

Plec de prescripcions tècniques que regulen el subministrament i manteniment d'una plataforma de mitigació d'atacs de Denegació de Servei Distribuïts (DDoS) per a l'Anella Científica

Barcelona, a la data de les signatures electròniques

Validat per,	Aprovat per,

Sumari

Prescripcions tècniques	5
1. Antecedents	5
2. Abast del projecte	8
3. Característiques de la solució	9
3.1. Arquitectura de la solució	9
3.2. Sistema de detecció, visualització i mitigació	9
3.3. Instal·lació, manteniment, formació i documentació	12
3.4. Política de creixement	14
3.5. Característiques tècniques i funcionals complementàries	14
4. Servei 24x7	15
Annex: Característiques actuals.....	15

Prescripcions tècniques

1. Antecedents

El Consorci de Serveis Universitaris de Catalunya (CSUC) va néixer per impulsar l'eficiència en la gestió de les universitats catalanes a través de la cooperació i la coordinació, a iniciativa de la Generalitat de Catalunya. Està integrat per la Generalitat de Catalunya i les següents universitats: la de Barcelona, l'Autònoma de Barcelona, la Politècnica de Catalunya, la Pompeu Fabra, la de Lleida, la de Girona, la Rovira i Virgili, i la de Vic-Central de Catalunya. A més, l'Oberta de Catalunya i la Ramon Llull hi participen com a membres agregats.

El CSUC ofereix un ampli ventall de serveis per a la universitat i la recerca, basant-se en diverses línies d'activitat: els sistemes per a càlcul científic; les xarxes de comunicacions; els portals i repositoris; l'administració electrònica; el suport per millorar els serveis bibliotecaris; la consorciació de serveis; la promoció d'aquests serveis, i l'operació i el manteniment de la infraestructura del Consorci.

Dins l'àmbit de les comunicacions, el CSUC gestiona l'Anella Científica, la xarxa acadèmica d'altres prestacions que connecta més d'una vuitantena d'institucions amb qualitat de servei i banda ampla; el node de RedIRIS a Catalunya, que proveeix de l'accés a les xarxes de les altres comunitats autònomes, a la paneuropea Géant i a les internacionals més avançades de recerca, i del Punt Neutre d'Internet a Catalunya (CATNIX), que afavoreix l'intercanvi de tràfic entre els diferents proveïdors d'internet i facilita l'accessibilitat de la informació.

Les institucions que es connecten a l'Anella Científica (vegeu Figura 1Figura 1), ho fan amb cabals que van des dels 50 Mbps fins als 200 Gbps usant diverses tecnologies (majoritàriament Ethernet com a connexió principal i *backup* en Ethernet, FTTH o 4G depenent de la connexió). Les connexions es fan o bé via un operador, que proveeix capacitat o línies dedicades, o bé mitjançant fibra òptica pròpia de les institucions o del CSUC o d'un operador.

