Serveis ciberseguretat

Annex Sobre B- Memoria tècnica serveis de ciberseguretat
LOT34 fins al LOT41

.

claranet | Make modern happen®

Índex

1. Proposta tècnica

Claranet, a través de la següent solució tècnica proposada, presenta totes les condicions i activitats per donar una resposta diferencial i de valor que garantiran un **servei de ciberseguretat** eficient a través d'un equip d'experts tècnics consolidats en **compliment normatiu, ISO27001, ENS i NIS2**, i amb un grup de consultors de Hacking ètic amb reputació internacional i amb un gran coneixement de les tècniques mes avançades de Hacking en qualsevol tipus de infraestructura i aplicacions.

La combinació dels dos equips proporciona totes les capacitats necessàries per oferir un servei d'assessoria i de formació en Ciberseguretat del mes alt nivell.

El model de gestió proposat el definim sobre un marc de treball, que s'establirà entre Claranet i el client, per garantir la gestió integral del projecte de forma coordinada i adaptat a les necessitats particulars de cada entintat.

Aquest marc de treball i servei està basat en els següents elements principals:

Més de 200 enginyers en ciberseguretat amb capacitats defensives, ofensives i d'auditoria, d'aquests, **més de 70 son auditors de seguretat** amb una àmplia experiència en la realització d'avaluacions de seguretat, projectes d'assessoria i compliment normatiu

Els nostres auditors son formadors reconeguts pel Black Hat, el major esdeveniment de formació en hacking ètic d'àmbit mundial, sent un dels principals socis de formació durant diversos anys. Aquesta col·laboració demostra **el nostre compromís amb l'excel·lència en la formació en hacking ètic i la capacitat en el camp de la ciberseguretat i les proves de penetració sobre qualsevol tipus de plataforma**.

Procés d'execució del servei que assegura una **comunicació constant i fluida amb el client al llarg de el projecte**. Això garanteix que **el client estigui informat en temps real sobre els avenços, resultats i qualsevol vulnerabilitat rellevant detectada**, permetent d'aquesta forma prendre decisions i treballar en conjunt per abordar qualsevol problema de seguretat crític identificat.

Més de **10 anys d'experiència oferint serveis de assessoria de seguretat i formacions** utilitzant una metodologia àmpliament provada. **Realitzem més de 500 serveis d'assessoria a l'any,** i alguns dels nostres clients son corporacions incloses a l'índex S&P500.

1.1 Prestació 172. Servei d'assessoria en ciberseguretat

Aquest servei té fonamentalment un objectiu, definir un pla d'acció que millori la postura de seguretat de la organització i que contempli els següents punts

1	Disseny d'un full de ruta per avançar cap a una infraestructura més segura, amb recomanacions específiques per a la millora tant del maquinari com del programari.
2	Anàlisi i proposta de solucions de ciberseguretat orientades a la prevenció d'amenaces com el ransomware i el phishing
3	Definició d'un pla per al compliment normatiu en ciberseguretat (ENS, NIS2 i altres)

1.1.1 Metodologia del servei

La metodologia del servei es divideix amb les següents fases:

A. Preparació: Establiment de les bases del servei mitjançant la presentació de l'equip de treball, la planificació de fites i la recollida d'informació.

B. Avaluació del compliment i maduresa de l'organització analitzant els actius, processos davant dels controls normatius aplicables del ENS

C. Resultats: Elaboració d'un pla d'acció detallat amb iniciatives per donar compliment a la ISO 27001 en un període determinat per l'organització.

1.1.2 Abast i nivell de detall del servei d'assessoria

A. Preparació

A.1 REUNIÓ D' INICI DEL PROJECTE
OBJECTIUS
Formalitzar el començament del servei mitjançant la presentació de les parts involucrades, l'enfocament i la resolució de dubtes o altres qüestions d'interès general.
DESCRIPCIÓ
Donarem inici al projecte mitjançant la realització d'una reunió inicial amb les parts involucrades per: • Presentarem l'equip de treball • Repassarem les activitats i principals fites del projecte • Identificar els interlocutors de clau • Resoldrem dubtes sobre la metodologia de treball.
LLIURABLES
En aquesta etapa s'obtindran els documents següents: • Presentació d'inici del projecte

A.2 PLANIFICACIÓ DE FITES I REUNIONS
OBJECTIUS
L'objectiu d'aquesta etapa serà planificar cadascuna de les principals reunions i metes del projecte per garantir que el servei es desenvolupa de manera eficient dins dels terminis establerts.
DESCRIPCIÓ
En primer lloc, per dur a terme aquesta etapa llistarem cadascuna de les reunions necessàries amb els interlocutors identificats. A continuació, llistarem els temes a tractar a les reunions i realitzarem l'enviament de convocatòries per a les reunions intentant minimitzar-ne la durada i evitant repeticions. Finalment, elaborarem el document de seguiment del projecte on reflectirem totes les tasques i lliurables amb les respectives dates i responsables per facilitar-ne el seguiment.
LLIURABLES
En aquesta etapa s'obtindran els documents següents: • Convocatòries de reunions i document de seguiment del projecte

A.3 RECOLLIDA DE INFORMACIÓ

OBJECTIUS

L'objectiu d'aquesta etapa és la recol·lecció de tota la informació d'interès que ens permeti obtenir el coneixement sobre l'estat actual de la seguretat en l'organització i els projectes en curs.

