d'incidents, notificació en temps real, escalat segons criticitat i participació en comitès de crisi.
S'explicita la coordinació amb el SOC Tàctic i la generació d'informes post-incident per millorar processos.
Un punt feble de la proposta és que la resposta pràctica (contenció i erradicació) depèn sovint de l'aplicació de mesures per part del client, i l'anàlisi forense només s'activa sota demanda i fora del servei bàsic.

Es proposa assignar a l'oferta de l'empresa SOTHIS SERVICIOS TECNOLÓGICOS SLU 4,5 punts.

- **VODAFONE ESPAÑA SAU**:

Vodafone basa la seva resposta en el model NIST, amb un procés complet que inclou preparació, detecció, anàlisi, contenció, erradicació, recuperació i activitats post-incidents. Disposa d'un equip DFIR especialitzat, capacitat forense i custòdia d'evidències, i protocols de comunicació amb el SOC Tàctic, CCN-CERT i altres organismes. La cadena de custòdia es garanteix amb eines com EnCase i protocols de hashing, però la proposta no concreta la ubicació ni la certificació ENS de la infraestructura, i el SIEM propi no està al CPSTIC.

Es proposa assignar a l'oferta de l'empresa VODAFONE ESPAÑA SAU 4,5 punts.

- **A2SECURE TECNOLOGÍAS INFORMÁTICA SL**:

A2SECURE té un rol de suport en incidents no crítics i de coordinació en incidents crítics, executant una primera anàlisi de l'afectació i proveint context al SOC Tàctic. El seu equip té formació en forense i resposta. El servei inclou anàlisi de les evidències. L'oferta garanteix que es recopilaran i analitzaran les evidències seguint un procés que en "garanteixi la integritat" i la "cadena de custòdia garantint-ne la validesa davant un possible procés judicial".
Per contra, la descripció del procediment tècnic específic per a l'adquisició i custòdia (eines, certificacions forenses específiques) és més conceptual que procedimentalment detallada i manca el detall sobre la metodologia forense que s'utilitzarà durant l'anàlisi de les evidències.

Es proposa assignar a l'oferta de l'empresa A2SECURE TECNOLOGÍAS INFORMÁTICA SL 4,5 punts.

- **SEIDOR SOLUTIONS SL**:

Disposa de capacitats avançades (N3) per implicar tècnics de resposta forense. Després de la contenció, activen l'anàlisi de causa arrel basat en la revisió d'evidències (logs, EDR, trànsit, etc.) per reconstruir l'escenari d'intrusió. L'informe postincident detalla el vector d'entrada, l'impacte i les vulnerabilitats explotades. Es fa èmfasi en la documentació de totes

les accions per a la rendició de comptes i es garanteix que l'informe final tindrà "valor probatori" i serà útil per a auditories i entitats reguladores.
A l'oferta manca detall del protocol tècnic (hashing, emmagatzematge segregat) durant la recollida d'evidències, la qual cosa és un risc crític des d'una perspectiva forense pura.

Es proposa assignar a l'oferta de l'empresa SEIDOR SOLUTIONS SL 4 punts.

- **ORANGE ESPAGNE SAU**:

Els incidents s'escalen al Nivell 3 (DFIR), que involucra nous especialistes i pot requerir anàlisi de *malware* o anàlisi profund d'esdeveniments. Orange coordina la notificació segons la "Guia nacional de notificació i gestió de ciberincidentes". El servei de gestió d'incidents es basa en el protocol NIST, però el detall sobre el seguiment de la cadena de custòdia de les evidències és escàs. Es parla de la gestió d'incidents, documents i SLA, però no s'especifica el procediment tècnic per assegurar la integritat de les evidències digitals o la seva validesa legal a nivell contractual explícit.

Es proposa assignar a l'oferta de l'empresa ORANGE ESPAGNE SAU 4 punts.

- **SISTEMAS AVANZADOS DE TECNOLOGÍA SA (SATEC)**:

La resposta a incidents de SATEC segueix una metodologia basada en l'estàndard NIST SP 800-61, cobrint totes les fases: preparació, detecció, contenció, investigació, remediació i recuperació. Inclou anàlisi forense digital (DFIR), seguiment estricte de la cadena de custòdia de les evidències i generació d'informes forenses segons la norma UNE 197001. El procés està automatitzat amb SOAR i coordinat amb el SOC Tàctic, assegurant la notificació, documentació i preservació de les evidències per a possibles procediments legals o auditories.
Proposta molt sòlida i alineada amb els estàndards, però amb marge de millora en la part de simulacres i revisió post-incident.

Es proposa assignar a l'oferta de l'empresa SATEC 4 punts.

- **ITGLOBAL SL**:

La resposta a incidents segueix la metodologia NIST SP 800-61, cobrint totes les fases: preparació, detecció, contenció, investigació, remediació i recuperació. Inclou anàlisi forense, cadena de custòdia, informes post-mortem i formació periòdica al personal. El procés està automatitzat amb SOAR, coordinat amb el CSIRT i el client, i inclou procediments d'escalat, preservació de proves i revisió post-incident.
Tot i així, si bé la metodologia és robusta i la preservació d'evidències està ben coberta, la proposta podria guanyar encara més força si posés més èmfasi en la realització de simulacres periòdics i en la formació pràctica dels equips interns, per tal d'assegurar que la resposta a incidents no només sigui teòricament impecable, sinó també àgil i efectiva en situacions reals.

Es proposa assignar a l'oferta de l'empresa ITGLOBAL SL 4 punts.

- **S2 GRUPO SOLUCIONES DE SEGURIDAD SLU**:

En resposta a incidents, S2GRUPO té una metodologia clara, protocols de contenció i erradicació, i una bona gestió d'evidències digitals. La seva integració amb el SOC Tàctic li permet escalar incidents crítics amb rapidesa i garantir la traçabilitat. Ara bé, la resposta és més reactiva que proactiva, i no incorpora elements com el grup d'intervenció ràpida, el comitè de crisi o l'anàlisi forense avançat. En aquest sentit, S2 Grupo ofereix una resposta fiable, però menys innovadora i menys orientada a la millora contínua

Es proposa assignar a l'oferta de l'empresa S2GRUPO SOLUCIONES DE SEGURIDAD SL 4 punts.

- **OMEGA PERIPHERALS SL**:

  El servei de resposta està alineat amb la guia STIC-817 del CCN-CERT. L'escalat a Nivell 2 o 3 inclou la capacitat de realitzar anàlisi forense i contenció avançada. També ofereixen l'activació de serveis de resposta reforçada en casos crítics, incloent anàlisi forense complet garantint la traçabilitat i el compliment normatiu.
  Com a mancança vers altres propostes la descripció se centra més en el compliment normatiu (STIC-817, ENS) i la visibilitat del registre que en la formalització tècnica de la cadena de custòdia per a la validesa legal.

  Es proposa assignar a l'oferta de l'empresa OMEGA PERIPHERALS SL 4 punts.

- **GMV SOLUCIONES GLOBALES INTERNET SAU**:

  La proposta de GMV destaca per la presència d'una figura especialitzada, el Perit Judicial, encarregat de garantir la custòdia de les evidències en situacions que ho requereixin. S'explica amb detall el procés d'adquisició, la cadena de custòdia, la documentació i la preservació de les proves, així com la capacitat d'actuar tant en laboratori com en escenaris de camp.
  Tanmateix, tot i la solidesa metodològica, la proposta no concreta quines guies o estàndards internacionals (com les guies NIST) s'utilitzaran per a la recol·lecció d'evidències. També presenta mancances en l'alineament amb estàndards internacionals i en la coordinació amb altres actors clau de la resposta a incidents.

  Es proposa assignar a l'oferta de l'empresa GMV SOLUCIONES GLOBALES INTERNET SAU 4 punts.

