PLEC DE PRESCRIPCIONS TÈCNIQUES QUE REGEIX LA CONTRACTACIÓ DEL SERVEIS GESTIONATS DE FORMACIÓ I CONSCIENCIACIÓ EN CIBERSEGURETAT PER AL PERSONAL DE LA CORPORACIÓ CATALANA DE MITJANS AUDIOVISUALS, SA.

EXPEDIENT NÚM. 2602OB06

1. Objecte del contracte

El present plec de prescripcions tècniques té per objecte la contractació **d'un servei integral de formació i conscienciació en ciberseguretat** per a la Corporació Catalana de Mitjans Audiovisuals, SA (CCMA). El servei comprendrà el disseny, desplegament i gestió d'un programa continu de **formació en ciberseguretat** adreçat a tot el personal de la CCMA (aproximadament 2500-2600 usuaris), amb la finalitat de millorar significativament la cultura de seguretat de la informació a l'entitat.

2. Objectius del servei

L'objectiu principal és **millorar la cultura de ciberseguretat dels professionals de la CCMA** mitjançant un pla integral i escalable de conscienciació. Això es tradueix en els objectius específics següents:

- **Conscienciació i canvi cultural:** Fomentar bons hàbits en l'ús de les eines digitals i reforçar el comportament proactiu en ciberseguretat de tot el personal. Es pretén incidir especialment en el **factor humà** de la seguretat, de manera **interactiva i efectiva**, superant els models tradicionals de formació que fins ara no han estat del tot exitosos.
- **Capacitació per a identificar amenaces:** Augmentar la capacitat dels usuaris per **detectar correus maliciosos, campanyes de phishing i altres atacs comuns**. Els professionals de la CCMA han d'estar preparats per reconèixer aquestes amenaces en el correu electrònic i altres entorns, reduint així el risc d'incidents.
- **Avaluació i millora contínua:** Mesurar periòdicament el **nivell de conscienciació i coneixement** en ciberseguretat dels usuaris, identificant les àrees de millora i les necessitats formatives específiques. Això permetrà ajustar el pla de formació de forma contínua, assegurant que els continguts siguin rellevants i efectius.
- **Reducció del risc i compliment normatiu:** Minimitzar la probabilitat d'èxit dels ciberatacs (especialment del phishing i enginyeria social) mitjançant una plantilla informada i vigilant. Mantenir un **entorn de treball segur** i contribuir al compliment de les polítiques internes de seguretat i la normativa vigent, disminuint els riscos que podrien afectar la infraestructura i la reputació de la CCMA.

3. Requisits i característiques del servei

El servei de formació i conscienciació en ciberseguretat haurà de complir els **requisits generals** següents, així com incloure les **prestacions formatives** descrites:

3.1. Requisits generals

- **Continguts en llengua catalana:** Tot el contingut formatiu i de conscienciació ha d'estar disponible **íntegrament en idioma català** (tant els materials escrits com audiovisuals, simulacions de phishing, mòduls e-learning, etc.). Això garanteix que els usuaris rebin la formació en la seva llengua de treball i assegura la comprensió òptima dels conceptes. (En cas que la plataforma tecnològica associada tingui interfície d'usuari, es valorarà que també estigui disponible en català, si bé s'acceptarà com a mínim en anglès o castellà).
- **Adaptació als perfils d'usuari:** Els materials i accions formatives s'han d'**adaptar als diferents perfils professionals** existents a la CCMA. En particular, s'estableixen tres segments de destinataris amb necessitats diferenciades: **personal tècnic informàtic**, **personal directiu/comandaments** i **usuaris finals o personal no tècnic**. El proveïdor haurà de personalitzar els continguts, exemples i profunditat tècnica per a cada col·lectiu, assegurant la rellevància de la formació per a cada perfil.
- **Accessibilitat i multi plataforma:** El servei s'ha de proporcionar mitjançant una **plataforma accessible en línia** (preferentment al núvol) que permeti accedir als continguts de formació des de qualsevol lloc i dispositiu. Els usuaris han de poder participar en els mòduls formatius i activitats tant des dels ordinadors corporatius com des de dispositius mòbils o tauletes, de forma senzilla i sense necessitat d'instal·lacions especials. La solució haurà de ser fàcil d'utilitzar i compatibilitzar amb els principals navegadors web.
- **Escalabilitat i gestió autònoma:** El pla de conscienciació ha de ser **escalable** en volum d'usuaris i adaptable al llarg del temps. Es requereix que gran part del programa estigui **automatitzat i pre-configurat**, de manera que les accions (enviament de tests de phishing, assignació de mòduls, recordatoris, etc.) es puguin executar sense intervenció manual constant. Tot i això, la CCMA ha de tenir la possibilitat de personalitzar la planificació i introduir canvis o accions addicionals segons convingui.
- **Confidencialitat i protecció de dades:** El proveïdor haurà de garantir que totes les dades generades (resultats de tests, estadístiques de participació, etc.) es gestionin de conformitat amb la normativa de protecció de dades vigent. A més, les simulacions de phishing i altres exercicis s'han de dissenyar de manera que no comprometin la seguretat real dels sistemes ni les dades corporatives.