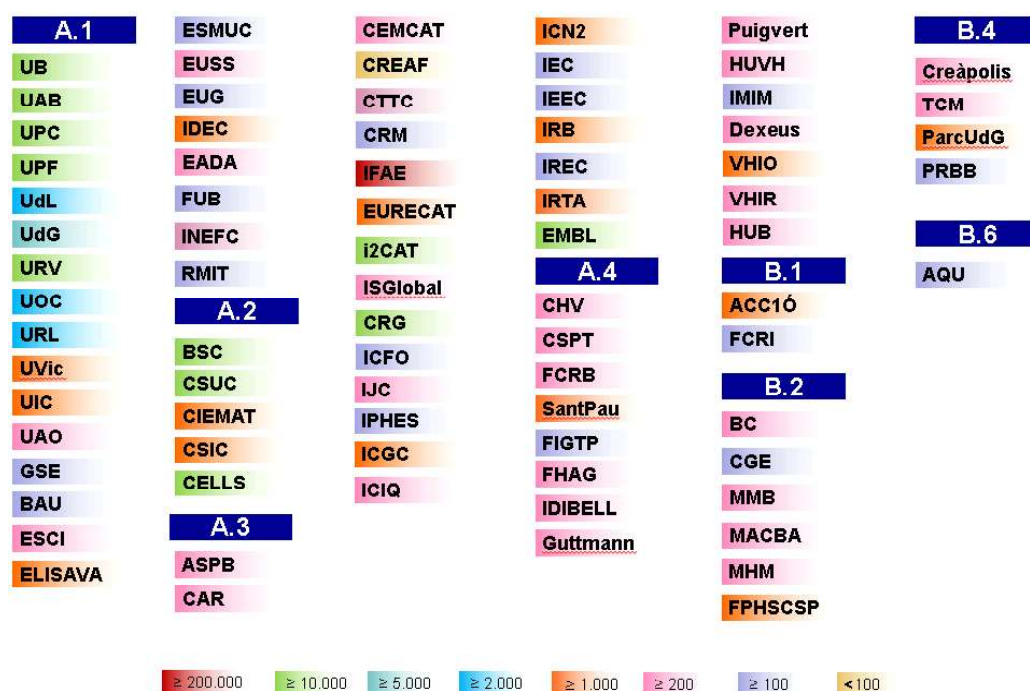


Figura 1. Institucions connectades i cabal de connexió

Els equips troncal de l'Anella Científica es divideixen actualment en dos nivells (commutació i encaminament, o *switching* i *routing*) i estan distribuïts en dos nodes, Campus Nord (CSUC-CN) i Equinix (CSUC-T) amb un commutador i un router en cada node, quatre en total. Els enllaços entre aquests quatre equips són de 200 Gbps entre equips de diferent nivell dins del mateix node (2x100 Gbps en cada node), de 200 Gbps entre commutadors de diferents nodes (2x100 Gbps) i de *backup* de 40 Gbps entre encaminadors de diferents nodes (4x10 Gbps), formant un rectangle.

Els enllaços amb RedIRIS pel tràfic regular en ambdós nodes són de 100 Gbps, als que s'han de sumar els enllaços de projectes especials, els enllaços entre nodes troncal i els nodes del Vallès, fins arribar a un total de 8 enllaços de 100 Gbps i 3 enllaços de 10 Gbps amb Campus Nord, (2 a l'encaminador i 9 al commutador) i 5 enllaços de 100 Gbps i 2 enllaços de 10 Gbps a Equinix (2 a l'encaminador i 5 al commutador). La Figura 2 mostra els equips y enllaços amb RedIRIS.

