Contractació d'un servei de plataforma per a la gestió de programes de recompensa per errors (*bug bounty*) als sistemes d'informació del sector públic de Catalunya

CO-01-2024

Salvador Espriu, 45-51
08908 L'Hospitalet de Llobregat
Tel. 93 557 42 40

Índex

1. Introducció

1.1. L'Agència de Ciberseguretat de Catalunya

L'Agència de Ciberseguretat de Catalunya (en endavant, Agència) és una entitat de dret públic de l'Administració de la Generalitat de Catalunya que actua amb plena autonomia orgànica i funcional, objectivitat i independència tècnica i professional, i resta adscrita al Departament de la Presidència de la Generalitat de Catalunya.

L'Agència actua en compliment de la Llei 15/2017 de 25 de juliol de 2017, de l'Agencia de Ciberseguretat de Catalunya.

L'Agència és l'ens públic que succeeix a la Fundació Centre de Seguretat la Informació de Catalunya (CESICAT), creada l'any 2010, arran de l'acord de govern GOV/50/2009 del 17 de març i se subroga en el convenis i contractes subscrits de l'Agència, amb data 1 de gener de 2020, en virtut d'allò establert a la disposició addicional segona de la Llei 15/2017, del 25 de juliol, de l'Agència de Ciberseguretat de Catalunya, així com el Decret 223/2019, de 29 d'octubre, pel qual s'aproven els Estatuts de l'Agència, que detalla els béns i actius que s'adscriuen a l'Agència, així com els drets i obligacions a què l'Agència se subroga.

Aquest marc legislatiu estableix que l'Agència és l'entitat encarregada d'executar i de governar les polítiques públiques i l'estratègia en matèria de Ciberseguretat de la Generalitat de Catalunya, sent l'organisme que governa la Ciberseguretat del sector públic a Catalunya.

L'Agència com a encarregada d'establir i de liderar el servei públic de ciberseguretat, té com a objectiu garantir una Societat de la Informació segura i confiable per al conjunt de la ciutadania catalana i de la seva Administració Pública, amb la voluntat d'esdevenir un referent a nivell nacional i internacional en matèria de ciberseguretat.

Com a organisme competent en matèria de ciberseguretat, l'Agència es responsabilitza de l'establiment i el seguiment dels programes d'actuació en matèria de ciberseguretat, sota la direcció estratègica del Govern de la Generalitat de Catalunya, en coordinació amb les entitats del sector públic de l'Administració de la Generalitat de Catalunya, i col·laborant amb governs locals de Catalunya, centres sanitaris, entitats del sector educatiu, universitats i centres de recerca, entre d'altres.

En les funcions que li són pròpies, l'Agència és l'ens idoni per gestionar les tasques necessàries per assolir aquest objectiu de protecció de la informació i la infraestructura TIC de les institucions i ciutadania de Catalunya i, en especial la del Govern de la Generalitat.

1.2. Context del Servei

Mentre els programes de recompensa per errors (*bug bounty*) són habituals en entorns corporatius o privats, encara no són una pràctica habitual en el sector públic. En aquesta línia, el 2016 va tenir lloc el primer programa de *bug bounty* del govern dels EUA, "Hack the Pentagon", una pràctica que va esdevenir exitosa i que encara es du a terme a dia d'avui. A la UE, els Països Baixos han estat pioners des del 2013, però no ha estat fins el 2019, amb el *bug bounty* EU-FOSSA 2, que la UE va endegar un programa destinat a detectar errors en el programari obert utilitzat per les institucions europees.

A l'estat espanyol, el mes de desembre de 2020, l'Agència juntament amb la Direcció General d'Atenció Ciutadana van ser pioners a l'hora de posar en marxa una prova pilot de *bug bounty* sobre un conjunt d'actius de la Generalitat de Catalunya. L'exercici va servir per posar a prova l'ús d'aquest tipus de programes en el sector públic de Catalunya, ja que serveixen per identificar vulnerabilitats en els sistemes d'informació i prevenir possibles escletxes de seguretat.

Així, al llarg de dues setmanes, un nombre restringit de reputats professionals de la ciberseguretat, entre els qual hi figuraven alguns dels *hackers* ètics més ben valorats al món, hi van participar de manera desinteressada a través d'una invitació personal i exclusiva. L'equip de resposta a incidents Catalonia-CERT de l'Agència va supervisar activament tot el desenvolupament de la prova pilot amb la validació de les vulnerabilitats identificades i la gestió de la seva corresponent solució per evitar possibles atacs en un futur.

Malgrat l'abast limitat de la prova pilot, en durada i quantitat d'actius a analitzar, els resultats van constatar que un programa de *bug bounty* és un mecanisme idoni per incentivar la participació dels experts en ciberseguretat de la societat civil en el reforç de la seguretat dels sistemes d'informació de l'administració pública. Els investigadors de ciberseguretat participants en la recerca van informar de cinc vulnerabilitats: dues presents en webs de la Generalitat i tres en aplicacions corporatives, fet que va permetre procedir a la seva verificació i resolució.

A partir d'aquesta experiència positiva, l'Agència ha incorporat l'ús d'una nova eina per aconseguir uns sistemes d'informació del sector públic de Catalunya: els programes de *bug bounty*. Al mateix temps, aquests programes esdevenen un mecanisme per incentivar i donar visibilitat al talent en ciberseguretat, així com apropar l'administració pública a la participació ciutadana.

2. Un servei per a la gestió de programes de recompensa per errors (*bug bounty*) als sistemes d'informació del sector públic de Catalunya

2.1. Objecte i context

El compromís de la Generalitat de Catalunya per oferir els millors serveis públics possibles a la ciutadania i empreses comporta l'obligació de transformar-se digitalment, adoptar noves tecnologies i orientar els processos a la dada. Ara bé, al mateix temps que els entorns digitals complexos creixen, també ho fa el nivell de ciberamenaça, ja que augmenta el risc que apareguin vulnerabilitats que puguin ser explotades per un ciberatacant.

En ciberseguretat, una vulnerabilitat és una feblesa d'un sistema informàtic que posa en risc la seva seguretat i pot permetre que un atacant en comprometi la informació. Segons la llista CVE (*Common Vulnerabilities and Exposure*), el 2023 se'n van identificar 29.065[1], un 16% més que el 2022. El nombre de deteccions de vulnerabilitats en software i hardware segueix una tendència creixent, i augmenta al mateix temps que es desenvolupa la societat digital amb la incorporació de noves tecnologies com els sistemes al núvol, el 5G, l'IoT o la intel·ligència artificial.

Per fer front a aquesta amenaça cibernètica, actualment es duen a terme accions com els escanejos de vulnerabilitats i les anàlisis de *pentest*. No obstant això, són proves que presenten certs reptes: poden resultar insuficients, ja que estan limitades en el temps i els recursos dedicats són limitats; la periodicitat entre anàlisis pot resultar massa baixa si es vol garantir un nivell de seguretat continuat; i el desconeixement dels elements de *shadow IT* (software o hardware fora del control dels serveis de TI) dificulta fixar un abast prou complet.

Per aquest motiu, l'Agència considera convenient complementar les anàlisis de seguretat tradicionals amb la realització de programes de recompensa per errors (*bug bounty*), de manera que es donarà accés controlat a actius específics del sector públic de Catalunya a un conjunt d'investigadors de seguretat informàtica especialitzats en la detecció de vulnerabilitats.

