Plec de requisits tècnics que regulen la prestació de serveis de ciberseguretat i protecció de dades per a les entitats que integren el grup de compra.

Barcelona, a la data de la signatures

Validat per,	Aprovat per,

Sumari

1. Context del sistema dinàmic d'adquisició de programari i serveis associats

1.1. Objecte de la licitació

L'objecte d'aquesta licitació és l'acreditació de proveïdors de serveis de ciberseguretat i protecció de dades per part del Consorci de Serveis Universitaris de Catalunya (en endavant CSUC) i de les entitats participants i la posterior contractació d'aquests serveis.

1.2. Abast i estructura en categories de l'SDA

La present licitació estableix el procediment de contractació de serveis de ciberseguretat i protecció de dades a partir de l'acreditació de proveïdors mitjançant un sistema dinàmic d'adquisició (d'ara endavant SDA) per a la posterior tramitació dels corresponents contractes específics.

Queden exclosos d'aquest SDA tots els serveis de ciberseguretat i protecció de dades que ja formin part d'un altre contracte vigent per les entitats que hi participen.

La licitació s'estructura en 2 categories:

- **Categoria 1**: Serveis professionals de ciberseguretat. Fan referència a la prestació de serveis en l'àmbit de la ciberseguretat TIC de les organitzacions.

- **Categoria 2:** Serveis professionals de protecció de dades. Fan referència a la prestació de serveis en l'àmbit de la protecció de dades de les organitzacions.

Els licitadors hauran de ser proveïdors de serveis de ciberseguretat i protecció de dades amb solvència econòmica i tècnica en les categories on es vulguin acreditar.

1.3. Informe de seguiment de l'SDA

Els adjudicataris hauran de facilitar semestralment al CSUC la informació detallada dels contractes específics que s'hagin realitzat en base a aquest SDA per part de les Entitats adherides. Aquesta informació serà facilitada al CSUC entre l'1 i 15 de juliol i l'1 i 15 de gener de cada any.

2. Descripció de les Categories de l'SDA

Categoria 1. Serveis professionals de ciberseguretat.

Aquesta categoria agrupa els serveis especialitzats orientats a protegir, avaluar i millorar la postura de seguretat de les organitzacions. Inclou activitats d'auditoria i compliment normatiu, gestió de riscos i vulnerabilitats, detecció i resposta davant ciberamenaces, consultoria estratègica, operació de plataformes de seguretat i formació en enginyeria social. L'objectiu és oferir solucions integrals i adaptades que garanteixin la confidencialitat, integritat i disponibilitat dels sistemes i dades, assegurant el compliment dels marcs normatius i la resiliència davant incidents.

A continuació es detallen les subcategories d'aquesta categoria:

Subcategoria	Servei	Descripció
Auditories i Avaluacions de Compliment	Auditories internes ENS, NIS2, ISO 27001, ISO 27002, ISO 27031, ISO/IEC 27017	Servei orientat a realitzar auditories formals i tècniques per verificar el grau de conformitat de l'organització amb marcs normatius i estàndards de ciberseguretat com l'Esquema Nacional de Seguretat (ENS), la Directiva NIS2 i les normes de la família ISO/IEC 27000, incloent-hi ISO 27001 (sistema de gestió), ISO 27002 (controls), ISO 27031 (continuïtat de les TI) i ISO/IEC 27017 (seguretat al núvol). Aquest servei pot incloure l'anàlisi documental i evidencial, la verificació de controls tècnics i organitzatius, entrevistes amb equips clau, proves de compliment, identificació de no conformitats i l'elaboració d'informes d'auditoria amb recomanacions accionables. L'objectiu és garantir una avaluació precisa i independent que permeti a l'organització complir requisits normatius, preparar-se per certificacions i millorar contínuament la seva postura de seguretat.
Auditories i Avaluacions de Compliment	Auditoria IoT i OT	Servei orientat a avaluar la seguretat d'entorns de tecnologia operativa (OT) i dispositius d'Internet de les Coses (IoT), identificant vulnerabilitats, configuracions inadequades i riscos que puguin afectar la continuïtat operativa, la integritat dels sistemes industrials o la protecció de dispositius connectats. Aquest servei pot incloure l'anàlisi de xarxes industrials, protocols específics (com Modbus, OPC-UA o DNP3), revisió de firmware i configuracions, proves d'intrusió adaptades a entorns crítics,

