

**PLEC DE CLÀUSULES TÈCNiques PARTICULARS QUE REGEIX EL PROJECTE
“MANTENIMENT DE LA OPERATIVA DE L’EQUIP DE RESPOSTA A INCIDENTS DEL CENTRE
DE SEGURETAT DE LA INFORMACIÓ DE CATALUNYA” MITJANÇANT PROCEDIMENT
NEGOCIAT.**

Exp.

Índex de clàusules i annexos

1.	PRESCRIPCIONS TÈCNiques PARTICULARS.....	2
1.1.	Antecedents	2
1.2.	Objecte del concurs	2
1.3.	Objectius del projecte/servei	2
1.4.	Descripció de la situació actual	3
1.4.1.	Infraestructura tecnològica utilitzada.....	4
1.5.	Esforz sol·licitat	5
1.6.	Condicions d’execució	6
1.6.1.	Mesures de qualitat en l’execució dels contractes.....	6
1.7.	Contingut i estructura de la presentació de l’oferta	6

1. PRESCRIPCIONS TÈCNIQUES PARTICULARS

1.1. Antecedents

El Centre de Seguretat de la Informació de Catalunya (CESICAT), constituït el 2 de Febrer del 2010, és l'organisme executor del pla nacional d'impuls de la seguretat TIC aprovat pel govern de la Generalitat de Catalunya el 17 de Març del 2009.

La missió del CESICAT es garantir una societat de la informació catalana segura per a tots, a com a eina per a la generació d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui referent nacional i internacional.

Els objectius estratègics del CESICAT son:

- Establiment d'una estratègia nacional de seguretat TIC.
- Suport a la protecció de les infraestructures crítiques TIC del país.
- Promoció d'un teixit empresarial català sòlid en seguretat TIC.
- Increment de la confiança i protecció dels ciutadans catalans en la societat de la informació.

Els serveis del CESICAT s'adrecen al següent públic objectiu:

- Els ciutadans/es de Catalunya, amb una atenció especial als col·lectius amb més riscos de seguretat de la informació, com són els infants, joves, gent gran i altres col·lectius de recent incorporació a la xarxa.
- Els professionals i les entitats privades, amb una atenció especial a les PIME i altres organitzacions de reduïda dimensió.
- Les administracions públiques, amb una atenció especial als governs locals de Catalunya de petita i mitjana població.
- Les universitats i els centres de recerca, amb independència de la seva naturalesa pública o privada.

Les seves principals àrees d'actuació son la reactiva, preventiva, promoció i dinamització.

Per tal de cobrir les necessitats reactives, la Fundació compta amb un Equip de Resposta a Incidents (ERI) anomenat CESICAT-CERT que és l'encarregat de donar resposta als incidents de seguretat de les seves comunitats usuàries.

1.2. Objecte del concurs

L'objecte d'aquesta procediment és la contractació de serveis de suport a l'Equip de Resposta a Incidents del CESICAT, en matèria de formació, anàlisi de laboratori i suport en la gestió d'incidents de seguretat.

Actualment, l'ERI del CESICAT està duent a terme aquesta tasca dirigida als diferent col·lectius a qui s'adreça, i donat el gran volum de peticions rebudes, és vol contractar un suport addicional per reforçar el servei per tal que no disminueixi la qualitat i l'eficiència.

1.3. Objectius del projecte/servei

L'objectiu principal d'un equip de gestió d'incidents és minimitzar i controlar els danys que es produeixen en cas d'incident, proporcionar o assistir amb capacitats de resposta i recuperació a la seva comunitat donant una resposta eficaç i treballar per prevenir futurs esdeveniments semblants. Sovint, aquests equips són els grups que coordinen l'anàlisi de la resposta i la seva aplicació, fet que implica analitzar i resoldre els esdeveniments i els incidents que són reportats pels usuaris finals o que s'observen a través de la vigilància preventiva.

