CONTRACTE RELATIU AL SERVEI DE CIBERSEGURETAT GESTIONADA DE LA UNIVERSITAT OBERTA DE CATALUNYA

EXPEDIENT HSE00029/2023

PROCEDIMENT OBERT
SUBJECTE A REGULACIÓ HARMONITZADA

PLEC DE PRESCRIPCIONS TÈCNIQUES

Universitat Oberta de Catalunya

ÍNDEX

1. Introducció

La Universitat Oberta de Catalunya (en endavant, “la UOC”) és una universitat innovadora, arrelada a Catalunya i oberta al món, que forma les persones al llarg de la vida contribuint al seu progrés i al de la societat, alhora que duu a terme recerca sobre la societat del coneixement. El seu model educatiu es basa en la personalització i l'acompanyament de l'estudiant mitjançant l'*e-learning*; en aquest sentit, es tracta de la primera universitat a la xarxa a l’estat espanyol.

La UOC vol ser una universitat que, connectada en xarxa amb la resta d'universitats del món, impulsa la construcció d'un espai global de coneixement i la recerca frontera en societat del coneixement. Innova en el model educatiu propi que se centra en l'estudiant, oferint una formació de qualitat i personalitzable, per fomentar la seva competitivitat i contribuir al progrés de la societat.

Dins de la universitat, l’Oficina de Seguretat de la Informació (d’ara endavant, “OSI”) vetlla per protegir els serveis que ofereix la institució i garantir la integritat, la confidencialitat i la disponibilitat de la informació en l'organització.

Per poder assolir aquest objectiu, sorgeix la necessitat de dotar de major capacitat a l’OSI per ampliar la vigilància i detecció d’amenaces de manera continuada, de donar resposta immediata en cas de qualsevol incident i de vetllar per la prevenció i protecció dels actius crítics de la institució.

2. Objecte del Contracte

El present contracte té per objecte la contractació d'un servei de Ciberseguretat Gestionada què doni resposta a les necessitats i reptes actuals de la Universitat Oberta de Catalunya (UOC), d'acord amb les prescripcions tècniques que es descriuen en el present plec.

Centrat en la prestació d'un servei especialitzat de ciberseguretat en general, seguretat en les telecomunicacions i ciberseguretat en el núvol, així com l’administració de les plataformes de seguretat especificades en present plec, i la prevenció i gestió d'incidents de seguretat. Tot això emprant les eines pròpies de la UOC descrites i les eines que aporti l'adjudicatari.

2.1. Objectius del Contracte

L'objectiu de la contractació d'aquest servei serà gestionar la seguretat de la UOC en base a les especificacions descrites en el present plec. I els objectius que es volen assolir inclouen:

- Disposar d'un servei de monitoratge en temps real de la ciberseguretat en mode 24x7x365 de vigilància i detecció.

- Resolució de peticions, incidències, tasques i problemes relatius a l'àmbit de la ciberseguretat per tal de proveir la màxima disponibilitat dels serveis.

- La gestió, operació, manteniment regular i administració de les infraestructures i eines de seguretat que s'integren en el servei, així com dels nous sistemes que es puguin incorporar durant tot el període que cobreix el contracte, garantint en tot moment la disponibilitat i la continuïtat del servei.

  Serveis d'anàlisi i gestió de les vulnerabilitats en el marc dels sistemes d'informació de la UOC i les infrastructures TIC, incloent-hi Pentests periòdics i Hacking ètic.

- Serveis de consultoria i de suport a la gestió de la ciberseguretat en el marc de compliance tecnològic, de nous desenvolupaments de projectes o en el marc de la transformació tecnològica de la UOC.

- Serveis de govern de la ciberseguretat per a la definició d'indicadors, quadres de comandament i gestió del coneixement.

- Serveis especialistes en peritatges informàtics i d'elaboració d'informes forenses.

- Realització d'exercicis de ciberseguretat que permetin avaluar el grau de resiliència de l'organització enfront a amenaces cibernètiques.

I, per tant, aquests serveis objecte de la contractació hauran de permetre a la UOC:

- Facilitar la mesura de la qualitat del servei en relació a la seguretat tecnològica mitjançant Acords de Nivell de Servei específics.

- Permetre assegurar que la UOC compleix amb els requeriments legals i normatius.

- Millorar la satisfacció i confiança dels estudiants de la UOC en els serveis TIC.

- Alimentar de forma continuada, metòdica el quadre de comandament de ciberseguretat. Aquest quadre només haurà de ser visible per la Oficina de Seguretat i els diferents comitès de seguretat de la UOC.

- Disposar de manera metòdica de diferents informes del servei de forma clara i diàfana.

2.2. Abast del servei

L'abast del servei és la contractació d'un servei de ciberseguretat que ajudi a gestionar la Seguretat Tecnològica de la UOC a tots els nivells (proactiu, preventiu i reactiu) i en les disciplines més rellevants de l'àmbit de la ciberseguretat.

Aquest servei inclou la gestió de la seguretat de la totalitat de sistemes d'informació (serveis TIC) de la UOC, tant en la forma de Public Cloud, Private Cloud i On-premise. Tanmateix

s'inclouen tant aquelles infrastructures TIC que estiguin ubicades en les instal·lacions de la UOC com aquelles que puguin estar en serveis externs subcontractats per la UOC basats en Cloud.

Les disciplines o especialitzacions, que es descriuran en aquest document són, almenys:

- Operacions de seguretat: monitorització continua de logs i esdeveniments de seguretat, capacitat de detecció primerenca d'incidents i amenaces, i vigilància d'amenaces.

- Gestió d'incidents de ciberseguretat, desastres, recuperació de les operacions després d'un incident de ciberseguretat, suport a les investigacions i requeriments, registre i seguiment d'activitats, mesures de prevenció i contramesures.

- Tractament de les vulnerabilitats: gestió del cicle de vida de les vulnerabilitats,

- Seguretat dels actius: controls de seguretat de les dades, protecció de la privacitat, incloent els actius situats al núvol.

- Seguretat de les comunicacions i de les xarxes (locals i al núvol): estratègies de proves, proves de controls de seguretat, vulnerabilitats de l'arquitectura en general, incloent

- Auditoria dels sistemes d'informació: auditoria, reporting, informes de situació i seguiment de les auditories.

- Suport de consultoría en matèria de ciberseguretat.

El servei prestat per l'adjudicatari serà flexible i alineat amb l'evolució tecnològica i organitzativa de la UOC, a fi i efecte d'adaptar-se a les necessitats sorgides de la implantació de noves infraestructures, aplicacions i/o projectes tant dins de la UOC com en el núvol.

3. Situació Actual i volumetria

La situació actual (infraestructura i volumetries) serà proporcionada per la UOC als potencials licitadors que ho sol·licitin com a *Annex I PPT. Descripció de la infraestructura tecnològica actual i volumetria del servei*, i després de la signatura d'un acord de confidencialitat que es proporcionarà seguint les indicacions del Plec de Clàusules Particulars. En concret, caldrà atendre a allò previst a l'apartat V del Quadre de Característiques i l'Annex 15 del mateix document.

L'adjudicatari haurà d'assumir variacions puntuals de les volumetries previstes de fins a un 20% d'increment o decreixement sense necessitat de fer cap modificació del contracte ni del preu.

4. Descripció del Servei

L'adjudicatari haurà de disposar d'un equip complet de professionals d'operacions de seguretat i de resposta a incidents, les instal·lacions del qual podran ser visitades per la UOC. Els detalls i condicions quedaran especificades al llarg d'aquest plec.

El proveïdor adjudicatari haurà de cobrir els següents serveis:

- Servei regular
    1. Detecció, anàlisi i gestió de vulnerabilitats.
    2. Auditories tècniques de ciberseguretat, pentest i hacking ètic.
    3. Monitorització de seguretat, detecció primerenca d'incidents i amenaces, i correlació d'esdeveniments en temps real.
    4. Administració i evolució de la plataforma SIEM.
    5. Administració i evolució de la plataforma EDR i anti-virus.
    6. Realització de millores i evolució del servei regular.
    7. Servei d'elaboració del quadre de comandament.
    8. Servei de suport a l'Oficina de Seguretat de la Informació.

- Serveis sota demanda
    1. Manteniment i evolutiu.
    2. Elaboració d'informes de petició d'evidències i tècnica forense.
    3. Exercicis de ciberseguretat.

4.1. Servei Regular:

4.1.1. Detecció, anàlisi i gestió de vulnerabilitats

L'adjudicatari gestionarà el cicle de vida de les vulnerabilitats detectades i què provinguin de fonts o comunicacions externes (CERTS, alertes primerenques, fabricants, zero days o bug bounty, etc …), fonts o comunicacions internes de la UOC (detectades i degudes a incidents de seguretat reportats, notificacions del propi personal UOC, detectades pel propi servei de ciberseguretat, derivades de les auditories de seguretat o dels propis escanejos de vulnerabilitats, etc …) i d'altres vulnerabilitats detectades per organismes externs a la UOC.

L'àmbit de la gestió de vulnerabilitats abarca tots els actius de la infrastructura on-premise i la dels núvols privats i públics gestionats pels sistemes d'informació de la UOC.

El servei de detecció, anàlisi i gestió de vulnerabilitatsi ha de ser prestat com a mínim per aquests perfils:

- Coordinador del servei.
- Analista de seguretat.
- Tècnic especialista en hacking ètic i pentesting.

En relació a la detecció, anàlisi i gestió de vulnerabilitats, l'adjudicatari, com a mínim, haurà de:

- Prioritzar la resolució de les vulnerabilitats detectades.
- Adaptar la puntuació associada a una vulnerabilitat en funció de les característiques i *statu quo* d'aquesta dins la UOC.
- Assegurar que no es proporcionen falsos positius, amb verificacions manuals i personalitzades.
- Fer el seguiment del cicle de vida de la gestió de les diferents vulnerabilitats reportades.
- Proposar mitigacions si s'escau o informar tècnicament que queda impossibilitada la resolució de la vulnerabilitat via pegat o canvi de versió.
- Donar suport als equips responsables de la correcció de les vulnerabilitats (Àrea de Tecnologia TI).
- Fer el seguiment de la planificació de la correcció de la vulnerabilitat, donar suport en el procés de mediació i en la comprovació de la correcció.
- Realitzar informes de seguiment a diferents nivells: tècnics per la Oficina de Seguretat UOC i a nivell més executiu per la direcció i que proporcionin un indicador del nivell d'exposició i risc dels sistemes auditats i sota la gestió de les vulnerabilitats.