3.2. Prestacions formatives incloses

El pla de formació haurà d'incloure, com a **mínim**, les actuacions i **continguts següents**, que es desenvoluparan de manera distribuïda al llarg de cada any del contracte:

- **Simulacions de phishing regulars:** realització de **campanyes simulades de phishing** dirigides als usuaris de forma periòdica, amb una **freqüència mínima de 9 simulacions a l'any**. S'inclourà una simulació inicial de referència (test de base) per avaluar el nivell inicial de susceptibilitat al phishing, i posteriorment almenys vuit campanyes addicionals distribuïdes durant l'any. Cada simulació ha de ser **realista i variada**, abastant diversos tipus de trampes (phishing per

correu electrònic, enllaços, adjunts, etc.) i temàtiques rellevants. Després de cada test, es proporcionarà *feedback* immediat a l'usuari (per exemple, notificació si ha fet clic en l'enllaç fraudulent) i consells o materials educatius adients. Es recopilaran mètriques de resultats per poder mesurar la millora al llarg del temps (percentatge d'usuaris que piquen, que informen del correu sospitós, etc.).

- **Micro-mòduls de formació amb inscripció automàtica:** desenvolupament i disponibilitat de **mini mòduls formatius en línia** (autoformació interactiva), d'una durada curta (p. ex. 5-15 minuts cadascun), sobre diverses temàtiques de ciberseguretat. La plataforma ha de permetre **l'assignació automàtica** d'aquests mòduls als usuaris objectiu corresponents. Per exemple, es podrà inscriure automàticament un usuari a un micro-curs específic després que hagi fallat un test de phishing, o bé programar la inscripció general de tots els empleats en determinats mòduls de forma escalonada. Aquests cursos breus cobriran matèries essencials (p. ex., seguretat del correu electrònic bàsica i avançada, prevenció del *ransomware*, enginyeria social, gestió segura de contrasenyes, navegació segura i identificació d'URLs sospitoses, etc.), i hauran d'incloure elements interactius o multimèdia per afavorir l'aprenentatge actiu.
- **Newsletter mensual de bones pràctiques:** elaboració i enviament a tot el personal d'un **butlletí informatiu mensual** en matèria de ciberseguretat. Aquest newsletter, redactat en català, contindrà consells pràctics, recordatoris de bones pràctiques, novetats sobre amenaces emergents i recomanacions adaptades a l'entorn de la CCMA. El butlletí s'entregarà preferentment per correu electrònic (o via intranet corporativa) cada mes, mantenint així un **fil constant de conscienciació**. Es procurarà que el contingut sigui breu, atractiu visualment i rellevant, de manera que engresqui els empleats a llegir-lo i aplicar-ne els consells.
- **Sessions formatives per a perfils directius i tècnics:** organització de **sessions de formació específiques**, sigui de manera presencial o mitjançant webinars en directe, adreçades als col·lectius de **directius** i de **personal tècnic informàtic** de la CCMA. Atès que aquests perfils tenen requeriments especials, com a mínim es durà a terme **una sessió anual per a directius** (focalitzada en la gestió de riscos corporatius, la importància de la ciberseguretat des d'una perspectiva estratègica i de compliment, protocols de resposta a incidents a nivell executiu, etc.) i **una sessió anual per a personal tècnic** (amb continguts més aprofundits sobre amenaces tècniques, gestió d'incidents operatius, noves vulnerabilitats, etc.). Aquestes sessions podran realitzar-se a les instal·lacions de la CCMA o en format de seminari web interactiu, segons convingui, i tindran una durada i programa adequats a cada perfil. Es valorarà que els formadors disposin d'experiència en comunicació amb perfils d'alta direcció, en el primer cas, i expertesa tècnica contrastada en el segon.
- **Píndoles de formació audiovisual:** subministrament periòdic de **materials audiovisuals breus** (*vídeos* o animacions curtes, de 2-5 minuts) que reforcin les campanyes de conscienciació. Aquests recursos es poden utilitzar com a *píndoles formatives* complementàries, difonent-los a través del portal del empleat, correu electrònic o en pantalles internes. Les píndoles han de tractar

