

# PLEC DE CLÀUSULES TÈCNIQUES PARTICULARS QUE REGEIX LA CONTRACTACIÓ DEL MATERIAL DEL LABORATORI FORENSE TIC DEL CENTRE DE SEGURETAT DE LA INFORMACIÓ DE CATALUNYA

## 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.



Fig.1 – Àmbit d'actuació del CESICAT

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.

## 2. Objectius i condicions generals

L'objectiu d'aquest plec és **la provisió i desplegament de la infraestructura necessària per a l'ampliació del Laboratori del CESICAT amb l'objectiu de donar suport als processos avançats de resposta a incidents** tals com l'anàlisi forense d'evidències i la investigació digital.

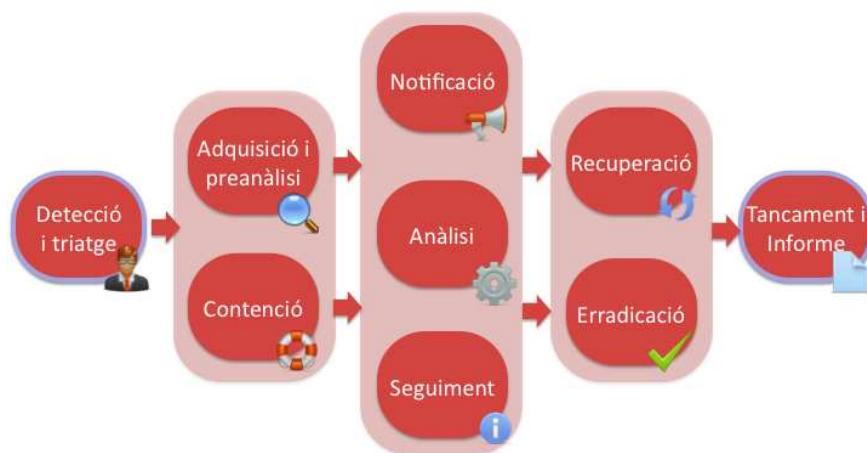


Fig.2 – Fases del cicle de vida de la resposta a incidents (IR)

Els processos d'investigació i anàlisi de primer (*front-end*) i segon nivell (*back-end*) realitzats durant els casos tractats pel CESICAT-CERT poden comportar entre d'altres els següents àmbits d'actuació:

- Suport remot o presencial a incidents i vulnerabilitats
- Adquisició i preservació d'evidències electròniques
- Anàlisi, tractament i correlació d'informació i troballes
- Anàlisi forense i d'enginyeria inversa
- Avaluació de vulnerabilitats i proves de concepte

Els recursos a aprovisionar poden complementàriament donar **suport a l'escalat de consultes i peticions de servei provinents d'altres àrees del CESICAT**, com per exemple dels serveis de seguretat gestionada (SOC) o de processos d'assessorament tecnològic, comportant entre d'altres les següents activitats:

- Servei de detecció/prevenició d'intrusions (IDS/IPS)
  - Creació, adaptació i afinament de configuracions i polítiques de detecció
  - Desenvolupament de signatures específiques
  - Investigació de noves amenaces i tipus de codi maliciós
  - Proves basades en reinjecció de tràfic sintètic o real
- Servei d'anàlisi de vulnerabilitats externes (VA)
  - Creació, adaptació i afinament de configuracions i polítiques d'anàlisi
  - Desenvolupament de mòduls de prova de concepte de vulnerabilitats
  - Investigació i proves de noves vulnerabilitats
  - Proves basades en entorns simulats vulnerables

- Generació de pegats o contramesures
- Servei de llistes de configuració segura (fortificació)
  - Creació, adaptació i afinament de llistes
  - Proves de concepte en entorns simulats amb debilitats
- Servei d'agregació i correlació d'esdeveniments de seguretat (SIEM)
  - Creació, adaptació i afinament de configuracions i polítiques de correlació
  - Desenvolupament de mòduls d'agregació d'esdeveniments i regles de correlació
  - Proves basades en la càrrega d'esdeveniments prèviament generats
- Assessorament tecnològic
  - Creació adaptació i afinament de configuracions d'eines o productes
  - Desenvolupament d'*scripts* de revisió, monitoratge i configuració d'eines

Per a les àrees anteriors, sempre que sigui possible, es delimitaran les eines o productes als quals es prestarà suport amb especial atenció a aquelles basades en codi obert i/o programari lliure.