Les tasques que, com a mínim, haurà de realitzar l'adjudicatari són:

- Els escanejos periòdics, amb un mínim requerit d'un (1) escaneig trimestral per cadascun dels actius de la UOC. Els actius de la UOC estan especificats en l'Annex I: Descripció de la infraestructura tecnològica actual i volumetria del servei.
- La gestió conjunta de la remeiació de les vulnerabilitats detectades amb els responsables de seguretat i de la infraestructura TI de la UOC.
- La gestió dels zero-days amb l'avaluació de l'impacte i l'anàlisi de riscos associats.
- Manteniment operatiu de les eines i sistemes que suporten la gestió de vulnerabilitats.
- La posada a disposició de la UOC d'una eina, amb accés via web, per a la creació i manteniment de les bases de dades de vulnerabilitats a gestionar i d'una sèrie d'indicadors de qualitat i de seguiment (Key Performance Indicator) derivats. Haurà de ser accesible pel personal de la UOC i haurà de disposar d'un panell de seguiment.
- La realització d'informes mensuals de les activitats realitzades.
- Proporcionar suport puntual al equip de DEVSECOPS sobre les vulnerabilitats complexes que emergeixin i/o s'hagin detectat.
- Identificar i gestionar les vulnerabilitats en els Dockers i diferents imatges dels contenidors al núvol i on-premise en cas que n'hi hagin.
- Per a la gestió de les vulnerabilitats, incloent-hi les configuracions inadequades i les vulnerabilitats trobades durant el procés del servei, es documentaran i classificaran d'acord amb les mètriques més habituals, vg. CVE, CWE i CVSS.

- Realitzar l'alta en el sistema de ticketing corporatiu (JIRA) de la UOC de les diferents tasques, generades a partir de la gestió de la cartera de vulnerabilitats detectades.

Lliuraments mínims per cada anàlisis efectuat:

- Un informe executiu que contingui com a mínim:
    - la valoració real del risc en l'entorn de l'UOC de les vulnerabilitats trobades.
    - nivell de criticitat de l'actiu.
- Un informe tècnic que contingui com a mínim:
    - les debilitats trobades i la seva classificació.
    - la documentació de les proves realitzades amb la seva evidència.
    - recomanacions de seguretat.
    - explicació de la metodologia seguida per explotar les vulnerabilitats.

En l'actualitat la UOC disposa de les eines de Nessus Professional i Microsoft 365 Defender (només punts de treball) per la detecció de vulnerabilitats. El proveïdor adjudicatari podrà fer servir aquestes eines o altres.

Les eines addicionals correran a càrrec del proveïdor adjudicatari, tant pel que fa a l'adquisició del programari com la infraestructura necessària per a poder proveir aquest servei. En aquest cas l'eina aportada pel contractista haurà de complir amb els següents requeriments:

- Efectivitat dels escanejos de vulnerabilitats: Hauran de ser efectives i reconegudes a nivell de mercat amb un nivell de falsos positius (six-sigma accuracy) per sota de .50 fer cada $1x10^6$ escanejos.
- Un repositori únic per gestionar les vulnerabilitats detectades com a resultat de les diferent auditories que es realitzin i què permeti:
    - Categoritzar les vulnerabilitats en funció de criteris de valoració estàndard CVSS2 i CVSS3 (de preferència).
    - Importar de manera automàtica els resultats de diferents eines d'escanejos de vulnerabilitats.
    - Exportació en diferents formats (HTML, PDF, MS-Word, CSV) de la base de dades d'actius i de les vulnerabilitats perquè els equips de la UOC puguin tractar aquesta informació de manera més àgil o distribuïda.
    - Realitzar recerques d'actius afectats per una vulnerabilitat concreta.
- La eina haurà de facilitar indicadors i poder fer el seguiment de la gestió de les vulnerabilitats, així com la planificació dels treballs i un resum del nivell d'exposició de l'organització davant possibles atacs.

- En general la eina ha de permetre una gestió del risc què possibiliti establir diferents terminis de resolució en funció de la criticitat dels actius i de les vulnerabilitats associades.
- Elaborar gràfics configurables i quadre de comandament i mostrar una evolució de la seguretat al llarg del temps.
- Disposar d'una interfície web accessible per la UOC.
- L'eina utilitzada ha de garantir el compliment de la normativa europea de protecció de dades

La UOC facilitarà accés a la seva CMDB (AssetExplorer ManageEngine) de la qual el proveïdor adjudicatari en descarregarà les dades que precisi per la correcta identificació dels actius inclosos en el servei.

La UOC podrà modificar la planificació dels anàlisis de vulnerabilitats, en cas de necessitat i de forma justificada. Es requerirà per part del contractista un temps de resposta de 5 dies laborables com a màxim per l'inici de les noves tasques d'escaneig.

4.1.2. Auditories tècniques de ciberseguretat, Pentest i Hacking Ètic

En el marc de la prestació del servei regular el contractista s'encarregarà de la planificació i realització de les auditories tècniques de ciberseguretat (Pentest i Hacking Ètic), automàtiques i manuals, als sistemes d'informació, xarxes i aplicacions de la UOC de manera planificada o també sota demanda.

El servei d'auditories tècniques de ciberseguretat, Pentest i Hàcking ètic ha de ser prestat com a mínim per aquests perfils**:**

- Coordinador del servei.
- Tècnic especialista en hacking ètic i pentesting.

Les activitats i lliuraments que, a nivell general, l'adjudicatari haurà d'establir en un pla d'auditories tècniques d'ofici són:

- Es realitzaran un mínim d'una (1) auditoria anual en mode caixa negra a tota la superfície UOC exposada a Internet, incloent-hi els actius que estiguin en el núvol públic de la UOC. La durada mínima de cada auditoria serà de 200 hores incloent-hi la recopilació de resultats i la generació dels informes preceptius.
- Un mínim d'una (1) auditoria l'any en mode caixa gris a tota la superficie UOC interna incloent-hi els actius que estiguin en el núvol privat de la UOC. La durada mínima de cada auditoria serà de 200 hores incloent-hi la recopilació de resultats i la

generació dels informes preceptius.

- Un mínim d'un (1) test d'intrusió anuals (pentest) o hacking ètic, en mode caixa negra per a aplicacions web i/o serveis (aplicacions mòbils i productes propis). La durada mínima de cada pentest serà de 100 hores incloent-hi la recopilació de resultats i la generació dels informes preceptius.

- Per cada auditoria el contractista lliurarà:
    - Un informe executiu.
    - Un informe de compliment/no compliment.
    - Un informe tècnic detallat seguint la normativa i recomanacions de la guia CCN-STIC-802.
    - En el cas de detecció de vulnerabilitats, aquestes s'incorporan en la cartera i base de dades de seguiment de la gestió de vulnerabilitat, punt 4.1.1 d'aquest document, i el cicle de vida passarà a ser tal com queda definit en el mateix punt.

- Els materials generats/entregables/treballs seran propietat de la UOC qui ostenta la titularitat plena autoritzant el seu ús a l'adjudicatària i/o subcontractista exclusivament amb l'abast necessari per tal d'executar el servei durant la vigència del present contracte d'acord amb la clàusula 42 del PCP "Drets de propietat intel·lectual i industrial dels treballs".
- El contractista ha d'assegurar que els desenvolupaments realitzats per la prestació dels Serveis a la UOC i les seves eines utilitzades durant el servei compleixen les lleis de propietat intel·lectual i no vulneren cap legislació, normativa, contracte, dret, interès o propietat de tercers, permentent a la UOC el seu ús pacífic.

4.1.3. Monitorització de seguretat, detecció i resposta primerenca d'incidents i amenaces, i correlació d'esdeveniments en temps real (SOC)

La funció d'un centre d'operacions de seguretat (SOC o Security Operations Center) és la de supervisar, prevenir, detectar, investigar i respondre a les ciberamenaces en mode 24x7x365.

Els equips d'un SOC s'han d'encarregar de supervisar i protegir els actius d'una organització, incloent-hi la propietat intel·lectual, les dades del personal, els sistemes empresarials i la integritat de la marca. L'equip d'un centre d'operacions de seguretat implementa l'estrategia de ciberseguretat general de l'organització i actua com a punt central de col·laboració en els esforços coordinats per a supervisar, avaluar i protegir contra els atacs cibernètics.

L'adjudicatari prestarà el servei de monitorització en modalitat 24x7x365 mitjançant la plataforma SIEM de la UOC, donant suport i gestió a les alertes generades, incloent la integració amb la plataforma de ticketing JIRA UOC.

El servei de monitorització de seguretat, detecció i resposta primerenca d'incidents i amenaces, i correlació d'esdeveniments en temps real, ha de ser prestat com a mínim per aquests perfils**:**

- Coordinador del servei.
- Analista de seguretat.
- Tècnic especialista en seguretat de la resposta a incidents de seguretat de la Informació. (Tècnic SOC Sènior).

Requeriments sol·licitats:

- El contractista disposarà d'un centre operatiu (SOC) en mode 24x7x365 on es rebran, notificaran, gestionaran i escalaran si s'escau, les alertes i incidents de ciberseguretat. La UOC es reserva el dret de visitar, prèvia sol·licitud, les dependències del centre operatiu del contractista.

- Monitorització constant (24x7x365) de les alertes i events generats i rebuts dins la plataforma SIEM de la UOC. El contractista farà pel seu compte totes aquelles tasques necessàries per integrar les alertes i notificacions amb les seves dependències SOC i el seu personal.

- Monitorització constant (24x7x365) de les alertes i events que siguin generats per altres canals que no són el SIEM, vg. JIRA i alertes provinents dels serveis tècnics d'Amazon o Azure. La UOC proveirà de les adreces de correu o d'altres canals perquè aquestes alertes arribin el més aviat possible al SOC del contractista.

