



PLEC DE PRESCRIPCIONS TÈCNIQUES QUE HA DE REGIR EL CONTRACTE RELATIU AL SERVEI D'ASSESSORAMENT EXTERN PER DONAR SUPORT TÈCNIC A LA POLICIA DE LA GENERALITAT-MOSSOS D'ESQUADRA MITJANÇANT L'ELABORACIÓ D'UN PLA DIRECTOR DE SEGURETAT AIXÍ COM L'ESTABLIMENT D'UNA OFICINA TÈCNICA DE COMPLIMENT DE L'ESQUEMA NACIONAL DE SEGURETAT, PER L'ANY 2026 I 2027

1. Objecte

Servei d'elaboració d'un Pla Director de Seguretat i establiment d'una Oficina Tècnica de Compliment de l'Esquema Nacional de Seguretat alineada amb l'esmentat Pla.

2. Descripció bàsica

L'objectiu final d'aquest plec és, per una banda, la creació del Pla Director de Seguretat de la Direcció General de la Policia que ens permetrà desenvolupar les competències atribuïdes en la nova estructura recollida al Decret 57/2023¹ i donar resposta a les funcions que li atorga la resolució de 7 de febrer de 2023² al o a la responsable de Seguretat en Tecnologies de la Informació de la Direcció General de la Policia.

Per altra banda, l'establiment d'una Oficina Tècnica de Compliment de l'Esquema Nacional de Seguretat, per tal de fer un acompanyament en l'adequació de tots els sistemes TIC de la Direcció General de la Policia amb l'objectiu final de rebre la certificació de conformitat de l'ENS pels nostres serveis i sistemes i així poder donar compliment al Reial Decret 311/2022³. Aquest servei no implicarà establir una oficina física, el servei es realitzarà mitjançant visites del personal assignat al projecte a les instal·lacions de la Direcció General de la Policia.

Tots dos eixos d'actuacions tot i estar emmarcats en diferents projectes interns, hauran d'estar totalment imbricats i s'hauran de desenvolupar en paral·lel i retroalimentant-se l'un amb l'altre.

3. Requisits de qualificació

El Pla Director de Seguretat haurà d'establir les directrius estratègiques i el marc general per la gestió de la seguretat de la informació, recollint les definicions i prioritzacions de les diferents accions en matèria de ciberseguretat així com un full de ruta que ens permetrà anar avançant en la reducció dels riscos als que està exposada l'organització fins a uns nivells acceptables. Més concretament, l'adjudicatari haurà d'elaborar un Pla Director de Seguretat que contingui com a mínim les accions següents:

- Una descripció prèvia a l'elaboració del pla, alineada amb els objectius estratègics de l'organització i la definició de l'abast del Pla.

¹ Decret 57/2023, de 21 de març de 2023, de reestructuració de la Direcció General de la Policia

² RESOLUCIÓ, de 7 de febrer de 2023, per la qual s'aprova l'organització interna per a la ciberseguretat i la protecció de dades de caràcter personal del Departament d'Interior

³ Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat



- Les anàlisis pertinents considerant aspectes tècnics, organitzatius, regulatoris i normatius entre d'altres, per tal de fer un modelat de l'arquitectura de l'organització i dels actius que intervenen en la protecció de les dades.
- Una descripció on es detalli les funcions i la identificació dels perfils associats a les responsabilitats sobre els actius conforme els requeriments de l'ENS.
- Elaboració d'una anàlisi diferencial entre l'estat actual de l'organització en matèria de seguretat de la informació i el compliment de l'ENS.
- Realització d'una anàlisi de riscos seguint la metodologia MAGERIT que contempli la identificació dels actius rellevants, les vulnerabilitats i amenaces a les que es troben exposats, així com la seva probabilitat d'ocurrència i l'impacte de les mateixes.
- Determinació dels controls adequats per acceptar, disminuir, transferir o evitar l'ocurrència del risc.
- Elaboració d'un full de ruta que permeti la implementació d'accions de millora, amb l'objectiu d'esmenar les mancances dels sistemes en el marc de la ciberseguretat, d'acord amb la política, els procediments, les normatives i regulacions que siguin d'aplicació, tenint sempre present com a marc l'ENS.

