LES PÍNDOLES DEL DPD

PÍNDOLA 51.- Actualització de l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Pública

I. Introducció

El Consell de Ministres va aprovar el passat 3 de maig de 2022 el Reial Decret 311/2022 que actualitza l'Esquema Nacional de Seguretat (ENS) en l'àmbit del sector públic i d'aquells proveïdors tecnològics del sector privat que col·laboren amb l'administració.

L'Esquema Nacional de Seguretat vigent a data d'avui, publicat l'any 2010 i posteriorment modificat l'any 2015, busca amb aquesta actualització adaptar-se a l'evolució radical que ha sofert tant el context normatiu, el social, com el tecnològic.

Entre les novetats del nou ENS es troba la incorporació de la figura del **perfil de compliment**, l'objectiu del qual és aconseguir una adaptació a l'Esquema més eficaç i eficient, racionalitzant els recursos requerits sense menystenir la protecció perseguida i exigible. També s'inclou l'establiment d'un **protocol d'actuació davant de ciberincidents**, on s'estableixen les condicions de notificació a l'Equip de Resposta a Incidents (CERT) pertinent. S'actualitzen els **principis bàsics i les mesures de seguretat**, l'objecte del qual és facilitar de manera proporcional la seguretat dels sistemes d'informació, la seva implantació, així com la seva auditoria. Entre les noves mesures de seguretat s'inclouen, per exemple, les relatives als **serveis al núvol, interconnexió de sistemes, protecció a la cadena de subministres, vigilància i altres dispositius connectats a la xarxa**.

Amb el nou text normatiu es persegueix garantir la protecció dels sistemes d'informació de les entitats en el seu àmbit d'aplicació, reduint vulnerabilitats i promovent la vigilància contínua, establint mecanismes de resposta i mesures de seguretat òptimes, dins del marc jurídic, tecnològic, estratègic i de ciberamenaces actuals.

II. Estructura del nou Esquema Nacional de Seguretat

L'estructura del nou Esquema Nacional de Seguretat es renova seguint la següent disposició:

- **Capítols (7)**
    1. Capítol: Disposicions generals (Articles 1-4)
        - Objecte, àmbit d'aplicació, definicions i estàndards aplicables
    2. Capítol: Principis bàsics (Articles 5-11)
        - Seguretat integral, gestió de seguretat basada en riscos, prevenció, detecció, resposta i conservació, línies de defensa, vigilància continua i reevaluació periòdica, diferenciació de responsabilitats.

3. Capítol: Política de seguretat i requisits mínims de seguretat (Articles 12-30)
    - la **política de seguretat** per a la protecció adequada de la informació tractada i els serveis prestats a través d'un plantejament comú de principis bàsics (7), requisits mínims (15), mesures de seguretat i mecanismes de conformitat i monitoratge
4. Capítol: Auditoria de seguretat, Estat de la seguretat dels sistemes de Prevenció, Detecció i Resposta a incidents de seguretat (Articles 31-34)
    - Es detalla les característiques dels procediments d'auditories, així com dels corresponents informes d'auditories i d'estat de la seguretat.
5. Capítol: Normes de conformitat (Articles 35-38)
6. Capítol: Actualització de l'ENS (Article 39)
    - S'estableix l'obligació d'actualitzar permanentment l'ENS per tal d'adequar-se a l'evolució tecnològica.
7. Capítol: Categorització dels sistemes d'informació (Articles 40 i 41)
    - Es desenvolupa el procediment de categorització dels sistemes d'informació, definint les categories de seguretat i les facultats al respecte.

- **Disposicions addicionals (3)**
    1. Regulació dels programes de sensibilització, conscienciació i formació, que desenvoluparà el Centre Criptogràfic Nacional i l'Institut Nacional d'A.P.
    2. S'estableix el desenvolupament de les instruccions tècniques de seguretat per a una millor implantació de l'ENS.
    3. Respecte del principi de 'no causar un perjudici significatiu al medi ambient'.
- **Annexos (4)**
    1. Categories de seguretat
    2. Mesures de seguretat estructurades en tres grups:
        - Marc organitzatiu
        - Marc operacional
        - Mesures de protecció
    3. Auditoria de seguretat
    4. Glossari de termes i definicions
- **Disposició transitòria única**
    1. Es fixa un termini de 24 mesos per tal que els sistemes d'informació de l'àmbit d'aplicació de l'ENS, preexistents a la seva entrada en vigor, assoleixin la seva plena adequació a l'ENS.

III. Principals canvis del nou Esquema Nacional de Seguretat

A continuació es detallen els principals canvis incorporats a la darrera versió de l'ENS.

- **Alineament amb el marc legal actual:**
    - Des de 2010 en el pla normatiu s'ha modificat tant el marc europeu; amb quatre Reglaments i una Directiva dirigits a incrementar el nivell de ciberseguretat dels sistemes d'informació, com l'espanyol; referit a la seguretat nacional, regulació del procediment administratiu i el règim jurídic del sector públic, de **protecció de dades personals** i de la seguretat de les xarxes i sistemes d'informació, així com l' evolució del marc estratègic de ciberseguretat.