- **INETUM ESPAÑA SA:**

  L'oferta descriu de manera exhaustiva els procediments de resposta, incloent anàlisi forense, cadena de custòdia i protocols de notificació i erradicació. L'alineament amb NIST i ISO és un punt fort, també destaca per l'anàlisi forense segons ISO/IEC 27037:2021, seguiment de la cadena de custòdia, reunions de lliçons apreses. Detalla procediments per a la resposta, documentació i millora contínua.
  Davant un incident no parla clarament de comunicar-ho al SOC Tàctic. Aquesta absència és una mancança important, ja que la coordinació amb el SOC Tàctic és imprescindible per garantir una resposta efectiva i alineada amb els protocols del sector públic. També presenta mancances a la cadena de custòdia, la manca de detall sobre el procediment tècnic específic per a l'adquisició i custòdia (eines, hashing tools o procediments d'adquisició pericial) per garantir la validesa legal de la prova. La descripció se centra més en el valor probatori de l'informe final que en el rigor tècnic del procés d'adquisició de proves.

  Es proposa assignar a l'oferta de l'empresa INETUM ESPAÑA SA 4 punts.

Grup B – Idoneïtat mitjana (2–3 punts):

Ofertes que cobreixen els requisits mínims, però amb mancances en la profunditat i formalització dels processos.

Característiques destacades:

- Presenten procediments genèrics per a la resposta a incidents, amb cobertura parcial de les fases clau.

- Inclouen anàlisis forenses bàsiques, però sense eines especialitzades ni capacitat de correlació avançada.
- La coordinació amb el SOC Tàctic és indicada però no detallada, amb poca claredat en els protocols.
- El seguiment de la cadena de custòdia és mencionat però no estructurat, amb risc de pèrdua d'evidències.
- Els mecanismes de notificació i escalat són funcionals però no sistemàtics.

Les empreses incloses en aquest grup són: CLARANET SAU, CONNECTIS ICT SERVICES SAU, SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS DELECTRÓNICOS i ATECH ADVANCED SOLUTIONS S.A.

- **CLARANET SAU**:

  La proposta de CLARANET estructura la resposta a incidents segons la metodologia FIRST i la col·laboració amb CSIRT, però la descripció és força teòrica i no aporta protocols específics, fluxos de comunicació detallats ni exemples pràctics de gestió d'incidents complexos. La capacitat d'anàlisi forense i manteniment de la cadena de custòdia es descriu de manera correcta, però sense diferenciar-se ni aportar valor afegit respecte a altres licitadors que han presentat metodologies de recollida i custodi d'evidències. No es coordina amb el SOC Tàctic de l'agència.

  Es proposa assignar a l'oferta de l'empresa CLARANET SAU 2 punts.

- **CONNECTIS ICT SERVICES SAU**:

  La resposta a incidents es basa en la guia NIST Special Publication 800-61, i per a la recopilació d'informació després d'un ciberincident es fa referència a la metodologia anglesa GPG-13. Això aporta rigor metodològic teòric, però la proposta es queda curta en detall operacional. Inclouen anàlisis forenses bàsiques, però sense eines especialitzades ni capacitat de correlació avançada. El seguiment de la cadena de custòdia és mencionat però no estructurat, amb el risc de pèrdua d'evidències.
  Un altre punt febles seria que a la proposta no s'explica com es coordinarà amb el SOC Tàctic. Aquesta absència és una mancança important, ja que la coordinació amb el SOC Tàctic és imprescindible per garantir una resposta efectiva i alineada.
  La proposta presenta un compliment bàsic dels criteris exigits, però amb una manca important de formalització en la coordinació amb el SOC Tàctic i un dèficit de detall tècnic en els protocols de custòdia i automatització.

  Es proposa assignar a l'oferta de l'empresa CONNECTIS ICT SERVICES SAU 2 punts.

- **ATECH ADVANCED SOLUTIONS SA**:

  En l'àmbit de la protecció, la descripció de les contramesures i l'automatització és molt bàsica i no es concreta cap desplegament efectiu ni es mostren casos d'ús reals. La resposta a incidents segueix el marc NIST i ISO, però es queda en la descripció teòrica de les fases i no aporta protocols específics, exemples pràctics ni detalls sobre la coordinació amb el SOC tàctic o la cadena de custòdia. La manca d'anàlisi de l'exposició de l'entitat i la descripció genèrica dels processos justifiquen la seva puntuació.

  Es proposa assignar a l'oferta de l'empresa ATECH ADVANCED SOLUTIONS SAL 2 punts.

- **SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS (SERMICRO)**:

  SERMICRO s'alinea amb NIST i CCN-CERT, presenta protocols DFIR, anàlisi forense, cadena de custòdia i coordinació amb el SOC Tàctic. La metodologia és clara, però la

descripció de la gestió automatitzada i la integració amb plataformes de ticketing presenta mancances importants.

Es proposa assignar a l'oferta de l'empresa SERMICRO 2 punts.

Grup C – Idoneïtat limitada (0–1 punt):

Ofertes que no garanteixen una resposta eficaç ni controlada davant incidents de seguretat.

Característiques destacades:

- No presenten procediments clars per a la resposta a incidents.
- No s'inclou cap anàlisi forense ni coordinació amb el SOC Tàctic.
- No hi ha seguiment de la cadena de custòdia ni protocols de gestió d'evidències.
- El procés de notificació i erradicació és inexistent o molt superficial.

Les empreses incloses en aquest grup són: APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA i TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU.

- **APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA**:

  En resposta a incidents, la proposta estructura el procés en les fases clàssiques (preparació, identificació, contenció, erradicació, recuperació, lliçons apreses), amb un esquema de treball per capes i escalat segons la complexitat de l'incident. Es fa referència a la capacitat d'anàlisi forense, manteniment de la cadena de custòdia i coordinació entre equips, però la descripció és força teòrica i no aporta protocols específics, exemples pràctics ni detalls sobre la coordinació amb el SOC tàctic.

  Es proposa assignar a l'oferta de l'empresa APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA 1 punt.

- **TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU**:

  La informació aportada sobre la resposta a incidents és mínima sense aportar informació sobre els procediments forenses, l'aplicació de la cadena de custòdia, ni la coordinació amb el SOC Tàctic.

  Es proposa assignar a l'oferta de l'empresa TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU 1 punts.

"**2. Prestacions tècniques del SIEM, fins a un màxim de 10 punts:**

Es valoraran les automatitzacions i correlacions a implantar en el SIEM, així com la inclusió d'elements que facilitin la integració amb les eines de l'ecosistema del Centre Criptològic Nacional i l'enviament de trànsit de xarxa de manera selectiva a aquestes.

Es presentarà una memòria descriptiva del/s SIEM proposat/s que inclogui l'arquitectura, incloent els elements de recol·lecció amb la seva ubicació, agregació i processat d'esdeveniments, el dimensionament i mètriques de llicenciament, automatitzacions i correlacions, així com de registres d'activitat i els elements a incloure de cara a la integració amb el Centre Criptogràfic Nacional."

S'agrupen les ofertes en diferents grups per rang de puntuació.

Grup A: Prestacions avançades (8–10 punts):

Aquest grup inclou les ofertes amb el nivell més alt de detall tècnic, màxima maduresa arquitectònica i compromisos formals de compliment i integració amb l'ecosistema del CCN-CERT.

Característiques destacades:

- SIEM reconegut al catàleg CPSTIC, desplegat i operatiu 24x7. Les arquitectures són federades, escalables i distribuïdes, amb segmentació de dades (HOT/WARM/OFFLINE) i suport per a alta volumetria
- Automatització Avançada (SOAR/ML): Alta concreció en les automatitzacions, incloent playbooks, correlació d'esdeveniments i resposta automàtica. S'inclou la integració amb plataformes SOAR.
- Integració CCN Completa: La integració és completa amb l'ecosistema CCN-CERT i SOC Tàctic. Les ofertes detallen la integració d'eines com LUCIA, SAT-INET, REYES i microClaudia no només com a connectors, sinó com a components operatius dins del SIEM

Les empreses incloses en aquest grup són: SISTEMAS INFORMÁTICOS ABIERTOS SAU, S2 GRUPO SOLUCIONES DE SEGURIDAD SLU, GMV SOLUCIONES GLOBALES INTERNET SAU, EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL, SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL, A2SECURE TECNOLOGÍAS INFORMÁTICA SL, CAPGEMINI ESPAÑA SL, EVOLUTIO CLOUD ENABLER SAU.