DESCRIPCIÓ

Compartirem amb els responsables dels processos i els controls de seguretat i TI, una llista inicial de documentació a recopilar.
Aquesta llista inclourà polítiques i procediments de seguretat, metodologia de gestió de riscos i compliment normatiu, procediments tècnics i informes d'auditoria entre d'altres.
Aquest llistat inicial pot variar segons el model de l'Organització o la maduresa de cada procés.

LLIURABLES

En aquesta etapa s'obtindran els documents següents:

- Llistat de documentació inicial

B. Avaluació

B.1 – REVISIÓ DOCUMENTAL

OBJECTIUS

L'objectiu d'aquesta etapa és fer una revisió preliminar de la maduresa dels controls a partir d'un anàlisi de les polítiques, els procediments i les instruccions documentades de l'organització.

DESCRIPCIÓ

Es realitzarà una revisió documental on analitzarem la política de seguretat de la informació i el cos normatiu per obtenir més detall dels controls implementats i els requisits de seguretat existents.
Per això revisarem, entre altres, els documents següents:
Política de seguretat de la informació, metodologia d'avaluació i tractament de riscos, anàlisi de riscos i pla de tractament de riscos, inventari i ús acceptable dels actius, Política de control d'accés, Procediments d'operació per a la gestió de TI, Procediment de gestió d'incidents, Requeriments legals, ...

Aquest anàlisi permetrà a l'equip de treball preparar d'una manera eficient les reunions que es faran a l'etapa posterior.

LLIURABLES

En aquesta etapa s'obtindran els documents següents:

- Avaluació de controls documentals

B.2 – ENTREVISTES AMB PERSONES CLAU

OBJETIUS

En aquesta etapa el principal objectiu és conèixer el grau d'implementació i maduresa dels processos i controls de seguretat de l'organització respecte a la normativa escollida de referencia ISO 27001, ENS, NIS2

DESCRIPCIÓ

En primer lloc, ens reunirem amb el responsable de seguretat de la informació per conèixer de primera mà quin és el model de govern i els processos de seguretat implementats (gestió de riscos, compliment normatiu, gestió de tercers, gestió de vulnerabilitats, incidents, esdeveniments, etc.).
En aquest punt ens reunirem amb els responsables de les funcions següents per conèixer com es porten alguns dels processos tècnics i quins controls s'han implementat.
A continuació, llistem les àrees que participaran en aquestes sessions:

- Sistemes d'informació / Administració / Comercial / Productiva / Jurídic
- Recursos Humans / Compres / Qualitat / Finances /

LLIURABLES

En aquesta etapa s'obtindran els documents següents:

- Avaluació de compliment de l'organització respecte a la normativa escollida de referencia

B.3 AVALUACIÓ DE MADURESA I GRAU DE COMPLIMENT

OBJECTIUS

L'objectiu d'aquesta etapa és obtenir una visió detallada dels aspectes necessaris a implementar per al compliment de la normativa de referencia.

DESCRIPCIÓ

En aquesta etapa farem una avaluació del nivell de maduresa dels controls de la normativa de referencia que apliqui i determinarem el grau de compliment.
Un cop obtingut l'estat actual dels controls, estudiarem quina és la bretxa per cobrir per complir la normativa
Analitzarem per cada control al seu entorn d'afectació dins l'abast de l'SGSI, determinarem quines són les mesures que cal implementar i de quina manera per respondre satisfactòriament als requisits de la norma.
Finalment, realitzarem l'anàlisi control per control per veure si compleix la normativa i validarem els resultats amb el responsable de seguretat i sistemes de l'organització.
Posteriorment documentarem l'anàlisi juntament amb la recomanació de millora a implementar.