La creació de l'oficina de compliment que acompanyi a l'adequació dels sistemes TIC de la DGP a l'Esquema Nacional de Seguretat, haurà de realitzar les accions següents:

- Elaboració d'un pla d'adequació on s'identifiquin els sistemes que es sotmetran als processos de certificació de l'ENS.
- Definició dels requisits necessaris a l'organització pel compliment d'adequació de l'ENS tant en el marc documental com en l'organitzatiu.
- Categorització dels sistemes segons la valoració de l'impacte que tindria sobre l'organització un incident que afectés a la seguretat de la informació o dels sistemes.
- Elaboració del document de la Declaració d'Aplicabilitat on es formalitzi la relació de mesures de seguretat que resultin d'aplicació al sistema d'informació conforme a la seva categoria⁴.
- Definició dels riscos que assumirà l'organització un cop aplicades la relació de mesures de seguretat recollides en la Declaració d'Aplicabilitat.
- Posada en marxa i gestió de les mesures de seguretat a aplicar als nostres sistemes així com el seu seguiment.

⁴ Annex II. Mesures de Seguretat, de l'Esquema Nacional de Seguretat



- Assessorament i coordinació de les feines encaminades a aconseguir la certificació de Conformitat de l'Esquema Nacional de Seguretat

4. Personal que l'empresa adjudicatària adscriurà a l'execució del contracte

- El personal assignat al projecte per part de l'empresa adjudicatària, haurà de ser un equip interdisciplinar amb perfils jurídics, organitzatius i tècnics amb demostrada experiència en la implantació de l'ENS a grans organitzacions.
- El personal assignat al projecte per part de l'empresa adjudicatària, haurà de tenir les qualificacions i acreditacions pertinents per poder fer l'adequació a l'ENS així com en altres certificacions com la família ISO/IEC27000 i el NIST Cybersecurity Framework.
- Tant els consultors especialistes com els enginyers assignats al projecte per part de l'empresa adjudicatària, hauran de tenir experiència demostrada en el desenvolupament de projectes relacionats amb processos de certificació de sistemes de seguretat de la informació.
- El personal assignat al projecte per part de l'empresa adjudicatària, haurà de tenir demostrada experiència en auditories de compliment tant de l'ENS com de la legislació en matèria de protecció de dades de caràcter personal.
- El personal assignat al projecte per part de l'empresa adjudicatària, haurà de posseir alta especialització i experiència tècnica en temes relatius a la ciberseguretat i hauran d'estar familiaritzats amb les guies de la família 800 del CCN-CERT relatives a l'ENS.
- El personal assignat al projecte per part de l'empresa adjudicatària, haurà de conèixer i estar familiaritzat amb les eines relatives al compliment de l'ENS que ofereix el CCN-CERT, com ara l'eina d'anàlisi de risc PILAR.
- Com a mínim un dels membres assignat al projecte per part de l'empresa adjudicatària, haurà de tenir disponibilitat i dedicació de forma exclusiva al projecte durant la duració d'aquest.

L'empresa adjudicatària ha de complir les obligacions respecte del personal que adscriurà a l'execució del contracte que són:

- a) Correspon exclusivament a l'empresa adjudicatària la selecció del personal que, acreditant els requisits de titulació i experiència exigits en els plecs, formarà part de l'equip de treball adscrit a l'execució del contracte.
- b) L'empresa adjudicatària haurà de designar almenys un coordinador tècnic o responsable, integrat en la seva pròpia plantilla, que tindrà entre les seves obligacions, la d'actuar com a interlocutor de l'empresa adjudicatària davant de l'Administració, canalitzant la comunicació entre aquella i l'equip integrant de



l'equip de treball adscrit al contracte en tot el que es refereix a les qüestions derivades de l'execució del contracte.

Capacitats específiques en relació amb el contracte.