temes concrets (per exemple, consells per detectar un correu sospitós, com crear contrasenyes robustes, com actuar davant una infecció de malware, etc.) i tenir un estil amè i entenedor. Aquest format audiovisual servirà per **reforçar el missatge** i mantenir l'interès dels usuaris, complementant els mòduls i els newsletters.

- **Ciberexercici anual de simulació d'incident:** planificació i execució d'un **exercici pràctic anual de resposta a incidents de ciberseguretat** (*ciberexercici*). L'objectiu és posar a prova la capacitat de reacció de l'organització davant una ciberamenaça realista i millorar la preparació per a situacions de crisi. El proveïdor haurà de proposar un escenari de simulacre (per exemple, un atac de *ransomware* a gran escala, o una campanya de phishing dirigida que desencadena un incident) i coordinar-ne el desenvolupament en col·laboració amb els responsables de seguretat de la CCMA. L'exercici ha d'involucrar els equips clau (tant tècnics de seguretat informàtica com responsables de negoci i comunicació, segons correspongui) i permetre avaluar els protocols de resposta, la comunicació interna en crisi i la presa de decisions per part dels directius. En finalitzar el simulacre, es durà a terme una sessió *post-mortem* per analitzar els resultats, detectar punts febles i extreure lliçons apreses, que serviran per actualitzar els procediments de seguretat de la CCMA.
- **Informes de seguiment i evolució:** elaboració d'**informes periòdics** que permetin avaluar l'efectivitat del programa i l'evolució de la conscienciació al llarg del temps. En concret, el proveïdor haurà de lliurar un **informe semestral** cada sis mesos i un **informe anual** al final de cada any de servei. En aquests informes s'inclourà, almenys: un resum de les accions formatives realitzades en el període (tests de phishing efectuats, mòduls impartits, sessions realitzades, materials difosos), dades quantitatives de participació (percentatge de personal que ha completat els cursos, índex de participació a les sessions, etc.), mètriques de resultat (p. ex. taxa de clic en phishing al principi vs. al final, evolució de les puntuacions en qüestionaris, nombre d'incidents simulats reportats pels usuaris, etc.), identificació de les àrees on s'ha observat millora i aquelles on cal reforçar, i recomanacions per al següent període. Els informes semestrals i anuals es presentaran tant en format electrònic com mitjançant una reunió de revisió amb els responsables de la CCMA, per comentar-ne els continguts i acordar ajustos o accions addicionals si escau.

4. Planificació temporal (cronograma de 12 mesos)

Es demana que es presenti un **cronograma orientatiu per als primers 12 mesos** del servei, en el qual es distribueixen les diverses accions al llarg de l'any, a mode d'exemple i que caldrà pactar amb la CCMA.

L'empresa adjudicatària haurà de presentar, en el seu **pla de treball, un calendari detallat confirmant aquestes activitats o proposant-ne de complementàries, mantenint com a mínim les freqüències i accions requerides**.