		així com la verificació de mesures de segmentació, monitoratge i control. L'objectiu és garantir que els ecosistemes IoT i OT disposin de proteccions adequades, tant des del punt de vista tecnològic com operatiu, minimitzant l'exposició a amenaces i preservant la continuïtat del servei.
Auditories i Avaluacions de Compliment	Auditoria de software (codi + aplicació)	Servei orientat a analitzar el codi font d'aplicacions i components desenvolupats internament o per tercers, amb l'objectiu d'identificar vulnerabilitats, males pràctiques de programació i riscos de seguretat que puguin comprometre la integritat, disponibilitat o confidencialitat del sistema. Aquest servei pot incloure revisions manuals i assistides per eines SAST, l'avaluació de dependències i biblioteques externes, la detecció de patrons d'explotació habituals, així com la verificació del compliment de guies de codificació segura. L'objectiu és garantir que el software sigui robust, resilient i alineat amb els estàndards de seguretat, facilitant la correcció d'errors i reduint el risc d'incidents futurs.
Auditories i Avaluacions de Compliment	Auditoria de TI i de processos (IT Governance & Process Audit)	Servei orientat a analitzar i avaluar la maduresa, eficàcia i adequació dels processos i la governança de les TIC dins de l'organització, garantint que les pràctiques de gestió, control i suport tecnològic s'alineen amb els objectius estratègics i els marcs de referència internacionals. Aquest servei pot incloure la revisió de processos basats en bones pràctiques com COBIT, ITIL o ISO 20000, l'avaluació del model de governança, la gestió del canvi, la gestió d'incidents i problemes, la planificació i control de serveis, així com la identificació de bretxes operatives o de compliment. L'objectiu és proporcionar una visió independent i estructurada del funcionament dels processos TIC, facilitant la millora contínua, la presa de decisions i la consolidació d'un model de governança eficient i robust.

Auditories i Avaluacions de Compliment	Auditoria de continuïtat i resiliència (BCP/DRP)	Servei orientat a avaluar el grau de preparació de l'organització per mantenir o restablir els seus serveis essencials davant interrupcions, incidents greus o situacions de crisi, mitjançant la revisió del Pla de Continuïtat de Negoci (BCP) i del Pla de Recuperació davant Desastres (DRP). Aquest servei pot incloure l'anàlisi de riscos operatius, la validació de l'estructura i contingut dels plans, l'avaluació de l'eficàcia dels procediments de recuperació, la revisió dels requisits de RTO/RPO, la verificació de dependències tecnològiques i organitzatives, així com la valoració de proves de continuïtat realitzades. L'objectiu és garantir que els plans siguin viables, actuals i operatius, i que l'organització disposi d'un nivell adequat de resiliència per minimitzar l'impacte d'interrupcions i assegurar la continuïtat dels serveis crítics.
Auditories i Avaluacions de Compliment	Auditoria de seguretat física relacionada amb TI	Servei orientat a avaluar les mesures de seguretat física que protegeixen les infraestructures TIC de l'organització, garantint que els espais, equips i recursos crítics disposen de controls adequats per prevenir accessos no autoritzats, manipulacions o interrupcions del servei. Aquest servei pot incloure la revisió de l'accés físic a CPDs, sales tècniques i punts d'interconnexió, l'avaluació de sistemes de control d'accés, vigilància i detecció, la inspecció de proteccions ambientals (climatització, incendis, electricitat), així com la verificació de protocols d'entrada, visites i gestió de personal extern. L'objectiu és identificar riscos físics que puguin comprometre la seguretat funcional dels sistemes TIC i proposar millores que reforcin la resiliència global de l'entorn.
Auditories i Avaluacions de Compliment	Identificar i avaluar riscos potencials (Pentesting / Risk Assessment) - Avaluació i mitigació de riscos	Servei orientat a identificar vulnerabilitats, exposicions i riscos potencials en els sistemes i serveis TIC de l'organització mitjançant activitats d'auditoria tècnica i anàlisi estructurada del risc. Aquest servei pot incloure la realització de proves d'intrusió (pentesting) internes o externes, l'avaluació de configuracions i superfícies d'atac, l'anàlisi de vulnerabilitats, així com l'aplicació de metodologies formals de Risk Assessment per valorar l'impacte i la probabilitat de