Per ultim, però no menys important, **el propi ERI compta amb tota una sèrie de processos interns de vigilància tecnològica, entrenament del personal, avaluació de noves amenaces i eines d'atac o de defensa** que també estaran suportats per la infraestructura de laboratori.

Aquesta infraestructura haurà de comptar amb un **conjunt de recursos especialitzats de programari i maquinari** que seran ubicats física i lògicament dintre d'una àrea restringida que permetrà al personal especialista en resposta incidents la realització de tasques avançades d'investigació i anàlisi en les diverses fases segons el flux de treball indicat a la següent figura:



Fig.3 – Flux de treball de la investigació d'un incident

Alguns d'aquests recursos han de conformar un **kit de resposta a incidents (IR/Forensic jumpbag)** que permeti realitzar accions de camp tals com adquisició d'evidències, interceptió de xarxes comunicacions amb i sense fils, i la investigació o anàlisi forense d'informació preliminar durant una resposta presencial.

En la selecció dels components i disseny de la proposta cal tenir en compte els següents aspectes globals:

- Qualitat  
Es necessari incloure elements que realitzin les funcionalitats associades als àmbits descrits en aquest plec cobrint els requeriments establert amb **un nivell de qualitat màxim i prestacions de rendiment adequats**.
- Escalabilitat  
Sempre que sigui possible, els productes o solucions inclosos han de permetre el seu increment en capacitat o prestacions amb el mínim d'inversió considerant

aspectes tals com la modularitat dels seus components tant a nivell funcional com de rendiment.

- Flexibilitat

Es valorarà la capacitat d'adaptació del component en la realització de múltiples funcionalitats en la màxima diversitat d'entorns possibles tant a nivell de funcionalitat com respecte al llicenciat d'aquest per realitzar la seva execució sense simultaneïtat en diversos sistemes o màquines virtuals.

- Seguretat

Els recursos han d'incorporar un mínim de funcionalitats de seguretat de manera nativa com per exemple d'integritat i confidencialitat tant del propi recurs com de la informació tractada per aquest, apart d'intentar proveir mecanismes d'autenticació, autorització (segons diversos rols) i registre de totes les activitats realitzades.

En aquest cas cal **posar especial èmfasi en els mecanismes que permetin garantir la integritat i traçabilitat per a la preservació de la cadena de custòdia d'evidències electròniques i la confidencialitat mitjançant xifrat de la informació sensible.**

- Integració

Es desitjable comptar amb eines que es puguin integrar fàcilment amb eines o productes ja sigui per la existència explícita de mòduls, interfícies (API) o bé mitjançant **l'ús de protocols o formats estàndards d'intercanvi d'informació**, com per exemple les versions més noves d'esdeveniments IODEF/IDMEF, flux de tràfic IPFIX/Netflow, captures de tràfic PCAP, adquisicions forenses de sistemes de fitxers DD/AFF/EWF, entre d'altres.

- Control de les comunicacions

Sempre que sigui possible el programari o maquinari proposat haurà de permetre la configuració d'elements de control de les comunicacions, com per exemple servidors 'proxy' per poder així restringir per política les comunicacions d'aquest a nivell d'aplicació

- Invisibilitat i protecció antiforenses

Considerant que gran part de les eines seran utilitzades en un entorn d'investigació, cal que aquestes incorporin **mecanismes per identificar la seva presència davant de possibles tècniques antiforenses** implementades a les troballes de codi maliciós (*malware*) o codis d'aprofitament de vulnerabilitat (*exploits*) analitzats en aquest entorn.

- Autonomia

Son preferibles les eines que puguin treballar de manera autònoma sense la intervenció de servidors de correlació o intel·ligència centralitzats, normalment proveïts pel fabricant d'aquesta, amb el motiu d'evitar la fuga d'informació sensible de les investigacions cap a recursos externs al laboratori.

En models client/servidor això vol dir comptar desitjablement també amb la versió 'servidor' al propi entorn privat. En el cas d'eines o recursos oferts al núvol (*cloud computing*) en format programari (SaaS), plataforma (PaaS) o infraestructura (IaaS) cal justificar la motivació i descriure tant la arquitectura com els mecanismes de protecció aplicats en el servei.