- **SISTEMAS INFORMÁTICOS ABIERTOS SAU**:

  SIA proposa com a SIEM principal MÒNICA NGSIEM, homologat pel CPSTIC i certificat ENS Alta, amb alternatives com Microsoft Sentinel i IBM QRadar. L'arquitectura és federada, escalable i distribuïda, amb capacitat d'ingesta de fins a 4 TB/dia, segmentació HOT/WARM/OFFLINE i suport per MongoDB i HDFS. Aquesta robustesa és un punt fort per entorns amb alta volumetria de logs.
  Sobre les automatitzacions s'inclouen més de 140 casos d'ús amb correlacions natives i via TheHive/Cortex.
  SIA presenta un catàleg de més de 800 casos d'ús, estructurats segons MaGMa i MITRE ATT&CK, amb 5 nivells de maduresa.
  SIA presenta la seva arquitectura MONICA NGSIEM (solució certificada pel CCN), garantint una plataforma distribuïda i robusta amb SOAR/OXEN per a l'automatització de la resposta a incidents. La proposta destaca per una integració operativa completa i detallada amb les eines clau de l'ecosistema CCN-CERT (LUCIA, SAT-INET, REYES), la qual cosa assegura la màxima coordinació institucional. Finalment, inclou el compromís legal i explícit de lliurar els registres d'activitat complets en format interoperable cada tres mesos, complint rigorosament els requisits d'auditoria.

  Es proposa assignar a l'oferta de l'empresa SISTEMAS INFORMÁTICOS ABIERTOS SAU 10 punts.

- **A2SECURE TECNOLOGÍAS INFORMÁTICA SL**:

  Proposa SIEM reconeguts al catàleg CPSTIC (Chronicle, Sentinel, Splunk i QRadar). Detalla l'automatització i optimització de l'ecosistema, així com l'ús de SOAR integrat en diverses solucions (SIEM, ITSM, XDR), amb processos per a la selecció de playbooks. Els casos d'ús s'alineen amb MITRE ATT&CK.
  L'oferta compleix explícitament amb el requisit d'interoperabilitat legal, comprometent-se a lliurar els registres d'activitat complets cada tres mesos en format interoperable. La retenció mínima és de trenta dies per a l'operació i sis mesos per a l'arxivat.
  Destaca també per la seva capacitat d'instal·lació i automatització de les eines CCN (Carmen i Claudia) sense requerir intervenció del personal municipal.

Es proposa assignar a l'oferta de l'empresa A2SECURE TECNOLOGÍAS INFORMÁTICA SL 10 punts.

- **GMV SOLUCIONES GLOBALES INTERNET SAU**:

Presenta Splunk com a SIEM. També proposa l'ús de Splunk SOAR i casos d'ús amb metodologia detallada (MITRE ATT&CK).
GMV es compromet a la integració tècnica completa amb totes les eines de l'ecosistema del CCN-CERT (incloent LUCIA, CARMEN, MicroCLAUDIA i SATINET). Però l'oferta presenta una feblesa administrativa en la garantia de la traçabilitat dels logs perquè no confirma explícitament el compromís de lliurar els registres d'activitat complets en format interoperable almenys cada tres mesos tot i que sí detalla la documentació i el registre dels resultats.

Es proposa assignar a l'oferta de l'empresa GMV SOLUCIONES GLOBALES INTERNET SAU 9,5 punts.

- **S2 GRUPO SOLUCIONES DE SEGURIDAD SLU**:

La proposta inclou la Suite pròpia GLORIA, que a banda de tenir molts mòduls propis de recol·lecció, agregació i processat d'esdeveniments també te un API REST per a la integració amb altres eines d'altres fabricants.
Utilitza el motor ADITS utilitza IA per detectar anomalies i el SOAR permet automatitzar l'entrenament i la sintonització de paràmetres. Utilitza playbooks per a la gestió de la resposta amb més de 600 regles d'automatització.
Disposen de diferents eines pròpies desenvolupades amb ML també per automatitzacions.
Presenta el compromís explícit d'implementació i parametrització de totes les eines CCN: CARMEN, LUCIA, CLAUDIA i SAT-INET, també s'integra amb REYES per a la notificació d'incidents.
S2 Grupo CERT és Membre de FIRST, TF-CSIRT, CSIRT.ES, i de la Xarxa Nacional de SOC a espanya .
La feblesa que presenta és la manca de formalització en la Memòria Arquitectònica (ubicació/agregació) per ser la solució determinada "en cada cas". Manca també de compromís formal de lliurament trimestral de logs en format interoperable.

Es proposa assignar a l'oferta de l'empresa S2 GRUPO SOLUCIONES DE SEGURIDAD SLU 9 punts.

- **EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL**:

Presenta un SIEM amb la plataforma Splunk, amb una arquitectura al núvol amb escalabilitat total.
Presenta automatitzacions amb SPLUNK SOAR, millorant l'eficiència operativa. EY disposa d'una base dades d'ús específics per a SPLUNK que cobreix les principals amenaces totes amb MITRE ATT&CK.
Registre d'activitats: la normalització de dades a la plataforma es realitza mitjançant el Common Information Model (CIM). El CIM està alineat amb l'Open Cybersecurity Schema Framework (OCSF).
SIEM s'integra amb SAT-INE, CLAUDIA i CARMEN, però manca el detall operatiu d'implementació de les eines de CCN com LUCIA.

Es proposa assignar a l'oferta de l'empresa EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL 9 punts.

- **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL (SIRT)**:

  Proposa la solució de SIEM basada en Splunk (utilitzant Enterprise Security), una arquitectura escalable que utilitza automatització avançada (Splunk SOAR) amb accés a una base de més de 2.800 accions per a la mitigació d'incidents. La proposta compleix el requisit d'arquitectura (Edge Processor, CIM/OCSF) i es compromet a la integració tècnica per a l'enviament selectiu de trànsit a eines CCN com CARMEN i MicroCLAUDIA. Aquesta solvència tècnica es complementa amb una metodologia de correlació rigorosa (MaGMa, MITRE ATT&CK) i un servei CSIRT operatiu 24x7. La feblesa de la proposta és que no formalitza el compromís explícit de lliurar els registres d'activitat complets en format interoperable almenys cada tres mesos.

  Es proposa assignar a l'oferta de l'empresa SIRT 9 punts.

- **CAPGEMINI ESPAÑA SL:** Proposa la plataforma ICDP basada en Devo o Sentinel i l'automatització amb SOAR (Devo SOAR o Azure Sentinel Lighthouse). Utilitza la Use Case Factory (UCF), que manté una llibreria de 1500 casos d'ús estàndard. Les deteccions s'alineen amb Mitre ATT&CK. Inclou la capacitat d'automatitzar respostes com aïllar sistemes o bloquejar adreces IP malicioses.
  La seva arquitectura oberta (Devo / Sentinel) facilita la integració amb les eines del CCN. Es compromet a la instal·lació d'eines com SAT-INET, MicroCLAUDIA, CARMEN i LUCIA. Aquesta capacitat permet l'enviament selectiu de trànsit de xarxa a aquestes eines.
  La deducció de punts es deu al fet que, tot i la gran quantitat de casos d'ús (1500), hi ha una manca de quantificació del catàleg de regles de detecció inicial. A més, la proposta no confirma de manera explícita el compromís de lliurament trimestral de logs complets en format interoperable. També es va observar una manca de profunditat en la descripció de l'arquitectura de recol·lecció. Finalment, l'automatització sembla més enfocada a tasques (Task Automation) que a una orquestració avançada formalitzada (SOAR dedicat)

  Es proposa assignar a l'oferta de l'empresa CAPGEMINI ESPAÑA SAL 8,5 punts.