LLIURABLES

En aquesta etapa s'obtindran els documents següents:

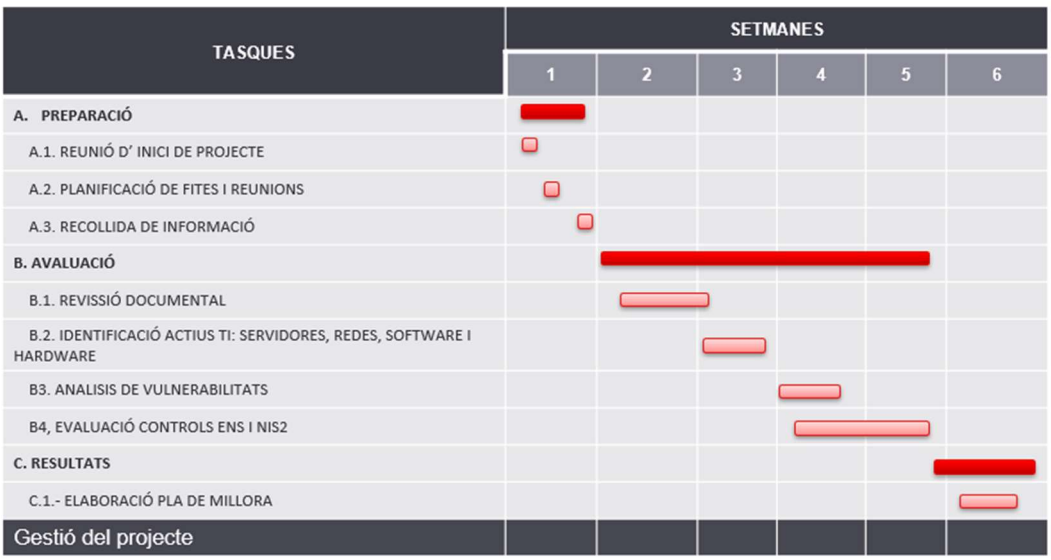
- Anàlisi GAP i recomanacions de seguretat

C. Resultats

D.1 - PLAN DE ADECUACIÓ
OBJECTIUS
El principal objectiu d'aquesta etapa és definir el pla de projectes integral de seguretat, definint el full de ruta que permeti implantar de forma ordenada les accions i incitatives necessàries per al compliment de normatiu, establint les dependències amb altres accions o projectes.
DESCRIPCIÓ
Definició del full de ruta per a la implantació dels projectes tant tècnics com organitzatius establint les precedències i les dependències entre projectes. • Iniciatives relacionades amb riscos crítics o objectius de seguretat prioritaris per a l'organització. • Dependències identificades entre projectes que componen el pla. • Requisits d'implementació i recursos (materials i personals) necessaris per a la implantació de mesures. • Estimació de temps i terminis d'implementació i execució. • Estimació de costos, tenint en compte les despeses i/o inversió i recurrències.
ENTREGABLES
En aquesta etapa s'obtindran els documents següents: • Pla d'adequació a la normativa

1.1.3 Planificació

Proposem fer les activitats en un temps efectiu de 6 setmanes i una dedicació mínima de 50 hores de consultor. Aquests treballs es poden fer en remot i/o presencials. En el cas de tasques realitzades de forma presencial, el temps de desplaçament des de les oficines de Claranet fins a les oficines de l'entitat es comptabilitzarà com hores de feina efectiva.



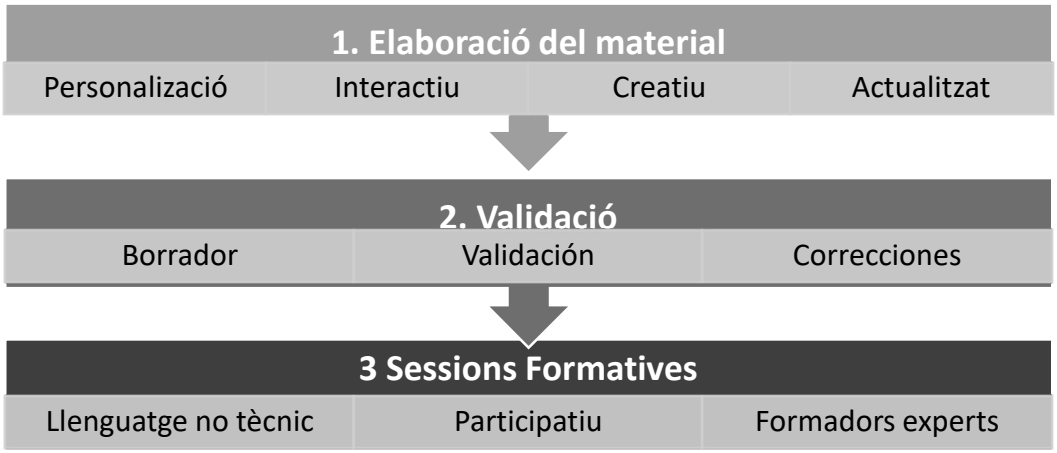
1.2 Prestació 172. Servei de Formació General en Ciberseguretat