		materialització de cada risc. L'objectiu és obtenir una visió clara i prioritzada de les debilitats existents, facilitant la presa de decisions i la definició de mesures de mitigació per reforçar la seguretat global de l'organització.
Adequació, Consultoria i Compliment Normatiu	Adequació ENS (AR ENS)	Servei orientat a donar suport a l'organització en el procés d'adequació a l'Esquema Nacional de Seguretat (ENS), incloent-hi la realització de l'Anàlisi de Riscos (AR ENS) segons els requisits i metodologies definides pel marc normatiu. Aquest servei pot abastar la identificació d'actius, l'avaluació d'amenaces i vulnerabilitats, la determinació del nivell de seguretat requerit, la valoració de l'impacte potencial i la definició de mesures de seguretat alineades amb el Catàleg de mesures de l'ENS. L'objectiu és garantir una adequació sòlida, coherent i documentada que permeti complir amb les obligacions del sector públic i establir una base robusta per a la gestió del risc i la certificació futura.
Adequació, Consultoria i Compliment Normatiu	Confecció inventari d'actius	Servei orientat a identificar, catalogar i mantenir actualitzat l'inventari complet dels actius TIC de l'organització, incloent equips, sistemes, aplicacions, serveis, dades, comptes i dependències associades. El servei pot abastar la recopilació d'informació tècnica, la classificació d'actius segons la seva criticitat i sensibilitat, la detecció de bretxes o elements no controlats, així como l'establiment de mecanismes de governança per garantir la seva actualització contínua. L'objectiu és disposar d'una visió precisa i estructurada dels actius, essencial per a la gestió del risc, el compliment normatiu i la correcta planificació de mesures de seguretat.
Adequació, Consultoria i Compliment Normatiu	Suport en processos de certificació	Servei orientat a acompanyar l'organització en totes les fases necessàries per obtenir, renovar o mantenir certificacions en l'àmbit de la seguretat de la informació, la protecció de dades o la gestió de serveis TIC. Aquest servei pot incloure l'anàlisi de requisits de certificació (com ISO 27001, ENS, ISO 20000, ISO 22301 o altres estàndards aplicables), la preparació de documentació, l'assessorament en la implantació de controls i bones pràctiques, la realització de preauditories i la coordinació amb entitats certificadores.

		L'objectiu és garantir que l'organització arribi al procés formal de certificació amb garanties, reduint riscos de no conformitats i facilitant un procés d'auditoria eficient i exitós.
Adequació, Consultoria i Compliment Normatiu	Compliment normatiu (ENS, NIS2, ISO, RGPD…)	Servei orientat a donar suport a l'organització en l'adopció, implantació i manteniment dels requisits normatius i estàndards de seguretat aplicables, com l'Esquema Nacional de Seguretat (ENS), la Directiva NIS2, les normes ISO de la sèrie 27000, el Reglament General de Protecció de Dades (RGPD) i altres marcs reguladors sectorials. Aquest servei pot incloure l'anàlisi de bretxes de compliment, la definició i supervisió de plans d'adequació, la preparació de documentació formal, l'assessorament en controls tècnics i organitzatius, així com el suport en auditories internes o externes. L'objectiu és assegurar que l'organització compleixi els requeriments legals i normatius, reforçant la seva postura de seguretat i reduint riscos derivats d'incompliments.
Adequació, Consultoria i Compliment Normatiu	Determinació de polítiques, normes i procediments de seguretat	Servei orientat a definir, revisar i actualitzar el conjunt de polítiques de seguretat de la informació que han de guiar la gestió, protecció i ús dels sistemes i dades de l'organització. Aquest servei pot incloure l'anàlisi del marc normatiu aplicable (com ENS, ISO 27001 o RGPD), la identificació de necessitats específiques del context operatiu, la redacció i estructuració de polítiques, normes i procediments interns, i la definició de plans de resiliència i continuïtat així com l'alineament amb les bones pràctiques de governança en ciberseguretat. L'objectiu és establir un marc normatiu clar, coherent i aplicable que faciliti el compliment, millori la maduresa de seguretat i proporcioni una base sòlida per a la presa de decisions i la gestió dels riscos.
Adequació, Consultoria i Compliment Normatiu	Determinació d'estratègies de resposta	Servei orientat a definir les estratègies i línies d'actuació que l'organització ha d'adoptar davant incidents o amenaces de ciberseguretat, assegurant una resposta coherent, eficient i alineada amb el risc. Aquest servei pot incloure l'anàlisi de vectors d'atac potencials, la identificació de capacitats