- El contractista integrarà els seus sistemes de gestió interns de les alertes i incidents amb la eina de ticketing de la UOC (Atlassian JIRA), que permeti, entre d'altres, conèixer el nombre d'alertes i incidents gestionats i el seu estat.

- La UOC proveirà d'un repositori Google Drive o Atlassian Confluence on deixar de forma ordenada tota la documentació generada en el decurs del servei. Aquesta documentació inclourà també les evidències necessàries i annexos propis de treball.

- L'adjudicatari s'integrarà amb els diferents organismes oficials en què la UOC estigui subjecte per llei (RGPD) o amb el que es considerin oportuns per la due diligence per la cooperació a la gestió i detecció d'incidents (CSUC CDIRT, Agència de Ciberseguretat de Catalunya, CCN-CNI). I si el servei ho requereix, es durà a terme la ingesta dels sistemes de registre i notificació d'incidents corporatius.

- El contractista farà una gestió dels indicadors de compromís que puguin ser d'utilitat per la UOC. En base a les diferents fonts d'informació l'adjudicatari determinarà quins IOCs són necessaris incorporar a altres elements de la infraestructura i dispositius de protecció de l'organització.

  Es requerirà una traçabilitat dels IOCs en aquests altres elements, que permeti conèixer quins s'afegeixen, quins s'eliminen o quins es modifiquen diàriament, així com el nombre d'IOCS desplegats en qualsevol moment.

  La UOC no proporcionarà cap base de dades d'IOCs, ni comercial ni en fonts

obertes i haurà de ser el propi contractista qui disposi d'accés a bases de dades reputades d'IOCs.

- L'adjudicatari serà responsable de la creació, manteniment i depuració dels casos d'ús associats a les alertes del SIEM i en general de la creació, manteniment i depuració dels playbook associats als anteriors. Serà responsabilitat del contractista la definició de la resposta i les estratègies relatives a les alertes de ciberseguretat recepcionades pel SOC.

  La UOC revisarà i aprovarà tots i cadascun dels playbook nous que hagin d'entrar en servei. Tanmateix es provaran i es donarà validesa al seu ús.

  El model formal de playbook serà el que té actualment la UOC i si cal fer alguna modificació i millora es decidirà en el moment de la due dilligence.

- Els casos d'ús nous quedaran documentats en el repositori Confluence o Google Drive de la UOC i pasaran per les següents fases inclosa la de creació del playbook associat:

  - **Definició**: el contractista presentarà les seves propostes i aquestes s'acordaran conjuntament amb la UOC. De preferència el contractista basarà les seves propostes en l'estàndar de facto MITRE ATT&CK.

  - **Anàlisi**: aquesta fase correrà a càrrec totalment del contractista, incloent-hi l'anàlisi de les fonts de LOG necessàries i la incorporació d'aquestes en el SIEM de la UOC. Es podrà sol·licitar suport puntual al departament de la UOC propietari d'aquella font de LOG per assolir la integració en el SIEM.
    El contractista podrà usar un entorn de proves per aquesta i les següents fases.

  - **Desenvolupament**: també correrà a càrrec del contractista. Inclou totes les tasques de correlació, integració, recepció pels analistes de SOC, dashboards, etc.

  - **Depuració**: correrà també a càrrec del contractista totes aquelles tasques i proves destinades a reduir al màxim la presència de falsos positius associats al cas d'ús.

  - **Pas a producció**: el cas d'ús entrarà en producció i tota la documentació pròpia i associada passarà a la base de dades de coneixement de la UOC en format Atlassian Confluence.

  - La propietat intel·lectual dels casos d'ús actuals i nous i dels seus playbooks associats pertany 100% a la UOC.

4.1.3.1. Incident handling. Resposta a incidents crítics/molt crítics o d'alt risc per la UOC:

El contractista prestarà dins del servei de monitorització de la seguretat - SOC, un servei de resposta ràpida a incidents crítics o d'alt risc per la UOC. Aquest servei haurà d'estar dotat d'una bossa anual de cent (100) hores dins del servei regular recurrent. Un cop s'exhaureixi aquest bossa, les hores addicionals aniran contra el servei sota demanda.

Per tant, la retribució de les primeres 100 hores de dedicació relatives al servei de resposta ràpida a incidents crítics o d'alt risc es farà mitjançant el preu a tant alçat ofert per l'adjudicatari respecte del servei regular recurrent

Es requerirà un temps de resposta màxim per aquest tipus d'incidents de menys de 30 minuts (les prioritats es determinaran de manera conjunta entre UOC i proveïdor en fase d'inici del servei o due diligence).

El servei d'Incident handling ha de ser prestat com a mínim per aquests perfils:

- Coordinador del servei
- Tècnic especialista en seguretat de la resposta a incidents de seguretat de la Informació.

Per a aquest tipus d'incidents el contractista complirà els següents requeriments:

- Modalitat 24x7x365 per la recepció i atenció d'incidències.
- L'existència d'un equip específic per a aquesta atenció que serà diferent, o almenys no ha de poder coincidir amb el de SOC.
- Escalat a perfils específics i amb majors nivells d'expertesa.
- El procediment de gestió dels incidents seguirà com a mínim el de la guia CCN-STIC-817 i estarà basat en les millors pràctiques de ciberseguretat.
  Entre d'altres, les fases, capacitats de l'equip i tasques que es demana són:
  - Investigació forense.
  - Classificació i tipologia de l'incident d'acord a estàndards: MITRE, ENISA, NIST, CCN-CNI.
  - Coordinació amb diferents equips. Treball multi-disciplinar. Tasques de comunicació.
  - Avaluació de l'impacte i estudi d'avaluació de riscos informàtics
  - Existència de perfils i felxibilitat en la incorporació als equips de treball i contenció segons necessitats.
  - Recuperació d'entorns.
  - Assesoria tecnològica.
  - Peritatge forense.
  - Expertesa en temes legals.

4.1.4. Administració i evolució de la plataforma SIEM UOC

El contractista és el responsable de l'operació, administració i evolució de la plataforma de seguretat SIEM de la UOC, així com de la integració de noves fonts de LOG, de les regles de correlació, alertes i ofenses de seguretat, creixement de l'espai en disc de les dades, temps de retenció dels LOG i totes aquelles taules i bases de dades auxiliars necessàries pel funcionament dels casos d'ús tal i com s'explica en el punt 4.1.3 d'aquest document.

La UOC disposa d'una plataforma SIEM model "IBM QRadar 3199 - Console, versió 7.5.0":

- Event Limit 5100/30000
- Flow Limit 15000/1200000

El servei d'Administració i evolució de la plataforma SIEM ha de ser prestat com a mínim per aquests perfils:

- Coordinador del servei.
- Analista de seguretat.
- Tècnic administrador de plataformes tecnològiques (SIEM).

Les tasques que haurà de fer el contractista són:

- La revisió periòdica de l'estat i l'activitat dels usuaris.
- Definir i implantar les polítiques de seguretat.
- Definir i implantar els quadres de comandament d'activitat segons la tipologia d'usuari: compliance, risk, application, threats, system.
- Definició i seguiment de les polítiques de retenció de LOGs.
- Seguiment i tunning de rendiment de l'equip. Inclosos els paràmetres d'operació.
- Monitoratge i comprovació de l'estat del sistema.
- Comprovació de l'estat dels recol·lectors, fonts de LOG i coalescència de dades.
- Anàlisi de la volumetria de les capacitats del dispositiu.
- Registre i processat dels error o events que pugui mostrar el dispositiu i que pugui afectar al servei.
- Revisió periòdica de les fonts de LOG i DSMs.
- Detecció d'errors de sistema i performance del dispositiu.
- Actualització a noves versions, previa comunicació i d'acord amb els responsables de la UOC.
- Instal·lació de patches, plugins i d'altres apps.
- Revisió del correcte funcionament de les regles en producció.

- Integració i incorporació de noves fonts de LOG en coordinació amb la UOC i només si aquestes fonts són pertinents per algun cas d'ús.
- Integració de noves fonts de LOG a petició dels responsables UOC i a efectes de recerca forense o retrospectiva.
- Configuració de regles de correl·lació específiques d'una font ja proporcionada pel fabricant i configuració del cas d'ús específic proporcionat pel fabricant.
- Configuració i manteniment dels building blocks (conjunt re-utilitzable de regles i proves que poden ser usades dins d'unes altres regles).
- Configuració i manteniment dels reference sets (conjunt de dades organitzades i categoritzades que poden usar-se com a referència dins d'una regla).
- Manteniment dels diferents subsistemes i serveis de Qradar (Network Hierarchy, Index Management, Asset Profiler, Custom Asset Properties, DSM Editor, Log Sources, Custom Event Properties, Event Retention, User Behavoir, etc.).
- Gestió d'informes que es poden gestionar desde QRadar, proposant nous informes al personal de seguretat de la UOC i, un cop aprovats, implementació dels mateixos.

Tasques anuals que haurà de fer el contractista:

- **Incorporació de noves fonts de LOG al sistema SIEM**: Un mínim de 25 sempre que hi hagi projecte i planificació de nous casos d'ús que necessitin de la incorporació d'aquestes noves fonts de LOG.
- **Nombre de sistemes a incorporar en les fonts de LOG**: Un mínim de 350 sistemes. Els protocols o serveis homòlegs s'integraran com una sola font de LOG a QRadar, mitjançant algun tipus de peça agregadora intermèdia via rsyslog, syslog o syslog-ng.
- **Nombre de casos d'ús nous**: Un mínim de 24 casos d'ús nous a l'any seguint les recomanacions i la metodologia MITRE ATT&CK. Cada cas d'ús estarà composat d'una o més Rules de QRadar, un o més Building Blocks (pot ser també que sigui zero), un o més Reference Set (pot ser també que sigui zero), un PlayBook amb les tasques detallades de Tier 1 i de Tier 2 de SOC incloent-hi el IR adequat pel Cas d'Ús.