- **EVOLUTIO CLOUD ENABLER SAU**:

  La seva proposta de SIEM es fonamenta en la plataforma nativa al núvol Google Security Operations (SecOps) (o Chronicle), amb SOAR integrat per a l'orquestració de la resposta automatitzada. Fa servir la metodologia MITRE ATT&CK. La proposta destaca pel seu fort compromís legal i formal, ja que es compromet explícitament a lliurar els registres d'activitat complets dels sistemes oferts en format interoperable almenys cada tres mesos.
  Així mateix, EVOLUTIO formalitza la instal·lació i/o automatització d'agents de totes les eines clau de l'ecosistema CCN-CERT, com LUCIA, SAT-INET, CLAUDIA, CARMEN i microCLAUDIA, assegurant la màxima integració institucional. La feblesa de la proposta és principalment la manca de detall granular sobre l'arquitectura de recol·lecció i processament, i a la baixa concreció en la quantificació i descripció dels fluxos de treball d'automatització (SOAR).

  Es proposa assignar a l'oferta de l'empresa EVOLUTIO CLOUD ENABLER SAU 8,5 punts.

Grup B Solucions Sòlides i Adaptació Tècnica (8-7 punts):

Aquest grup utilitza plataformes de mercat molt sòlides i de renom (Splunk, QRadar, Sentinel) i demostra capacitats tècniques avançades (SOAR, UEBA, CTI). El que els diferencia del Grup A és la manca de formalitat en els compromisos administratius o la menor concreció en la integració operativa CCN.

Característiques destacades:

- Tecnologia Líder i Capacitat d'Evolució: Utilitzen tecnologies de gran abast com Google Security Operations (SecOps), Sentinel, o QRadar, amb Arquitectures amb Alta Disponibilitat (HA) i enfocament Cloud-native.
- Automatització i ML: Fort ús de SOAR, sovint integrat amb ITSM (Remedy per EVOLUTION) o amb playbooks nadius. Utilització de ML i IA per a la detecció (Sentinel, QRadar).
- Manca de Formalitat en Registres: Aquestes ofertes sovint no especifiquen la periodicitat de lliurament del registre d'activitat complet en format interoperable (el PPT indica que hauria de ser cada 3 mesos), penalitzant la seva puntuació respecte al Grup A
- Integració CCN (Intel·ligència vs. Operació): La integració amb el CCN és ferma, però menys detallada que el Grup A en els mecanismes d'automatització operativa.

Les empreses incloses en aquest grup són: INETUM ESPAÑA SA, SISTEMAS AVANZADOS DE TECNOLOGÍA SA, SOTHIS SERVICIOS TECNOLÓGICOS SLU, OMEGA PERIPHERALS SL, SEIDOR SOLUTIONS SL, ORANGE ESPAGNE SAU.

- **INETUM ESPAÑA SA**:

  La proposta de SIEM es basa en Microsoft Sentinel en modalitat Cloud multi-tenant, destacant la seva escalabilitat i l'ús de funcionalitats natives d'IA i Machine Learning per a la detecció d'amenaces.
  El catàleg de casos d'ús no es basa en les directrius MITRE ATT&CK.
  Inetum és membre de la Xarxa Nacional de SOC (RNS) del CCN-CERT i utilitza la seva plataforma MISP federada per a la compartició d'Indicadors de Compromís (IoC). No obstant això, hi ha manca de compromís explícit de lliurar els registres d'activitat complets en format interoperable almenys cada tres mesos. A més, l'oferta no detalla de manera clara i específica els mecanismes d'automatització de tasques operatives amb les eines CCN com LUCIA o l'enviament selectiu de trànsit de xarxa a CARMEN.

  Es proposa assignar a l'oferta de l'empresa INETUM ESPAÑA SA 8 punts.

- **SISTEMAS AVANZADOS DE TECNOLOGÍA SA**:

  Pel que fa a l'arquitectura ofereix varies plataformes robustes (IBM QRadar / Splunk). QRadar manté registres d'activitats administratives i d'anàlisi complint la normativa de retenció de logs.
  Per les automatitzacions utilitza Cortex XSOAR (SOAR) de Palo alto en modalitat MSSP (gestionat per un SOC extern professional), per a l'orquestració de la resposta, amb playbooks per contextualitzar incidents i coordinar tecnologies. Tot i que esmenta la necessitat d'una sonda com a pont per a l'automatització XSOAR, la descripció no detalla la integració explícita i formalitzada amb altres eines clau de l'ecosistema CCN (com SAT-INET o MicroCLAUDIA).
  La proposta no inclou el compromís formal i explícit d'entregar els registres d'activitat complets dels sistemes oferts en format interoperable almenys cada tres mesos. A més, la proposta no detalla amb claredat el grau de personalització de les regles de correlació per a cada entitat ni la formalitat del cicle de millora contínua de les seves automatitzacions i deteccions, cosa que redueix la valoració de la seva maduresa operativa en el SIEM. Tampoc detalla la integració amb el ecosistema de CCN amb claredat.

  Es proposa assignar a l'oferta de l'empresa SISTEMAS AVANZADOS DE TECNOLOGÍA SA 8 punts.

- **OMEGA PERIPHERALS SL**:

  La proposta utilitza arquitectures SIEM/SOAR d'última generació; aquesta destaca per la seva capacitat d'automatització amb l'ús d'Intel·ligència Artificial (IA) i l'Anàlisi de Comportament d'Usuaris i Entitats (UEBA) per detectar anomalies i correlacions complexes

d'amenaces. Aquest sistema, a més, s'alinea amb les directrius nacionals (CCN-STIC) i s'integra amb els indicadors d'amenaces (IoC) de la Xarxa Nacional de SOC (RNS).
No obstant això, OMEGA no formalitza el compromís explícit de lliurar els registres d'activitat complets en format interoperable almenys cada tres mesos. La proposta tampoc concreta com es duria a terme l'enviament selectiu de trànsit de xarxa i el desplegament operatiu de les eines clau de l'ecosistema del Centre Criptològic Nacional (CCN-CERT), com CARMEN o microCLAUDIA.
En resum, la solidesa de la tecnologia i l'automatització de la detecció d'amenaces queden garantides, però hi ha una deficiència en els compromisos administratius formals i en el detall de la integració institucional requerida.

Es proposa assignar a l'oferta de l'empresa OMEGA PERIPHERALS SL 8 punts.

- **SEIDOR SOLUTIONS SL**:

Proposa DEVO, una solució nativa al núvol, altament escalable i *multitenant*. L'Anàlisi de comportament d'usuaris i entitats (UEBA) que pot orquestrar accions automatitzades (SOAR), com ara bloquejos en tallafocs o quarantena de dispositius, mitjançant integració amb plataformes externes com ServiceNow o XSOAR. Les regles es basen en la taxonomia MITRE ATT&CK.
El registre de cada incident es fa de manera completa dins la plataforma de gestió però no es confirma el compromís de lliurament trimestral de logs complets en format interoperable.
A la proposta manca l'esment explícit a la instal·lació o automatització d'eines com CARMEN o CLAUDIA. SEIDOR es basa en l'intercanvi de feeds d'intel·ligència i en l'alineament amb les guies, però sense detallar el mecanisme tècnic per a l'enviament selectiu de trànsit de xarxa a aquestes eines del CCN.
En essència, l'oferta de SEIDOR és bona, però li manquen els compromisos formals de documentació i en la descripció detallada dels mecanismes operatius per a la integració profunda amb l'entorn de seguretat institucional nacional.

Es proposa assignar a l'oferta de l'empresa SEIDOR SOLUTIONS SL 8 punts.