		defensives disponibles, l'establiment de criteris de priorització, la definició de mecanismes de contenció i mitigació, així com la proposta de seqüències d'actuació adaptades a diferents escenaris. L'objectiu és dotar l'organització d'un marc de resposta clar i operatiu que faciliti la presa de decisions en situacions crítiques i minimitzi l'impacte dels incidents.
Adequació, Consultoria i Compliment Normatiu	Desenvolupament de plans de resposta i resiliència	Servei orientat a definir i implementar plans efectius de resposta a incidents i de resiliència operativa, establint rols, procediments, capacitats de detecció, contenció i recuperació, així com mesures de continuïtat que permetin mantenir o restablir els serveis essencials amb el mínim impacte. Inclou l'alineament amb estàndards de ciberseguretat i la realització d'exercicis per validar i millorar la capacitat de resposta.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	SOC (ACC, SOCaaS o SOC consorciat)	Servei orientat a la vigilància, detecció i resposta davant amenaces mitjançant un Centre d'Operacions de Ciberseguretat, ja sigui propi, externalitzat o compartit. Inclou la monitorització contínua d'esdeveniments i vulnerabilitats, l'anàlisi i correlació d'alertes, la gestió d'incidents i la generació d'informes operatius, garantint una protecció proactiva i adaptada a les necessitats de l'organització.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Detecció d'activitat de ciberamenaces	Servei orientat a identificar de manera proactiva activitats malicioses o indicadors de compromís mitjançant l'anàlisi contínua de fonts internes i externes, intel·ligència de ciberamenaces i tècniques de correlació avançada. Permet detectar comportaments anòmals, campanyes actives i vectors d'atac emergents per reforçar la resposta preventiva i reduir el risc d'incidents.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Gestió de regles de detecció (creació, ajust, validació contínua)	Servei orientat al disseny, desenvolupament i desplegament de regles de detecció en plataformes SIEM, EDR, NDR o solucions equivalents, amb l'objectiu d'identificar activitats anòmales, TTPs d'amenaces i indicadors de compromís rellevants. Inclou l'ajust fi, validació i revisió contínua de les regles per millorar-ne la precisió, reduir falsos positius i garantir una detecció alineada amb els riscos i l'entorn tecnològic de l'organització.

Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Anàlisi i gestió prioritzada d'alertes	Servei enfocat a revisar, classificar i prioritzar les alertes generades per les plataformes de seguretat, aplicant criteris de criticitat, context operatiu i risc real per l'organització. Inclou l'anàlisi tècnica inicial, la identificació de falsos positius, l'enriquiment amb intel·ligència d'amenaces i l'escalat eficient cap als equips corresponents, assegurant una resposta més ràpida i centrada en les alertes amb major impacte potencial.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Operació d'eines de ciberseguretat	Servei orientat a la gestió quotidiana, manteniment i optimització de les plataformes i solucions de ciberseguretat de l'organització (com SIEM, EDR, NDR, firewalls, WAF, PAM, entre d'altres). Inclou el seguiment del seu funcionament, l'aplicació de millores de configuració, l'actualització de signatures i polítiques, la resolució d'incidències operatives i la verificació contínua que les eines proporcionen una protecció eficaç i alineada amb els requisits de seguretat i compliment normatiu.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Recomanació de polítiques sobre eines	Servei orientat a definir i proposar polítiques d'ús, configuració i governança per a les diferents eines de ciberseguretat de l'organització, assegurant-ne una aplicació coherent, segura i alineada amb els requisits normatius i operatius. Inclou l'anàlisi de l'estat actual, la identificació de millores i la formulació de directrius que permetin optimitzar-ne l'eficàcia i reduir riscos derivats d'un ús inadequat o inconsistent.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Bloqueig d'indicadors de compromís	Servei destinat a aplicar, mantenir i actualitzar mecanismes de bloqueig automàtic o manual davant indicadors de compromís (IOCs) com adreces IP, dominis, URL o hashes maliciosos. Inclou la integració d'aquests IOCs en les diferents eines de seguretat (firewalls, proxies, EDR, NDR, etc.), així com la verificació del seu funcionament i la revisió periòdica per garantir una protecció eficaç i evitar bloquejos indeguts que afectin l'operativa.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Automatització de primera resposta	Servei dirigit a dissenyar i implementar fluxos automatitzats que executin accions immediates davant alertes o incidents de seguretat, com ara l'aïllament d'equips, la revocació de credencials, l'aplicació de bloquejos o la recopilació inicial d'evidències. L'objectiu és reduir el temps de resposta,