El contractista haurà de presentar, com a mínim, el següents informes com a comprovació de les tasques de manteniment:

- Un informe setmanal amb les tasques realitzades des del darrer control.
- Un informe mensual amb les propostes de millora que necessitin de l'aprovació dels responsables de la UOC.
- Un informe ad-hoc si hi ha qualsevol incidència relacionada amb el funcionament, activitat i servei SIEM adreçat als responsables de la UOC.

4.1.5. Administració i evolució de la plataforma EDR i antivirus UOC

La solució actual de la UOC és Microsoft 365 Defender Advanced Thread Protection, desplegada en 1.840 dispositius personals i de sobretaula i 32 servidors.

La volumetria actual al voltant del nombre d'alertes i incidents actuals detectats per l'EDR en l'últim període de 6 mesos es troba a l'**Annex I Infraestructura tecnològica i volumetria del servei**

El servei d'Administrador i evolució de la plataforma EDR i antivirus ha de ser prestat com a mínim per aquests perfils**:**

- Coordinador del servei.
- Analista de seguretat.
- Tècnic especialista en seguretat de la resposta a incidents de seguretat de la Informació.

Les tasques què haurà de realitzar són:

- L'administració de les polítiques pròpies de l'EDR respecte a la detecció i contenció d'alertes i incidències.

- L'administració de les polítiques pròpies de l'antivirus MS Defender i la configuració de polítiques adhoc per perfils que li puguin ser sol·licitades.

- La gestió dels IOCs relacionats amb l'EDR, tant en llista blanca com en llista negra.

- Mantenir una llista dels IOCs afegits en aquesta plataforma i revisarà periòdicament la validesa d'aquests.

- Gestionar les vulnerabilitats dels dispositius sota control de l'EDR i farà els informes de vulnerabilitats relacionats, tal i com es descriu a l'apartat 4.1.1 d'aquest document.

- Consolidació i processat dels "Reports" que genera la eina de forma estàndard, de tal manera que presentarà als responsables UOC informes de tendència i d'amenaces basats en les dades extretes del propi EDR. Aquestes dades hauran de ser completades amb les que es puguin extreure de l'API MS Graph, si no estan presents en els propis reports. Aquests informes s'hauran de presentar mensualment i les dades hauran d'estar integrades tant a nivell d'indicadors de qualitat i de seguiment (Key Performance Indicator) com de dashboard general del servei com es descriu a l'apartat 4.1.7 d'aquest document.

- Explotació de la funcionalitat Hunting i Advanced Hunting de la eina. L'adjudicatari presentarà mensualment una proposta de noves queries/informes basats en l'explotació de dades mitjançant aquesta eina, dels quals la UOC en seleccionarà 2. El licitador presentarà un informe, en forma de fitxer electrònic o integrat en un dashboard, amb la periodicitat acordada per cada cerca. Tanmateix s'integraran també a nivell d'indicadors de qualitat i de seguiment (KPI Key Performance Indicator) si aquest fos el propòsit de

la cerca realitzada, com es descriu a l'apartat 4.1.7 d'aquest document.

- Suport a la integració de l'agent EDR en els nous servidors en què hagi de ser instal·lat.

- Comprovar i testejar aleatòriament, amb periodicitat setmanal, que les sondes i agents de l'EDR funcionen correctament i generen alertes que acaben ingestades en el SIEM UOC. Aquestes comprovacions s'hauran de fer obligatòriament en aquelles màquines de tipus Server i amb una rutina específica que haurà de definir l'adjudicatari en la due dilligence (especificada al punt 8.1 Fase de Transferència).

- Utilitzar les capacitats de l'EDR integrades en la resposta a incidents i molt especialment en la resposta a Resposta a incidents crítics/molt crítics o d'alt risc, apartat 4.1.3.1 d'aquest document.

4.1.6. Realització de millores i evolució del servei regular

El contractista haurà de posar a disposició del servei un procés de millora continua amb propostes escrites de recomanacions sobre solucions i serveis nous i actuals, canvis i d'altres millores correctives que potenciïn l'evolució positiva del servei.

L'aplicació de les millores serà a decisió i criteri dels responsables de la UOC.

El servei d'evolució i millores s'ha d'encarregar de liderar, gestionar i controlar l'evolució dels serveis regulars per a ser més eficients i eficaços en la realització de les tasques operatives que té encomanades, sempre amb visió a l'alineament d'aquestes accions amb els objectius de seguretat de UOC.

Aquest servei ha d'estar alineat a donar compliment a les necessitats de transformació, evolució, correctives i/o estratègiques que es donin, per una banda les que s'originin en l'àmbit dels serveis prestats, i en l'altre, aquelles que s'esdevinguin com una millora de la seguretat de la UOC i tinguin entitat de projecte propi.

El servei de realitzacó de millores i evolució del servei regular ha de ser prestat com a mínim pel perfil:

- Coordinador del servei.

Aquest servei de manera general i no limitativa, ha de cobrir les funcions de:

- Avaluació i gestió continua de la maduresa dels serveis regulars, argumentant progressivament els nivells de maduresa que es van assolint (a través dels plans de transformació dels diferents serveis), tenint el focus principal en l'àmbit sobre el qual versa tota l'activitat (prevenció, detecció, protecció, resposta).

- Definir els plans d'acció/transformació dels serveis i vetllar pel compliment i l'assoliment dels objectius i fites descrits, per tal d'aportar valor i millora contínua als serveis regulars

i a la seguretat general de UOC.

- Analitzar i identificar processos i activitats operatives dels serveis regulars que poden ser susceptibles d'automatització o industrialització, permetent una optimització dels recursos tècnics i professionals que es poden orientar a aportar valor afegit en la prevenció, protecció, detecció i resposta a esdeveniments de seguretat, millorant la seguretat global de la UOC.

- Industrialització i automatització, no només ha de contemplar l'aportació tecnològica, sinó també la definició de models i estàndards operatius que assoleixin una eficàcia i eficiència objectiva sobre les activitats dels serveis regulats prestats.

Els processos de millora continua que, com a mínim, haurà d'analitzar i millorar l'adjudicatari són:

- Modelatge d'amenaces (threat modeling). El propòsit és proporcionar a la UOC un anàlisi sistemàtic de quins controls i mecanismes de defensa s'han d'incloure, quin és el perfil de l'atacant tipus per la UOC, quins poden ser els vectors d'atac més factibles i quins serien els actius més cobejats per l'atacant tipus.
    - El contractista aportarà les eines necessàries i haurà de proporcionar un accés a la interfície de les mateixes als responsables de la UOC.
    - S'usaran de manera preferent les metodologies basades en MITRE o CAPEC.
    - El modelatge d'amenaces connectarà directament amb la creació i manteniment dels casos d'ús de la UOC i dels playbook o procediments operatius.

- Definició d'un pla estratègic pel desenvolupament i evolució del servei i especialment del SOC.

  L'adjudicatari haurà de realitzar una proposta de pla d'evolució i transformació on detalli les actuacions previstes en el servei d'acord amb les funcions anteriorment indicades. El pla haurà de ser detallat, amb actuació concretes, planificades en el temps i caldrà definir-ne la seva aproximació i metodologia d'execució. S'haurà de definir un indicador d'evolució mensual i global per tal de poder avaluar l'avanç del Pla d'Evolució que s'ha definit.

  En aquest servei el licitador haurà de fer seguiment de tots els projectes de transformació i evolució que s'estigui executant la UOC i haurà de detectar i notificar el més aviat possible qualsevol factor de risc que sorgeixi, tant en tasques associades a projectes, com als projectes en si.

4.1.7. Servei d'elaboració del Quadre de comandament

El proveïdor haurà de dissenyar i implementar un quadre de comandament integral (dashboard) tàctic amb els indicadors i KPIs dels serveis anteriorment descrits, així com d'altres indicadors de seguretat corporatius.

Aquest quadre de comandament actuarà com un agregador de tots els punts anteriors descrits en aquest document i de tots els indicadors mesurables que se'n puguin desprendre.

El servei d'elaboració del Quadre de comandament ha de ser prestat com a mínim per aquests perfils**:**

- Coordinador del servei.
- Consultor en seguretat de la informació.
- Analista de seguretat.

Com a mínim el quadre de comandament ha de contenir:

- Indicadors d'amenaces, alertes i incidents.
- Indicadors vulnerabilitats.
- Indicadors d'incidents.
- Indicadors dels serveis descrits en els apartats anteriors.

L'adjudicatari pot proposar altres indicadors que es considerin necessaris per poder desplegar accions de millora contínua als diferents serveis o bé, prendre decisions sobre l'estratègia de seguretat i el seu Pla director.

L'adjudicatari haurà d'utilitzar la plataforma Microsoft Power BI que la UOC posarà a la seva disposició per implementar aquest dashboard.

4.1.8 Servei de suport a l'Oficina de seguretat de la Informació

L'Oficina de Seguretat de la Informació (OSI) de la UOC disposa d'una estratègia de seguretat basada en la identificació dels riscos sobre els seus actius tecnològics clau amb una orientació al processos de negoci i el seu valor en l'organització.

En aquest sentit, el servei de suport a l'OSI té com a principal funció donar suport a la responsable de seguretat de la UOC per a identificar i concretar mesures efectives per millorar la postura de seguretat de l'organització, la reducció de riscos i el compliment d'estàndards de seguretat.

El servei de suport a l'Oficina de seguretat de la Informació ha de ser prestat com a mínim per aquests perfils**:**

- Coordinador del servei.
- Consultor en seguretat de la informació.

Aquest servei de manera general i no limitativa, ha de cobrir les funcions de:

- Elaboració dels informes executius de compliment, risc i seguretat.
- Definició de controls, polítiques i mesures de seguretat existents sobre els àmbits de protecció del servei de ciberseguretat.
- Definició i implantació d'un quadre de comandament amb visió estratègica.
- Gestió de projectes de seguretat.
- Definició i desplegament de processos de gestió de la seguretat.
- Suport en l'elaboració i actualització del Pla Director de Seguretat.

- Suport en la supervisió contínua del compliment de les mesures i polítiques de seguretat corporativa.

- Assessorament i suport en la definició de tasques o dubtes que puguin sorgir de l'OSI per a incrementar la seguretat global de la UOC.