- **ORANGE ESPAGNE SAU**:

El servei s'aplica sobre la plataforma d'ORANGE, que comprèn SIEM de tecnologia Elastic i l'orquestrador XSOAR.
Utilitza la plataforma XSOAR, amb playbooks per a la contramesura automàtica, l'obertura de tiquets, el bloqueig de dispositius perimetrals i l'anàlisi de reputació. Els casos d'ús s'alineen amb MITRE ATT&CK.
La gestió d'incidents utilitza el protocol NIST, però sense un compromís explícit de lliurament trimestral de logs complets en format interoperable.
Manca el detall operatiu o el compromís d'instal·lació de les eines CCN (CARMEN, CLAUDIA) o mecanismes d'enviament selectiu de trànsit, no confirma el lliurament trimestral de logs en format interoperable.
En resum, Orange presenta una solució de detecció tecnològicament avançada i amb una alta maduresa en automatització, però la seva puntuació es veu limitada per la manca de formalitat legal respecte a l'exportació periòdica de logs i la descripció operativa genèrica de la integració amb les sondes i eines del CCN.

Es proposa assignar a l'oferta de l'empresa ORANGE ESPAGNE SAU 7,5 punts.

- **SOTHIS SERVICIOS TECNOLÓGICOS SLU**:

L'oferta de SOTHIS es basa en la plataforma IBM QRadar, que es proporciona en modalitat Cloud compartit.
SOTHIS aplica metodologies de detecció avançades basades en la guia NIST 800-154, el framework MITRE ATT&CK i la Cyber Kill Chain, i utilitza anàlisi de comportament d'usuari

(UEBA) per a la detecció d'anomalies i l'aprenentatge automatitzat (Machine Learning). Pel que fa a la integració amb l'ecosistema del CCN, SOTHIS s'integra amb eines clau com MicroCLAUDIA, CARMEN, CLAUDIA i SAT-INET.
Per una altra banda, SOTHIS no confirma el compromís explícit de lliurar els registres d'activitat complets en format interoperable almenys cada tres mesos. Un altre mancança és que la seva solució mostra un nivell baix en l'automatització de la resposta davant deteccions crítiques en comparació amb les ofertes de puntuació superior. L'oferta no entra en el detall dels mecanismes d'orquestració avançada (SOAR).

Es proposa assignar a l'oferta de l'empresa SOTHIS SERVICIOS TECNOLÓGICOS SLU 7 punts.

Grup C Compliment i Propostes Esquemàtiques(< 7 punts):

Aquest grup inclou les ofertes que, o bé presenten una arquitectura molt genèrica o poc detallada, o bé fallen a l'hora de concretar els mecanismes d'automatització i la integració operativa, limitant-se al compliment genèric del Plec.

Característiques destacades:

- Arquitectura Genèrica o Incompleta: La proposta és sovint molt esquemàtica. Molts licitadors no proporcionen la memòria descriptiva obligatòria completa (ubicació dels components, dimensionament, llicenciament per EPS/GB.
- Automatització Superficial: Esmenten l'ús de sistemes de correlació o eines SOAR, però de forma genèrica, sense entrar al detall de l'automatització.
- Manca de Formalitat en Registres: La majoria d'aquest grup no assumeix el compromís formal de lliurament trimestral de logs en format interoperable.
- Integració CCN Limitada: La proposta es limita a esmentar que s'adapten a les polítiques del CCN , o només esmenten les eines CCN sense concretar la integració.

Les empreses incloses en aquest grup són: VODAFONE ESPAÑA SAU, ITGLOBAL SL, CONNECTIS ICT SERVICES SAU, SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS (SERMICRO), ATECH ADVANCED SOLUTIONS S.A, CLARANET SAU, APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA i TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU.

- **VODAFONE ESPAÑA SAU**:

Arquitectura presentada està enfocada a l'automatització. El seu SIEM propi és una solució Cloud (Kubernetes) Elastic multitenant, que utilitza el motor d'Elastic com a element principal) i un XSOAR de Palo Alto Networks.
Per les automatitzacions el model de Vodafone és d'alta maduresa, amb la integració de fonts i casos d'ús al SIEM i *playbooks* als orquestradors que automatitzen la monitorització i les respostes.
No concreta pel que fa amb les integracions amb les eines de CCN.
En resum, Vodafone ofereix una visió tecnològica avançada i moderna amb un fort enfocament en l'automatització mitjançant XSOAR, però la seva puntuació queda limitada per deficiències en l'homologació de la plataforma en el context del sector públic i la manca de formalització en els requisits de documentació legal i tècnica detallada, no s'especifica el compromís formal de traçabilitat dels logs.

Es proposa assignar a l'oferta de l'empresa VODAFONE ESPAÑA SAU 6,5 punts.

- **ITGLOBAL SL**:

  A nivell d'arquitectura presenta una solució robusta, amb una clara adaptació al creixement de logs i integrable amb una amplia gama de fabricants, sense identificar el seu Soft de SIEM.
  No detalla la implementació de SOAR ni proporciona un catàleg de casos d'ús/correlacions avançades.
  La proposta no es compromet a lliurar els registres d'activitat complets en format interoperable almenys cada tres mesos.
  L'oferta no inclou cap menció específica als elements clau per a la integració amb l'ecosistema del Centre Criptològic Nacional (CCN), com ara l'automatització amb LUCIA, el desplegament de CARMEN o mecanismes per a l'enviament de trànsit de xarxa de manera selectiva.
  En resum, malgrat presentar una arquitectura robusta, la proposta d'ITGLOBAL es considera massa genèrica i no aporta el nivell de detall tècnic i els compromisos formals de traçabilitat d'altres ofertes.

  Es proposa assignar a l'oferta de l'empresa ITGLOBAL SA 6,5.

- **CONNECTIS ICT SERVICES SAU**:

  Presenten la plataforma de SIEM de Microsoft Sentinel amb MSSP, que es un servei al núvol multitenant. Per la correlació d'events utilitzen ML, aquesta automatització de playbooks són pròpies del SIEM proposat.
  Sobre el registre d'activitats mostra compliment de les fases de la gestió forense (recol·lecció, anàlisi, interpretació, informe). No hi ha compromís explícit de lliurament trimestral.
  Te un apartat propi de integració amb CCN, però no concreta quines eines.
  La solució de Connectis es veu, per tant, com a funcional i basada en una tecnologia de mercat líder, però li falta la profunditat tècnica operativa i la formalització administrativa necessàries per al context institucional i l'alta puntuació.

  Es proposa assignar a l'oferta de l'empresa CONNECTIS ICT SERVICES SAU 6,5 punts.

- **SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS (SERMICRO)**:

  La proposta de SERMICRO es basa en una arquitectura que combina el FORTISIEM per a la gestió de la informació de seguretat i la plataforma Wazuh per a la gestió de logs.
  Pel que fa a la integració amb l'ecosistema del CCN, la proposta esmenta la implantació del SIEM amb eines clau com LUCIA, SAT-INET, microCLAUDIA i APT.
  SERMICRO presenta una solució basada en tecnologies reconegudes, però manquen els detalls tècnics sobre el dimensionament i l'automatització. No s'aprofundeix en la plataforma SOAR, el catàleg de *playbooks* per a la resposta automatitzada o l'alineament amb el *framework* MITRE ATT&CK. Tampoc s'explicita el compromís formal de traçabilitat dels logs.

  Es proposa assignar a l'oferta de l'empresa SERMICRO 6 punts.

- **ATECH ADVANCED SOLUTIONS SA**:

  Utilitzen una plataforma de gestió d'esdeveniments i informació de seguretat (SIEM), sense especificar un fabricant concret. Sobre la integració amb eines del CCN, la proposta només fa referència al CCN en el context de compliment normatiu (ENS) i certificació.
  Tot i que s'esmenta l'ús de MITRE ATT&CK, la proposta pateix una absència de detall en SOAR/Playbooks detallats. Les descripcions sobre les contramesures i l'automatització es

consideren molt bàsiques i es queden en la descripció teòrica sense mostrar casos d'ús reals ni protocols específics.
En síntesi, la proposta d'ATECH es queda en el pla teòric de l'ús de tecnologies reconegudes, sense aportar valor diferencial ni l'evidència d'adaptació operativa. Tampoc s'explicita el compromís formal de traçabilitat dels logs.

Es proposa assignar a l'oferta de l'empresa ATECH ADVANCED SOLUTIONS SAL 6 punts.