		minimitzar l'impacte de l'amenaça i descarregar tasques repetitives dels equips operatius, assegurant alhora coherència i traçabilitat en totes les accions automatitzades.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Elaboració de mètriques d'activitat gestionada	Servei orientat a definir, calcular i mantenir un conjunt de mètriques que reflecteixin el rendiment, l'eficàcia i la qualitat dels serveis de ciberseguretat gestionats. Inclou la identificació d'indicadors clau (KPIs i KRIs), la generació periòdica d'informes i quadres de comandament, i l'anàlisi de tendències per facilitar la presa de decisions i la millora contínua de les operacions de seguretat.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Execució d'escanejos de vulnerabilitats	Servei orientat a realitzar anàlisis periòdiques de vulnerabilitats sobre sistemes, xarxes i aplicacions mitjançant eines especialitzades, amb l'objectiu d'identificar debilitats de seguretat explotables. Inclou la planificació i execució dels escanejos, la validació dels resultats, la classificació segons criticitat i la generació d'informes que permetin prioritzar accions de mitigació i reforçar la postura de seguretat de l'organització.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Gestió del cicle de vida de vulnerabilitats	Servei orientat a administrar de manera contínua i estructurada totes les fases del tractament de vulnerabilitats, des de la seva detecció fins al tancament final. Inclou l'anàlisi i validació de resultats, la priorització segons risc, la coordinació amb els equips tècnics per a la seva correcció, el seguiment del progrés i la verificació posterior de la mitigació, assegurant una reducció efectiva de l'exposició i una millora sostinguda de la seguretat.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Serveis de vigilància (dark web, credencials, domini…)	Servei dedicat a monitoritzar de manera contínua espais externs com la dark web, fòrums clandestins, repositoris de filtracions i fonts obertes per detectar possibles exposicions de credencials, dades corporatives o activitats relacionades amb el domini de l'organització. Inclou l'alerta proactiva davant qualsevol indici de compromís, l'anàlisi de la informació trobada i recomanacions immediates per reduir l'impacte i reforçar la seguretat.

Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Proporcionar indicadors d'intel·ligència operativa	Servei orientat a subministrar indicadors accionables de ciberamenaces —com IOCs, comportaments, TTPs i signatures emergents— obtinguts a partir de fonts d'intel·ligència fiables. Inclou l'anàlisi i contextualització d'aquests indicadors perquè puguin ser incorporats ràpidament a les eines de detecció i protecció, reforçant la capacitat de resposta i la vigilància proactiva de l'organització.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Proporcionar contramesures davant amenaces	Servei orientat a oferir recomanacions i mesures específiques per mitigar o neutralitzar amenaces identificades, basant-se en l'anàlisi de TTPs, indicadors de compromís i intel·ligència operativa disponible. Inclou la definició d'accions tècniques i operatives — com ajustos de configuració, bloquejos, reforç de controls, actualitzacions o canvis de política— que permetin reduir el risc de manera ràpida i efectiva, millorant la protecció global de l'organització.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Determinació de grau d'exposició d'amenaça	Servei orientat a avaluar fins a quin punt l'organització està exposada a una amenaça concreta, analitzant la seva presència en l'entorn, els vectors potencials d'explotació i la rellevància segons els actius, tecnologies i configuracions existents. Inclou la correlació amb vulnerabilitats, dependències i intel·ligència d'amenaces per determinar el risc real i facilitar la priorització d'accions de mitigació.
Serveis Gestionats de Ciberseguretat (SOC / SOCaaS)	Elaboració de pronòstics d'amenaça	Servei orientat a anticipar l'evolució de ciberamenaces mitjançant l'anàlisi de tendències, patrons d'activitat maliciosa i intel·ligència prospectiva. Inclou la identificació de possibles vectors d'atac futurs, l'avaluació de la seva probabilitat i impacte, i la generació d'informes que permetin preparar mesures preventives i reforçar la postura de seguretat de manera proactiva.
Resposta a Incidents i Gestió de Crisi	Investigació d'incidents	Servei orientat a analitzar en profunditat incidents de seguretat per identificar-ne l'origen, l'abast, el vector d'entrada i les accions realitzades per l'atacant. Inclou la recopilació i preservació d'evidències, l'anàlisi de logs i sistemes afectats, la reconstrucció cronològica dels fets i l'elaboració d'informes tècnics amb conclusions i recomanacions per