- Exportació/personalització dels resultats

Es molt aconsellable que es permeti la exportació dels resultats generats per les eines en peces d'informació amb o sense format (*raw*) que permetin fàcilment la seva importació en d'altres eines per al seu tractament manual/automatitzat i incorporació en la documentació del cas.

- Idoneïtat

Cal considerar que l'àmbit d'ús i aplicació de les eines a oferir és el d'un equip de resposta governamental on es poden tractar incidents amb informació sensible i

alguns donant suport a forces policials (LEO) tals com el Cos de Mossos d'Esquadra (CME). Per **tant es preferible optar per eines que siguin d'ús extès per aquestes comunitats i productes amb experiència** per aquestes comunitats.

- Documentació/formació i certificacions professionals

Els aspectes de documentació de la eina, formació remota (en línia) o presencial, i certificacions existents que puguin acreditar el coneixement dels professionals afegeixen un valor afegit substancial a la proposta.

- Política de recompra tecnològica, certificacions i codi obert/dipòsit

Es valoraran les diverses polítiques industrials dels fabricants dels productes oferts en relació a aspectes destacables tals com la política de recompra (en els casos de maquinari) o de descomptes (en el cas de programari) per evolucionar a noves versions 'grans' del producte, la possessió de certificacions de seguretat nacionals o internacionals que acreditin la seguretat del producte (*Common Criteria*, FIPS...).

També cal considerar aspectes com disposar del codi obert i/o llicenciat amb programari lliure, o fins amb un acord de dipòsit per al seu accés en cas necessari (*escrow*).

- Compliment de garantia del maquinari

Tots el maquinari ofert haurà de disposar d'una garantia de 3 anys com a mínim.

- Llicències

Tot el programari ofert ha d'incloure les llicències d'ús per els propers 3 anys, incloses les actualitzacions menors de producte.

### 3. Situació actual

#### 3.1. Infraestructura bàsica

El laboratori ha de comptar amb una infraestructura bàsica que permeti 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'accés 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.

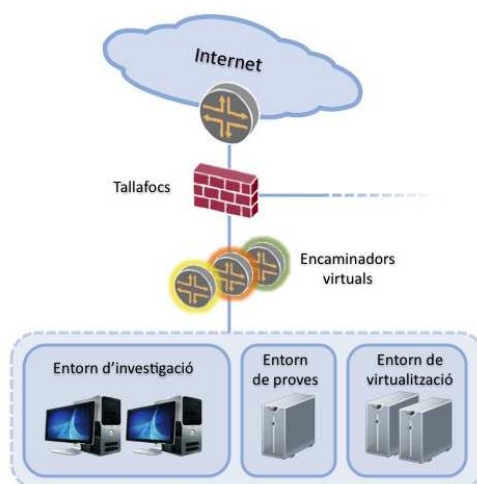


Fig.4 – Diagrama lògic de la infraestructura de laboratori

A efectes informatius, aquest entorn compta actualment amb els següents recursos:

- Armari ignífug per a la preservació d'evidències electròniques
- Armari en format 19" de mig cos d'alçada amb rodes per allotjament del maquinari
- Base de corrent per armari (1U) per a la connexió de tots els elements inclosos
- Infraestructura de cablatge entre l'armari i els punts d'accés a la xarxa
- Línia de comunicacions ADSL per connectivitat fora de banda amb mínim de 4Mbps
- Eina de tiqueting per a la comunicació i documentació dels casos investigats
- Tallafocs de xarxa amb un mínim de 3 interfícies *FastEthernet* i capacitats VPN
- Commutador de nivell 2-3 amb mínim 24p *GigabitEthernet* i capacitats VLAN/VRF
- Servidor de virtualització d'altres prestacions basat en Intel Xeon amb 32GB de RAM, 2 disc durs de sistema SAS de 146 GB (15000 rpm) en RAID i 2 disc durs de dades SATA de 300GB (1000 rpm) - Programari VMWare ESXi
- Estació de treball basada en Intel Core i7 amb 16GB de RAM i 2 TB de disc local
- 2 discs durs SATA d'1TB per a la preservació i càrrega de màquines virtuals

### 3.2. Entorn de resposta presencial

Per a la prestació de serveis de resposta de manera presencial es fa necessari comptar amb una sèrie de recursos que permetin realitzar accions de camp tals com adquisició d'evidències, intercepció de xarxes comunicacions amb i sense fils, i la investigació o anàlisi forense d'informació preliminar. Aquest conjunt de recursos es normalment conegut com a **kit de resposta a incidents (IR/Forensic jumpbag)**.