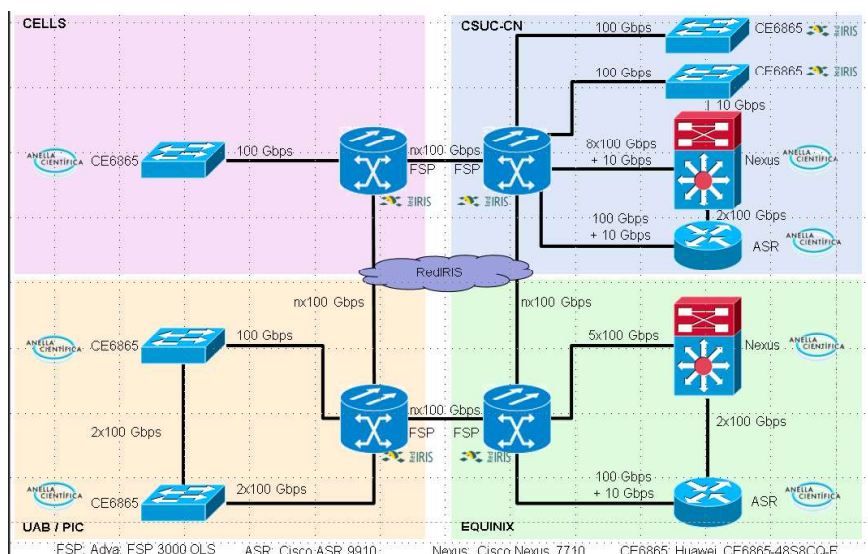


Figura 2. Equips i enllaços entre RedIRIS-NOVA100 i l'Anella Científica

Com a complement de la sortida a internet a través de RedIRIS, l'Anella Científica disposa en ambdós nodes d'una sortida pròpia de 10 Gbps a través d'Orange per les institucions que no compleixen els requisits d'afiliació amb RedIRIS. Aquesta connexió es troba redundada amb un enllaç de *backup* d'1Gbps a cadascun dels dos nodes via Cogent. A més a més, l'Anella Científica disposa d'una excel·lent connectivitat amb altres operadors a través de CATNIX, el Punt Neutre d'Internet a Catalunya, al que l'Anella Científica es connecta amb quatre enllaços de 10 Gbps (4x10 Gbps) a cadascun dels seus nodes.

Tant al troncal com amb les institucions, s'utilitzen mecanismes de redundància a nivell d'encaminament dinàmic, establint sessions BGP de diversos tipus: entre els dos nodes troncal (CSUC-CN i CSUC-T), amb RedIRIS als seus nodes de presència a TELMAD i CIEMAT i, finalment, amb les institucions. A la Figura 3 es poden veure els diversos circuits on s'utilitza la redundància BGP: amb les institucions connectades, entre els nodes del CSUC, amb RedIRIS i al CATNIX.

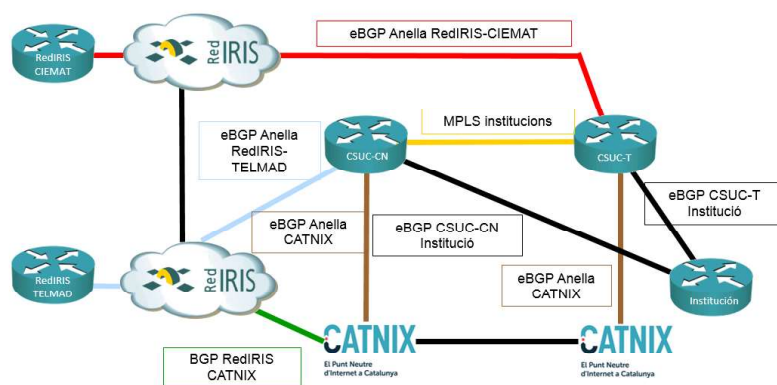


Figura 3. Encaminament i redundància a l'Anella Científica

Els encaminadors troncal tenen definits diferents entorns o encaminadors virtuals (VRF, *VPN Routing and Forwarding*) en que se separen les diferents comunitats:

- Institucions amb adreçament de RedIRIS i sortida via RedIRIS.
- Institucions amb adreçament de l'Anella Científica i sortida via RedIRIS.
- Institucions amb adreçament de l'Anella Científica i sortida via proveïdors comercials.
- Connexió al Punt Neutre d'Internet a Catalunya, CATNIX.

Aquests encaminadors virtuals permeten l'exportació i importació selectiva de rutes per encaminar el tràfic entre ells de manera transparent per a les institucions.

També hi ha altres encaminadors virtuals (VRF) dedicats a la gestió i monitoratge

Actualment el CSUC té en producció una plataforma de mitigació d'atacs de denegació de servei. L'arquitectura actual de la plataforma consta de dos *VRF*, una pel tràfic brut i una altra pel tràfic net. A la *VRF* brut, s'anuncia la xarxa que és vol mitigar, d'aquesta forma solament la xarxa anunciada serà objecte de la mitigació. A la *VRF* net una vegada s'hagi aplicat el procés de mitigació, el tràfic torna cap a la institució.