- **CLARANET SAU**:

Treballen en dos fabricants de SIEM: Microsoft Sentinel i Fortisiem, que empren segons necessitats del client. Fa una definició molt reduïda sobre l'arquitectura i la recol·lecció de logs i correlació d'esdeveniments. La informació se centra en el procés d'anàlisi forense, no en les automatitzacions del SIEM/SOAR.
No parla del registre d'activitats, sinó es mena el procés de creació d'informes forenses, tampoc parla de la integració amb eines CCN, nomes mostra un compromís genèric.
En resum, CLARANET es limita a complir el Plec de Prescripcions Tècniques descrivint de manera molt bàsica i genèrica les capacitats dels seus SIEM, sense desenvolupar la concreció tècnica necessària ni formalitzar els compromisos de traçabilitat legal requerits per la licitació.

Es proposa assignar a l'oferta de l'empresa CLARANET SAU 6 punts.

- **APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA**:

La proposta es molt esquemàtica, no entra en gaire detall sobre la seva implantació. Queda pales que l'empresa té experiència en serveis SOC, però manca detall tècnic de la proposta.

Es proposa assignar a l'oferta de l'empresa APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA 4 punts.

- **TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU**:

La proposta no identifica el fabricant o model del SIEM, l'arquitectura, els elements de recol·lecció, ni es justifiquen les mètriques de dimensionament.
No es detalla l'ús de plataformes SOAR, catàlegs de casos d'ús, ni l'alineació amb marcs com MITRE ATT&CK. Es fa una referència genèrica als processos.
No hi ha informació disponible sobre la retenció de logs ni s'assumeix el compromís formal de lliurament trimestral de registres complets en format interoperable.
No es fa referència a la integració amb les eines de l'ecosistema CCN (CARMEN, LUCIA, etc.) ni a l'enviament selectiu de trànsit, un requisit clau per a la valoració.

Es proposa assignar a l'oferta de l'empresa TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU 4 punts.

"**3. <u>Implantació del SOC</u>, fins a un màxim de 5 punts:**

Es valorarà la millor idoneïtat per analitzar i adaptar-se a la infraestructura de l'entitat, mitjançant la concreció de la proposta de processos, procediments i estratègia d'implantació.

Les empreses presentaran una proposta de processos, procediments i estratègia d'implantacio."

<u>Grup A – Lideratge i màxima concreció metodològica (4,5 a 5)</u>:

Aquest grup inclou les ofertes que assoleixen les màximes puntuacions, destacant-se per la seva alta concreció, l'ús de marcs normatius avançats i la integració de processos de millora contínua des de la fase inicial d'implantació. Superen el mer compliment de l'estratègia amb documents de governança i gestió del canvi.

Característiques destacades:

- Concreció i Avaluació Contínua: Proposta molt desglossada i amb avaluació contínua per garantir el compliment dels objectius.
- Marcs Normatius Robuts: La metodologia d'implantació es basa i s'adapta en els principals estàndards i marcs normatius: ENS, NIST, NIS2, MITRE i SANS. I utilitzen marcs com ISO 270001 i ITIL basats en la millora contínua.
- Adaptació i Reducció de Bretxes: La implantació inclou una avaluació inicial que permet generar un pla director de seguretat vigent durant tot el contracte.
- Gestió del Coneixement: Quan es preveu diferents reunions per arribar a un consens en la configuració dels serveis i automatitzacions, i una fase de transició gestionada per personal amb certificacions ITIL.

Les empreses incloses en aquest grup són: SISTEMAS INFORMÁTICOS ABIERTOS SAU, EVOLUTIO CLOUD ENEBLER SAU, SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL, INETUM ESPAÑA SA i OMEGA PERIPHERALS SL.

- **SISTEMAS INFORMÁTICOS ABIERTOS SAU**:

  La proposta de SISTEMAS INFORMÁTICOS ABIERTOS SAU es distingeix per la seva aproximació exhaustiva, metodològica i formalitzada per garantir una transició fluida i la màxima qualitat en la posada en marxa del servei. Durant la implementació del SOC, l'empresa aborda l'adquisició i gestió del coneixement per part de l'ens adjudicatari del servei.
  La proposta de processos, procediments i estratègia d'implementació, presenta una proposta molt desglossada i amb avaluació continua, per garantir el compliment dels objectius.
  La proposta de SIA no només compleix amb la definició de processos, sinó que ofereix una estructura de desplegament per fases amb concreció i detall exhaustiu, amb lliurables intermedis i la previsió d'una fase de transició.

  Es proposa assignar a l'oferta de l'empresa SISTEMAS INFORMÁTICOS ABIERTOS SAU 5 punts.

- **EVOLUTIO CLOUD ENABLER SAU**:

  La proposta de l'empresa EVOLUTIO destaca per posar èmfasi en l'anàlisi preliminar i la gestió del canvi controlada, assegurant una adaptació òptima a la infraestructura de cada entitat. Disposa de 3 SOCS Madrid, Linares, Barcelona i Lisboa.
  Utilitzarà Handbooks inicials per descriure els protocols de comunicació, però seran modificats de manera reactiva i proactiva per utilitzar-los durant la vida del contracte. Inclou multitud de quadres de comandament per tal de poder veure en els informes mensuals el seguiment i control del servei.
  EVOLUTIO presenta una proposta de servei que és metodològicament robusta, exhaustiva i explícita formalitzant processos de consultoria *in situ*, de gestió del canvi i de governança (comitès).

  Es proposa assignar a l'oferta de l'empresa EVOLUTIO CLOUD ENABLER SA 5 punts.

- **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL**:

La proposta de SIRT se centra en la creació d'una Cybersecurity Office que integra funcions de SOC Operatiu, CSIRT, NOC i DevOps, amb un fort èmfasi en l'adaptabilitat i personalització a les necessitats, infraestructura i processos de cada entitat. Els processos, procediments i estratègia d'implantació del serveis de SOC Operatiu proposat, que es basen i adapten en els principals estàndards i marcs normatius (ENS, NIST, NIS2, MITRE i SANS) Dins la metodologia d'implantació inclou un pla d'acció per reduir les bretxes de seguretat detectades amb una classificació per riscos, per tal de tenir una gestió optimitzada dels riscos existents.
Si bé l'anàlisi inicial i la planificació basada en riscos són molt detallades, la fase de transició i l'encaix organitzatiu no estan tan formalitzats com l'anàlisi inicial. L'oferta no aporta massa detall dels lliurables de gestió del canvi i documentació de governança per a la fase de transició.

Es proposa assignar a l'oferta de l'empresa SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL 4,5 punts.

- **INETUM ESPAÑA SA**:

La proposta presenta una metodologia adaptada i altament formalitzada, essencial per complir amb els requeriments de concreció i idoneïtat on també s'inclou els KPI i mètriques per a l'avaluació d'objectius. El pla és detallat i inclou cronograma, assignació de recursos i estratègies de contingència per assegurar la bona execució de las fases de desplegament. Mostren un pla de implantació molt madur i concorde amb la normativa de ciberseguretat ITIL, però no inclou els perfils detallats dels recursos que gestionaran el SOC.

Es proposa assignar a l'oferta de l'empresa INETUM ESPAÑA SA 4,5 punts.

- **OMEGA PERIPHERALS SL**:

L'estratègia d'implantació (Modalitat BULHOST) de l'empresa OMEGA es considera estructurada, progressiva i altament enfocada a l'adaptació al compliment normatiu i a la infraestructura de l'entitat pública. El seu objectiu és assegurar una transició sense impacte. La descripció de les fases de setup inicial per adaptar el SOCaaS a l'entorn del client és genèrica, mancant el detall de l'inventariat i la recol·lecció d'evidències.

Es proposa assignar a l'oferta de l'empresa OMEGA PERIPHERAL SL 4,5.

<u>Grup B – Lideratge i màxima concreció metodològica (4 punts)</u>:

Aquestes ofertes presenten una estratègia d'implantació robusta i metodològicament sòlida. La puntuació és alta perquè defineixen rols, fites i utilitzen metodologies formals, tot i que reben penalitzacions menors per no concretar la relació amb el SOC Tàctic (ACC) o la manca de detalls en l'avaluació post-implementació.