A efectes informatius aquest entorn ja compta amb els següents recursos:

- Maletí d'alumini robust per al transport de tots els elements
- Portàtil d'altres prestacions amb 4GB de RAM, disc dur d'estat sòlid (SSD) de 200GB i interfície Serial ATA externa
- Dispositiu de signatura, clonació i esborrat segur d'altres prestacions (>500 Mbps) per suports IDE/SATA
- Lector de targetes de memòria i suports flexibles com disquets
- Dispositius de bloqueig d'escriptura IDE/SATA/USB/SCSI
- Cablejat i adaptadors per discs durs de diversos formats
- Adaptadors de corrent per diversos connectors internacionals
- Kit d'eines per muntat/desmuntat de portàtils i dispositius
- Camara fotogràfica i de gravació d'audio digital
- Concentrador USB de 4 o mes ports
- Concentrador *Ethernet* de 4-8 ports
- Kit de preservació (bosses), documentació de custòdia i etiquetat d'evidències
- 4 discs durs SATA de 1TB per a la còpia d'evidències i recollida d'informació
- Dispositiu d'intercepció passiva de tràfic (tap) amb tecnologia FastEthernet 10/100
- Llicència de programari d'anàlisi forense Encase
- Màquina virtual VMWare amb diverses eines preinstal·lades de programari lliure i comercials cobrint aspectes tals com recuperació de dades, anàlisi de logs, identificació/classificació de fitxers, manipulació i anàlisi de binaris, esborrat de suports, trencat de contrasenyes, anàlisi forense d'aplicacions tipus navegador/client de correu, eines antivirus, anàlisi forense de xarxa, etc.

### 3.3. Eines de laboratori bàsiques

Per a la investigació i anàlisi forense de gran part dels casos tractats per l'ERI s'hauran de carregar les dades recollides durant l'adquisició d'evidències remota o presencial i fer-ne el seu adequat tractament amb una gran diversitat d'eines específiques.

Aquest entorn compta actualment amb els següents recursos:

- Diverses caixes USB SATA/IDE de 2,5" i 3,5"
- Programari d'investigació digital *Paterva Maltego 2*
- Programari d'enginyeria inversa *DataRescue IDA Pro Advanced*
- Programari d'enginyeria inversa *DataRescue Hex-Rays decompiler*
- Programari de suport remot *F-Response Tactical*
- 2 discs durs SATA de 1TB per a la còpia d'evidències i càrrega d'informació

### 3.4. Eines de laboratori avançades

Considerem com a eines de laboratori avançades, el següent conjunt de productes:

- **Recuperació i trencat de contrasenyes**

Aquestes han d'oferir la possibilitat de realitzar atacs de força bruta sobre fitxers de contrasenyes o peces d'informació per obtenir informació respecte a les contrasenyes o accedir als continguts protegits o xifrats d'informació (fitxers comprimits, sistemes de fitxers xifrats, captures de tràfic, ...)

- **Anàlisi forense de xarxa**

Eines específiques per al tractament de captures de tràfic de xarxes amb o sense fils en temps real o diferit que permeti la obtenció d'informació útil a nivell estadístic, recuperació de continguts, identificació de protocols, entre d'altres.

- **Anàlisi de codi maliciós**

Per a l'anàlisi d'artefactes digitals que continguin codi maliciós es fa necessari comptar amb eines avançades d'anàlisi de comportament, enginyeria inversa, anàlisi de codi, etc. Aquestes han de permetre anàlisi automàtic generant informes resum (accions al sistema, captures de tràfic, captures de pantalla...), però també de caire manual per ésser controlat per l'analista en un entorn simulat o fins i tot amb interconnexió amb la Internet.

- **Recuperació de dades**

Aquestes eines ofereixen capacitats de recuperació d'informació dintre de suports de diversos tipus (òptics, magnètics...) que s'hagin corromput a nivell lògic o físic. En cas de problemes físics compten amb els recursos adients per migrar la informació de suport físic.