L'objectiu del servei es reforçar l'equip actual de l'ERI en els següents àmbits:

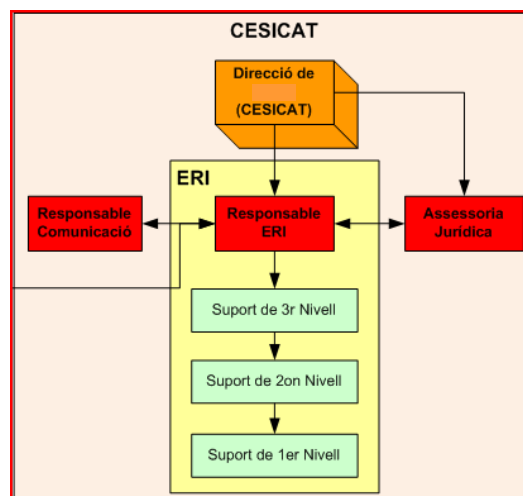
- **Ampliació de la formació:** Impartició dels següents cursos als membres de l'ERI:
 - Investigació d'informació bàsica.
 - Investigació d'informació avançada.
 - Anàlisi dinàmic de codi maliciós amb programari i fonts públiques
 - Anàlisi forense avançat
 - Utilització avançada d'eines forense

- **Laboratori d'anàlisi d'incidents.** Servei que consisteix en l'anàlisi de tota la informació disponible i de les evidències electròniques i artefactes relatius a un incident de seguretat, amb l'objectiu d'identificar l'àmbit de l'incident, l'extensió del dany causat per l'incident, la seva naturalesa i les estratègies de resposta i recuperació.

- **Suport en la gestió d'incidents de seguretat:** La sol·licitud de recursos s'emmarca dintre de la prestació de serveis de suport a la producció de l'ERI del Cesticat i en particular, dins del subministrament de recursos tècnics especialitzats en intel·ligència operativa en la gestió i resolució d'incidents de seguretat. La capacitat dels recursos sol·licitats ha de garantir la qualitat del servei i la correcta gestió del risc associat a la pròpia activitat de l'ERI del CESICAT. Per aquest motiu els recursos hauran d'ajustar-se als paràmetres de funcionament intern de l'ERI definits pels seus responsables en els darrers mesos.
 - Suport de 1er nivell en la gestió d'incidents en moments d'excés de demanda.
 - Suport de 2n nivell en la gestió i resolució d'incidents de seguretat durant l'operativa normal de l'ERI.
 - Suport de 3r nivell (serveis de laboratori) en la gestió i resolució d'incidents de seguretat.
 - Gestió d'incidents greus (troians, botnets... relacionats amb programari maliciós avançat)
 - Suport en la gestió d'incidents per a destinataris principals del CESICAT.
 - Suport a l'equip del CESICAT en aspectes tècnics i de gestió relacionats amb resolució d'incidents, intel·ligència operativa i estratègies de resposta.

1.4. Descripció de la situació actual

Actualment l'estructura organitzativa de l'ERI és la següent:



L'ERI disposa d'una persona que exerceix les tasques de responsable, 3 consultors sèniors que realitzen les tasques de 3er i 2on nivell, i un conjunt d'operadors que realitzen les tasques de 1er nivell. A continuació es descriuen les tasques de cadascun d'aquests nivells:

Tasques de 1er nivell:

- Atendre les notificacions realitzades per membres de la Comunitat pels canals de comunicació que s'han establert (via correu electrònic, notificacions a través d'un portal web, telefònicament, via fax, etc.), en la modalitat de 24 hores els 7 dies de la setmana.
 - Realitzar un primer filtrat destinat a:
 - Determinar si la notificació és efectivament d'un incident en que estigui involucrat un membre de la Comunitat o no.
 - Discriminar entre incidents i consultes o situacions que clarament no són incidents de seguretat.
 - Registrar els incidents en la BBDD d'Incidents i documentar les informacions inicials.
- Monitoratge de alertes i esdeveniments de seguretat de manera preventiva (SOC) per comunicar-ne els més rellevants que puguin esdevenir un cas d'anàlisi per part de l'ERI tals com incidents o vulnerabilitats altes o greus.