Els programes de *bug bounty* són iniciatives d'empreses o organitzacions que ofereixen recompenses a investigadors de seguretat (hackers ètics) per identificar i informar de vulnerabilitats en els seus sistemes, aplicacions o llocs web. L'objectiu principal és detectar i corregir vulnerabilitats abans que siguin explotades per ciberdelinqüents, millorant així la seguretat de manera proactiva i incentivant la col·laboració de la comunitat de ciberseguretat. El funcionament es basa en la publicació del programa amb les seves regles i abast, la investigació per part dels hackers ètics, la notificació de vulnerabilitats trobades, i finalment la verificació per part de l'empresa, que recompensa l'investigador segons la gravetat de l'error. Aquests programes són una eina clau per reforçar la seguretat digital de manera col·laborativa i eficaç.

Amb aquesta iniciativa, l'Agència donarà resposta als reptes que plantegen les anàlisis tradicionals; s'incrementarà la potència per identificar possibles vulnerabilitats gràcies a la participació de tota una comunitat d'investigadors; es garantirà la supervisió continuada de la seguretat per mitjà de programes de llarga durada; i s'assegurarà que tota la infraestructura està dins de l'abast de la recerca gràcies al plantejament flexible dels programes.

Més enllà de ser una eina de millora de la seguretat cibernètica, els programes de *bug bounty* conformen una solució molt rendible, ja que el cost és proporcional a les vulnerabilitats

[1] https://www.cvedetails.com/vulnerability-list/year-2023/vulnerabilities.html?page=1&order=1&trc=29065&sha=9394f1baca42a3ef74adb541404db24e1859fcef

descobertes. Així mateix, els programes *bug bounty* permeten incentivar i donar visibilitat al talent en ciberseguretat existent entre la població i contribueixen a crear una cultura d'obertura, transparència i responsabilitat.

2.2. Descripció del servei

L'Agència requereix un servei de plataforma per a la gestió de programes de recompensa per errors (*bug bounty*) sobre els actius del sector públic de Catalunya.

L'adjudicatari serà responsable de gestionar la participació de la comunitat d'investigadors i dur a terme les tasques necessàries per garantir l'èxit de les diferents fases de desenvolupament dels programes *bug bounty* que es despleguin durant l'execució del contracte (veure apartat 2.5):

1. Definició de la política del programa.
2. Activació del programa.
3. Recollida dels informes de vulnerabilitats.
4. Triatge dels informes de vulnerabilitats.
5. Pagament de les recompenses.
6. Supervisió i validació de la resolució de les vulnerabilitats.

Fases del servei per a la gestió de programes de recompensa per errors (bug bounty)

L'Agència serà responsable de la definir la política del programa, activar el programa, validar el pagament de les recompenses i sol·licitar la validació de les solucions de les vulnerabilitats.

L'adjudicatari serà responsable de recollir els informes de vulnerabilitats, fer-ne el triatge, executar el pagament de les recompenses després de la validació de l'Agència i supervisar la validació de la resolució de les vulnerabilitats.

Per al correcte desenvolupament de les seves responsabilitats, l'adjudicatari haurà de disposar d'un equip gestor per atendre les necessitats de l'Agència i fer-se càrrec de la interacció amb els investigadors, disposar també d'un equip de triatge per recollir, revisar i tramitar els informes de vulnerabilitats generats pels investigadors, així com subministrar una

plataforma en línia per a la gestió de tota l'activitat vinculada als programes en curs (veure apartats 2.6 i 2.7).

2.3. Objectius del servei

— Millorar la seguretat cibernètica del sector públic de Catalunya maximitzant el rendiment de la inversió econòmica realitzada.

— Realitzar anàlisis de vulnerabilitats eficaços, freqüents, àgils i dinàmiques, amb l'objectiu de mitigar les limitacions que presenten les pràctiques de ciberseguretat tradicionals:

  - Els escanejos automàtics sovint no detecten vulnerabilitats lògiques, configuracions errònies específiques del context i fallades de seguretat complexes que requereixen comprensió humana o interaccions personalitzades.
  - Les pràctiques i tests de seguretat en el codi (*Security-by-default*) sovint són insuficients per garantir l'absència de vulnerabilitats.
  - Els temps entre les proves de *pentest* i el *Go-To-Market* resulten excessivament elevats i endarrereixen el desenvolupament de nous desenvolupamets.
  - Els elements de *shadow IT*, fora del conjunt d'actius coneguts, sovint queden fora de l'abast de les anàlisis de seguretat.

— Incentivar la creació d'una cultura de ciberseguretat col·laborativa dins dels organismes i entitats del sector públic de Catalunya.

— Promoure la transparència i la participació ciutadana per a la millora de la ciberseguretat dels actius digitals del sector públic de Catalunya.

— Identificar i mobilitzar el talent existent en matèria de ciberseguretat entre la ciutadania per donar suport a les iniciatives de l'Agència, amb especial focus als experts de Catalunya.

2.4. Abast del servei

— L'adjudicatari proveirà:

  - L'organització d'un nombre il·limitat de programes de *bug bounty*.
  - El triatge d'un màxim de 500 informes de vulnerabilitats.

— L'adjudicatari disposarà d'una bossa econòmica dedicada exclusivament al pagament de les recompenses als investigadors.

2.5. Desenvolupament d'un programa *bug bounty*

2.5.1. Definició de la política del programa

— L'Agència definirà la política dels diferents programes i, en tots els casos, serà imprescindible la seva validació abans de l'activació dels programes.

— La política dels programes serà un document viu, de manera que en qualsevol moment es podran acordar modificacions, establir limitacions o flexibilitzar les normes establertes.

— La política de cada programa haurà d'estar disponible en línia a la plataforma web subministrada per l'adjudicatari perquè els investigadors la puguin consultar en qualsevol moment.

— A continuació, s'especifica un conjunt de criteris per a la definició d'una política genèrica de referència, tot i que l'adjudicatari podrà suggerir modificar-los en benefici del servei.

Abast i definició dels actius a analitzar

- L'Agència acordarà els actius a testejar amb els titulars/responsables corresponents.
- Els actius poden consistir en adreces IP, pàgines web, apps, API, infraestructures, etc. Ja sigui en entorns productius o de preproducció.
- Addicionalment, es podran especificar actius que quedin expressament exclosos de l'abast del programa.
- Els actius es podran categoritzar en funció del grau de preocupació que inspirin. Es definiran com a mínim 2 categories de criticitat per a cada actiu ($Valor_{Actiu}$):

Nivell de l'actiu	$Valor_{Actiu}$
Categoría B	1
Categoría A	2

Taula de categorització dels actius (exemple amb nivells A i B, amb valors de 2 i 1 respectivament, de més a menys preocupació)

- Aquesta categorització dels actius permetrà prioritzar la recerca dels investigadors sobre aquells que tinguin un valor més alt. Això beneficiarà la resolució de vulnerabilitats allà on la preocupació pels sistemes d'informació és més alta i el dany potencial d'un ciberatac seria més gran.