- **Adquisició i anàlisi de dispositius mòbils**

La particularitat de les plataformes mòbils fa necessari comptar amb eines específiques per a la adquisició d'informació continguda en aquests a diversos nivells (*firmware*, SO, suports...). Aquestes permeten recuperar a baix nivell informació comuna en aquestes plataformes com poden ésser els missatges SMS/MMS, informació de trucades, etc.

Actualment no és disposa cap d'aquestes eines.

## 4. Requeriments del maquinari i programari a oferir.

Tots els dispositius proveïts per l'adjudicatari hauran de ser productes catalogats i que gaudeixin de manteniment del fabricant. En cap cas es proveirà material descatalogat.

L'adjudicatari haurà de proveir de tots els cables de xarxa i elèctrics, connectors i altres elements necessaris per tal d'enracar i posar en marxa tot el maquinari.

Tots els dispositius hauran de ser de fabricants de fiabilitat contrastada, i es valoraran els dispositius amb tecnologia evolucionada.

A continuació es descriu els requeriments del maquinari i del programari que han de formar part obligatòriament de l'oferta:

### 4.1. Descripció del maquinari:

- 1 Servidor de virtualització d'altres prestacions equivalent o superior a l'indicat anteriorment suportat pel programari de virtualització VMWare ESXi
- 1 Servidor físic de prestacions mitjanes per a proves sense virtualització amb 8GB de RAM i discs durs SATA amb un mínim de 100-200GB de capacitat
- 1 x Estació de treball equivalent o superior a l'indicada anteriorment
- 1 x *Kit* conformat pel maletí i tots els elements de maquinari i programari descrits anteriorment per tal de redundar els recursos i ampliar la capacitat de resposta simultània
- 8 x discs durs SATA de 1TB o superior
- 2 x *Kit* de Pantalla, teclat i ratolí de dimensions reduïdes amb adaptadors (USB-Sèrie, VGA/DVI...) per poder treballar amb maquinari propi o de tercers
- 1 x Caixa ignífuga portàtil per al transport segur de suports o dispositius sensibles des de la seva recollida presencial fins al tractament i dipòsit al laboratori.
- 4 x Bosses amb aïllament de tipus "caixa de *faraday*" per a la recollida de dispositius amb capacitats de comunicacions sense fils (WLAN, Bluetooth, 3G) tals com terminals de telefonia mòbil, PDA, telèfons intel·ligents, etc.
- 2 x Punts d'accés sense fils amb tecnologia 802.11g (WLAN) i mecanismes de seguretat WPA2 (AES-CCMP) amb connectivitat de tipus 3G HSDPA (WWAN)
- 2 x Kit sense fils conformat per targeta 802.11g o superior amb connector per targeta externa, fuetons coaxials i un parell d'antenes omni/direccionals.
- 1 x Dispositiu Voom Shadow d'emascament i memòria de transaccions de suports que permeti el treball en viu en un sistema amb la capacitat de tornar enrere al seu estat original.
- 1 x Lector de targetes de memòria de múltiples formats: CF, MMC, MS, MD, XD, SD...
- 1 x Lector de targetes SIM
- 2 x Estacions de reduïdes dimensions (sonda) en format *barebone* o *nettop* per entorns d'intercepció de tràfic i anàlisi forense de xarxa amb un mínim de 3 interfícies de xarxa *FastEthernet* amb fil i 1 sense fil *802.11g* amb possibilitat de connexió d'antena externa.
- 1 x Tableau Drive Cooler
- 1 x Tableau Forensic Brige per a workstation
- 1 x Rainbow tables

## 4.2. Descripció del programari:

- 2 x Llicències de programari eFense Helix 3 Pro d'adquisició d'evidències
- 2 x Llicències de programari AccesData FTK 3.0 d'anàlisi forense
- 2 x Llicència de programari DeepFreeze de congelació/instantànies del sistema tipus per als servidors físics de proves
- 4 x Llicències VMWARE workstation.
- 2 x Llicències LiveView
- 2 x Llicències Encase
- 2 x Màquines virtuals VMWARE forense
- 1 x Llicència de Zynamics PDF Dissector
- 1 x Eina d'anàlisi interactiu Norman Analyzer pro
- 3 x Eina d'anàlisi automàtic Norman Online

L'oferta de l'adjudicatari inclourà la llicència complerta per al programari descrit permetent-ne la seva explotació d'acord amb els requeriments del CESICAT. A tal efecte, per llicència complerta s'entendrà la totalitat de drets i permisos necessaris sobre la versió del programari sol·licitada i que inclogui les funcionalitats descrites pel fabricant per la versió en cada moment.