La plataforma actual consta de dos equipaments del fabricant Netscout; el sistema de detecció (Sightline SP-7000) i visualització, i el sistema de mitigació (TMS 2800).

La plataforma de mitigació d'atacs de denegació actual pot mitigar fins a 10 Gbps i és necessari actualitzar-la d'acord amb els enllaços actuals de l'Anella Científica, amb interfícies de 100 Gbps i tenint en compte el seu futur creixement.

A més, la plataforma actual es troba a prop del *EoM* (*End of maintenance*) i es fa necessari l'adquisició d'una nova plataforma per poder fer front als atacs que es produeixin.

2. Abast del projecte

L'objectiu d'aquesta licitació és l'adquisició d'una plataforma per a la mitigació d'atacs de denegació de servei. Aquesta plataforma ha de permetre:

- Detectar atacs de DDoS fora de línia mitjançant Netflow.
- Mitigar els atacs de DDoS desviant el tràfic atacat mitjançant el protocol d'encaminament dinàmic BGP, sense desviar o interferir en la resta del tràfic regular o de projectes de la resta d'institucions.
- Disposar d'una sola consola per a la gestió, independentment de si la plataforma està formada per un o diversos equips.

3. Característiques de la solució

En aquesta secció es descriuen els requisits mínims que ha de complir la solució. En primer lloc es detalla com ha de ser l'arquitectura de la plataforma, en segon lloc el sistema de detecció, visualització i mitigació, , en tercer lloc, es detallen les condicions d'instal·lació, manteniment, formació i documentació i, a continuació la política de creixement. Per acabar, s'enumeren les millores addicionals que els licitadors poden oferir.

3.1. Arquitectura de la solució

Els requisits mínims de la solució pel que fa a la seva arquitectura són:

- 1 Funcionament totalment fora de línia.
- 2 Hardware dedicat *on premise*.
- 3 Tots els components i llicències han de ser del mateix fabricant per garantir la interoperabilitat i optimització en la resolució d'incidències.
- 4 Ha de proporcionar un panell únic per gestionar totes les operacions.
- 5 Ha de ser capaç de detectar alertes i mitigar, des de el primer moment de la instal·lació, sense esperar a cap aprenentatge.
- 6 Integració total en l'arquitectura de l'Anella Científica, permetent la detecció i mitigació d'atacs per a qualsevol institució, independentment de l'encaminador virtual al que es trobi.
- 7 En cap cas l'equipament proposat ha d'interferir en el funcionament normal de l'Anella Científica ni provocar retards o problemes a la xarxa o els serveis implementats en ella.

3.2. Sistema de detecció, visualització i mitigació

Els requisits mínims del sistema de detecció, visualització i mitigació són:

1. Configuració d'objectes de gestió mitjançant rangs d'adreces amb les seves corresponents màscares.
2. Monitoratge i detecció d'atacs mitjançant la correlació i anàlisi del tràfic rebut amb el protocol d'encaminament dinàmic BGP, els estàndards d'exportació de paquets Netflow i/o sFlow i el protocol de gestió de xarxa SNMP.
3. Visualització de tràfic amb filtratge per aplicació, protocol, port, IP origen i destí o sistema autònom, entre altres.
4. Capacitat de configurar intervals de temps diferents en la visualització de tràfic.
5. Monitoratge en temps real.
6. Detecció basada en canvis de comportament en els patrons de tràfic respecte els perfils històrics prèviament recollits i/o configurats mitjançant mostreig.
7. S'han de poder configurar *baselines* per protocols ICMP, TCP, UDP, GRE, ESP entre altres i per objectes gestionats.