Característiques destacades:

- Metodologia i Expertesa: Apliquen metodologies àgils per desgranar la implementació i detectar problemes ràpidament.
- Estructura de Projecte Clara: Mostren una estratègia d'implantació robusta, posant èmfasi en la involucració de l'entitat. Utilitzen Handbooks inicials per descriure protocols que seran modificats.
- Coneixement i Rols: Les ofertes descriuen clarament l'equip de treball, els rols i les fites.
- Alineació amb el SOC Tàctic (ACC): les empreses declaren incloure el SOC Tàctic de l'ACC.

Les empreses incloses en aquest grup són: EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL, SOTHIS SERVICIOS TECNOLÓGICOS SLU, CAPGEMINI ESPAÑA SL, SEIDOR SOLUTIONS SL, ORANGE ESPAGNE SAU, SUMINISTROS, IMPORTACIONES Y

MANTENIMIENTOS DELECTRÓNICOS, S2 GRUPO SOLUCIONES DE SEGURIDAD SLU i A2SECURE TECNOLOGÍAS INFORMÁTICA SL.

- **EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL**:

  La proposta de l'empresa EY TRANSFORMA SERVICIOS DE CONSUTORÍA SL destaca per la seva metodologia àgil, la governança estructurada i l'èmfasi en l'adaptació constant i la millora contínua, així com per l'aplicació de metodologies àgils per a la implementació del SOC amb diferents fases clarament orientades a detectar qualsevol problema ràpidament. Pel que fa a l'adaptació del SOC a l'entitat disposa de una fase de personalització del SIEM on es preveu una implementació de playbooks referents a las amenaces possibles detectades en la fase d'implementació.
  La seva proposta per d'implantació del SOC és molt extensa i mostra una expertesa clara en la metodologia i autoavaluació constant del SOC per la seva millora i adaptació a l'entitat. El punt més feble de la proposta és que no formalitza o detalla l'avaluació post-implementació ni tampoc concreta l'operativa de la integració institucional de les eines del CCN (LUCIA/CARMEN)

  Es proposa assignar a l'oferta de l'empresa EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL 4 punts.

- **A2SECURE TECNOLOGÍAS INFORMÁTICA SL**:

  Mostra un gran nivell d'adaptació a l'entitat en la implementació del SOC, inclou tot el necessari per a la seva implementació (hardware i software).
  La fase embrionària del projecte d'implantació del SOC inclou la realització d'un estudi preliminar per part d'un tècnic propi *in situ* per conèixer la infraestructura tecnològica i la identificació dels processos, procediments i les polítiques d'operació per a una correcta adequació del SOC a l'entitat pública.
  La proposta, tot i ser sòlida en l'anàlisi, manca de la presentació d'una estructura de desplegament per fases (cronograma, fites i tasques) amb concreció i detall.

  Es proposa assignar a l'oferta de l'empresa A2SECURE TECNOLOGÍAS INFORMÁTICA SL 4 punts.

- **SOTHIS SERVICIOS TECNOLÓGICOS SLU**:

  La proposta es caracteritza per una implementació que posa èmfasi en la gestió del projecte mitjançant marcs reconeguts i la millora contínua. Utilitza metodologies àgils per a la implantació del projecte, la proposta inclou adaptació de l'entitat amb feedback del disseny del projecte abans de la implantació amb el client amb la memòria tècnica d'implantació i el catàleg de regles de correlació.
  Tot i que la proposta de SOTHIS és forta en els aspectes tècnics (com el dimensionament), manca el detall dels procediments organitzatius i de transició no tècnica.

  Es proposa assignar a l'oferta de l'empresa SOTHIS SERVICIOS TECNOLÓGICOS SLU 4 punts.

- **SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS (SERMICRO)**:

  La proposta destaca per la seva èmfasi en la gestió del projecte i la formalització documental per al seguiment.
  Presenten una proposta d'implantació amb una gestió documental robusta (GANTT, SOW) i un lideratge experimentat, que garanteix la traçabilitat durant el desplegament. No obstant això, la proposta no detalla els mecanismes per a l'avaluació del servei un cop el SOC es

troba en operació per tal de verificar el bon funcionament de la plataforma i les directrius implementades.

Es proposa assignar a l'oferta de l'empresa SERMICRO 4 punts.

- **CAPGEMINI ESPAÑA SL**:

La proposta d'implementació del SOC de CAPGEMINI es considera robusta i metodològica, amb un fort èmfasi en l'ús de plataformes tecnològiques homologades i una metodologia pròpia per a la transició.
Es fa un inventariat d'actius al principi del projecte per detectar possibles vulnerabilitats, que es complementa amb un servei continu de gestió d'aquestes vulnerabilitats.
Pel que fa als processos, procediments i estratègia d' implantació, destaca gràcies a la seva Use Case Factory (UCF), que permet una ràpida posada en marxa i optimització d'alertes. L'estratègia d'implantació segueix la seva GTM amb l'objectiu principal de capturar el coneixement de l'estructura i processos del client.
No obstant això, la descripció del procés d'adaptació és poc granular, amb manca de concreció en la planificació per fases (cronograma, fites i tasques).

Es proposa assignar a l'oferta de l'empresa CAPGEMINI ESPAÑA SL 4 punts.

- **SEIDOR SOLUTIONS SL**:

La proposta de SEIDOR es fonamenta en una estratègia d'implementació modular, adaptable i rigorosa, amb l'objectiu d'aconseguir la màxima qualitat en la posada en marxa del SOC. La fase d'activació inclou un qüestionari tècnic, entrevistes i sessions de treball amb els responsables TIC. El seu procés d'inventari és continu (fase inicial de descoberta i fase de manteniment) i classifica els actius TIC tenint en compte les particularitats de cada organització. L'estratègia d'implantació es basa en 4 grans fases (Activació i Disseny Compartit, Desplegament Tècnic, Posada en Marxa/Go Live, i Revisió Post-Implantació i Millora Contínua). El procés inclou l'harmonització de formats i la normalització d'esdeveniments.
La penalització menor es deu a la manca de documents de governança (RACI/GANTT) explícits. Aquesta omissió implica que, tot i que les fases són clares, no es detalla la gestió del projecte i la transició no tècnica.

Es proposa assignar a l'oferta de l'empresa SEIDOR SOLUTIONS SL 4 punts.

- **ORANGE ESPAGNE SAU**:

La proposta destaca per la seva àmplia adaptació metodològica i el seu enfocament en l'avaluació contínua del servei**.**
L'oferta d'Orange presenta una estratègia d'implantació metodològicament robusta i madura (basada en ITIL, NIST, i SOC-CMM, amb focus en la millora contínua). No obstant això, manca claredat en l'encaix institucional del SOC Tàctic (ACC) dins del seu model de govern.

Es proposa assignar a l'oferta de l'empresa ORANGE ESPAGNE SAU 4 punts.

- **S2 GRUPO SOLUCIONES DE SEGURIDAD SLU**:

L'oferta es fonamenta en la plataforma GLORIA, que opera com a SIEM, i es distingeix per un sòlid enfocament en la prevenció i una estreta coordinació amb el SOC Tàctic. El servei final s'adapta a l'entorn del sector públic local. L'arquitectura és flexible, ja que el SIEM final pot ser qualsevol eina del mercat. El disseny de la plataforma final s'ha de "determinar en cada cas per a cada entitat contractant". Manca la detallada estructura per fases

(Assessment, Desplegament Tècnic, Transició, Devolució) amb els passos i lliurables intermedis explícitament definits.

Es proposa assignar a l'oferta de l'empresa S2 GRUPO SOLUCIONES DE SEGURIDAD SLU 4 punts.