Les llicències de programari sol·licitades hauran de permetre al CESICAT la prestació dels seus serveis als clients propis així com la posada a disposició del programari als seus clients per a oferir serveis als col·lectius finals a qui es dirigeixin. Les llicències hauran de ser vàlides per un període mínim de tres anys (a comptar des de la data de posada a disposició del programari), incloent en el preu les actualitzacions, millores o desenvolupaments que es realitzin durant aquest període. Les llicències hauran de tenir caràcter mundial permetent l'ús del programari per part dels usuaris autoritzats a qualsevol ubicació. Així mateix, el nombre de llicències indicat per a cada programari fa referència al nombre d'usuaris del CESICAT que haurà de poder utilitzar el programari de manera simultània, essent acceptable qualsevol llicència col·lectiva que amplii el nombre mínim d'usuaris sol·licitat mantenint els perfils mínims requerits.

En cas que el programari estigui disponible sota alguna llicència reconeguda com a "open source" o codi obert el CESICAT haurà de disposar de tots els drets i mitjans necessaris per a explotar el programari i desenvolupar-lo per tal de donar cobertura a les necessitats comunicades en el present procediment de contractació. L'adjudicatari aportarà els diferents elements d'aquest programari (codi font, codi objecte, etc.) per tal de permetre la correcta explotació per part del CESICAT.

En qualsevol cas, el resultat de l'ús del programari i les dades gestionades mitjançant el mateix són i hauran de romandre titularitat del CESICAT sense que aquest en garanteixi cap dret a l'adjudicatari o al titular dels drets del programari. Per tant, no s'acceptarà cap llicència de programari, inclòs en els casos d'ús del programari en línia o d'altres, que contravingui aquesta previsió o que garanteixi cap dret a l'adjudicatari o al titular del programari sobre les dades, informació o d'altres elements titularitat del CESICAT i gestionats mitjançant el programari.

## 5. OFERTA DE VALOR AFEGIT.

Opcionalment el licitador per tal d'incrementar el valor de la seva oferta pot afegir maquinari i/o programari adicional. Tot seguit, presentem un llistat d'elements que poden ser d'interès per al CESICAT, tot i que també es valorarà l'oferiment d'altra equipament relacionat amb la investigació digital i l'anàlisi forense.

### 5.1. Es valorarà la incorporació dels següents recursos opcionals:

- Programari de suport amb capacitats de control gràfic de sistemes remots multiplataforma amb un mínim de 2 llicències simultànies tipus NTRSupport, Cisco WebEx, etc.
- Fuetons de xarxa UTP necessaris per a la connexió dels elements als punts de xarxa
- Sistema d'alimentació ininterrompuda (SAI) exclusiu per als sistemes de laboratori
- Eina o sistema que permeti la destrucció física de suports òptics, magnètics i electrònics (DVD/CD, discs durs, memòries/pendrives)
- 2 x terminals mòbils i/o mòdems 3G HSDPA per a connectivitat WWAN del portàtil
- 1 x Dispositiu d'emascament i memòria de transaccions (*shadow*) de suports que permeti el treball en viu en un sistema amb la capacitat de tornar enrere al seu estat original.
- Dispositiu d'intercepció (tap) 10/100/1000 Base-T
- Estació en format *barebone* o *nettop* per entorns d'anàlisi forense de xarxa amb un mínim de 3 interfícies de xarxa *FastEthernet* amb fil i 1 sense fil *802.11g* amb antena externa.
- Macbook (gamma baixa) entorn OSX.
- 1 x dispositiu d'intercepció (tap) de fibra monomode 1000LX
- Llicència tipus NortonGhost o equivalent.
- Llicència RealVNC.
- Llicència F-Response Tactical Gov
- Llicència X-Ways d'anàlisi forense
- Fred SC + Elcomsoft o workstation amb GPUs equivalent
- Tap de fibra multimode amb connectors LC i SC.
- Hub USB
- Hub SATA
- Connectors USB-Ethernet, USB-Serie.
- Càmera fotogràfica
- Shredder per a suport paper, CD/DVD/smartcard, etc.