		evitar recurrències i millorar la postura de seguretat.
Resposta a Incidents i Gestió de Crisi	Resposta d'incidents no crítics	Servei orientat a gestionar incidents de seguretat de baixa o mitjana severitat de manera àgil i eficient, aplicant les mesures necessàries per contenir, mitigar i resoldre l'incident sense afectar la continuïtat dels serveis. Inclou l'anàlisi inicial, l'aplicació d'accions correctives bàsiques, el seguiment fins al tancament i la documentació de les lliçons apreses per reforçar la prevenció i millorar els processos operatius.
Resposta a Incidents i Gestió de Crisi	Resposta d'incidents crítics	Servei orientat a gestionar incidents de seguretat d'alt impacte que comprometen serveis essencials, dades sensibles o infraestructures crítiques de l'organització. Inclou l'activació immediata d'equips especialitzats, l'anàlisi accelerada de l'incident, la contenció ràpida per limitar-ne l'abast, la recuperació segura dels sistemes afectats i la coordinació amb agents interns i externs. També incorpora la documentació completa de l'incident i recomanacions per reforçar la resiliència i evitar recurrències.
Resposta a Incidents i Gestió de Crisi	Retorn a l'estat inicial després d'incident	Servei orientat a restaurar els sistemes, serveis i configuracions afectats per un incident de seguretat fins al seu estat operatiu normal, garantint que la recuperació es fa de manera segura i controlada. Inclou la neteja o reinstal·lació dels equips compromesos, la recuperació de còpies de seguretat, la verificació de la integritat i funcionalitat dels serveis, i l'aplicació de mesures addicionals per evitar reincidentacions i reforçar la resiliència futura.
Resposta a Incidents i Gestió de Crisi	Suport en cas d'incidents greus de mig/llarg termini	Servei orientat a mantenir l'assistència especialitzada i la coordinació operativa durant incidents sostinguts en el temps, assegurant la gestió continuada de contenció, recuperació i comunicació. Inclou l'establiment d'un comandament operatiu, seguiment 24/7, pla de treball iteratiu amb fites i dependències, coordinació amb proveïdors i tercers, informes d'estat periòdics, i l'adaptació de mesures tècniques i organitzatives a l'evolució de l'incident fins al seu tancament segur.

Resposta a Incidents i Gestió de Crisi	Anàlisi inicial i primeres contencions	Servei orientat a realitzar una avaluació ràpida de les alertes o indicis d'incident per determinar-ne la naturalesa, l'abast i la severitat, aplicant alhora mesures de contenció immediata per limitar-ne l'impacte. Inclou la revisió preliminar de logs i evidències, la identificació d'actius afectats, l'aïllament temporal de sistemes sospitosos i l'adopció d'accions preventives bàsiques per frenar la propagació o explotació de l'amenaça mentre es prepara la investigació i resposta completa.
Peritatge Informàtic	Peritatge informàtic per a procediments legals	Servei orientat a la realització de peritatges tècnics en l'àmbit digital amb preservació d'evidències i cadena de custòdia rigorosa, aplicant metodologies forenses reconegudes per garantir integritat, traçabilitat i imparcialitat. Inclou l'adquisició i anàlisi de dispositius, sistemes i logs, la redacció d'informes pericials clars i defensables, així com el suport i compareixença com a perit davant autoritats judicials o administratives, assegurant la validesa probatòria del resultat.
Enginyeria Social i Conscienciació	Simulacions i gestió d'enginyeria social (Phising)	Servei orientat a la detecció, anàlisi i gestió d'intents de phishing provinents de correu electrònic, missatgeria o altres canals de comunicació i dispositius USB manipulats o maliciosos. Inclou la identificació ràpida de missatges sospitosos, l'avaluació del seu contingut i origen, l'aplicació de mesures de bloqueig i contenció, i l'assessorament per reforçar la protecció dels usuaris i reduir el risc de compromís a través de tècniques d'enginyeria social.
Enginyeria Social i Conscienciació	Intents d'accés a oficines	Servei orientat a identificar, analitzar i gestionar situacions en què actors no autoritzats intenten accedir físicament a les instal·lacions de l'organització. Inclou la verificació d'alarmes o avisos, la revisió d'enregistraments de videovigilància, la coordinació amb personal de seguretat física, l'avaluació del risc potencial i la proposta de mesures preventives o correctives per reforçar el control d'accessos i reduir la possibilitat d'intrusions futures.
Enginyeria Social i Conscienciació	Altres accions d'enginyeria social	Servei orientat a dissenyar i executar proves avançades d'enginyeria social que permetin identificar vulnerabilitats en el factor humà més enllà de les simulacions de phishing