GRUP C – Concreció mínima i compliment esquemàtic (< de 4 punts):

Aquest grup aplega les ofertes que es limiten a complir l'índex del Plec, descrivint les fases de manera molt genèrica sense aportar la concreció necessària per a la seva avaluació qualitativa (processos, adaptació, gestió del projecte)

Característiques detallades:

- Falta de Detall en Adaptació: Les propostes són genèriques i no fan referència a l'adaptació a l'entitat en cap dels apartats.
- Manca de Metodologia i Avaluació: L'estratègia d'implantació és molt esquemàtica i no s'explica amb profunditat

Les empreses incloses en aquest grup són: ATECH ADVANCED SOLUTIONS S.A, VODAFONE ESPAÑA SAU, GMV SOLUCIONES GLOBALES INTERNET SAU, ITGLOBAL SL, CLARANET SAU, CONNECTIS ICT SERVICES SAU, APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA, SISTEMAS AVANZADOS DE TECNOLOGÍA SA i TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU.

- **ATECH ADVANCED SOLUTIONS S.A**:

  La proposta és massa genèrica en l'estratègia d'implantació, limitant-se a enumerar tasques d'oficina tècnica i de govern sense proporcionar la visió metodològica. ATECH segueix el marc NIST, DFIR, i ISO, però es queda en la descripció teòrica de les fases i no aporta protocols específics, exemples pràctics ni detalls. A més, no detalla els mecanismes de millora contínua o d'avaluació post-implantació, elements clau d'aquest criteri.

  Es proposa assignar a l'oferta de l'empresa ATECH ADVANCED SOLUTIONS SA 3,5 punts.

- **VODAFONE ESPAÑA SAU**:

  La proposta de VODAFONE es basa en una arquitectura altament automatitzada i moderna (Elàstic SIEM + XSOAR), i demostra maduresa en la gestió operativa amb marcs com ITIL i SOC-CMM. Vodafone es basa en el marc de referència SOC-CMM (Security Operations Center - Capability Maturity Model) per avaluar i millorar contínuament el seu nivell de maduresa en el servei. L'oferta de Vodafone es caracteritza per una arquitectura moderna i altament automatitzada, però manca el detall sobre la integració amb l'ecosistema públic (CCN/CPSTIC) i la formalització de processos i procediments de l'anàlisi inicial de la infraestructura del client que són clau en les etapes inicials i de prevenció.

  Es proposa assignar a l'oferta de l'empresa VODAFONE ESPAÑA SAU 3,5 punts.

- **GMV SOLUCIONES GLOBALES INTERNET SAU**:

  La proposta de GMV és tècnicament molt sòlida en gairebé tots els àmbits, destacant especialment en l'ús d'automatització avançada (SOAR) i l'experiència forense. La seva principal deficiència rau en la manca de detall procedimental i la formalització exhaustiva requerida per als processos inicials d'adaptació. La descripció de la metodologia d'implantació (procés i fases) és més conceptual que procedimental.

Es proposa assignar a l'oferta de l'empresa GMV SOLUCIONES GLOBALES INTERNET SAU 3 punts.

- **ITGLOBAL SL**:

  La proposta parla sobre las diferents fases d'implantació de manera genèrica, no fa referencia a la adaptació a l'entitat en cap dels apartats. El mateix passa amb els procediments d'implantació, parla de manera genèrica. Tampoc no concreta ni demostra la integració operativa necessària amb el SOC Tàctic en la seva proposta d'implantació.

  Es proposa assignar a l'oferta de l'empresa ITGLOBAL SL 3 punts.

- **CLARANET SAU**:

  Mostren una proposta molt bàsica i Standard sobre la implantació del SOC a l'entitat. Tot i estar estructurada en diferents fases, no inclou metodologies d'avaluació del servei per a la millora continua.

  Es proposa assignar a l'oferta de l'empresa CLARANET SAU 3 punts.

- **CONNECTIS ICT SERVICES SAU**:

  És una proposta genèrica d'implantació del SOC, on explica que hi haurà adaptació però no acaba de concretar. L'estratègia d'implantació és molt esquemàtica, no s'explica amb profunditat.
  No parla de coordinació amb el SOC Tàctic.

  Es proposa assignar a l'oferta de l'empresa CONNECTIS ICT SERVICES SAU 3 punts.

- **APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA**:

  Sobre la implantació del SOC, parla de manera genèrica: no es detallen els procediments.

  Es proposa assignar a l'oferta de l'empresa APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA 2 punts.

- **SISTEMAS AVANZADOS DE TECNOLOGÍA SA**:

  La proposta d'implantació no parla de metodologies d'implantació ni de millora continua. No te en compte l'adaptació a l'entitat. Parla de manera genèrica sobre què implantaran, però no de com es farà.

  Es proposa assignar a l'oferta de l'empresa SISTEMAS AVANDADOS DE TECNOLOGÍA 2 punts.

- **TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU**:

  La seva proposta, amb l'evidència disponible, és massa genèrica en l'estratègia d'implantació del SOC, limitant-se a enumerar tasques d'oficina tècnica i de govern sense proporcionar la visió metodològica. Tampoc es detallen els mecanismes de millora contínua o d'avaluació post-implantació.

  Es proposa assignar a l'oferta de l'empresa TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU 2 punts.

4 Valoració final dels criteris la quantificació dels quals depèn d'un judici de valor

A continuació es presenta una taula resum de les puntuacions obtingudes per les empreses licitadores dels criteris d'adjudicació la quantificació dels quals depèn d'un judici de valor:

	1				2	3	Total
	1.1	1.2	1.3	1.4			
SISTEMAS INFORMÁTICOS ABIERTOS SAU	10,00	10,00	5,00	5,00	10,00	5,00	45,00
EY TRANSFORMA SERVICIOS DE CONSULTORÍA SL	10,00	10,00	5,00	5,00	9,00	4,00	43,00
EVOLUTIO CLOUD ENABLER SAU	10,00	10,00	4,50	5,00	8,50	5,00	43,00
SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES SL	9,00	9,00	5,00	5,00	9,00	4,50	41,50
A2SECURE TECNOLOGÍAS INFORMÁTICA SL	9,00	9,00	3,00	4,50	10,00	4,00	39,50
S2 GRUPO SOLUCIONES DE SEGURIDAD SLU	9,00	9,00	4,50	4,00	9,00	4,00	39,50
INETUM ESPAÑA SA	8,50	8,00	4,50	4,00	8,00	4,50	37,50
CAPGEMINI ESPAÑA SL	7,50	8,00	4,00	4,50	8,50	4,00	36,50
SEIDOR SOLUTIONS SL	9,00	7,00	4,00	4,00	8,00	4,00	36,00
GMV SOLUCIONES GLOBALES INTERNET SAU	8,00	6,50	4,50	4,00	9,50	3,00	35,50
ORANGE ESPAGNE SAU	7,00	8,00	4,50	4,00	7,50	4,00	35,00
SISTEMAS AVANZADOS DE TECNOLOGÍA SA	8,00	8,00	4,00	4,00	8,00	2,00	34,00
OMEGA PERIPHERALS SL	7,00	5,00	4,50	4,00	8,00	4,50	33,00
SOTHIS SERVICIOS TECNOLÓGICOS SLU	8,00	7,00	2,50	4,50	7,00	4,00	33,00
ITGLOBAL SL	6,00	8,00	4,00	4,00	6,50	3,00	31,50
VODAFONE ESPAÑA SAU	3,00	9,00	2,00	4,50	6,50	3,50	28,50
CONNECTIS ICT SERVICES SAU	5,50	6,00	2,00	2,00	6,50	3,00	25,00
CLARANET SAU	3,00	3,00	2,00	2,00	6,50	3,00	19,50
SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS SAU	1,00	3,00	2,00	2,00	6,00	4,00	18,00
ATECH ADVANCED SOLUTIONS SA	1,00	3,00	2,00	2,00	6,00	3,50	17,50
TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA SAU	3,00	3,00	2,00	1,00	4,00	2,00	15,00
APLICACIONES Y TRATAMIENTOS DE SISTEMAS SA	3,00	3,00	2,00	1,00	4,00	2,00	15,00

Eva Guijarro
Cap de l'Àrea de Transformació Digital i Tecnologies