Consorci
Administració Oberta
de Catalunya

Plec de prescripcions tècniques pel servei de suport a la Unitat de CiberSeguretat del Consorci AOC.

Generalitat
de Catalunya

Consorci de governs locals
per a la societat de la informació

Contenido

1. Introducció

El Consorci AOC està immers en un procés de desplegament de mesures de seguretat, tant tècniques com organitzatives, per poder adequar els seus sistemes als requeriments de seguretat de l'Esquema Nacional de Seguretat.

Per poder adequar els sistemes, el Consorci AOC necessita un servei de suport per la Unitat de Seguretat, que recolzi les activitats pròpies d'aquesta unitat, amb experts en ciberseguretat i amb experts en el marc de treball de l'Esquema Nacional de Seguretat.

2. Descripció del servei de suport

El servei de suport estarà dividits en els següents àmbits:

- Àmbit normatiu
- Àmbit Ciberseguretat
- Àmbit de gestió del projecte

2.1 Àmbit normatiu

2.1.1 Anàlisis de riscos

L'adjudicatari haurà de fer els anàlisis de riscos segons estableix la mesura op.pl.1 de l'annex II del Real Decreto 311/2022, de 3 de maig, per sistemes de nivell ALT.

La metodologia dels anàlisis de riscos s'adaptaran al nivell de categorització del servei a analitzar, però en el nivell ALT, hauran de ser de ser formals, que permeti validar el conjunt de mesures de seguretat implantades, detectar les mesures addicionals necessàries i justificar l'ús de mesures alternatives.

Els anàlisi de riscos es faran amb l'eina PILAR o qualsevol altre que compleixi amb la mesura op.pl.1, sempre i quan el Consorci AOC estigui d'acord.

El licitador haurà d'explicar la seva metodologia per fer els anàlisi de riscos, però com a mínim haurà d'incloure les següents activitats:

- Liderar les entrevistes amb els diferents responsables del serveis per obtenir la informació necessària per l'elaboració de l'anàlisi de riscos.
- Suport en la categorització dels serveis.
- Preparar la Declaració d'Aplicabilitat d'acord amb el format i contingut establert per l'ENS.
- L'informe resultant de l'anàlisi de riscos haurà d'estar enfocat a poder identificar clarament les debilitats del sistema i poder determinar el risc residual.
- Preparar el Pla de Tractament de Riscos, proposar les mesures necessàries per baixar llindar de risc i fer seguiment del tractament dels riscos.

Inicialment, es preveu la realització de 3 anàlisis de riscos que s'hauran d'actualitzar anualment.

Abans de l'execució de cada anàlisi de riscos, l'adjudicatari haurà de presentar un pla de projecte justificant l'esforç en hores de l'activitat. En cap cas, l'esforç dedicat a 1 anàlisi de riscos fet des de l'inici podrà superar les 15 jornades del perfil assignat, o les 8 jornades si és una actualització.

2.1.2 Suport en la certificació de serveis en l'ENS

El licitador haurà de liderar el procés de certificació en el ENS, preparant la informació que sigui requerida per l'ENS en el format que sigui requerit.

El licitador podrà proposar la metodologia que cregui convenient, però com a mínim haurà d'incloure les següents activitats:

- Suport en la interpretació de les mesures de seguretat requerides per l'ENS en l'Annex II.
- Suport en la execució d'anàlisi de compliment de les mesures de seguretat que siguin d'aplicació.
- Suport en l'elaboració del pla d'adequació.
- Revisió i gestió en la contractació de proveïdors.
- Elaboració de Anàlisis d'Impacte de Negoci (BIA) segons estableix la mesura op.cont.1, el Pla de Continuïtat segons estableix la mesura op.cont.2, i les proves de continuïtat segons estableix la mesura op.cont.3 de l'annex II de l'ENS.
- Elaborar la documentació que sigui requerida per l'ENS per fer la certificació.

3.1 Àmbit Ciberseguretat

3.1.1 Revisió d'events de seguretat.

L'adjudicatari haurà de fer processos de revisió del registres d'events de les diferents eines de seguretat del Consorci AOC (IDS, Antivirus, PAM, etc.), interpretar els events i proposar iniciatives de mitigació.

La revisió serà periòdica i manual.

No s'espera de l'adjudicatari que sigui expert en les eines, ja que cada una tindrà un partner que la gestionarà.

3.1.2 Assessorament en configuracions de seguretat.

L'adjudicatari haurà de donar suport en definir totes aquelles configuracions relacionades amb la seguretat del programari base, com per exemple servidors Apache i IIS, Office 365, Sistemes Operatius, etc. per poder mitigar riscos i vulnerabilitats.