8. Capacitat de monitorar les interfícies a totes les velocitats existents actualment a l'Anella Científica, des de 50 Mbps a 200 Gbps.
9. Capacitat de crear un mínim de 1000 objectes gestionats diferents, per aplicar criteris de detecció i llindars diferents per a 1000 institucions i/o subxarxes.
10. Notificació d'alertes, excés de tràfic respecte al funcionament normal de la xarxa i violacions en l'ús dels protocols (patrons de tràfic inclouen TCP SYN, TCP FIN, TCP RST, TCP ACK, TCP SYN-ACK y TCP URG, TCP PSH, TCP slow, TCP Null, ICMP, IP Null, fragments IP i tràfic des d'adreces *multicast* entre d'altres).
11. Ha de permetre la identificació d'inici i final de les anomalies, gravetat, patró de tràfic i objecte administrat.
12. Capacitat d'identificar l'adreça o adreces IP origen de l'atacant/s.
13. Ha de poder enviar alertes per correu electrònic, diferenciades segons el client o objecte atacat.
14. Ha de poder generar missatges SNMP i enviar remotament missatges via *syslog*.
15. Les alertes proporcionades pel sistema s'han de poder classificar en tres nivells segons la seva importància: baix, mitjà i alt.
16. S'han de poder generar alertes quan:
 - Es sobrepassin uns determinats llindars.
 - El procés de recollida BGP deixi de funcionar.
 - Es produeixi un canvi de configuració en el sistema.
 - El protocol SNMP no sigui accessible als encaminadors.
17. Ha de permetre diferents rols per als usuaris, i poder restringir la visualització per a cada usuari segons l'objecte.
18. Ha de permetre fer informes d'anàlisi de tràfic per *peer*, per prefix, per interfície, per objecte i per institució.
19. Diferents nivells d'informes per a diferents objectes amb detalls en temps real i informació històrica.
20. Ha d'executar informes programats i en temps real que incloguin:
 - Anomalies classificades per nivells de gravetat.
 - Anomalies per tipus, incloent com a mínim: fragmentació IP, protocol, amplada de banda, ICMP, TCP/SYN.
21. Ha d'executar informes amb:
 - Alertes i mitigacions (actives o anteriors), incloent paquets/segon descartats i no descartats en cada opció de mitigació
 - Distribució d'amplada de banda
 - Per protocol
 - Les adreces IP que més utilitzen la xarxa
 - Per aplicació
 - Per tràfic multicast
 - Registre de sistemes autònoms origen/destí
 - Mida del paquet
 - QoS
 - Un classificador de cucs (worms)
 - Per lloc i aplicacions caigudes
 - Per tràfic IPv6