Vulnerabilitats a analitzar

- L'adjudicatari detallarà la tipologia de vulnerabilitats que puguin afectar els sistemes i es que es consideraran vàlides de cara a l'obtenció de recompensa (p. ex. execució remota de codi -RCE-, fuita de dades, XSS, suplantació d'identitat, etc.).
- L'adjudicatari detallarà la tipologia de vulnerabilitats no incloses al programa, és a dir, que no es consideraran vàlides de cara a l'obtenció de recompensa. P. ex:
  - Vulnerabilitats explotables amb tècniques d'enginyeria social.
  - Vulnerabilitats dependents de versions de navegador obsoletes.
  - Vulnerabilitat CSRF sense impacte o sense prova de concepte que en demostri l'impacte.
  - Atacs de tipus *Man-in-the-Middle* o que requereixin accés físic a l'equip de l'usuari.
  - Atacs d'injecció de *Comma Separated Values* (CVS) sense demostrar una vulnerabilitat.
  - Atacs de DoS/DDoS.
  - Absència de bones pràctiques en la configuració de SSL/TLS.
  - *Flags* de galetes desactivades.
  - *Headers* de seguretat no activats.

- Problemes de suplantació de contingut i injecció de text sense mostrar un vector d'atac/sense poder modificar HTML/CSS.
- Etc.

- L'Agència llistarà les vulnerabilitats conegudes que, per ser de criticitat baixa o no explotables, encara no estan mitigades tot i que ja estan degudament identificades, les quals no seran vàlides per al programa.

Recompenses

- L'Agència elaborarà una taula de recompenses econòmiques segons el valor de l'actiu en el qual es descobreix la vulnerabilitat (ValorActiu).
  - La magnitud de les recompenses estipulades ha de ser prou competitiva com per atraure la pràctica dels investigadors.
  - Es definirà una taula de recompenses per a cada programa i, durant l'execució, es podrà modificar amb l'objectiu de maximitzar la seva rendibilitat. Per exemple, si el reconeixement econòmic inicial fos excessivament baix, eventualment es podria augmentar per tal d'incentivar la participació dels investigadors amb l'objectiu d'accelerar el descobriment de vulnerabilitats.
- A banda de la recompensa econòmica, l'Agència podrà proveir altres tipus de reconeixements per la tasca realitzada, com una samarreta, un diploma i/o una menció pública a un *hall of fame*.

Regles generals del programa i de l'activitat dels investigadors

- L'adjudicatari garantirà que tots els investigadors han de tenir edat legal per a treballar. Els investigadors per sota de divuit anys i majors de setze anyshan de ser estudiats cas per cas i poden requerir una autorització signada per part del tutor legal tant per participar en els programes endegats per l'Agència.
- L'activitat dels investigadors només és permesa sobre els actius inclosos a l'abast del programa.
- En cap cas, un investigador podrà fer pública una vulnerabilitat descoberta sense l'aprovació formal per escrit de l'Agència. Tota la informació relacionada amb les vulnerabilitats identificades en el marc dels programes de *bug bounty* serà estrictament confidencial.
- Els investigadors reportaran les vulnerabilitats identificades i que siguin vàlides segons el que estableixi la política del programa.
- No es permet que els investigadors executin proves disruptives/destructives. Abans de realitzar qualsevol activitat que pugui suposar un dany real o a l'activitat dels sistemes, l'investigador informarà de les troballes de què disposa i sol·licitar autorització per continuar amb les proves.
- No es permet incórrer en violacions de privadesa, destrucció de dades, interrupció o degradació de productes o serveis del propietari del programa.
- No es permet fer investigacions utilitzant informació d'altres investigadors participants en el programa. Es definirà si es permet la col·laboració entre investigadors i, en cas afirmatiu, quines condicions s'aplicaran per a la divisió de la recompensa.
- No es permet emprar enginyeria social.

- Una vegada una vulnerabilitat sigui acceptada, es procedirà a ser apedaçada pels responsables de l'actiu, i una vegada fet, l'Agència podrà demanar a través de la plataforma de l'adjudicatari que l'investigador validi que ha quedat degudament resolta.
- La infracció de les regles d'un programa pot comportar que l'investigador sigui exclòs, se li impedeixi rebre qualsevol recompensa i, fins i tot se li exigeixi responsabilitat civil i penal.

2.5.2. Activació del programa

— L'Agència crearà i publicarà el programa a la plataforma web proporcionada per l'adjudicatari:
  - Es definirà un títol descriptiu de l'abast del programa.
  - Es detallarà la política del programa definida.
  - Es descriurà la informació que els investigadors necessitin saber abans d'iniciar la cerca de vulnerabilitats: el titular dels actius, els objectius del programa, les normes addicionals del programa, etc.
  - S'especificaran els passos i procediments que cal que els investigadors segueixin, des de la descoberta de vulnerabilitats fins a obtenir la recompensa corresponent.

— L'activitat dels investigadors serà monitoritzada per l'Agència i haurà de poder ser degudament identificada per tal de distingir-la d'altres possibles ciberatacs. Per fer-ho possible, els següents requisits seran necessaris:
  - Els investigadors hauran de fer ús d'un *user-agent* identificatiu: els investigadors incorporaran una cadena específica a totes les sol·licituds HTTP per tal d'assegurar la identificació de l'investigador responsable de l'activitat detectada.
    - El format pot ser d'aquest tipus: "BBounty:nickname".
  - Si el programa es duu a terme sobre un entorn restringit per IP, l'adjudicatari proveirà als investigadors d'un accés via VPN per tal de:
    - Limitar els accessos a entorns restringits només a les adreces IP de la VPN.
    - Facilitar la distinció del la font del trànsit de dades generat per les proves.
    - Bloquejar l'accés via VPN d'un investigador si aquest és bloquejat.

2.5.3. Recollida dels informes de vulnerabilitats

— Quan els investigadors identifiquin una vulnerabilitat, faran arribar l'informe corresponent a l'equip de triatge.

— Els informes hauran d'incloure la següent informació:
  - Adreça IP des d'on s'ha identificat la vulnerabilitat.
  - Capçalera HTTP emprada, si s'escau.
  - Cercador, sistema operatiu i/o versió d'aplicació emprada durant les proves.
  - Data i hora aproximada del descobriment.
  - Descripció de la vulnerabilitat.
  - Llista d'actius (IP, URL, apps...) i paràmetres afectats.
  - Passos a seguir per reproduir la vulnerabilitat reportada.

- Proves de l'explotació (captures de pantalla, vídeo, etc.).
- Impacte sobre l'usuari o organització.
- Puntuació CVSSv3[2] (sense les mètriques *Temporal* i *Environmental*).
  - Calculadora CVSSv3 que el FIRST posa a disposició per obtenir la puntuació de la vulnerabilitat de forma totalment transparent: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- Proposta de solució/mitigació.

— Els investigadors documentaran cadascuna de les vulnerabilitats identificades en informes independents, excepte en aquells casos que calgui proporcionar una cadena de vulnerabilitats per justificar l'impacte.

— La vulnerabilitat descoberta només podrà ser recompensada si l'equip de triatge és capaç de reproduir i verificar la fallada de seguretat.

2.5.4. Triatge dels informes de vulnerabilitats

— Tan bon punt l'equip de triatge rebi l'informe d'una vulnerabilitat descoberta, es posarà en marxa la fase de triatge per avaluar la validesa de la vulnerabilitat i el mereixement de recompensa.