- **Incorporació de la figura dels Perfils de compliment:**
    - Els perfils de compliment introdueixen la capacitat d'ajustar els requisits de seguretat a necessitats específiques, mitjançant la definició d'un conjunt de mesures de seguretat que resultin d'activitat a una entitat o sector d'activitat concreta, i per a una determinada categoria de seguretat. Rellevant per aquelles administracions

- **Introducció dels reforços:** un dels nous elements que s'incorporen a la darrera actualització de l'ENS és la possibilitat d'introduir reforços addicionals alienants amb el nivell de seguretat perseguit. Aquests reforços poden afegir-se per tal de satisfer les següents necessitats:
    - Aclarir com s'incrementa el nivell d'exigència d'una mesura (si correspon) segons com apliqui en categories superiors.
    - Flexibilitzar com es requereixen aquests increments d'exigència.
    - Recollir l'exigència de la protecció d'informació classificada.

  La implicació d'introduir reforços provoca, per una banda, la necessitat de precisar molt més les Declaracions d'Aplicabilitat per a especificar els reforços implementats, i per altra banda provoca que les certificadores han de flexibilitzar el seu procés d'auditoria i entendre detalladament la implementació de l'ENS.

- **Revisió dels principis bàsics**, **els requisits mínims i les mesures de seguretat**. Reducció de 75 a 73 mesures, de les quals:
    - 24 mesures (33%) han augmentat el seu nivell de requeriment, 14 lleugerament i **10 de manera significativa:**
        - Gestió de la capacitat, identificació, configuració de seguretat, gestió de la configuració de seguretat, manteniment i actualitzacions de seguretat, protecció davant de codi maliciós, registre d'activitat, detecció d'intrusions, sistemes de mètriques i acceptació i posada en servei.

- **Hi ha 7 de noves (10%):**
  - Protecció de la cadena de subministrament, interconnexió de sistemes, serveis al núvol, mitjans alternatius, vigilància, altres dispositius connectats a la xarxa i protecció de navegació web.
- **6 s'han simplificat (8%).**
- **Mesures a les quals cal prestar especial atenció:**
  - Protecció de dispositius portàtils, separació de fluxos d'informació en la xarxa, dades personals (**anonimització i pseudonimització per defecte a partir de categoria mitja**), qualificació de la informació, segells temporals com a evidència, protecció de serveis i aplicacions web.
  - Quan el sistema tracti **dades personals**, el responsable de seguretat recollirà els requisits de protecció de dades que siguin fixats pel responsable o per l'encarregat del tractament, comptant amb l'assessorament del DPD, i que siguin necessaris implementar en els sistemes d'acord amb la naturalesa, abast, context i fins d'aquest, així com dels riscos per als drets i llibertats d'acord amb el que s'estableix en els articles 24 i 32 del RGPD, i d'acord amb l'Avaluació d'Impacte en Protecció de Dades (AIPD)[1].

- **Grau d'implantació de les mesures**
  - Per tal de verificar el compliment de les mesures de l'ENS s'estableix una classificació amb relació a la maduresa de la seva implementació (L0-L5) i, com a novetat, amb els següents tres graus:
    - No implementada (G0): Sense subcontrols essencials
    - En procés d'implementació (G1): Subcontrols essencials implementats
    - Implementada (G2): S'implementen tots els subcontrols de la mesura

- **Protocol d'actuació davant de ciberincidents**
  - El Centre Criptológico Nacional (CCN), del Centre Nacional d'Intel·ligència (CNI) adscrit al Ministeri de Defensa, articularà la resposta als incidents de seguretat d'entitats del sector públic – En el cas de les entitats del sector públic català també es poden adreçar, preferentment, a **l'Equip de Resposta a Incidents de l'Agència de Ciberseguretat de Catalunya**: CATALONIA-CERT®. Les entitats del sector privat que prestin serveis a les entitats públiques notificaran la resposta a incidents de seguretat a l'Institut Nacional de Ciberseguretat d'Espanya (INCIBE).

[1] Plataforma per realitzar AIPD: https://aipd.ticsalutsocial.cat/dashboard

LES PÍNDOLES DEL DPD

- **Interpretació dels certificats**
  - Les noves certificacions de conformitat amb l'ENS no informen dels nivells en els que s'avaluen cada una de les dimensions: confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat.
  - Si totes les dimensions son avaluades com a nivell alt caldrà implementar les mesures corresponents a la categoria ALTA en totes les seves dimensions.
  - Si únicament es considera de nivell ALT una dimensió caldrà implementar les mesures de seguretat de categoria ALTA únicament per aquella dimensió.
  - Això és especialment preocupant a l'hora revisar certificacions de proveïdors de serveis, ja que la informació del certificat serà incompleta i caldrà sol·licitar l'informe de certificació.

Per qualsevol dubte o aclariment addicional podeu adreçar-vos al DPD de Salut:

dpd@ticsalutsocial.cat

https://ticsalutsocial.cat/dpd-salut/

Tel.: 93 553 26 42 (9:00 a 14:00 h.)