- Per localització
22. Gestió via interfície gràfica d'usuari amb accés https, consola CLI accessible amb ssh i SNMPv2.
 23. Ha de suportar 25 usuaris de gestió simultanis
 24. Ha d'existir un control d'accés sobre la interfície de gestió per evitar accessos no desitjats.
 25. Ha de permetre fer *backup* de les bases de dades d'objectes, *templates* i informes i guardar-los remotament.
 26. Ha de disposar d'un mínim de dues interfícies de 10 Gbps per a la gestió amb els *transceivers* SFP+ corresponents.
 27. Tots els components han de tenir fonts d'alimentació redundants en AC a 220 V.
 28. La potència màxima necessària per alimentar la solució ha de ser inferior a 2500 W.
 29. Ha de permetre emmagatzemar les actualitzacions de programari de la pròpia plataforma.
 30. Ha de disposar de dos ports de 100 Gbps per a connectar amb els equips troncal de l'Anella Científica per a la mitigació. S'inclouran quatre QSFP28 SR4 o LR4, dos per la plataforma de mitigació, i els altres dos per l'ASR9910 compatibles entre ells.
 31. Capacitat mínima de mitigació de 20 Gbps.
 32. Possibilitat d'ampliació a una capacitat de mitigació màxima de fins a 400 Gbps.
 33. Capacitat de fer fins a 300 mitigacions simultànies.
 34. Escalabilitat, permetent l'ampliació de les seves capacitats de mitigació sense canviar el maquinari complet ofert.
 35. En cas d'atac, el sistema ha de permetre bloquejar el tràfic i limitar l'amplada de banda que pot consumir una aplicació.
 36. Ha de ser capaç de mitigar atacs d'una sola màquina (prefix /32) fins a prefixos /16 en IPv4.
 37. Ha de ser capaç de mitigar atacs d'una sola màquina (prefix /32) fins a prefixos /128 en IPv6.
 38. Ha de permetre fer mitigacions de les següents maneres:
 - Injecció de *blackhole* mitjançant BGP
 - Desviament de l'anunci mitjançant Flowspec cap a l'equip de mitigació per IPv4 i IPv6
 - Filtrat amb llistes d'accés
 - Desviament mitjançant BGP a l'equip de mitigació en IPv4 i IPv6
 39. No interrupció del tràfic legítim, filtrant el tràfic maliciós mentre es permet el tràfic vàlid cap a les adreces atacades.
 40. Ha d'entendre AS_PATH complets i comunitats BGP de múltiples Sistemes Autònoms (AS, *Autonomous System*), incloent Sistemes Autònoms privats.
 41. Proveir firmes d'atacs coneguts per a la seva detecció immediata (intel·ligència).
 42. Mitigació d'amenaques no conegudes (amenaces de dia zero).
 43. Anàlisi i filtratge d'atacs DNS, HTTP Get flood, HTTP post flood, establiment HTTPS, connexions inactives o SIP, entre d'altres. Ha de ser capaç d'oferir la creació de *fingerprints* basats en ports TCP i UDP i també generats automàticament segons els perfils de tràfic maliciós detectat i netejar el tràfic en funció d'aquests *fingerprints*.

44. Ha de disposar d'una anàlisi i creació dinàmica dels filtres que es puguin adaptar a l'objecte protegit i el tipus d'atac detectat, eliminant únicament el tràfic perjudicial.
45. Ha de permetre la selecció de la mitigació a aplicar i generar informes i modificacions en funció dels resultats de la mitigació.
46. La mitigació ha d'oferir com a mínim les següents característiques:
 - Mitigació de SYN Flood específic
 - Mitigació del DNS (protocol mal format i basat en autenticació)
 - Mitigació de capa d'aplicació basat en expressions regulars per HTTP i DNS.
 - Mitigació de VoIP/SIP, limitació de taxa de peticions SIP (*rate-limiting SIP requests*) des d'una sola adreça origen i filtrat de paquets SIP malformats
 - Mitigació amb opció d'aplicar *traffic shapping* (per protegir contra pics de consultes massives sobtades o *flash crowds*)
 - Que permeti la definició de plantilles (templates) diferents per poder ser aplicats com a llindars en cas de mitigacions
 - Mitigació amb taxa límit per client de HTTP Get Flood i per objecte
 - Mitigació per llindar en el nombre d'autenticacions HTTP
 - Detecció de zombis (amb selecció de llindars en bps i pps des del portal de gestió)
 - Mitigació basada en amenaces conegudes, amb actualització regular automàtica de noves amenaces.
 - Detecció de botnets i mitigació dels atacs massius llançats automàticament per aquestes
 - Atacs d'esgotament de la taula d'estats com Slowloris, Pyloris i LOIC
 - Mitigació d'atacs segons els país origen
47. Durant la mitigació, el sistema ha de permetre la visualització de tràfic en temps real.
48. Ha de permetre el control manual sobre les respostes als atacs sense aturar la neteja activa.
49. Les mitigacions s'han de poder iniciar manualment des de la consola de gestió, mitjançant el desviament del tràfic via BGP cap a l'equip de mitigació.
50. Ha de tenir opció d'automitigació, per poder engegar les mitigacions sense intervenció humana.
51. El sistema ha de proporcionar la possibilitat de netejar automàticament les alertes històriques per evitar l'acumulació d'esdeveniments.
52. Ha de permetre descarregar arxius amb informació sobre cada mitigació per poder ser avaluats fora de línia.