Aquest servei té fonamentalment un objectiu de crear un pla de formació en ciberseguretat e impartir-lo i que contempli els següents punts:

1	Formació adreçada al personal de l'ens contractant, amb l'objectiu de millorar la seguretat digital mitjançant: • Continguts pràctics per a la identificació i prevenció de riscos digitals com el phishing, malware i altres amenaces comunes. • Bones pràctiques en la gestió segura de contrasenyes, ús responsable d'eines digitals i protecció de dades. • Presentació de casos reals per afavorir la comprensió i la conscienciació. .
2	Formació adreçada específicament a personal tècnic i responsables de sistemes d'informació • Gestió tècnica de la seguretat: cursos especialitzats en la gestió d'infraestructures segures, protocols de resposta davant incidents de ciberseguretat i desplegament de mesures de protecció avançades. • Marc normatiu i de compliment: actualització sobre la legislació vigent i els estàndards aplicables, incloent la LOPD-GDD, l'Esquema Nacional de Seguretat (ENS), la Directiva NIS2 i la norma ISO/IEC 27001, entre d'altres

1.2.1 Metodologia del servei

La metodologia del servei es divideix amb les següents fases:



1.Elaboració del material

OBJECTIUS

Personalitzar la formació segons les necessitats de cada Ens contractant

DESCRIPCIÓ

Duran aquesta fase del servei es realitzaran les següent tasques

- Reunió amb els responsables del ENS
- Presentació proposta de cursos, contingut, durada i format
- Presa de requeriments a mida del ENS

LLIURABLES

En aquesta etapa s'obtindran els documents següents:

- Presentació d'inici del projecte

2 Validació

OBJECTIUS

Validar el contingut dels cursos de formació

DESCRIPCIÓ

Duran aquesta fase del servei es realitzaran les següent tasques

- Presentació pla de formació
- Presentació calendari de formacions

LLIURABLES

En aquesta etapa s'obtindran els documents següents:

- Continguts i pla de servei

3. Sessions formatives

OBJECTIUS

Realitzar els cursos acordats als empleats de la entitat contractant

DESCRIPCIÓ

Duran aquesta fase del servei es realitzaran les següent tasques

- Els cursos poden ser online o presencials segons necessita el Ens
- Els cursos son de una durada de 90 min per sessió

LLIURABLES

En aquesta etapa s'obtindran els documents següents:

- Acta d'assistència al curs i feedback dels assistents

1.2.2 Planificació

Es proposa fer un pla de formació anual que inclou:

- 4 hores per la preparació dels cursos i material a mida.
- 1 sessió trimestral genèrica
- 1 sessió trimestral per a personal tècnic

Les hores mínimes per a realitzar els cursos de formació son 20 hores anuals

Els cursos es realitzaran de forma online, en el cas de requerir que els cursos es facin a les oficines del client, les hores de desplaçament des de la oficina del Claranet fins a les oficines del client es comptabilitzaran com hores de formació.

1.3 Model organitzatiu

Claranet compta amb una estructura organitzativa orientada al client, amb un equip tècnic especialitzat en auditories de seguretat i consultors que també són formadors experts en ciberseguretat. Disposa de caps de projecte que asseguren un seguiment proper i una comunicació fluida amb el client. Aquest model facilita la interlocució i el coneixement profund dels serveis. Per a cada servei, s'assignen perfils adequats segons l'abast i sempre hi ha un responsable designat.

PMO - Responsable del seguiment i coordinador global del servei

PMO - Responsable del seguiment i coordinador global del servei amb una visió estratègica i integral. Actua com a referent per a CLIENT, amb capacitat per respondre sobre l'estat i evolució del servei. Té autoritat per intervenir en qualsevol nivell de l'equip per garantir que el servei es mantingui alineat amb els requisits i necessitats del client.

Equip tècnic de consultors en auditories de seguretat

Claranet disposa d'un equip tècnic de mes de 70 consultors en auditories de seguretat que formen part del Centre de Excel·lència de Ciberseguretat, per al correcte desenvolupament del servei s'assignaran els consultors especialistes segons el abast a auditar i el tipus de formació a realitzar

Auditors proves tècniques – Equip de Consultors en seguretat, equip tècnic especialitzat encarregat de de les auditories de seguretat i proves tècniques amb mes de 3 anys d'experiència per realitzar les proves de penetració amb diferents infraestructures i aplicacions.

Auditors especialistes en compliment Normatiu – Equip de Consultors experts en compliment normatiu, ENS, ISO27001 i NIS2, amb mes de 3 anys d'experiència, anàlisi de riscs i plans d'adequació de les principals normatives de seguretat.