- L'empresa ha de comptar amb una plantilla de més de 50 consultors experts en l'eina GRC/IRM (Govern, Risc i Compliment: metodologia per estructurar i gestionar el programa de seguretat de la companyia que integra la governança, la gestió de riscos i el compliment normatiu per mantenir la seguretat a gran escala).
- L'empresa ha d'haver dut a terme més de 10 projectes en l'àmbit de l'ENS
- L'empresa ha d'estar certificada en el nivell mig de l'ENS: ha d'haver superat l'auditoria de certificació del CCN-CERT per obtenir el "Certificat de Conformitat amb l'Esquema Nacional de Seguretat" (nivell Mig)

5. Projecte de treball

L'empresa adjudicatària haurà de presentar documentalment un projecte de treball en el qual consti el contingut següent:

- L'informe de l'estat de la seguretat actual de l'organització
- Un document amb la identificació i categorització dels sistemes d'informació
- L'informe d'anàlisi diferencial en relació al marc de l'ENS
- L'informe de l'anàlisi de riscos
- L'informe de declaració d'aplicabilitat
- L'informe de pla de millora de la seguretat
- El Pla Director de Seguretat
- Un document amb la descripció detallada dels diferents projectes per assolir la certificació de conformitat de l'ENS

6. Programació de les actuacions

Les actuacions s'han dividit en quatre fases:

- **Fase 1:** Elaboració del Modelat de l'arquitectura empresarial (a nivell de capa de negoci, capa de sistemes i aplicacions de negoci i capa de Tecnologies de la Informació) dels actius que intervenen a la ciberseguretat de l'organització. Any 2026
- **Fase 2:** Elaboració d'una anàlisi diferencial amb la finalitat de detectar el nivell de compliment dels controls de seguretat del marc de referència (ENS). Any 2026
- **Fase 3:** Realització d'una anàlisi de riscos que valori els impactes i vulnerabilitats per a cada servei, procés i sistema. Després de l'anàlisi de riscos es detallarà un pla de tractament de riscos que serà la base del Pla d'Accions de millora. Any 2026



- **Fase 4:** Elaboració d'un Pla d'Accions de millora (Pla d'implementació) ordenat, que pugui ser executat de manera progressiva, que permeti esmenar les debilitats trobades, d'acord amb la política, els procediments, les normatives i regulacions que siguin d'aplicació. Any 2027

7. Persona responsable del contracte per part de l'Administració

Amb independència de la unitat o grup de treball encarregat del seguiment i l'execució ordinària del contracte, la Policia de la Generalitat-Mossos d'Esquadra designarà una persona responsable del contracte que exercirà les funcions següents:

- Supervisar l'execució del contracte i prendre les decisions i dictar les instruccions necessàries per assegurar la realització correcta de la prestació.
- La posada en coneixement del seus superiors la no conformitat en qualsevol aspecte relatiu al desenvolupament del projecte.

8. Obligacions de les empreses licitadores

Els licitadors hauran d'acreditar que no tenen interessos que puguin entrar en col·lisió amb l'assessorament i desenvolupament previst en aquest contracte, aportant documentació on consti l'objecte social de l'entitat i una declaració on s'especifiqui que no concorren circumstàncies que puguin suposar possibles conflictes d'interessos, signada per una persona amb poders suficients a l'efecte.

9. Obligacions de l'empresa adjudicatària

L'empresa adjudicatària haurà de respectar el caràcter confidencial de la informació a la qual tingui accés amb motiu de l'execució del contracte. Tant la que se li hagi donat a través del plec tècnic com aquella que per la seva pròpia naturalesa hagi de ser tractada com a tal. Aquesta obligació es mantindrà durant un termini de 5 anys des del coneixement de la informació.

En cas que el personal de l'empresa adjudicatària accedeixi a dades personals incidentalment, quedarà subjecte al compliment del Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE, d'ara endavant RGPD a la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals i a la resta de normativa vigent en matèria de protecció de dades, en relació amb les dades personals a les quals tingui accés amb ocasió del contracte.

10. Termini execució

L'execució del treball començarà un cop l'empresa adjudicatària signi el contracte pertinent i tindrà una durada com a màxim de 24 mesos des de l'inici de la signatura.



11. Criteri mediambiental

L'empresa adjudicatària donarà preferència a la utilització de mitjans audiovisuals (videoconferència, etc.) com a forma d'interrelació i farà el lliurament de documents preferentment en format electrònic. En cas de ser necessari realitzar alguna impressió serà exclusivament en paper 100% reciclat i amb un procés de fabricació lliure de clor, i a doble cara.

Comissari Miquel Àngel García Alvira

Cap de la Comissaria General de les Tecnologies de la Informació i la Comunicació