3.3. Instal·lació, manteniment, formació i documentació

Pel que fa a la instal·lació, manteniment, formació i documentació sobre la solució, el licitador ha d'incloure:

1. Les llicències han de ser perpètuas no han d'expirar quan finalitzi el període de contracte exceptuant les de subscripció d'intel·ligència.
2. Les llicències d'intel·ligència tindran com a durada mínima la durada del contracte.

3. A data de publicació de la present licitació, tots els elements que formen part de la solució no tindran data anunciada de finalització de cicle de vida (End Of Life) del fabricant, o bé s'haurà de complir algun dels següent supòsits:
 - Estarà anunciada i serà superior a 5 anys a partir de la data de publicació de la licitació actual.
4. Estarà anunciada i serà inferior a 5 anys a partir de la data de publicació de la licitació. En aquest cas, el contractista haurà de reemplaçar aquests elements abans de la seva fi de vida, per altres d'iguals o superiors característiques amb data de fi de vida posterior a 5 anys a partir de la data de publicació de la licitació. En aquest cas, el contractista portarà a terme totes les tasques necessàries per garantir la continuïtat del servei i assumirà tots els costos d'instal·lació i configuració.
5. S'han d'incloure els *upgrades* de software dins del manteniment de l'equip.
6. L'assistència tècnica necessària per a la instal·lació de l'equipament. L'adjudicatari es coordinarà amb el CSUC per garantir la instal·lació sense cap interrupció en els serveis actuals.
7. El manteniment per a un mínim de cinc (5) anys, a partir de la posada en operació de l'equipament. Aquest servei haurà de contemplar, com a mínim, els següents requisits:
 - Servei 24x7. Caldrà proveir un número de telèfon per contactar i una eina de gestió d'incidències per registrar-les i fer-ne el seguiment.
 - Els temps de resposta i resolució que l'adjudicatari haurà de complir s'indiquen a l'apartat 3.3.1.
 - En cas d'incompliment d'aquests temps s'aplicaran les penalitzacions indicades a l'apartat **¡Error! No se encuentra el origen de la referencia.**
8. La documentació que descriu la configuració dels equips proposada.
9. Un mínim de 20 hores de formació presencial amb personal certificat pel fabricant a les instal·lacions del CSUC, per a un mínim de 6 persones. El temari haurà d'incloure, com a mínim, el funcionament de la plataforma, la posada en marxa de mitigacions i la creació d'informes i configuració d'alertes, que permeti als tècnics del CSUC ser autònoms en la mitigació d'atacs i la generació d'informes.

3.3.1. Qualitat del servei

Es considera que una incidència és de **prioritat alta** quan per causa de la mateixa es produeixi una afectació total o parcial en el sistema que impedeixi la detecció i mitigació d'atacs o la generació d'informes. El temps de resposta des del seu inici ha de ser com a màxim de 30 minuts naturals i el temps de resolució de com a màxim 4 hores naturals.

Es considera que una incidència és de **prioritat mitja** quan els *logs* o missatges d'error dels equips indiquin que s'ha produït una alteració no esperada del seu comportament o bé quan s'hagi produït algun error que calgui esmenar. El temps de resposta des del seu inici ha de ser com a màxim d'1 hora natural i el temps de resolució com a màxim de 24 hores naturals.

Es considera que una incidència és de **prioritat baixa** quan sigui informativa. El temps de resposta des del seu inici ha de ser com a màxim el següent dia laborable i el temps de resolució com a màxim de 5 dies laborables¹.

En cas de produir-se una incidència de prioritat alta, el CSUC podrà demanar a l'adjudicatari informes puntuals d'incidències concretes, que hauran d'estar disponibles en el termini màxim de 3 dies laborables.

Se sol·licita que els licitadors especifiquin els perfils dels tècnics que portaran a terme el servei de suport.