Tasques de 2on nivell:

- Anàlisi tècnic de la informació dels incidents registrats pel grup de Suport de 1^{er} nivell.
- Encarregats de realitzar investigació dels incidents.
- Assessorament i resolució in-situ, en el lloc d'ocurrència de l'incident, en la mesura que sigui determinada pel Responsable de l'ERI.
- Funcionament de les eines de laboratori.
- Comunicació en diversos idiomes.
- Gestió de sistemes d'informació
- Donar suport al 3er nivell en la informació tècnica rellevant per a realitzar el triatge de l'incident.
- Anàlisi de vulnerabilitats.

Tasques de 3er nivell:

- Gestió d'incidentes complexos, que poden involucrar diversos clients, comunitats o equips de resposta.
- Coordinació amb terceres parts.
- Actuar com a responsable en funcions de l'ERI si fos necessari. Realitzar el triatge estratègic i tàctic dels incidents.
- Anàlisi tècnic d'incidentes, que pot incloure:
 - Anàlisi forense.
 - Anàlisi de codi maliciós.
 - Anàlisi de vulnerabilitats i tecnologies d'atac.
- Gestió de sistemes d'informació.

1.4.1. Infraestructura tecnològica utilitzada

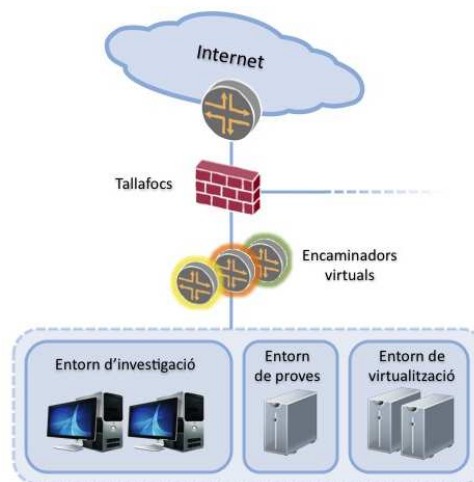
Totes les tasques realitzades pels diferents membres de l'ERI utilitzen infraestructura tecnològica pròpia del CESICAT. Aquesta infraestructura està formada per l'equipament bàsic de cadascun dels membres (portàtil, mòbil, etc.) més l'equipament del laboratori. També es disposa d'una eina de ticketing per fer la gestió dels incidents i d'una BB.DD d'estratègies de resposta i coneixement.

El laboratori compta amb una infraestructura que permet l'accés, tractament, emmagatzematge, preservació i transmissió de la informació tractada en les activitats d'investigació digital i anàlisi

forense realitzades. Aquests recursos es troben ubicats en una àrea d'accès restringit al personal autoritzat de CESICAT-CERT.

La infraestructura de laboratori està conformada a nivell lògic per les següents àrees funcionals:

- **Entorn d'investigació** per a l'anàlisi d'informació i evidències digitals
- **Entorn de proves** per a la simulació d'entorns amb requeriments físics dedicats
- **Entorn de virtualització** amb flexibilitat per a la realització de proves de concepte, creació d'entorns d'incidents, centralització d'eines d'anàlisi i tractament d'informació, entre d'altres.



1.5. Esforç sol·licitat

L'empresa adjudicatària haurà d'aportar els següent recursos:

- 1 Cap de projecte a temps parcial
- 1 Consultor sènior a temps complet (jornada laboral de 8x5).

