



**Consorci
Administració Oberta
de Catalunya**

Plec de prescripcions tècniques.

Pla de formació i conscienciació a usuaris en
Ciberseguretat

Expedient: AOC-2024-36

Contenido

1.	Objecte del contracte	3
2.	Desplegament de l'eina de formació	3
3.	Servei de formació i conscienciació.	3
4.1	Indicadors de clau de rendiment (KPIs)	4
4.2	Requeriments de seguretat	4
4.1.1	Certificacions de seguretat	4
4.1.2	Requeriments de protecció de dades	4
4.	Horari del servei	5
5.	Devolució del servei.	5

1. Objecte del contracte

L'objecte del contracte és un servei de formació i conscienciació pels empleats del Consorci AOC. L'adjudicatari haurà de fer les següents tasques:

- Desplegar un programari dissenyat específicament per executar plans de formació conscienciació.
- Executar el pla de formació i conscienciació segons els requeriments del plec tècnic
- Extreure indicadors de clau de rendiment per mesurar l'èxit del pla.

2. Desplegament de l'eina de formació

L'adjudicatari haurà de desplegar una eina dissenyada específicament per a plans de formació i conscienciació en modalitat SaaS.

L'eina escollida haurà de ser una eina aprovada pel CCN. Per acreditar l'aprovació, l'eina haurà d'estar present al Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i Comunicació (CPSTIC) del CCN, dins de la família "Formación y concienciación". Enllaç al catàleg CPSTIC: [CCN-STIC 105](#)

L'eina haurà de ser capaç d'enviar correu phishing simulat i extreure estadístiques detallades de la interacció que el empleats han fet amb aquest correu.

Haurà d'oferir mòduls de formació interactius amb exercicis pràctics, per entrenar als empleats en el reconeixement del atac. L'eina haurà d'oferir estadístiques d'assoliment dels mòduls formatius.

Els mòduls formatius hauran d'estar classificats per temàtiques, i hauran d'incloure com a mínim phishing, frau d'enginyeria social i privacitat de dades

L'eina haurà d'oferir un complement pel client de correu per a que els empleats reportin els correu sospitosos de ser maliciosos. L'eina haurà de poder fer una primera avaluació automàtica del correu i informar a l'usuari.

En funció de de la interacció amb els correus de phishing simulat i del assoliment dels mòduls formatiu, l'eina haurà de poder avaluar el risc de l'organització i mesurar el progres del pla de formació i conscienciació.

Si existeix una guia del CCN de desplegament segur de l'eina escollida, l'adjudicatari haurà de tenir-la en compte en el desplegament.

3. Servei de formació i conscienciació.

L'adjudicatari haurà d'executar campanyes cícliques de formació i conscienciació per a tots el empleats del Consorci AOC. El número d'empleats podrà variar, però com a màxim seran 120 usuaris.

Cada campanya estarà formada per enviaments de píndoles formatives, enviament de correu phishing simulat, i enviament de cursos de formació, amb els següents requeriments:

Enviament de píndoles i formatives.

Un cop al mes, l'adjudicatari haurà d'enviar una píndola informativa, que abans haurà d'estar validada per la Unitat de Seguretat del Consorci AOC.

L'idioma de la píndola haurà de ser en català.

Enviament de correu phishing simulat.

Un cop cada 2 mesos, l'adjudicatari haurà d'enviar un correu phishing simulat a tots els empleats del Consorci AOC. El correu haurà d'estar validat prèviament pel Consorci AOC.

Enviament de cursos formatius.

Un cop cada 3 mesos, l'adjudicatari haurà d'enviar un curs formatiu a tots els empleats del Consorci AOC, que abans haurà d'estar validat pel Consorci AOC.

Entrega de resultats.

Al finalitzar cada campanya, l'adjudicatari haurà d'entregar els resultats de la mateixa.

Les periodicitats dels diferents exercicis dins de les campanyes de formació i conscienciació podran variar en funció dels resultats de les campanyes anteriors, o si es vol potenciar o relaxar el pla de formació.

L'administració íntegra de l'eina de formació a usuari en ciberseguretat serà responsabilitat de l'adjudicatari. No obstant, el Consorci AOC disposarà d'usuaris administradors de l'eina.

4.1 Indicadors de clau de rendiment (KPIs)

L'adjudicatari haurà proposar indicadors de rendiment (KPIs) del procés de formació i conscienciació.

Com a mínim 1 cop l'any, l'adjudicatari haurà de fer un informe resum de les campanyes executades, el resultats i mesures dels indicadors clau de rendiment.

4.2 Requeriments de seguretat

4.1.1 Certificacions de seguretat

El licitador haurà de tenir en vigor una declaració de conformitat de compliment de l'Esquema Nacional de Seguridad de nivell baix, o bé un certificat de conformitat del Esquema Nacional de Seguridad de nivell mig o alt.

4.1.2 Requeriments de protecció de dades

Si l'eina ho permet, les dades es tractaran en un país de l'EEE.

Si hi ha transferència internacional de dades, el fabricant de l'eina proposada pel licitador haurà d'estar adscrit a un conveni de tractament de dades amb la Unió Europea. En molts casos, si el fabricant és d'origen dels EUA, haurà d'estar adscrit al conveni entre el EUA i UE anomenat Data Privacy Framework.

L'adjudicatari haurà d'eliminar totes les dades relatives al servei una vegada hagi finalitzat el contracte.

4. Horari del servei

El servei s'executarà en horari laboral, de dilluns a divendres de 9 a 18h.

5. Devolució del servei.

L'adjudicatari es compromet ha eliminar tota la informació propietat del Consorci AOC que tingui en els seus sistemes i ens els sistemes dels subencarregats del tractament.

Barcelona,

Rafael Carrasco Caballero

Cap de Projectes