		habituals. Aquestes accions poden incloure intents de vishing, smishing, suplantacions a través de xarxes socials o canals corporatius, així com interaccions presencials controlades o escenaris a mida que posin a prova els processos interns de verificació d'identitat i de resposta operativa. L'objectiu és detectar punts febles en comportaments i procediments, reforçar la cultura de seguretat i establir mesures preventives més robustes.
Suport en Seguretat TIC	Assessorament i suport tècnic de seguretat	Servei orientat a proporcionar assistència tècnica especialitzada en matèria de ciberseguretat per reforçar la protecció operativa i estratègica de l'organització. Aquest suport pot incloure l'anàlisi i resolució d'incidents, l'assessorament en configuració segura d'infraestructures i aplicacions, l'acompanyament en la implantació de controls de seguretat, la revisió de polítiques i procediments, i l'assistència en l'avaluació de riscos. L'objectiu és garantir una resposta eficient davant necessitats quotidianes o puntuals, millorar el nivell de seguretat global i facilitar la presa de decisions informades en l'àmbit de la ciberprotecció.
Suport en Seguretat TIC	Anàlisi i gestió de la seguretat de plataformes TIC	Servei orientat a avaluar, monitorar i reforçar la seguretat de les plataformes tecnològiques de l'organització, garantint-ne un funcionament robust, segur i alineat amb les millors pràctiques del sector. Inclou l'anàlisi de vulnerabilitats, la revisió de configuracions, el control de versions i parxes, l'avaluació de superfícies d'exposició, la verificació del compliment normatiu i la implantació de mesures de protecció preventives i reactives. El servei també pot abastar la supervisió contínua de l'estat de seguretat, la detecció de desviacions o riscos emergents i la proposta d'accions correctores per mantenir un nivell de seguretat adequat al llarg del temps.
Suport en Seguretat TIC	Revisió de configuracions	Servei orientat a analitzar i validar les configuracions de sistemes, plataformes i dispositius TIC per garantir que segueixen les millors pràctiques de seguretat, les recomanacions dels fabricants i els requisits normatius vigents. El servei pot incloure la revisió de paràmetres crítics, la detecció de configuracions febles o inconsistents,

		l'avaluació de permisos i rols, la verificació de l'enduriment d'equips i serveis, així com la proposta d'ajustos per reduir superfícies d'atac i millorar la postura de seguretat global de l'organització.
Suport en Seguretat TIC	Hardening / millores puntuals	Servei orientat a aplicar accions específiques de reforç de la seguretat en sistemes, plataformes i components TIC, amb l'objectiu de reduir superfícies d'atac i corregir debilitats concretes detectades durant auditories o tasques d'operació. Aquest servei pot incloure l'enduriment de sistemes operatius i aplicacions, l'ajust de configuracions crítiques, l'eliminació de serveis innecessaris, la millora de polítiques d'accés, la implementació de controls addicionals o la resolució d'inconsistències puntuals que puguin posar en risc la seguretat. L'enfocament és pràctic i orientat a obtenir resultats immediats que augmentin la protecció global de l'entorn tecnològic.
Rol externalitzat de CISO / CISOaaS	CISO externalitzat	Servei orientat a proporcionar a l'organització una figura de responsable de seguretat de la informació (CISO) en modalitat externalitzada, capaç d'assumir funcions estratègiques i operatives en la gestió integral de la ciberseguretat. Aquest servei pot incloure la definició i supervisió del pla director de seguretat, l'establiment de polítiques i procediments, la gestió de riscos, el seguiment del compliment normatiu (incloent-hi ENS, ISO 27001, RGPD), la coordinació d'incidents de seguretat i la interlocució amb direcció i tercers. L'objectiu és garantir un lideratge expert i continuat en seguretat sense necessitat de disposar d'un rol intern dedicat, assegurant coherència, governança i una visió estratègica alineada amb les necessitats de l'organització.
Serveis Especialitzats i Avançats	Threat Intelligence (operativa + estratègica/prospectiva)	Servei orientat a identificar, analitzar i monitorar amenaces sofisticades que poden afectar l'organització, proporcionant informació accionable per anticipar riscos i reforçar la postura de seguretat. Aquest servei pot incloure la recopilació de dades de fonts obertes, comercials i privades, l'anàlisi de TTPs d'actors hostils, la detecció d'indicadors de compromís específics, el seguiment de tendències emergents, així com l'elaboració