3.4. Política de creixement

El licitador ha de descriure a l'oferta la seva política per al creixement futur de la solució, tant el creixement de la capacitat de mitigació ampliant llicències sense canviar tot el maquinari com les possibles ampliacions de l'equipament o evolució de cadascun dels components de la solució si escau.

3.5. Característiques tècniques i funcionals complementàries

Aquesta secció descriu les millores addicionals que els licitadors poden oferir:

- Fins a 100 usuaris de gestió simultanis.
- Autenticació d'usuaris via federació basada en el protocol SAML.
- Capacitat de mitigació de fins a 50 Gbps.
- Temps de retenció de dades de Netflow en cru d'un any com a mínim (per les característiques indicades a l'Annex), de manera que no es perdi granularitat en canviar els intervals de temps de visualització del tràfic.
- Capacitat d'aplicar simultàniament filtres en la visualització del tràfic per aplicació, protocol, port, IP origen i destí o sistema autònom, entre altres (és a dir, capacitat per aplicar 3, 4 o més filtres simultàniament)...
- Capacitat d'identificar amenaces generades per campanyes de *phishing*, *bots* de control remot, atacs de força bruta, explotació de vulnerabilitats conegudes i intents de filtració de dades des de o cap a servidors malignes coneguts.
- Configuració i visualització en la mateixa plataforma de mitigacions basades en *Flowspec* amb paràmetres diferents per cada objecte, incloent les automàtiques.
- Proveir interfícies addicionals de 100 Gbps per a la connexió amb el troncal de l'Anella Científica, inclosos els *transceivers*, tant pels equips troncal com per la plataforma de mitigació d'atacs DDoS.
- Ampliar el número d'hores de formació amb personal qualificat fins a 28 hores.

¹ Es considera el calendari laboral de la ciutat de Barcelona.

4. Servei 24x7

El CSUC haurà de disposar d'un servei d'operació de la plataforma de mitigació d'atacs de denegació de servei en horari 24x7, mitjançant un equip tècnic especialitzat en la mitigació d'aquest tipus d'atacs.

Aquest servei ha d'incloure:

- El monitoratge sense limitació dels atacs rebuts per les institucions de l'Anella Científica, que s'ha de fer de manera coordinada amb el CSUC.
- La mitigació sense limitació dels atacs rebuts, sota demanda del CSUC o, en cas que aquests es produeixin fora de l'horari laboral del CSUC, de la institució o institucions atacades. S'aplicaran les contramesures necessàries per aturar l'atac en coordinació amb el CSUC i/o les institucions atacades en cada cas.
- La coordinació amb el servei de mitigació d'atacs de DDoS oferta per RedIRIS (actualment anomenada EGIDA).

El temps en posar en marxa qualsevol mitigació un cop feta la sol·licitud per part del CSUC o la institució haurà de ser inferior a 15 minuts. En cas de no complir-se aquest temps s'aplicaran les penalitats especificades a l'apartat O del PCAP.

A l'inici de cada mes, l'adjudicatari farà un informe dels atacs i les mitigacions fetes durant el mes anterior. El CSUC i l'adjudicatari es reuniran mensualment per avaluar l'impacte en els serveis. En casos puntuals, el CSUC podrà demanar a l'adjudicatari informes d'incidències concretes, que hauran d'estar disponibles en el termini màxim de 3 dies laborables.

Qualsevol canvi de configuració de la plataforma ha de ser fet o autoritzat pel CSUC.

S'establiran els procediments per fer el monitoratge i per a que les institucions puguin demanar la mitigació d'atacs concrets quan aquests es produeixin fora de l'horari laboral del CSUC.

El proveïdor haurà d'incloure a la seva proposta una descripció de les capacitats de l'equip tècnic, així com la descripció dels procediments proposats per posar en marxa el monitoratge i la mitigació.

Annex: Característiques actuals

Les característiques del mostratge actual:

- Netflow v9
- Mostreig 1 de cada 1200.
- Fluxos/s: 1500