L'adjudicatari haurà de posar a disposició del servei un Consultor en Seguretat de la informació, amb una dedicació mínima de 25 hores al mes., tenint la UOC potestat de demanar canvi en el consultor sempre i quan, i de manera justificada, aquest no presti el servei de forma satisfactòria per la UOC.

L'adjudicatari es compromet a mantenir el consultor durant la vigència del contracte, podent-lo substituir només per causes justificades. En aquest cas, la persona que el substitueixi haurà de complir amb la solvència requerida, sent la UOC qui validarà que el perfil s'ajusti a la solvència.

Per altra banda, l'adjudicatari haurà de sol·licitar per escrit qualsevol canvi en el perfil i amb una antelació suficient que garanteixi un correcte traspàs de coneixements per tal d'evitar afectacions en el servei. El canvi només podrà fer-se si prèviament s'ha validat per la UOC el compliment dels requisits de solvència anteriorment mencionats.

En el cas que la UOC necessiti una dedicació superior, s'acordarà amb l'adjudicatari la disponibilitat del consultor en funció de la seva disponibilitat respecte d'altres serveis en els que estigui participant.

4.2. Serveis Sota Demanda

4.2.1. Manteniment i evolutiu

La UOC disposarà d'un còmput d'hores per la realització de tasques sota demanda segons les necessitats de cada moment i relacionades amb el servei regular. Aquestes tasques aniran destinades a donar suport als responsables de la UOC tant en la prevenció, la gestió i la resposta en front d'incidents de seguretat de la informació, com a altres necessitats de seguretat.

Procediment davant d'una petició:

- La UOC farà la petició a l'adjudicatari amb els requeriments particulars sobre perfils i tasques a realitzar.

- L'adjudicatari haurà de fer una proposta en un termini màxim de dues (2) setmanes que posteriorment haurà de ser validada pels responsables de la UOC.

4.2.2. Elaboració d'informes de petició d'evidències i tècnica forense

De forma paral·lela i complementària a la resposta d'incidents de seguretat, es planteja l'existència d'un servei d'elaboració d'informes que poden ser requerits des de la pròpia àrea de ciberseguretat o d'altres de la UOC com ara els serveis jurídics.

Aquests informes haurien de servir per donar valor afegit i ajudar a la resolució de temes més generals.

Perfils relacionats amb aquest servei (PCP P: Solvència tècnica perfils):

- Coordinador del servei
- Tècnic especialista en informàtica forense i investigació interna

L'elaboració d'aquests informes es farà des de vessants diferents:

- Tasques relacionades amb informes pericials i de gestió de la prova electrònica:
    - Totes aquelles tasques i informes relacionades amb la formalització d'evidències electròniques i que poden ser usades en fases pericials com a mitjà de prova. També a petició dels serveis jurídics de la UOC per què puguin ser ratificats en judici per un pèrit informàtic.

- Tasques de prova electrònica o d'informàtica forense:
    - El servei disposarà de persones i tecnologia amb capacitats pericials per a processos en què es requereixi donar garanties de la cadena de custòdia d'actes administratius o d'evidències amb requeriments de tècniques d'anàlisi forense pericial (tecnologies de forense exhaustives amb cadenes de custòdia).
    - Aquest servei requereix d'alta especialització per personal indicat en el PCPI, Pèrit Judicial Forense informàtic. En aquest punt (Tasques de prova electrònica o informàtica forense) no es preveu un forense amb requeriments per defensar a la UOC amb actes probatòries per a requeriments o defenses en judici. Tan sols es tracta de donar resposta a requeriment judicials o interns requerits.
    - Forense: extracció d'informació rellevant pel cas que li sigui encomanat al contractista i què pot estar emmagatzemada en qualsevol dispositiu electrònic o en pàgines W3, fòrums d'Internet i deep web o correu electrònic. Respectant sempre el marc legal i els drets fonamentals de les persones.

- Tasques de peticions d'evidències i tècniques i informes forenses: L' adjudicatari, a petició de la UOC, realitzarà anàlisis forenses de determinats elements. En aquest sentit, haurà d'aplicar tècniques científiques forenses i analítiques sobre l'escenari d'un incident de seguretat.
    - Peticions formals d'informació/evidències tan a partir del sistema SIEM UOC com de diferents fonts d'informació estructurada o no (vg. Sistemes de fitxers)
    - Gestió de les cadenes de custòdia.
    - Clonats forenses. Entenent per tals aquells que són obtinguts mitjançant un mètode certificat i on una empresa tercera avala la obtenció de les dades.
    - Emmagatzemament i custòdia de suports d'informació i dades.
    - Investigació de successos informàtics sobre les fonts d'informació aportades.

- Quantificació no només dels danys informàtics soferts sinó també dels econòmics i reputacionals.
- Recuperació de dades esborrades, corruptes, en suports inestables o amagats, recuperació de dades enfront de desastres tipus Ransom.
- Realització de tots aquells procediments orientats a l'execució pel grup operatiu d'Operacions de Sistemes d'Informació, què siguin necessaris per a la generació d'imatges processables (disc i/o memòria) en qualsevol de les seves formes: màquina física, màquina virtual, servei de virtualització, cloud computing, contenidors, etc …
- Realització de tots aquells procediments orientats a l'execució de la captura, recollida i preservació d'evidències forenses en estacions de treball Windows, Linux o MacIntosh.
- Realització de tots aquells procediments orientats a l'execució de la captura, recollida i preservació d'evidències forenses en dispositius mòbils, tant Android com iOS.

Procediment davant d'una petició:

- La UOC farà la petició a l'adjudicatari amb els requeriments particulars sobre perfils i tasques a realitzar.
- L'adjudicatari haurà de fer una proposta en un termini màxim de 2 setmanes que posteriorment haurà de ser validada pels responsables de la UOC.

4.2.3.Exercicis de ciberseguretat

Es preveu la realització d'exercicis de ciberseguretat, que poden ser en mode competitiu tipus RedTeam vs. BlueTeam, on es posarà a prova la resiliència d'algun dels serveis de la UOC i la capacitat de reacció dels equips de resposta a incidents.

Aquests exercicis es decidiran anualment juntament amb el servei de suport de l'OSI, es dimensionaran en temps i en esforç.

L'adjudicatari, haurà de fer una proposta de perfils i de consums de recursos que la UOC validarà i repercutirà sobre aquesta partida alçada.

Entre altres exercicis podrien ser:

- Atacs de denegació de servei DoS/DDoS.
- Intrusió en equips core de la UOC.
- Simulacions de sustracció de dades de caràcter personal.
- Simulació d'un atac de Ransomware.
- Exercicis de phishing, spear phishing o smishing. Focalització amb persones clau de la UOC.
- Defacement i compromís de la imatge institucional.

Procediment davant d'una petició:

- La UOC farà la petició de col·laboració al proveïdor adjudicatari amb els requeriments particulars sobre perfils i tasques.

- El proveïdor adjudicatari haurà de fer una proposta en un termini màxim de 2 setmanes que posteriorment haurà de ser validada pels responsables UOC.

5. Model de relació

Estarà basat en la figura de l'interlocutor/coordinador únic entre l'adjudicatari i la UOC. Aquest interlocutor és fonamental per a acompanyar i donar suport en l'establiment de les polítiques, bones pràctiques i controls de seguretat en l'àmbit del servei.

5.1. Governança i reporting

El govern del servei de ciberseguretat gestionada ha de complir:

- Gestió centralitzada a nivell transversal i de tots els sub-serveis.
- Generació la capa de reporting a diferents nivells, tàctic i operatiu.
- Garantia de la implementació d'un Quadre de comandament (Dashboard) integral amb tots els indicadors identificats dels diferents subserveis.

5.2. Model organitzatiu de l'equip de treball

El present servei objecte de licitació ha de permetre certa autosuficiència a l'hora de contactar, gestionar i resoldre qualsevol tipus d'incidències o tasques de projectes que impliquin proveïdors externs, sense que la interlocució depengui exclusivament del responsables de la UOC.

Per donar resposta a les necessitats plantejades per la UOC, es demana tenir un model de relació basat en 3 nivells, amb l'objectiu de:

- Garantir el seguiment i bon govern del servei.
- Maximitzar el seu alineament a les necessitats estratègiques i operatives de la UOC mentre duri la prestació del servei.

Així doncs, aquest model organitzatiu es basa en l'establiment d'una relació entre l'adjudicatari i la UOC a tres nivells i comités:

- Nivell estratègic / Comité estratègic.
- Nivell tàctic / Comité tàctic.
- Nivell operatiu / Comité operatiu.

5.2.1. Nivell estratègic

Es defineix a nivell estratègic un comitè executiu que es reunirà de manera ordinària dues vegades l'any amb la finalitat de mantenir un punt de contacte a alt nivell per assegurar el bon funcionament del servei contractat. A aquest nivell, es proposa que per part de l'adjudicatari hi assisteixi com a mínim la persona responsable de compte, el/la coordinadora del servei, i per part de la UOC la persona responsable de la vicegerència a càrrec del servei, la persona responsable de seguretat i la persona responsable del servei.

Els/les assistents a aquest comitè tindran capacitat decisòria sobre els compromisos del mateix i en aquells aspectes que puguin originar la modificació del servei.

5.2.2. Nivell tàctic

Es proposen reunions mensuals per poder dur a terme un seguiment del servei i poder posar en comú els punts que es considerin necessaris exposar. Per part de l' adjudicatari, hi assistirà el coordinador del servei i, si fos necessari, un o més especialistes de servei que puguin aportar informació rellevant del servei. Per part de la UOC hi assistirà, la responsable de seguretat, el responsable del servei i, si fos necessari, els tècnics especialistes.

La finalitat d'aquestes reunions mensuals serà exposar:

- L'estat del servei.
- Les principals incidències que hagin sorgit o estiguin en actiu.
- La situació dels projectes i tasques en curs.
- Revisió del calendari previst.

5.2.3. Nivell operatiu

Es proposa una reunió setmanal de revisió tècnica tipus "clínic" per poder resoldre els temes més urgents que hi pugui haver i fer seguiment tècnic dels projectes i tasques. Per part del proveïdor adjudicatari hi assistirà el coordinador o els especialistes involucrats si ho vol delegar i per part de la UOC hi assistiran el responsable del servei i els tècnics especialistes de seguretat necessaris.