		d'informes estratègics, operatius o tècnics. L'objectiu és oferir visibilitat completa del panorama d'amenaces, permetent prendre decisions informades, prioritzar mesures de protecció i augmentar la capacitat de detecció i resposta davant atacs avançats.
Serveis Especialitzats i Avançats	Altres serveis analítics o R+D en ciberseguretat	Servei orientat a desenvolupar activitats avançades d'anàlisi, investigació i innovació en l'àmbit de la ciberseguretat, amb l'objectiu d'explorar noves tècniques defensives, millorar les capacitats existents i donar resposta a necessitats específiques o emergents de l'organització. Aquest servei pot incloure la realització d'estudis tècnics especialitzats, la recerca aplicada en metodologies de detecció o mitigació, el desenvolupament de prototips de seguretat, l'avaluació de tecnologies emergents, o la prova de concepte de solucions innovadores. L'objectiu és aportar coneixement de valor i generar capacitats diferencials que reforcin el nivell de protecció i adaptabilitat de l'organització davant un entorn d'amenaces en evolució constant.

Categoria 2. Serveis professionals de protecció de dades.

En aquesta categoria es contemplen aquells serveis vinculats a la protecció de dades en aquells àmbits on les entitats puguin requerir la contractació de serveis externs per complementar la prestació interna de serveis i/o el compliment legal.

A continuació es detallen les subcategories d'aquesta categoria.

Subcategoria	Servei	Descripció
Auditories	Protecció dades	Avaluar l'eficàcia de les mesures de seguretat, per demostrar el compliment i evitar sancions, recomanant-se revisions periòdiques o davant canvis substancials en els tractaments de dades per controlar riscos i millorar la seguretat de la informació personal.
Avaluacions d'impacte	Avaluació d'impacte en protecció de dades	Avaluació d'impacte a partir de la descripció sistemàtica de les operacions i les finalitats del tractament, avaluació de la necessitat i de la proporcionalitat de les operacions en relació amb la seva finalitat, avaluació dels riscos per als drets i les llibertats dels

		interessats, i les mesures proposades per mitigar els riscos.
Avaluacions d'impacte	Avaluació d'impacte sobre els drets fonamentals en l'ús d'intel·ligència artificial	Avaluació dels riscos per als drets dels interessats i el RIA fa èmfasi en l'avaluació de l'impacte en els drets individuals, independentment de l'ús de dades personals en el desenvolupament i la implementació de la IA
Anàlisi de riscos		L'Anàlisi de Riscos en Protecció de Dades (ARPD) és un procés clau per identificar, avaluar i gestionar els possibles perills per als drets i llibertats dels individus derivats del tractament de dades personals, sent un pas previ a l'Avaluació d'Impacte (AIPD) quan es requereix, i serveix per garantir la seguretat i el compliment normatiu, especialment amb el RGPD/LOPDGDD.
Suport protecció de dades/Servei d'oficina tècnica en protecció de dades	Suport a la protecció de dades	Serveis professionals d'ajuda a l'oficina del DPD per donar recolzament o suplir la oficina del DPD.
Compliment normatiu	Compliment normatiu en protecció de dades	Desenvolupament d'informes, anpalisi o redacció de normes en matèria de protecció de dades.