Els perfils requerits per l'execució de les tasques descrites en l'apartat 1.3 han de complir les següents habilitats en l'àmbit de la gestió d'incidents:

- Coneixement i identificació de tècniques d'intrusió, a partir de l'anàlisi dels informes de notificació de possibles incidents i altres dades. En particular, el personal ha d'estar preparat per identificar nous tipus de tècniques d'atac, indicis d'intrusió, eines d'intrusió o vectors d'atac), obtenir evidències i col·laborar amb el laboratori del gestor del Pla nacional de seguretat TIC de Catalunya en l'anàlisi dels mateixos.
- Tècniques de comunicació segura amb tercers, incloent-hi coneixement detallat de les eines emprades per a la comunicació (correu electrònic, per exemple), per identificar punts de contacte amb els tercers que resultin efectius, protegir (xifrar) les comunicacions de forma apropiada, i coordinar-se amb altres equips de resposta a incidents de seguretat, emprant les eines habitualment emprades pels mateixos (per intercanviar de forma segura informacions o evidències, per exemple).
- Entrenament en els procediments d'anàlisi d'incidents desenvolupats en compliment d'aquest contracte, incloent-hi la determinació de les parts

involucrades, l'incident, l'origen de l'atac, la finestra de temps de l'incident i de la seva resolució, els motius pels quals s'ha produït l'incident, quina era la vulnerabilitat o la debilitat que ha permès la producció de l'incident, quin era el motiu de l'atac, quina informació ha estat perduda o danyada, les eines emprades per a l'atac, el nivell d'accés no autoritzat aconseguit, els llocs tercers involucrats, etc.

En especial, cal considerar la formació de l'equip en les seves responsabilitats en relació amb el nivell i la profunditat de les anàlisis, guies de recol·lecció d'evidències electròniques, prioritats d'actuació i selecció de la resposta adequada.

- Formació en generació i gestió posterior de registres d'incidents, incloent-hi la creació de la documentació suficient i el seu manteniment amb les eines escollides, per facilitar la transmissió del coneixement de les activitats entre els membres del equip, amb el gestor del Pla nacional de seguretat TIC de Catalunya i amb tercers, segons es requereixi.
- Coneixement en les següents eines: eFense Helix, AccesData FTK, DeppFreeze, VMWARE, LiveView, Encase i Norma Analyzer.
- Comunicació en diversos idiomes

1.6. Condicions d'execució

Els recursos aportats pel licitador hauran d'estar ubicats en les instal·lacions del CESICAT i les seves tasques estaran coordinades pel responsable de l'ERI. Tanmateix, l'equipament necessari per dur a terme les seves tasques serà proporcionat pel CESICAT, tot i així, és valorarà l'aportació per part del licitador d'equipament addicional especialitzat que no disposi l'ERI.

1.6.1. Mesures de qualitat en l'execució dels contractes

Durant el desenvolupament dels serveis requerit, CESICAT realitzarà el seguiment dels nivells de qualitat establerts internament i aplicarà un sistema de mesura contínua de la qualitat, segons els estàndards vigents en cada moment. CESICAT farà un seguiment de la qualitat dels treballs realitzats.

1.7. Contingut i estructura de la presentació de l'oferta

El licitador pot adjuntar a la seva oferta tota la informació complementària que consideri d'interès, tot i això, haurà de presentar uns continguts mínims i estar obligatòriament estructurada de la forma següent:

1. Resum executiu.

Resum per a la direcció dels continguts més significatius de la proposta del projecte, destacant-ne la planificació, els recursos i les propostes de valor afegit.

2. Oferta econòmica

L'oferta econòmica haurà de constar de:

- Número de jornades del cap de projecte i el seu cost.
- Número de jornades del consultor sènior i el seu cost.
- Cost total de l'oferta

En totes les valoracions econòmiques, l'IVA ha d'estar inclòs en el preu.

3. Plantejament general del projecte.

Breu resum de la solució proposada als requeriments especificats en aquest plec

4. Solució proposada.

Descripció detallada de la solució proposada. Ha d'incloure una proposta tècnica per a la solució, així com una descripció de les eines que s'utilitzaran per dur-la a terme i una planificació en el temps.