L'objectiu bàsic serà tractar les problemàtiques específiques que afectin al servei prestat.

5.3. Funcions i activitats dels nivells del model organitzatiu

Nivell estratègic / Comité estratègic:

- Seguiment i control de l'execució del contracte.
- Seguiment i avaluació del servei prestat. Analitzarà les necessitats del servei i podrà decidir ampliacions o reduccions del mateix.

- Validar l'abast general, objectius i resultats esperats.
- Validació de la planificació de les tasques previstes a realitzar.
- Verificació del compliment de les especificacions sol·licitades.
- Propostes de modificacions/ampliacions d'Acords de Nivell de Servei (ANS).
- Seguiment econòmic del contracte.
- Resolució de conflictes.
- Comunicació de penalitzacions i afectació en les properes facturacions si s'escau.
- Lliurables mínims esperats:
    - Abans de la convocatòria:
        - Assistents convocats.
        - Ordre del dia.
        - Documentació auxiliar.
        - Informes necessaris dels temes a tractar.
    - Després de la reunió:
        - Acta amb els acord assolits i la presa de decisions.
        - Convocatòria per la segunt reunió: data, hora i lloc.

Nivell tàctic:

- Validació de les tasques de control de l'explotació i implantació dels serveis.
- Revisió d'informes mensuals dels diferents serveis.
- Verificació de l'acompliment dels acords de servei establerts.
- Aprovació de projectes de millores.
- Seguiment de la realització de millores i evolució del servei regular.
- Verificació de l'acompliment dels ANS.
- Resolució de conflictes.
- Anàlisi i priorització de tasques.
- Validació dels procediments de millora per part dels Responsables de Seguretat.
- Anàlisi i control de l'ocupació dels perfils assignats per la consecució del servei (informe setmanal i acumulat mensual).
- Lliurables mínims esperats:
    - Abans de la convocatòria:
        - Assistents convocats.
        - Ordre del dia.
        - Documentació auxiliar.
        - Informes necessaris dels temes a tractar.

- Després de la reunió:
  - Acta amb els acord assolits i la presa de decisions.
  - Convocatòria per la següent reunió: data, hora i lloc.

Nivell operatiu:

- Seguiment rutinari.
- Propostes de millora i canvis.
- En cas d'identificar-se riscos o canvis significatius en l'evolució del servei es convoquen les reunions operatives per tractar el tema en qüestió.
- En cas d'evidenciar un risc elevat, es procedirà a convocar el Comitè Estratègic o al Comitè Tàctic segons es consideri.
- Anàlisi d'incidències detectades dels operadors que impliquen sol·licitar una reunió operativa.
- Anàlisi de peticions que impliquin un control detallat degut a un impacte tècnic, econòmic, d'execució, etc.
- El comitè podrà ser convocat per iniciativa tant de UOC com de l' adjudicatari. El comitè es constituirà en un màxim de 24h des del moment de la convocatòria.
- Lliurables mínims esperats:
  - Abans de la convocatòria:
    - Assistents convocats
    - Ordre del dia
    - Documentació auxiliar
    - Informes necessaris dels temes a tractar
  - Després de la reunió:
    - Acta amb els acord assolits i la presa de decisions.
    - Convocatòria per la següent reunió: data, hora i lloc

6. Prestació del servei

6.1. Horari

L'adjudicatari haurà de cobrir els horaris de dilluns a divendres entre les 09:00 AM i les 18:00 PM, inclòs el període vacacional on es mantindrà operatiu el servei.

L'adjudicatari cobrirà fora de l'horari laboral definit la recepció i resolució d'incidents de nivell crític alt.

Aquest horari no aplicarà pels serveis requerits 24x7x365 especifcats als serveis regulars.

6.2. Localització física

Preferentment, el servei es durà a terme des de les oficines de l'adjudicatari. La UOC facilitarà que l'adjudicatari realitzi la major part de les tasques i les reunions de forma virtual utilitzant eines de videoconferència, eines col·laboratives o de connectivitat segura tipus VPN.

A petició de la UOC, algunes reunions o actuacions seran de presencialitat obligada en alguna de les dependències de la UOC, ubicades a Barcelona. Entre altres poden ser:

- Les reunions de nivell estratègic, tàctic i operacional.
- Les incidències de seguretat de nivell alt.
- Les tasques que requereixin la realització d'entrevistes o recollida d'evidències físiques.
- I totes aquelles tasques en que no sigui possible l'ús de la virtualitat per la realització de les mateixes.

En qualsevol moment durant l'execució del contracte, la UOC es reserva el dret de sol·licitar que la prestació temporal del servei s'ubiqui a les seves instal·lacions o bé en alguna ubicació designada per la UOC.

Les despeses que puguin generar a l'adjudicatari aquestes reunions o presencialitat temporal aniran a càrrec del propi adjudicatari.

En cas de presencialitat, el servei es prestarà a una de les següents adreces:

- Seu institucional: Avinguda Tibidabo 39-43, 08035 Barcelona.
- Campus UOC: Rambla del Poblenou 154 i 156, 08018 Barcelona.

En el cas que la UOC, durant la vigència del contracte, fes un canvi de seu, d´alguna de les anteriors a un altre edifici, i sempre que aquesta nova ubicació estigui dins de la província de Barcelona, l'adjudicatari es compromet a cobrir el servei sense repercutir cap cost addicional a la UOC.

7 Recursos assignats al servei

El nombre de recursos assignats per part de l'adjudicatari s'haurà d'ajustar permanentment a les necessitats de la UOC, d'acord amb la volumetria del servei de seguretat expressada l'Annex de volumetries i en els serveis recurrents descrits en plec de prescripcions tècniques → **Annex I Infraestructura tecnològica i volumetria del servei.**

A continuació es detallen els perfils que l'adjudicatari haurà d'assignar al servei:

- Responsable de compte.
- Coordinador del servei de seguretat.
- Especialistes.
- Consultor de seguretat de la informació.

7.1. Responsable de Compte

L'adjudicatari designarà un únic responsable de compte que serà el referent per tots els contractes que tingui amb la UOC, serà el darrer responsable dels de la prestació dels serveis.

Aquesta figura es mantindrà durant tota la vida del contracte en la gestió comercial, durant l'execució del servei i fins a la devolució d'aquest, i serà l'interlocutor i responsable en cas que es produeixin canvis en l'abast o cost dels serveis que impliquin una modificació contractual.

7.2. Coordinador del servei de seguretat

Serà l'interlocutor únic davant de la UOC i serà el responsable de garantir que la prestació del servei és correcta. És a dir, garantirà el servei assegurant l'optimització del mateix i, per tant, minimitzant els possibles riscos.

Haurà de realitzar principalment les següents funcions:

- Garantir l'execució del servei, tal i com s'especifica en aquest plec, assegurant tots i cadascun dels temps de resposta demanats i que la UOC pugui requerir.
- Coordinar i supervisar de forma periòdica l'equip al seu càrrec, comunicant si s'escau els possibles canvis en aquest, així com les seves causes.
- Gestió dels riscos detectats així com la presentació del pla de mitigació dels mateixos.
- Detectar oportunitats de millora.
- Elaboració dels informes de servei i justificació del compliment dels ANS.
- Garantir la implementació del quadre de comandament del servei .
- Proposar i incorporar, si són acceptades, millores en la gestió global del servei.

En quant al recurs assignat, la UOC tindrà la potestat de demanar canvi sempre i quan, i de manera justificada, aquest no presti el servei de forma satisfactòria per la UOC.

L'adjudicatari es compromet a mantenir el coordinador durant la vigència del contracte, podent-lo substituir només per causes justificades. En aquest cas, la persona que el substitueixi haurà de complir amb la solvència requerida, sent la UOC qui validarà que el perfil s'ajusti a la solvència.

Per altra banda, l'adjudicatari haurà de sol·licitar per escrit qualsevol canvi en el perfil i amb una antelació suficient que garanteixi un correcte traspàs de coneixements per tal d'evitar afectacions en el servei. El canvi només podrà fer-se si prèviament s'ha validat per la UOC el compliment dels requisits de solvència anteriorment mencionats.

7.3. Especialistes

Els especialistes seran els tècnics assignats al servei per l'adjudicatari que duran a terme les tasques i actuacions que requereixin una especialització tècnica per poder garantir un resultat satisfactori.

L'equip de l'adjudicatari que prestarà el servei a la UOC comptarà amb treballadors que tinguin perfils d'especialistes al menys en els següents àmbits:

- Tècnic especialista en hacking ètic i pentesting.
- Analista de seguretat.
- Auditor en seguretat de la informació i continuïtat de negoci.
- Tècnic especialista en seguretat de la resposta a incidents de seguretat de la Informació.
- Professional certificat en seguretat de la informació en entorns cloud.
- Tècnic administrador de plataformes tecnològiques (SIEM).
- Tècnic especialista en informàtica forense i investigació interna

Tant el coordinador del servei com els perfils especialistes assignats al servei hauran de complir els requeriments expressats a l'apartat de solvència tècnica del PCP.

7.4 Consultor en seguretat de la informació

El perfil de consultor en seguretat de la informació o consultor en ciberseguretat és qui prestarà el servei de Suport a l'Oficina de Seguretat de la Informació de la UOC.

Aquest perfil ha de complir les següents capacitats o competències:

- Coneixement profund en les millors pràctiques de seguretat de la informació i les tendències actuals en ciberseguretat.
- Capacitat per avaluar riscos i definir estratègies de mitigació.
- Coneixement de les regulacions de seguretat de la informació rellevants com RGPD.
- Capacitat per traduir problemes tècnics en termes de comprensibles per les persones no tècniques.
- Habilitat per analitzar situacions complexes de seguretat i trobar solucions efectives.
- Capacitat demostrada per crear informes de executius clars i concisos que resumeixin troballes o recomanacions de seguretat de manera comprensible per l'alta direcció o altres stakeholders.
- Habilitat per presentar dades tècniques i mètriques de seguretat de manera visualment atractiva mitjançant gràfics i taules.
- Experiència en la redacció d'informes d'avaluació de riscos i documentació tècnica que recolzi la presa de decisions informades en seguretat de la informació.
- Capacitat per gestionar una crisi en cas d'incident greu de seguretat.
- Compromís amb l'aprenentatge constant i l'actualització de coneixements, donat que la ciberseguretat és un camp en constant evolució.