3.1.3 Anàlisis de vulnerabilitats.

L'adjudicatari haurà de fer anàlisis de vulnerabilitats amb l'eina que li proporcionarà el Consorci AOC, actualment Nessus. L'adjudicatari haurà de fer les següents tasques:

- Executar els escanejos amb la periodicitat establerta, tant de xarxes internes com públiques.
- Revisar i reportar les vulnerabilitats trobades.
- Proposar accions de remediació de les vulnerabilitats.
- Mantenir un registre de vulnerabilitats pendents de remediació i acceptades.

No s'espera de l'adjudicatari que sigui un expert en l'eina d'escanejos, que sigui la que sigui tindrà una partner que la gestionarà.

3.1.4 Anàlisis de seguretat/PENTEST.

L'adjudicatari haurà de realitzar tests d'intrusió (PENTEST) en els serveis on el Consorci AOC ho sol·liciti.

Els test d'intrusió podran ser de serveis web o serveis API, amb metodologia de caixa negre i gris, i haurà d'incloure tècniques de moviment lateral.

L'abast del PENTEST es pactarà abans de la seva realització amb el Consorci AOC, i l'adjudicatari haurà d'avaluar el cost en hores del mateix, podent-se modificar l'abast en funció del cost.

Es preveuen 5 PENTEST anuals.

Abans de l'execució de cada PENTEST, l'adjudicatari haurà de presentar un pla de projecte justificant l'esforç en hores de l'activitat. En cap cas, l'esforç dedicat a 1 PENTEST podrà superar les 10 jornades del perfil assignat.

4.1 A nivell de gestió del projecte

4.1.1 Gestió de projecte, coordinació de recursos, control hores.

El servei es basa en el consum d'hores de diferents perfils professionals, la suma de les quals no podrà excedir el pressupost base de licitació del contracte, tenint en compte el preu/hora per perfil ofertat per l'adjudicatari.

L'execució de les diferents activitats del contracte es farà portant un control de les hores dedicades. Es podran balancejar la dedicació de l'esforç entre les diferents activitats i àmbits d'actuació, amb les úniques limitacions del preu base de licitació del contracte i si l'activitat té una limitació d'esforç definida en el requeriments tècnics.

L'adjudicatari haurà de valorar l'esforç abans de l'execució de cada activitat, i la seva execució dependrà de l'aprovació del Consorci AOC.

L'adjudicatari portarà el control de l'esforç dedicat i facturarà mensualment en funció del preu hora del perfil dedicat.

L'adjudicatari haurà d'aportar un perfil de Gestió de Projectes amb les següents responsabilitats:

- Interlocució amb el Consorci AOC.
- Valoració de l'esforç per cada activitat de contracte abans de la seva execució.
- Mesurar el consum real de l'esforç en hores i perfil.
- Coordinar les diferents activitats en curs amb el perfils corresponents.
- Detectar desviacions en les activitats en curs.

4.1.2 Model de relació: reunions de seguiment, coordinació i reporting

Per la gestió de totes les activitats, totes les tasques es gestionaran en l'eina de tiqueting del Consorci AOC.

L'adjudicatari proposarà el model de relació més adient per l'execució del projecte, amb l'objectiu de detectar desviacions en les activitats i en el consum d'hores.

5. Equip de treball i estimació d'hores

L'adjudicatari haurà d'aportar un equip multidisciplinar per executar totes les activitats previstes en el contracte.

Cada àmbit d'activitat podrà estar cobert per una o varies persones.

El Consorci AOC ha calculat l'esforç necessari que es dedicaran anualment a cada activitat com indica la taula següent:

Activitats	Hores previstes	PERFIL
A nivell normatiu		
Anàlisis de riscos	280	Perfil expert en Compliment
Suport en la certificació de serveis en l'ENS	160	Perfil expert en Compliment
A nivell tècnic		
Revisió d'events de seguretat	192	Perfil expert en Ciberseguretat
Assessorament en configuracions de seguretat	20	Perfil expert en Ciberseguretat
A nivell d'auditories		
Anàlisis de vulnerabilitats	64	Perfil expert en Ciberseguretat
Anàlisis de seguretat/PENTEST:	240	Perfil expert en Ciberseguretat
A nivell de gestió del servei		
Gestió de projecte, coordinació de recursos, control hores.	96	Perfil expert en Projecte
Reunions de seguiment, coordinació i reporting	96	Perfil expert en Projecte
	1148	

Dedicació per perfil:

Perfil	Dedicació prevista en hores
Compliment	440
Ciberseguretat	516
Gestió de projecte	192
Total	**1148**

6. Requeriments de seguretat

L'adjudicatari, ens els seus procediments interns, haurà de complir amb les mesures de seguretat de l'Esquema Nacional de Seguridad i per acreditar-ho, haurà de tenir un certificat de nivell MIG pels sistemes d'informació que donin suport al servei objecte del plec.

7. Horari

L'horari del servei serà l'horari d'oficina.

Barcelona,

Ivan Caballero Domínguez

Responsable de Sistemes de Seguretat.