5. Durada del servei

La durada del contracte serà de **tres anys**, estructurada de la manera següent: un **període inicial d'1 any** a comptar des de la data de formalització del contracte, amb la **possibilitat de pròrroga** anual **fins a 2 anys addicionals** (1+1 anys), pròrrogues que s'exercirien de forma successiva fins a assolir la durada màxima total de 3 anys.
Qualsevol pròrroga estarà condicionada a l'avaluació positiva del servei prestat i a les necessitats de la CCMA en aquell moment. En cas de pròrroga, el contractista haurà de presentar una actualització del pla de formació per al nou període anual, mantenint l'estructura bàsica però introduint continguts nous o actualitzats (per exemple, incorporant nous tipus d'amenaces emergents, refrescant els materials ja utilitzats per evitar repeticions, etc.), tot garantint com a mínim el mateix nivell de qualitat i esforç que en l'any inicial.

6. Requeriments de l'empresa licitadora

Per tal de garantir la qualitat del servei, l'empresa licitadora haurà d'acreditar el compliment dels següents requeriments mínims de solvència tècnica i experiència professional:

6.1. Experiència en projectes similars

L'empresa licitadora haurà d'acreditar experiència prèvia en el disseny, execució i seguiment de programes de conscienciació en ciberseguretat per a organitzacions de dimensió i complexitat similars a la CCMA.

Es valorarà especialment que aquests serveis s'hagin prestat en el sector públic, empreses de mitjans de comunicació, entitats amb alta exposició digital o en infraestructures crítiques.

S'hauran d'incloure com a mínim tres referències de projectes similars realitzats en els darrers 5 anys, indicant per a cadascun:

6.2. Equip de treball amb perfils certificats

L'equip de treball assignat al projecte haurà d'incloure com a mínim:

- Un/a responsable tècnic/a del servei amb experiència acreditada en gestió de projectes de seguretat de la informació.
- Un/a expert/a en conscienciació i formació en ciberseguretat, amb capacitats pedagògiques i coneixement del context cultural català.

Tècnics o consultors en ciberseguretat amb certificacions reconegudes internacionalment, com ara:

- CISA, CISM, CISSP, CEH, GIAC (per a l'àmbit tècnic).

- Certificacions específiques en Governança, Riscos i Compliment (GRC) com CRISC, ISO 27001 Lead Implementer o Lead Auditor.
- L'equip disposi de coneixements o certificació en formació o comunicació corporativa.

Per a tots els perfils clau caldrà aportar currículum i certificacions corresponents.

6.3. Eina tecnològica certificada

L'empresa haurà de fer ús d'una eina/plataforma de formació i simulació de phishing que compleixi els següents requisits:

- Disposar de certificació del Centre Criptològic Nacional (CCN) o de conformitat amb l'ENS (Esquema Nacional de Seguridad) en nivell mitjà o alt (si escau).
- Complir amb el RGPD i garantir la protecció de dades personals dels usuaris.
- Ser una eina contrastada al mercat, amb possibilitat de suport en llengua catalana, o en el seu defecte, personalitzable i gestionada per l'empresa en català.
- Permetre la generació automatitzada de informes, l'adaptació de continguts segons perfils d'usuari i la integració amb sistemes existents de la CCMA si és necessari.

6.4. Altres mèrits.

Altres requisits:

- Que l'empresa estigui certificada en normes de qualitat i seguretat rellevants (ex. ENS, ISO/IEC 27001, ISO 9001, ISO 22301).
- Que disposi d'un equip intern de desenvolupament de continguts pedagògics i recursos audiovisuals propis.
- Que tingui experiència prèvia amb l'Administració pública o amb entitats de comunicació amb entorns multicanal.

La CCMA estableix les bases perquè les empreses licitadores presentin les seves millors propostes per a un servei integral de formació i conscienciació en ciberseguretat.

El contractista adjudicatari haurà de **proporcionar un pla sòlid**, en **català**, adaptat als **diferents perfils de la corporació** i amb **accions variades al llarg de l'any**, amb **l'objectiu final d'assolir una millora palpable de la cultura de ciberseguretat a la CCMA**.

Els criteris de valoració prioritzaran tant l'eficiència econòmica com la qualitat i experiència tècnica, per tal de garantir l'èxit d'aquesta iniciativa estratègica per a la Corporació.

Sant Joan Despí, febrer del 2026