- No rebran recompensa aquells informes que corresponguin a falsos positius o a fallades de seguretat ja publicades.
- No podrà rebre recompensa el personal amb una activitat professional vinculada als actius del programa, els treballadors de l'Agència o els seus proveïdors.
- En el cas que un informe reporti múltiples vulnerabilitats causades per un mateix error de seguretat, només es considerarà la causa arrel com a recompensable.
- En el cas que es rebin múltiples informes per a una mateixa vulnerabilitat, únicament el primer informe rebut que compleixi tots els requisits establerts en el programa rebrà la recompensa.

— Per a cada informe, l'equip de triatge de l'adjudicatari realitzarà:

1) Verificació de la validesa de l'informe respecte de les normes especificades en la política del programa.
   - En el cas que no s'hagin seguit les indicacions estipulades en la política del programa per a la realització de les proves (p. ex. no fer ús de l'*user-agent*), es rebutjarà l'informe.
   - Si calgués una ampliació d'informació per part de l'investigador, es deixarà un marge de 24h durant el qual ningú més podrà obtenir recompensa per aquesta mateixa vulnerabilitat. Un cop expirat aquest termini, si no s'ha rebut l'ampliació de contingut, es consideraran els informes posteriors en estricte ordre de recepció.
   - En el cas que un investigador informi d'una vulnerabilitat ja registrada i acceptada amb antelació, se li notificarà que l'informe està duplicat i es tancarà l'informe.
   - Es comunicarà a l'investigador l'acceptació, o en el seu defecte el rebuig, del seu informe.

[2] CVSS (Common Vulnerability Score System) és un sistema de puntuació creat pel Forum of Incident Response and Security Teams (FIRST) que mesura l'impacte que podria tenir l'explotació d'una vulnerabilitat per part d'un ciberatacant.

2) Amb la validesa de l'informe, l'equip de triatge replicarà l'atac de l'investigador, segons els passos descrits a l'informe, amb l'objectiu de verificar la l'existència de la vulnerabilitat.

   · Si la vulnerabilitat reportada no és un problema de seguretat, sinó un mal funcionament d'una aplicació o sistema, es procedirà a la comunicació i tancament de l'informe.

   · Si calgués una ampliació d'informació per part de l'investigador per poder executar la prova de la vulnerabilitat, es deixarà un marge de 24h durant el qual ningú més podrà obtenir recompensa per aquesta mateixa vulnerabilitat. Un cop expirat aquest termini, si no s'ha rebut l'ampliació de contingut, es consideraran els informes posteriors en estricte ordre de recepció.

   · En cas que la vulnerabilitat hagi pogut ser provada, l'informe passarà a la fase següent.

3) L'equip de triatge assignarà el nivell de severitat de la vulnerabilitat descoberta, d'acord amb la seva puntuació CVSSv3.

   · Les vulnerabilitats es puntuaran de manera qualitativa a partir de la puntuació CVSS segons la calculadora del FIRST (https://www.first.org/cvss/calculator/3.1).

   · L'equip de triatge podrà consultar l'Agència sobre l'impacte real que l'explotació de la vulnerabilitat tindria sobre els actius del programa.

   · A partir d'una vulnerabilitat presentada en un informe vàlid, l'equip de triatge podrà proposar justificadament la modificació de la puntuació CVSS de la vulnerabilitat a l'informe obert per l'investigador, tant a l'alça com a la baixa, i l'import de la recompensa corresponent.

   · El nivell de severitat de la vulnerabilitat ($Valor_{Vulnerabilitat}$) serà proporcional a la puntuació CVSS de manera similar a la taula següent:

Vulnerabilitat	Puntuació CVSS	$Valor_{Vulnerabilitat}$
Baixa	0.1 – 3.9	4
Mitja	4.0 – 6.9	7
Alta	7.0 – 8.9	9
Crítica	9.0 – 10.0	10

Taula de valoració de les vulnerabilitats

4) L'equip de triatge assignarà la recompensa assignada per la vulnerabilitat descoberta, d'acord amb el seu nivell de severitat ($Valor_{Descobriment}$) i la criticitat de l'actiu en què s'ha descobert ($Valor_{Actiu}$).

   · L'import de la recompensa econòmica serà proporcional al valor de descobriment de la vulnerabilitat ($Valor_{Descobriment}$) i a la criticitat de l'actiu ($Valor_{Actiu}$), i serà calculat de forma similar a la fórmula següent:

$$Valor_{Descobriment} = Valor_{Actiu} * Valor_{Vulnerabilitat}$$

$Valor_{Descobriment}$			
$Valor_{Actiu}$		1	2
$Valor_{Vulnerabilitat}$	Baixa = 4	4	8
	Mitja = 7	7	14
	Alta = 9	9	18

	Crítica = 10	10	20

Taula de categorització orientativa amb el valor de descobriment de les vulnerabilitats en funció del valor de l'actiu i el valor de la vulnerabilitat

5) L'equip de triatge comunicarà la informació de la vulnerabilitat a l'Agència.

   · Tan bon punt l'informe de la vulnerabilitat descoberta estigui validat per l'equip de triatge, l'adjudicatari transferirà tota la informació disponible a l'Agència.

   · El termini màxim de resposta a una vulnerabilitat informada per un investigador serà de 72 hores.

2.5.5. Pagament de les recompenses

— A partir de l'avaluació aportada per l'equip de triatge, l'Agència comunicarà a través de la plataforma de l'adjudicatari que l'informe ha estat acceptat i aprovarà la recompensa que li correspon a l'investigador.

— El pagament de la recompensa es realitzarà per transferència bancària amb una aprovació prèvia i específica per part de l'Agència.

— Les recompenses les gestionarà l'empresa adjudicatària per a que siguin percebudes per l'investigador.

— Els pagaments de les recompenses als investigadors de seguretat hauran de ser transparents, traçables i conformes amb les obligacions legals i fiscals aplicables. Per assegurar-ho, la plataforma haurà de disposar d'un sistema de traçabilitat dels pagaments que permeti un seguiment adequat de totes les transaccions i recompenses atorgades.

— Per a la gestió del pagament de les recompenses, l'adjudicatari haurà de disposar d'una plataforma de pagament de tercers que verifiqui sistemàticament les identitats i les dades bancàries dels investigadors registrats a cada programa, mitjançant els controls KYC obligatoris per a qualsevol emissor de diners electrònics dins de la UE:

   o Verificació d'identitat: carnet d'identitat, passaport, etc.

   o Verificació de l'estructura jurídica: número d'identificació, estatuts certificats, etc.

   o Verificació de domicili: confirmació de residència per mitjà de factura d'aigua/llum/gas/ telèfon, rebut fiscal, assegurança, etc.

— A més, per garantir la conformitat legal i fiscal, l'adjudicatari haurà de requerir que els investigadors completin els formularis fiscals corresponents abans de processar qualsevol pagament.

— Finalment, existirà un rànquing de l'activitat dels investigadors per a cada programa i per al conjunt tots els programes promoguts per l'Agència.

2.5.6. Supervisió i validació de la resolució exitosa de les vulnerabilitats

— L'Agència procedirà a requerir la resolució de les vulnerabilitats a l'equip pertinent a cada actiu. La prioritat de resolució de les vulnerabilitats es podrà establir en funció de la seva criticitat, de manera que esdevindran més urgents aquelles amb la quantificació més alta.

— Una vegada l'Agència consideri que la vulnerabilitat ha estat resolta, ja sigui perquè ha estat apedaçada o s'han pres accions mitigadores, podrà sol·licitar a l'investigador que comprovi la seva explotació.