8. Fases de la prestació del servei

Tot seguit es descriuen les fase de la prestació del servei i una durada aproximada de les mateixes:

- **Fase de transferència del servei**
  S'entèn per fase de transferència del servei el període que va entre l'entrada en vigor del contracte adjudicat al nou contractista i el moment que aquest assumeix el servei de forma efectiva.

- **Fase de transició del servei**:
  S'entèn per transició quan l'adjudicatari inicia l'assumpció del servei, amb l'acompanyament de l'adjudicatari sortint, i fins que l'adjudicatari sortint deixa el servei i es comença a aplicar els nous ANS citats en el punt 9.

- **Fase regular**
  S'entèn per fase regular quan un cop finalitzada la fase de transició el contractista passa a prestar el servei en les condicions que s'especifiquen en aquesta licitació.

- **Fase de devolució del servei**:
  S'entèn per devolució del servei totes aquelles accions precises per tal de traspassar en condicions òptimes tot el servei sense cap merma ni pèrdua de funcionalitats al nou adjudicatari a la finalització o extinció prematura d'aquest contracte.

Les fases de transferència i transició del servei conjuntament tenen una duració d'un màxim de DOS MESOS a partir de la data de la signatura del contracte.

8.1. Fase de transferència.

La fase de transferència del servei començarà a partir de la formalització del contracte.

Definim:

- Adjudicatari entrant: és el nou proveïdor del servei
- Adjudicatari sortint: és l'antic proveïdor del servei

Aquesta fase no s'executarà en el cas que l'adjudicatari entrant i l'adjudicatari sortint siguin la mateixa empresa. En aquest cas, l'adjudicatari sí haurà de realitzar la due diligence, tal com s'explica més endavant, i elaborar el pla de transició cap al nou model de servei.

En aquesta fase es produeix la transferència del servei per part de l'actual adjudicatari del servei. L'adjudicatari entrant farà presa de contacte amb el servei, per visualitzar la seva forma de treball, procés d'escalat i forma d'interactuar.

Durant aquesta fase l'adjudicatari entrant rep la transferència del servei per part de l'adjudicatari sortint, i del responsable del servei de la UOC. Aquesta fase durarà un màxim d'un mes i mig a partir de la data d'inici del contracte.

L'adjudicatari sortint serà el responsable del servei complet durant aquest període. Durant aquesta fase el nou contractista rebrà tota la documentació de traspàs necessària i tindrà el suport del contractista actual, què facilitarà i col·laborarà en el traspàs de coneixement. Tanmateix, la UOC facilitarà a l'adjudicatari tota la informació dels actius i recursos implicats, detall dels serveis actuals, tecnologies, xarxes, infraestructures, coneixement del negoci, etc, Igualment, la UOC organitzarà el procés d'accés als usuaris per tal de coordinar-lo de la forma més eficaç possible.

Al finalitzar la fase, el nou contractista presentarà un pla de transició a mode de due diligence que indiqui les tasques a assolir el más aviat possible per assegurar la correcta assumpció dels serveis.

La realització de la due diligence del servei serà responsabilitat de l'adjudicatari entrant i es portarà a terme independentment de que l'adjudicatari entrant sigui el mateix que el sortint, de cara a preparar la transició cap al nou model de servei.

Els resultats i les conclusions de la due diligence seran lliurades a la UOC, les quals podran incorporar nous paràmetres i indicadors a la gestió del servei, sempre amb el vist i plau de la UOC i sense afectar als ANS requerits al plec.

La transferència de serveis entre contractistes serà responsabilitat del nou contractista entrant, tot i que el sortint col·laborarà plenament perquè la transferència afecti al mínim el funcionament del servei actual. Per garantir aquesta col·laboració, la UOC supervisarà els processos i les negociacions de la transferència.

Durant aquesta fase de transferència s'establirà una formació específica a càrrec del contractista sortint. De la mateixa manera, es lliurarà i informarà del contingut de tota la informació generada durant el servei actual per part del contractista sortint.

En aquells casos en què no hi hagi documentació prèvia necessària per a prestar el servei, el contractista haurà de planificar i executar la seva elaboració, d'acord amb els responsables UOC, i sense cap cost addicional per la UOC.

El contractista entrant té la obligació de generar documentació de totes les activitats del procés de transició i lliurar-la als responsables UOC tan aviat com acabi aquest.

Els resultats i les conclusions d'aquest pla de transferència seran lliurades a la UOC, les quals podran incorporar, de forma suficientment justificada en funció dels resultats, canvis en:

- Les volumetries
- Les planificacions i els terminis
- Els ANS

La UOC mostrarà el seu acord o desacord amb les conclusions i els canvis proposats. En qualsevol cas serà la UOC qui decideixi justificada i raonadament, finalment, quins canvis i quines consideracions considera acceptades. Aquestes conclusions o consideracions tindran caràcter vinculant pel contractista.

La dedicació i els recursos usats pel nou contractista dedicats al traspàs de coneixements i assimilació del nou entorn i característiques del servei seran sense cap cost addicional per la UOC.

A la finalització d'aquesta fase, l'adjudicatari haurà de disposar d'un pla, aprovat per la UOC, que implementarà paral·lelament a la fase de transició del servei.

Aquest pla de transició haurà de contemplar al menys:

- Un pla de transferència del coneixement
- Un pla de procediments i normatives tècniques. Amb revisió i canvis en els repositoris si s'escau.
- Definició acurada del model de relació, governança i informes definint els graus de participació del contractista sortint i de la UOC.
- Pla d'implantació dels nous ANS
- Planificació de la incorporació de recursos, definint actors, rols i responsabilitats per cadascun dels serveis definits al paràgraf 4.
- Pla de riscos i contingència durant la transició, què permetin garantir la continuïtat dels serveis.
- La definició dels recursos tècnics i humans què es posaran a disposició durant l'execució del servei.

8.2. Fase de transició

Al finalitzar la transferència, l'adjudicatari entrant assumirà el servei, quedant l'equip tècnic de l'adjudicatari sortint com acompanyament del servei, donant suport a l'adjudicatari entrant en la prestació del servei. A partir d'aquesta data, i durant 15 dies, l'adjudicatari entrant serà el responsable del servei, però sense que aquest pugui estar sotmès a penalitzacions.

L'adjudicatari sortint haurà de:

- Prestar suport funcional i tecnològic al nou equip de treball
- Portar una reunió de final de prestació amb la UOC i l'adjudicatari entrant

L'objectiu d'aquesta fase és la d'arribar a assumir el servei de manera regular per part de l'adjudicatari entrant. Un cop finalitzat aquest període, l'adjudicatari entrant assumirà plenament el servei i es compromet a complir tots els acords de nivell de servei demanats en aquest plec.

Com en la fase de transferència, totes les parts implicades (adjudicatari sortint, adjudicatari entrant i la UOC) faran les reunions i feines conjuntes presencials necessàries per garantir una transició adequada.

L'adjudicatari entrant podrà fer propostes de nous elements per a la gestió i seguiment del servei o proposar millores en el servei, i la seva implantació dependrà de l'aprovació per part de la UOC.

La durada d'aquesta fase serà de 15 dies i començarà amb la signatura del document d'acceptació del servei per part de l'adjudicatari entrant i la UOC, just en acabar la fase de transferència.

A l'igual que la fase de transferència, la fase de transició tampoc s'executarà en el cas que l'adjudicatari entrant i l'adjudicatari sortint siguin la mateixa empresa.

8.3. Fase regular

La fase regular s'inicia un cop acabades totes les tasques de la fase anterior 8.2. i s'estén fins l'extinció del contracte i abans de la fase de devolució del servei.

Tal com es descriu a l'apartat 5, el contractista haurà de funcionar en base al model i criteris descrits. Totes les activitats que, com a mínim, haurà de realitzar es descriuen a l'apartat 4 de descripció del servei i els acords de nivell de servei i penalitzacions queden descrites a l'apartat 9.

Addicionalment l'adjudicatari haurà de presentar propostes que permetin assegurar l'evolució del servei tant des del punt de vista tecnològic, com de governança o incorporació de noves funcionalitats i tasques al servei.

Els mecanismes d'evolució han d'incloure informació detallada sobre les pautes d'activació, els instruments de seguiment, integració de tasques i procediments de forma tant reactiva com proactiva per part de l'adjudicatari.

A banda dels criteris generals, els mecanismes d'evolució han de tenir en compte la incorporació de noves funcionalitats que no s'hagin previst inicialment o que l'evolució del mercat i de la demanda facin que la UOC decideixi incorporar-les (nous serveis al núvol, noves aplicacions, nous serveis de ciber-intel·ligència, etc ...).

8.4. Fase de devolució del servei

L'adjudicatari inclourà en la seva proposta un pla de devolució del servei detallat que inclogui i descrigui:

- Les obligacions i tasques que hauran de ser desenvolupades per cadascuna de les parts en relació amb la devolució.
- Els termes i condicions en que es realitzarà aquesta devolució.

El disseny d'aquest pla de devolució és una obligació adquirida pel contractista en signar el contracte i es farà sense cap càrrec addicional per la UOC. Estarà basat en la seva proposta tècnica presentada en el sobre 2.

El pla de devolució haurà de complir amb els següents principis i continguts:

- El termini d'execució serà de 2 mesos des de la notificació oficial d'expiració o cancel·lació, total o parcial del servei. L'adjudicatari haurà de posar en pràctica el pla de

devolució que hagi inclòs en la seva oferta. La UOC es reserva el dret de reduir o augmentar aquest termini de 2 mesos si es pot posar en risc l'execució del servei.