5. Model de relació i de gestió del projecte

Descripció detallada de l'estructura organitzativa i dels procediments de relació (vies de comunicació)

5.1. Model de relació.

5.2. Gestió i seguiment del projecte.

Descripció de les mesures proposades per controlar i assegurar el compliment del projecte realitzat. Cal descriure les eines que donaran suport a la realització del projecte i com seran utilitzades.

5.3. Gestió i control de la qualitat

6. Recursos.

6.1. Descripció de l'equip tècnic.

Descripció detallada de l'equip proposat per al projecte, amb el detall de la seva dedicació total per fases/activitats. També s'inclourà una descripció dels rols assignats.

6.2. Qualificacions(certificacions) del personal tècnic i de gestió assignat.

Detall dels perfils i recursos humans que participaran en el projecte, així com el CV.

7. Oferta de valor afegit.

Descripció de les millores aportades pel licitador. El licitador indicarà les prestacions que ofereix que no estiguin especificades o demanades en el plec i que consideri rellevants per a un millor desenvolupament del servei.

8. Referències en treballs similars.

En aquesta secció el licitador proporcionarà informacions sobre els seus coneixements i les seves referències en projectes similars

9. Annexos.

Adjuntar els annexos sol·licitats o informació addicional que el licitador consideri rellevant.

1.8. Criteris de valoració (en ordre de major a menor puntuació)

1.8.1. Oferta econòmica (de 0 a 50 punts)

Per valorar l'oferta econòmica s'aplicarà la fórmula següent:

$$\text{Puntsoferta} = \text{Màx.pE} \times \left[1 - \left(\frac{\text{Pof} - \text{Pb}}{\text{Pb}} \right) \times 2 \right]$$

On:

Puntsoferta: és la puntuació assignada a l'oferta.

Màx.pE: Màxima puntuació oferta econòmica

Pof: Preu de l'oferta a valorar.

Pb: Preu més baix de les ofertes presentades que no hagin estat desestimades per baixa temerària

1.8.2. Oferta de número de jornades (de 0 a 20 punts)

Per valorar el número de jornades aportades en l'oferta s'aplicarà la fórmula següent:

$$\text{Puntsjornades} = \left[\text{Màx.pJ} \times \left[1 - \left(\frac{\text{MJcp} - \text{OJcp}}{\text{MJcp}} \right) \times 2 \right] \right] \times 0,15 + \left[\text{Màx.pJ} \times \left[1 - \left(\frac{\text{MJcs} - \text{OJcs}}{\text{MJcs}} \right) \times 2 \right] \right] \times 0,85$$

On:

Puntsjornades: és la puntuació assignada a l'oferta.

Màx.pJ: Màxima puntuació per el número de jornades (20 punts).

MJcp: Nombre més alt de jornades oferides per el cap de projecte.

OJcp: Nombre de jornals del cap de projecte de l'oferta a valorar.

MJcs: Nombre més alt de jornades oferides per el consultor sènior.

OJcp: Nombre de jornals del consultor sènior de l'oferta a valorar

Les jornades oferides del cap de projecte tindran un pes del 15% de la puntuació i les jornades oferides del consultor sènior tindran un pes del 85% en la puntuació d'aquest apartat.

1.8.3. Valoració de la qualitat dels recursos aportats (de 0 a 25 punts).

Per valorar la qualitat dels recursos aportats en l'oferta del licitador, s'utilitzaran criteris subjectius tenint en compte el coneixement dels recursos, les certificacions obtingudes i l'experiència en projectes similars dins de l'àmbit dels CERTs.

1.8.4. Valoració de qualitat tècnica de l'oferta (de 0 a 5 punts).

Es valorarà la claredat i qualitat de les ofertes presentades.

Reus, 2 de Setembre de 2010

President de la Comissió Executiva
Fundació CESICAT