— Si l'investigador confirma que la vulnerabilitat no es pot explotar més, es considerarà que ha quedat resolta.

— L'adjudicatari s'ocuparà de facilitar la validació de la resolució de totes les vulnerabilitats que hagin estat descobertes durant l'execució del contracte, encara que la seva resolució s'hagi realitzat fora d'aquest període.

2.6. Gestió i dinamització de la comunitat d'investigadors

— L'adjudicatari serà responsable de gestionar la comunitat d'investigadors experts en ciberseguretat candidats a participar en els programes de *bug bounty* endegats per l'Agència.

  - Inicialment, els programes de *bug bounty* seran privats, o sigui, la participació estarà restringida als investigadors que rebin una invitació. Els participants convidats seran escollits en funció dels seus mèrits, com la seva posició en el *ranking*, la qualitat dels seus informes, habilitats (*skills*), etc.
  - A mesura que avancin els programes de *bug bounty*, el número d'investigadors podrà anar creixent, fins al punt que podrien acabar sent públics per a tota la comunitat d'investigadors.
  - L'Agència validarà la llista dels investigadors que participaran en cada programa i, en cas que ho sol·liciti, l'adjudicatari haurà de proporcionar la seva identitat.
  - Durant l'execució d'un mateix programa, es podrà canviar el grup d'investigadors convidat, d'acord amb les necessitats del programa.

— L'adjudicatari disposarà de mecanismes per a la gestió dels investigadors com:

  - Procediments d'alta/baixa d'investigadors.
  - Compromís contractual amb cada investigador, amb la signatura d'un acord de NDA (*Non Disclosure Agreement*) i pràctiques de r*esponsible disclosure.*

— L'adjudicatari donarà suport a l'Agència a identificar i mobilitzar talent existent en matèria de ciberseguretat per donar suport a les iniciatives de l'Agència.

2.7. Equip i eines del servei

2.7.1. Responsable del servei

El responsable del servei serà la persona dedicada a la gestió del servei, la coordinació amb l'Agència i responsable de l'assoliment dels objectius i l'èxit del servei.

— Serà una persona nominal i estarà a disposició de l'Agència via correu electrònic, telèfon i reunions telemàtiques.

— Tindrà formació en ciberseguretat adequada i capacitat de gestió per al desenvolupament de les seves tasques.

— La seva missió serà assegurar la qualitat del funcionament del servei i, per aconseguir-ho, la seva dedicació no tindrà una limitació en hores.

— Serà el canal de comunicació amb els investigadors i serà el responsable de la seva gestió i dinamització.

— Supervisarà i gestionarà l'evolució dels programes de *bug bounty* durant la seva execució per garantir-ne l'eficiència i, quan s'escaigui, proposarà revisar l'abast, canviar la política, modificar les recompenses, incorporar/excloure investigadors, etc.

— Informarà diligentment l'Agència de qualsevol risc o aspecte crític que identifiqui.

— Assistirà en reunions de seguiment amb els serveis de les àrees de l'Agència amb la periodicitat que sigui necessària per garantir el correcte funcionament del servei.

— Disposarà d'un mínim de 2 *backups* per substituir-lo en cas de no disponibilitat.

2.7.2. Equip de triatge

L'equip de triatge serà l'equip de persones responsable de rebre els informes de vulnerabilitats enviats pels investigadors, avaluar-los i fer seguiment de la seva conclusió en coordinació amb l'Agència.

— Serà un equip nominal, identificable i estarà a disposició de l'Agència via correu electrònic, telèfon i reunions telemàtiques.

— Tindran formació en ciberseguretat avançada per garantir el correcte desenvolupament de les seves tasques.

— Gestionaran els informes rebuts per part dels investigadors, en realitzaran la validació i els mantindran informats de:

  - El resultat de la comprovació de la vulnerabilitat registrada, el qual podrà ser de diferent tipologia (p. ex. : s'ha demostrat la vulnerabilitat / cal ampliar la informació / es descarta perquè correspon a una vulnerabilitat ja reportada prèviament / es descarta perquè no es tracta d'una vulnerabilitat / es descarta perquè no s'han complert les normes del programa, etc.).
  - La puntuació de la vulnerabilitat registrada, tenint en compte que la puntuació calculada per l'investigador pot ser modificada arran del valor dels actius afectats.
  - La quantitat de la recompensa assignada.
  - Etc.

2.7.3. Plataforma web per a la gestió dels programes de *bug bounty*

La plataforma ha de ser el sistema en línia des d'on estarà centralitzada la gestió dels programes de *bug bounty*, la interacció amb els investigadors, el control de les vulnerabilitats i la gestió dels pagaments.

— La plataforma permetrà la gestió dels programes de *bug bounty*, amb la corresponent comunicació de polítiques, administració dels investigadors participants, etc.

— La plataforma permetrà el control de les vulnerabilitats:

  - Mostrarà la informació completa dels informes de vulnerabilitats.
  - Registraran l'estat i l'històric en què es troba dins de tot el procediment.
  - La informació de les d'un programa podrà publicar-se a terceres parts per a la seva resolució.
  - La descàrrega de les dades de les vulnerabilitats registrades es podrà realitzar via API pública compatible amb JIRA, OTRS o REMEDY.

— La plataforma permetrà la comunicació amb els investigadors:

  - Els investigadors tindran accés als detalls de només aquells programes en què hagin estat convidats.
  - Els investigadors figuraran en rànquings, per a cada programa i per al seu conjunt, segons la rellevància de la seva activitat.

— La plataforma disposarà d'un quadre de comandament (*dashboard*) interactiu amb els indicadors de servei corresponents al conjunt de programes (p. ex. vulnerabilitats detectades, total de pagaments realitzats, etc.).

— L'Agència disposarà d'un nombre il·limitat d'usuaris a la plataforma per tal que el personal pugui realitzar el seguiment dels programes.

2.8. Requeriments de seguretat pel servei

La seguretat de les comunicacions i els sistemes d'informació és un element bàsic per a l'Agència. L'incompliment de qualsevol dels següents requeriments podrà significar la rescissió immediata del contracte.

— La plataforma ha d'estar allotjada a la UE, preservada de qualsevol jurisdicció externa.

— La plataforma web per a la gestió de programes de *bug bounty* ha d'estar sota un programa de *bug bounty* permanent organitzat per l'adjudicatari.

— La plataforma ha de disposar de la possibilitat d'utilitzar usuaris a la plataforma amb accés per mitjà d'autenticació de 2 factors (2FA).

— Les comunicacions i l'enviament d'informes entre l'adjudicatari, investigadors i l'Agència han d'estar degudament xifrats. En el cas que sigui necessari l'enviament de correus electrònics dins el marc del programa, hauran d'estar xifrats de forma segura mitjançant PGP.

— L'Agència haurà de disposar d'accés garantit i permanent a la informació crítica per a la gestió dels programes de *bug bounty* i dels seus resultats. L'adjudicatari haurà d'assegurar que l'Agència pugui accedir i gestionar els programes en tot moment, amb els permisos i les eines necessàries per a la seva supervisió i control efectiu.