- Haurà d´incloure la metodologia de transferència de coneixement dels aspectes fonamentals d'operacions i projectes en curs i que, com a mínim, descriurà:
    - L'assistència, la formació i la documentació sobre els procediments de negoci o sistemes de seguretat de la UOC al nou proveïdor adjudicatari.
    - L'accés al maquinari, el programari, la informació, la documentació i altre material utilitzat pel proveïdor adjudicatari o la UOC en la provisió del servei.
    - La formació pràctica tutelada, en la qual el personal designat per la UOC realitzi els treballs propis de cada procés o funcionalitat, tutelats pel personal del proveïdor adjudicatari.
- L'adjudicatari haurà d'oferir tota l'ajuda en la transferència a la UOC, o a terceres parts anomenades per ell mateix, dels serveis subcontractats, garanties o contractes de manteniment existents, fins al moment de la terminació en els mateixos termes pactats amb els adjudicataris d'aquest.
- Durant el primer mes i mig de la fase de devolució el proveïdor adjudicatari serà completament responsable de mantenir els mateixos nivells de servei que en la fase regular del servei.
- Durant els darrers 15 dies de la fase de devolució l' adjudicatari sortint acompanyarà al nou adjudicatari i donarà suport amb els següents recursos mínims, garantint la cobertura a tots els àmbits tecnològics actuals:
- L'adjudicatari haurà d'oferir un pla per definir les responsabilitats i gestionar la resolució de problemes entre el nou proveïdor adjudicatari i la UOC.
- Durant el primer mes del període de devolució del servei, l'adjudicatari sortint seguirà sent responsable de l'acompliment dels acords de nivell de servei. El pla de devolució no ha de causar cap discontinuïtat en el servei.

9 Resolució d'incidències

L'adjudicatari tindrà l'obligació d'informar en un termini no superior a una hora i a una bústia de correu electrònic de la UOC, que es comunicarà oportunament, de les incidències que es puguin produir en el desenvolupament de les prestacions contractuals tot indicant el motiu de les mateixes i el temps estimat de resolució.

10. Acords de Nivell de Servei Requerits (ANS)

Per poder personalitzar alguns ANS s'estableix un criteri de Criticitat de la Incidència, diferenciant així les considerades com a crítiques de les que no ho són:

Incidència crítica:

- Aquelles incidències que tenen un impacte considerable (afectació a la confidencialitat, disponibilitat i la integritat) en serveis i dades considerades crítics per a l'activitat de l'organització. Tot allò que, des del punt de vista de la seguretat informàtica, afectant a un servei provoqui una indisponibilitat o interrupció del mateix, implicant així una aturada en l'operativa normal de funcionament.

- Es classificaran també amb un nivell crític els incidents en els que es tingui constància de l'existència d'una amenaça que ha afectat o està afectant a sistemes TIC de la UOC i se sap que ha tingut un impacte més que considerable (afectació total de la confidencialitat, disponibilitat o la integritat) en informació considerada crítica per a la missió de la UOC i/o dels sistemes TIC crítics dins l'arquitectura de sistemes UOC.

Incidència no crítica:

- Tota la resta

10.1. ANS

10.1.1. Detecció, anàlisi i gestió de les vulnerabilitats

Descripció ANS	Càlcul	Periodicitat del càlcul	Llindar de compliment	Penalització	Codi
Notificació immediata de deteccions amb risc crític, molt alt i alt cap al responsable del servei segons procediment.	Diferència entre vulnerabilitats presents als informes i notificacions efectuades.	S'avaluarà el càlcul mensualment.	Immediat en tenir confirmació de la detecció.	1% facturació mensual	ANS_VUL_01
Lliurament d'informes d'alertes de vulnerabilitats detectades i gestionades.	Presentació de l'informe abans del cinquè dia laborable de cada mes.	S'avaluarà el càlcul mensualment.	Mensualment abans del 5è dia laborable de cada mes.	0,5% facturació mensual	ANS_VUL_02
Temps de resposta a la petició sota demanda d'un anàlisi de vulnerabilitats (puntual).	Dies transcorreguts entre la demanda i la resposta rebuda del contractista.	S'avaluarà el càlcul mensualment.	5 dies laborables.	0,5% facturació mensual	ANS_VUL_03
Lliurament d'informes.	Dies transcorreguts entre la finalització de les tasques d'anàlisi de resultats i el lliurament de l'informe tècnic i executiu.	S'avaluarà el càlcul mensualment.	7 dies laborables.	0,5% facturació mensual	ANS_VUL_04
Disponibilitat del servei.	Diferència entre el nombre d'escanejos actius previstos i el nombre d'escanejos actius ja realitzats	S'avaluarà el càlcul mensualment.	Inferior a 4.	1% de la facturació mensua	ANS_VUL_05

10.1.2. Auditories tècniques de ciberseguretat, pentest i hacking ètic

Descripció ANS	Càlcul	Periodicitat del càlc	Llindar de compliment	Penalització	Codi
Temps de resposta a la petició sota demanda.	Temps transcorregut entre la recepció per part del contractista de la petició i la resposta detallada del mateix.	S'avaluarà el càlcul mensualment.	5 dies laborables.	0,5% facturació mensual	ANS_AUD_01
Notificació immediata de deteccions amb risc crític, molt alt i alt cap al responsable del servei segons procediment.	Diferència entre vulnerabilitats presents als informes i notificacions efectuades.	S'avaluarà el càlcul mensualment.	Immediat en tenir confirmació de la detecció.	1% facturació mensual	ANS_AUD_02
Lliurament d'informes.	Dies transcorreguts entre la finalització de les tasques d'anàlisi de resultats i el lliurament de l'informe tècnic i executiu.	S'avaluarà el càlcul mensualment.	7 dies laborables per l'informe executiu. 10 dies laborables per l'informe tècnic.	0,5% facturació mensual	ANS_AUD_03

10.1.3. Monitorització de seguretat, detecció i resposta primerenca d'incidents i amenaces

Descripció ANS	Càlcul	Periodicitat del càlcul	Llindar de compliment	Penalització	Codi
Temps màxim de resposta per incidències Crítiques	Temps objectiu transcorregut entre que es detecta/notifica fins que es genera una resposta del servei.	S'avaluarà el càlcul mensualment	30 minuts 60 minuts > 60 minuts	5% facturació mensual 10% facturació mensual 25% facturació mensual	ANS_SOC_01

Temps màxim de resposta per incidències NO Crítiques.	Temps objectiu transcorregut entre que es detecta/notifica fins que es genera una resposta del servei.	S'avaluarà el càlcul mensualment.	120 minuts.	1% facturació mensual	ANS_SOC_02
Temps màxim de realització d'anàlisis preliminars per incidències crítiques.	Temps objectiu transcorregut entre que es detecta/notifica fins que es lliura el primer anàlisi.	S'avaluarà el càlcul mensualment.	180 minuts.	1% facturació mensual	ANS_SOC_03
Temps màxim de realització d'anàlisis preliminars per incidències NO crítiques.	Temps objectiu transcorregut entre que es detecta/notifica fins que es lliura el primer anàlisi.	S'avaluarà el càlcul mensualment.	5 hores (laborals).	0,5% facturació mensual	ANS_SOC_04
Temps màxim de lliurament d'informes de tancament en cas d'incidències crítiques.	Temps objectiu transcorregut entre que es tanca l'incident fins que es lliura l'informe.	S'avaluarà el càlcul mensualment.	8 hores (laborals).	0,5% facturació mensual	ANS_SOC_05
Temps màxim de lliurament d'informes en cas de declaració de bretxa de seguretat (RGPD).	Temps objectiu transcorregut entre que es detecta/notifica la bretxa fins que es lliura l'informe.	S'avaluarà el càlcul mensualment.	40 hores naturals.	25% facturació mensual	ANS_SOC_06
Informe mensual d'activitat i resum del servei.	Presentació de l'informe abans del cinquè dia laborable de cada mes.	S'avaluarà el càlcul mensualment.	Amb anterioritat al 5e dia laborable de cada mes.	0,5% facturació mensual	ANS_SOC_07

10.1.4. Administració i evolució de la plataforma SIEM UOC

Descripció ANS	Càlcul	Periodicitat del càlcul	Llindar de compliment	Penalització	Codi
Percentatge de temps en servei del servei SIEM. Disponibilitat.	Temps en que la màquina està uptime	S'avaluarà el càlcul mensualment	> 99,9% del temps total mensual en minuts	3% facturació mensual	ANS_SIEM_01
Pèrdua de LOGs	Gap entre LOGs no explicable excepte per pèrdua de la ingesta.	S'avaluarà el càlcul setmanalment	120 minuts	1% facturació mensual	ANS_SIEM_02
Temps màxim de realització d'anàlisis preliminars per incidències crítiques	Temps objectiu transcorregut entre que es detecta/notifica fins que es lliura el primer anàlisi	S'avaluarà el càlcul mensualment	180 minuts	0,5% facturació mensual	ANS_SIEM_03
Presentació dels informes de control de les activitats realitzades.	Informe lliurat als responsables UOC.	S'avaluarà el càlcul mensualment	2 informes per mes	0,5% facturació mensual	ANS_SIEM_04

10.1.5. Administració i evolució de la plataforma EDR i antivirus UOC

Descripció ANS	Càlcul	Periodicitat del càlcul	Llindar de compliment	Penalització	Codi
Lliurar informes amb el detall i periodicitat acordades.	Presència dels informes mensuals i KPIs associats segons és descriu a 4.1.5.	S'avaluarà el càlcul mensualment.	1 informe mensual	1% facturació mensual	ANS_EDR_01
Revisió del correcte funcionament de les sondes i agents EDR en servidors.	Notificació de les revisions als responsables UOC.	S'avaluarà el càlcul setmanalment.	Notificació escrita	1% facturació mensual	ANS_EDR_02

Gestió de les vulnerabilitats proporcionades pel servei EDR sobre equips sota control.	Presentació de l'informe abans del cinquè dia laborable de cada mes.	S'avaluarà el càlcul mensualment.	Mensualment abans d 5e dia laborable de cada mes.	0,5% facturació mensual	ANS_EDR_03

Signa,

Sra. Clara Beleña Luis
Directora de l'Oficina de Seguretat de la Informació