Queden fora de l'àmbit d'aquesta secció les llicències associades a les possibles màquines virtuals a incloure en els sistemes de virtualització i les targetes SIM associades als dispositius 3G com punt d'accés i terminal mòbil.

### 5.2. Formació

Es valorarà com a opcional la formació del programari/maquinari ofert o de les tecnologies/metodologies associades a aquests, i de les certificacions professionals a cursar que s'inclouin per al personal tècnic del CESICAT.

## 6. Compra i recepció del maquinari i programari.

Una vegada s'hagi adjudicat el plec, l'adjudicatari haurà de fer la compra del maquinari i programari als fabricants amb els següents requeriments:

- La recepció del material (maquinari i programari) la farà a les seves instal·lacions i es responsabilitzarà de rebre tot el material i que arriba en perfecte estat.
- L'emmagatzematge del material s'haurà de fer en instal·lacions de l'adjudicatari i en unes condicions de seguretat física adequades. L'adjudicatari serà responsable de garantir aquesta seguretat. En el cas de pèrdua de material, l'adjudicatari haurà de reposar el material perdut en un temps màxim de 20 dies.
- El licitador donarà instruccions a l'adjudicatari per realitzar l'entrega i instal·lació del material en les instal·lacions del CESICAT.

## 7. PRESSUPOST DE L'OFERTA

El pressupost estimat per a l'adquisició del maquinari i programari és de 130.000€ (l'IVA inclòs).

## 8. PRESENTACIÓ DE L'OFERTA

Les ofertes s'hauran de presentar en format electrònic (en MS Office o PDF) i hauran d'incloure la següent informació:

- **Descripció general de l'empresa** o empreses que es presentin conjuntament. Relació de referències en projectes similars amb una breu descripció de l'objectiu i abast de cadascun.
- **Solució proposada:**
  - Proposta del maquinari
  - Descripció del maquinari
  - Descripció del programari
  - Descripció de les garanties.
  - Calendari d'actuació.
  - Relació de documents a lliurar.
- **Oferta econòmica:**

L'oferta econòmica (amb l'IVA inclòs) estarà desglossada en els següents conceptes:

- Preu total de l'oferta
- Preu del maquinari.
- Preu del programari
- Preu de les garanties.

## 9. CRITERIS DE VALORACIÓ (en ordre de major a menor puntuació)

### 9.1. Oferta econòmica (De 0 a 70 punts).

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

$$rta = M\grave{a}x.pE \times \left[ 1 - \left( \frac{Pof - Pb}{Pb} \right) \times 2 \right]$$

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

### 9.2. Oferta valor afegit (De 0 a 20 punts)

Per valorar l'oferta de valor afegit s'utilitzaran criteris subjectius tenint en compte el valor, la qualitat i la quantitat dels elements ofertats.

### 9.3. Qualitat tècnica de la oferta (De 0 a 10 punts).

Es valorarà la claredat i qualitat de les ofertes.

## 10. Glossari

AES	Advanced Encryption Standard
AFF	Advanced Forensics Format
API	Application Programming Interface
AV	Anàlisi de Vulnerabilitats
CCMP	Counter mode with cyper block Chaining Message authentication code Protocol
CERT	Computer Emergency Response Team
CME	Cos dels Mossos d'Esquadra
COS	Centre d'Operacions de Seguretat
ERI	Equip de Resposta a Incidents
EWF	Expert Witness Format
FIPS	Federal Information Processing Standard
IaaS	Infrastructure as a Service
IDE	Integrated Device Electronics
IDS	Intrusion Detection System
IDMEF	Intrusion Detection Message Exchange Format
IODEF	Incident Object Description and Exchange Format
IPFIX	IP Flow Information eXport
IPS	Intrusion Prevention System
IR	Incident Response
LAN	Local Area Network
LEO	Law Enforcement Organization
OLA	Operational Level Agreement
NSP	Network Service Provider
PaaS	Platform as a Service
PCAP	Packet CAPture
PDA	Personal Digital Assistant
RAID	Redundant Array of Independent Disks
SaaS	Software as a Service
SATA	Serial Advanced Technology Attachment
SAI	Sistema d'Alimentació Ininterrumpoda
SCSI	Small Computer System Interface
SLA	Service Level Agreement
SIEM	Security Information Event Management
SSD	Solid State Disk
SOC	Security Operation Center
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VA	Vulnerability Analysis
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WPA	Wireless Protected Access