Pel que fa al compliment de normes de seguretat:

— L'adjudicatari haurà de garantir el màxim nivell de seguretat en el tractament de la informació gestionada a la plataforma. Per aquest motiu, com a requisit de solvència inicial, ja s'ha exigit el compliment de la certificació ISO 27001 o equivalent, assegurant així que la plataforma opera segons estàndards internacionals de seguretat de la informació. Aquest requisit permet constatar que l'adjudicatari disposa de sistemes i protocols robustos per protegir les dades contra accessos no autoritzats, pèrdues o manipulacions.

— El licitador ha de complir la *Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales* (LOPDGDD) i el Reglament General de Protecció de Dades (RGPD). En aquest sentit, les dades personals dels hackers ètics seran gestionades exclusivament per la plataforma, que actuarà com a responsable del seu tractament d'acord amb la normativa de protecció de dades aplicable, garantint-ne la seguretat, confidencialitat i ús exclusiu per a les finalitats del programa.

— L'adjudicatari haurà de complir qualsevol normativa d'aplicació de la UE, com el Reglament 2015/847, de 20 de maig de 2015, el qual permet garantir la traçabilitat dels fluxos financers.

2.9. Indicadors del servei

— L'adjudicatari farà el seguiment dels indicadors del servei per facilitar una presa de decisions adequada i estaran disponibles en un quadre de comandament (*dashboard*) accessible des de la plataforma web.

— Aquests indicadors seran, com a mínim, els següents:

- Origen dels investigadors dels informes (amb el detall d'investigadors amb origen o residència a Catalunya).
- Nombre total d'informes rebuts / en curs / descartats / validats.
- Motius pels quals els informes han estat descartats.
- Temps mitjà de resposta de l'equip de triatge.
- Import total de les recompenses pagades.
- Recompensa màxima / mitjana.
- Nivell de gravetat dels informes tancats.
- Tipologia de vulnerabilitats dels informes tancats.

3. Aspectes generals de l'expedient

3.1. Establiment del servei

Inicialment, i en el període de les dues setmanes posteriors a l'adjudicació d'aquest contracte, l'adjudicatari analitzarà la situació actual de l'Agència amb l'objectiu de de definir el model de gestió del servei que tingui en compte les millors pràctiques i, com a mínim, els següents punts:

- Metodologia i procediments.
- Model de *reporting* i seguiment d'indicadors.
- Eines de suport a la gestió.
- I tot allò que pugui ser requerit pel seu correcte funcionament.

Aquest model proposat haurà de ser validat per l'Agència i estarà subjecte a un procés de revisió i millora contínua per part de l'adjudicatari, durant tota la durada del contracte.

3.2. Governança del servei

Per realitzar la governança dels diferents lots, els adjudicataris seguiran la metodologia que s'hagi adoptat en la fase d'establiment del servei per tal que la gestió de les tasques i el seu seguiment siguin àgils, efectius i eficients. El personal de l'adjudicatari reportarà directament al responsable de l'Agència designat, l'estat, l'evolució i els riscos de les tasques del servei.

L'Agència contempla com a mínim, les fases i tasques en l'àmbit de la gestió del servei que es descriuen a continuació.

3.2.1. Inici i primers passos

És el període que va des de l'entrada en vigor del contracte fins l'estabilització dels serveis després de la realització del primer programa de *bug bounty*.

- Els membres de l'equip de treball de l'adjudicatari hauran de conèixer els responsables dels serveis de l'Agència i establir els procediments de coordinació necessaris.
- Les reunions de seguiment del servei en aquesta fase inicial tindran una periodicitat més elevada de l'habitual (p. ex. setmanal).
- L'adjudicatari proveirà els accessos necessaris a la plataforma de gestió dels programes de *bug bounty*: comptes d'usuari per als treballadors de l'Agència i una API per a la descàrrega de vulnerabilitats, etc.
- Després de l'execució dels programes de *bug bounty*, l'adjudicatari realitzarà una anàlisi dels resultats obtinguts i planificarà les accions de millora necessàries.

3.2.2. Prestació

És el període que comença quan hagi acabat el primer *bug bounty* i se n'hagin avaluat els resultats, fins quinze dies abans de que finalitzi la prestació del servei.

Durant aquesta fase, el servei estarà subjecte als ANS. Caldrà controlar el seu compliment mensualment i activar plans de seguiment i millora continua.

3.2.3. Devolució

És el període que comença quinze dies abans de l'extinció del contracte i s'emmarca al final de la prestació del servei.

— Tot el material generat i desenvolupat, serà propietat de l'Agència i romandrà a l'Agència un cop acabada la prestació del servei.

— El contingut de la plataforma de gestió dels programes de *bug bounty* que el proveïdor sortint hagi subministrat per tal de desenvolupar la seva tasca haurà de ser degudament esborrat i tota la informació traspassada a l'Agència.

4. Condicions d'execució

4.1. Horari

Els serveis de l'adjudicatari es desenvoluparan totalment en remot, però d'acord amb els horaris de servei de l'Agència. Es consideren horaris laborables els que corresponguin al centre de treball de l'Hospitalet de Llobregat i estiguin prèviament pactats amb l'Agència, orientativament entre les 9:00h i les 18:00h. S'espera que el servei garanteixi uns serveis mínims durant les vacances i els períodes de baixa productivitat fent ús dels mateixos integrants del servei i un sistema de torns.

Si durant l'execució del contracte l'Agència o l'adjudicatari detecten la necessitat de modificar l'horari del servei o equip descrit en aquest plec, l'Agència i l'adjudicatari consensuaran de forma conjunta la modificació, essent l'Agència qui finalment designi l'horari de prestació que s'adeqüi a les necessitats pròpies i que no perjudiqui de forma excessiva a l'adjudicatari.

A petició expressa de l'Agència, es podria requerir la realització d'algunes tasques fora de l'horari de dies laborables per tal de garantir el correcte desenvolupament del servei.

4.2. Localització física

L'equip prestatari del servei treballarà de forma remota. L'Agència pot requerir de forma excepcional el desplaçament dels recursos a les oficines de l'Agència, ubicades físicament a l'Hospitalet de Llobregat, o a d'altres pertanyents a clients i/o proveïdors.

En cap cas la ubicació dels professionals suposarà un increment dels costos vinculats a la prestació dels serveis.

4.3. Rotació de recursos

L'Agència tindrà dret a exigir justificadament a l'adjudicatari el canvi d'un recurs que d'ell depengui, quan així ho justifiqui l'execució dels treballs, quan no s'acompleixin els requisits demanats per a l'equip humà indicats en el present apartat o per tal de garantir la correcta prestació, dimensionament i organització dels serveis. Aquesta substitució s'haurà de fer efectiva en el termini de 15 dies a partir de la recepció de la comunicació per part de l'adjudicatari o bé la notificació de l'Agència al cap de servei. L'adjudicatari haurà de presentar en un termini màxim de 10 dies a partir de la comunicació de sol·licitud de substitució, el pla d'acció previst per resoldre les causes que han determinat la sol·licitud de substitució.

Per raons d'operativitat, de coneixement de les tasques a realitzar i de sensibilitat de la informació amb la que es treballa, cal garantir al màxim la continuïtat dels personal que donen servei a l'Agència evitant, sempre que sigui possible, la rotació del perfil corresponent al cap de servei, així com aquells que desenvolupin tasques rellevants en la prestació de serveis.

L'excessiva rotació del personal podrà ser penalitzada per l'Agència. Així mateix, les hores dedicades pel personal de l'adjudicatari a la transició i/o formació del personal sortint i entrant en cas de substitució no serà facturable. S'acordarà entre l'adjudicatari i l'Agència el temps estimat de transició per cada substitució que es produeixi, essent el període mínim establert per a la transició de 4 dies laborables.

Quan la rotació sigui necessària (baixes, etc.) l'adjudicatari haurà d'acreditar la idoneïtat del nou personal prèvia incorporació dels nous recursos. En els casos de rotació ordinària i previsible (vacances, permisos laborals, etc.) l'adjudicatari comunicarà a l'Agència amb la deguda antelació un pla de substitució i disposició de recursos que doni resposta a les necessitats de l'Agència en la seva prestació de serveis durant els esmentats períodes.

4.4. Eines i equipament

L'adjudicatari:

— Subministrarà tots els elements de maquinari, assumir el cost del llicenciament del programari i serveis, així com del seu manteniment, durant la durada del contracte, que siguin necessaris per complir amb els requeriments del servei.

— Es compromet a assumir i adaptar-se a les noves tecnologies i sistemes que desplegui l'Agència per donar el servei, així com participar activament en el procés de transició, formant i preparant el seu personal en aquestes noves tecnologies i sistemes implantats sense cost addicional per l'Agència.

L'Agència, quan l'adjudicatari es trobi en les seves instal·lacions, proveirà a les persones que prestin el servei:

— Ubicació física adequada per al desenvolupament i prestació del servei, a les instal·lacions de l'Agència.

— Accés a Internet a través de la xarxa local, restringit als llocs de treball que ho requereixin així com a les adreces o pàgines web que siguin necessàries per al desenvolupament del servei.

L'Agència no proveirà:

— Ordinadors de sobretaula amb sistema operatiu i programari habitual d'oficina.

— Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de l'Agència.

— Ordinadors portàtils (PC) o altres dispositius mòbils.

— Accés a Internet via comunicacions mòbils.

— Eines per al control de canvis i la gestió de versions.

— Cap altre recurs no especificat explícitament.

4.5. Seguretat corporativa

Tant l'empresa adjudicatària com el personal de l'adjudicatari s'haurà de sotmetre a les polítiques i regulacions internes que estableix l'àrea de Seguretat Corporativa en matèria de seguretat de la informació, com a mínim i no limitant-se a:

— Permetre i facilitar la realització d'auditories de compliment de les normatives establertes per Seguretat Corporativa, internes o externes, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les accions fetes per l'auditor per facilitar el seguiment d'aquestes i els seus possibles impactes no desitjats.

— Facilitar l'accés en qualsevol moment als equips i mitjans tècnics emprats pel personal de l'adjudicatari en les oficines de l'Agència (sigui o no per l'exercici de la seva funció).

— Acceptar les normes i polítiques que estableix l'àrea de Seguretat Corporativa tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions.

— Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte (LOPDGDD i RGPD, LSSI, etc.).

— A la finalització del contracte, l'adjudicatari quedarà obligat a lliurar o destruir, en cas de ser sol·licitat, qualsevol informació obtinguda o generada com a conseqüència de la prestació del servei.

4.6. Control de gestió

El personal del licitador haurà de col·laborar amb l'àrea de Control de Gestió de l'Agència per tal de:

— Definir un model de transparència en termes de capacitat i execució de tasques.

— Ajustar-se als procediments de facturació que determini l'Agència.

— Conformar les factures en relació amb el reportat de serveis efectuat i acceptat per l'Agència, d'acord amb els procediments establerts.

— Realitzar el *reporting* per l'Agència amb els següents conceptes:

- Fitxer mestre de persones.
- Fitxer mestre d'activitats realitzades.
- Assignació de tasques a persones.
- Facturació i conformació de factures.

4.7. Validació de la documentació

L'Agència és el propietari de tota la documentació elaborada pels adjudicataris referent al servei prestat pels adjudicataris i el seu personal i subcontractats que destini a l'execució dels serveis. L'adjudicatari s'encarregarà de disposar de totes les autoritzacions i permisos necessaris per tal de poder donar compliment a aquesta previsió, essent responsabilitat de l'adjudicatari qualsevol pagament o reclamació relativa a aquesta manca d'autoritzacions.

Els responsable de servei de l'Agència serà l'encarregat de la validació i aprovació dels documents elaborats pel personal de l'adjudicatari. En cas que la qualitat dels documents sigui molt baixa o de manera recurrent i/o perllongada en el temps de prestació dels serveis no assoleixi els nivells requerits s'aplicaran les penalitzacions establertes en la present licitació.

L'adjudicatari haurà de mantenir la documentació actualitzada en el sistema de gestió documental que l'Agència proporcioni per tal efecte.

4.8. Formació

El personal de l'adjudicatari disposarà de la formació adequada per al desenvolupament de les seves tasques. Sens perjudici d'aquesta qüestió el personal de l'adjudicatari realitzarà, si s'escau, formació continuada per tal de garantir l'actualització dels seus coneixements així com l'adquisició de nou coneixement que pugui ser de valor pels serveis de l'Agència.

5. Acords de nivell de servei i penalitzacions

L'adjudicatari resta obligat al compliment de l'execució total de les prestacions recollides en les ofertes que doni compliment als present plec i a les prescripcions del contracte.

Així mateix la prestació de serveis de l'adjudicatari haurà de complir uns estàndards de qualitat mínims que permetin fer-ne un aprofitament adequat i donin resposta a les necessitats de l'Agència. En cas que els serveis no assoleixin aquests mínims de qualitat requerits es considerarà l'existència d'un incompliment d'acord amb el model recollit en aquest apartat.

A continuació es descriu el model de penalitzacions que s'aplicaran per l'incompliment dels indicadors i Acords de Nivell de Servei ("ANS") definits, d'acord amb els criteris, quantificació i mètode de càlcul establerts més endavant, entenent que un mateix fet pot donar lloc a l'aplicació de diferents incompliments i les corresponents penalitzacions d'igual o diferent tipus.

En cap cas les penalitzacions tindran finalitat recaptatòria, de manera que la seva aplicació no substituirà ni minorarà la indemnització que per danys i perjudicis pogués resultar dels corresponents incompliments.

5.1. Indicadors i acords de nivell de servei

Tipus	Nom	Descripció	Càlcul	Periodicitat	Llindar Inicial (Li)	Llindar Final (Lf)	Penalització Màxima
Recursos	Rotació de personal	Índex de rotació dels efectius assignats al servei: el responsable del servei i l'equip de triatge	Índex de rotació de personal = (((A + D)/2) *100)/ES A = Admissions de personal del servei dins del període considerat. D = Desvinculacions de personal del servei dins del període considerat. ES = Número d'efectius del servei segons s'estableix en la proposta de servei pel període considerat; si hagués alguna ampliació del servei en número de recursos humans durant el període considerat, es considerarà el valor ponderat al temps d'aplicabilitat.	Trimestral	N/A	N/A	Índex de Rotació [%] x Import de la factura mensual
Recursos	Reposició de personal	Temps de reposició d'un recurs per un altre, ja sigui per baixa o per rotació de personal	Dies transcorreguts des de la falta d'un recurs fins a la seva reposició	Trimestral	5 dies	15 dies	Import equivalent al cost total temps de no disponibilitat d'un recurs
Recursos	No disponibilitat del servei	Temps sense disponibilitat de servei, sense justificació	Hores sense resposta als intents de contacte via correu electrònic i/o telèfon	Trimestral	N/A	N/A	Import equivalent de 2h de servei per cada hora de no disponibilitat
Recursos	No disponibilitat de la plataforma web	Temps sense disponibilitat o mal funcionament de la plataforma de gestió de programes de *bug bounty*	Hores sense poder utilitzar les funcionalitats de la plataforma de gestió de programes de *bug bounty*	Trimestral	N/A	N/A	Import equivalent de 2h de servei per cada hora de no disponibilitat
Gestió	No disponibilitat d'indicadors	Temps sense disponibilitat dels indicadors de govern del servei degudament actualitzats	Dies de desviació entre la data prevista de lliurament dels indicadors del servei i la data del lliurament efectiva	Trimestral	1 dia	10 dies	5% del cost anual del servei
Terminis	Retard de resposta de l'equip de triatge	Retard en la resposta de l'equip de triatge després de la recepció d'un informe per sobre del termini especificat en l'oferta de l'adjudicatari	Temps de resposta de l'equip de triatge des de l'entrada d'un nou informe fins a la resposta a l'investigador.	Trimestral	24 hores	48 hores	5% del cost trimestral del servei
Terminis	Retard de validació de l'equip de triatge	Retard en l'anàlisi i validació d'una vulnerabilitat informada per un investigador	Temps de resposta de l'equip de triatge des de l'entrada d'un nou informe fins a la seva validació.	Trimestral	24 hores	72 hores	5% del cost trimestral del servei

5.2. Model de penalitzacions pel servei

El licitador s'haurà d'ajustar al model penalitzacions que a continuació es descriu i que inclou els següents punts:

- Càlcul de les penalitzacions.
- Aplicació de les penalitzacions.
- Irregularitats en les mesures.

5.3. Càlcul de penalitzacions

Les penalitzacions s'aplicaran per incompliment dels Nivells de Servei indicats en la taula d'ANS.

El càlcul de l'import de la penalització es realitzarà sobre l'import de facturació del servei pel període de càlcul o per l'import assignat a un projecte concret.

Prèvia exposició de les fórmules, s'exposen a continuació les definicions dels conceptes principals:

- Llindar inicial (L_i): valor a partir del qual es començarà a penalitzar el servei. Sempre tindrà un valor positiu.
- Llindar final (L_f): valor a partir del qual la penalització és màxima (P_{max}). Sempre tindrà un valor positiu.
- P_{max}: penalització màxima aplicable per cada ANS quan s'arriba o es supera el llindar final.
- Tipus de penalització: les penalitzacions poden ser per projecte o bé per servei. En cada ANS se n'especificarà el tipus.
- Valor: és el valor de l'indicador del servei que es compararà amb els llindars establerts en el plec.
- Penalització (Valor): és el valor de la penalització en funció del valor de l'indicador.
- Import Facturable (IF): suma de l'import a facturar mensualment com a conseqüència de les penalitzacions per incompliment d'ANS.

A continuació s'indiquen les fórmules que seran d'aplicació per cada ANS especificat en el plec:

Si $L_i > L_f$	Si Valor ≥ L_i : P(Valor) = 0
	Si Li > Valor > L_f : P(Valor) = P_{max} [(L_i - Valor)/(L_i – Lf)]
	Si Valor ≤ L_f : P(Valor) = P_{max}
Si $L_i = L_f$	Situació no existent en els indicadors
Si $L_i < L_f$	Si Valor ≤ L_i : P(Valor) = 0
	Si L_i < Valor < L_f : P(Valor) = P_{max} [(Valor- L_i)/(L_f – L_i)]
	Si Valor ≥ = L_f : P(Valor) = P_{max}

Mensualment es calcularà l'import mensual dels ANS que són aplicables i es consolidarà en l'indicador IF (Import Facturable).

IF = ∑(Penalitzacions aplicables de tots els ANS)

IF serà l'import global de la factura mensual. La suma dels IFs acumulats de tots els mesos de la duració del contracte en cap cas pot superar el 10% de l'import total de contracte. En cas de fer-ho caldrà revisar amb detall els motius dels incompliments que han generat aquesta situació, sens perjudici de la disposició de les facultats de la Fundació de resolució contractual reconegudes a la normativa de contractació vigent.

5.4. Aplicació de les penalitzacions

L'Agència té la potestat de decidir aplicar les penalitzacions econòmiques o bé les compensacions en serveis equivalents.

L'Agència té la potestat de decidir no aplicar les penalitzacions associades per l'incompliment dels nivells de servei acordats en determinades casuístiques. Com a regla general queden excloses les penalitzacions quan:

- Existeixin situacions extraordinàries que donin lloc a alteracions que desvirtuïn la mesura.
- Quan es produeixi una situació excepcional d'un increment dràstic de l'activitat, no atribuïble a l'adjudicatari que impedeixi l'assoliment dels ANS acordats.
- Quan la desviació sigui provocada per components que no estan sota la responsabilitat de l'adjudicatari.
- Quan el servei quedi aturat per causes alienes al mateix servei, ja siguin aturades programades o no.

A l'inici del contracte, l'adjudicatari podrà sol·licitar a l'Agència la revisió temporal i transitòria de les penalitzacions sobre els ANS que cregui necessàries en atenció a elements de caràcter extraordinari. L'Agència estudiarà la seva viabilitat i/o aplicació i les aprovarà per escrit, si s'escau.

5.5. Incidències en les mesures d'indicadors

En cas d'incidències en la mesura del valor d'un Indicador associat a un ANS degudes a errors materials, o quan existeixi manca de col·laboració per part de l'adjudicatari en la determinació del valor correcte, es considerarà que l'indicador no ha arribat al Nivell Mínim de Servei, aplicant-se la penalització corresponent.

Es considerarà que hi ha incidència en la mesura d'un Indicador quan el valor d'aquest, facilitat per l'adjudicatari difereixi en més d'un 15% respecte del valor real auditat que resulti del procés d'auditoria que es descriu al Document tècnic de solució final.

Es considerarà manca de col·laboració quan conflueixin tots els següents factors:

- Que l'auditor que es designi en l'esmentat procés d'auditoria aporti evidència d'una sol·licitud d'informació en un termini concret dirigida a l'adjudicatari.
- Que la sol·licitud d'informació demanada i el termini siguin raonables a judici de l'Agència.
- Que l'adjudicatari no pugui aportar cap evidència que provi que s'hagi facilitat la informació demanada dins del termini especificat o en el seu defecte no hagi donat una explicació raonable del motiu del retard.

5.6. Facturació de les penalitzacions

L'import corresponent a les penalitzacions aplicades a l'adjudicatari és resultat de sumar els imports de penalització corresponents a l'incompliment dels nivells de serveis acordats en el contracte.

L'adjudicatari abonarà, mitjançant el procediment de compensació, les penalitzacions automàticament a la factura que pels seus serveis hagi d'abonar l'Agència. En cas de no poder compensar-se els imports per causes imputables a l'adjudicatari aquest haurà de satisfer l'import mitjançant el pagament corresponent a l'Agència.

La no incorporació d'aquesta reducció de l'import per qualsevol causa (tramitació, incidència en terminis de facturació, etc.) no eximirà a l'adjudicatari de la seva obligació de pagament en els termes que determini l'Agència.