

## LES PÍNDOLES DEL DPD

### PÍNDOLA 63.- EL CENTRO CRIPTOLÓGICO NACIONAL PRESENTA EL PERFIL DE CUMPLIMENT ESPECÍFIC EN SALUT DE L'ESQUEMA NACIONAL DE SEURETAT

Recentment el *Centro Criptológico Nacional* (CCN-CNI) ha presentat el perfil de compliment específic per al sector **salut** (PCE-Salut) per tal de facilitar la conformitat amb l'**Esquema Nacional de Seguretat** a les entitats orientades a la prestació sanitària de pacients relatives a l'execució dels serveis **d'atenció primària i atenció especialitzada**.

Aquest perfil de compliment pretén garantir **un nivell mínim de seguretat**, tenint en compte l'**anàlisi de risc** que contempla les **vulnerabilitats i amenaces** generalitzades a les que fan front aquest tipus d'entitats, i racionalitzant els recursos requerits sense menystenir la protecció perseguida i exigible.

#### I. ABAST D'APLICABILITAT

L'Esquema Nacional de Seguretat (RD 311/2022) és una norma jurídica d'obligat compliment per als sistemes d'informació de:

- Tot el sector públic (en aquest cas entitats públiques que prestin serveis d'atenció primària i atenció especialitzada)
- Les entitats del sector privat que prestin serveis (en aquest cas d'atenció primària i atenció especialitzada) a les entitats del sector públic per a l'exercici d'aquestes en les seves competències

Aquest perfil de compliment en salut **exclou una sèrie de serveis** que no son considerats de suport als serveis finalistes dirigits a pacients:

- Serveis administratius, de gestió comptable, pressupostària, de tresoreria i de compres.
- Gestió de personal: processos de selecció, nòmines, control laboral, etc.
- Serveis d'atenció i informació al pacient
- Serveis de tecnologies de la informació i comunicació relacionats amb els sistemes de gestió de la informació que donen suport als serveis assistencials

#### II. DECLARACIÓ D'APLICABILITAT

La declaració d'aplicabilitat és el **conjunt de mesures de seguretat** que son d'aplicació per al compliment de l'ENS en un sistema concret, depenent de la categoria del sistema i dels nivells associats a les dimensions de seguretat.

D'aquesta manera, en el **perfil de compliment del sector salut s'apliquen 54** de les 73 **mesures de seguretat** definides a l'Annex del RD 311/2022. Aquestes 54 mesures es consideren com a **requisits essencials mínims de seguretat**, podent ser que alguna les organitzacions, en base a les seves especificitats de risc, es vegin obligades a ajustar la declaració d'aplicabilitat a requisits més exigents aplicant mesures de reforç.

## LES PÍNDOLES DEL DPD

És el cas de les de les entitats que tractin **categories especials de dades sensibles de salut**, que hauran de tenir en compte **possibles salvaguardes resultants de l'anàlisi de riscos** de protecció de dades (art. 24 RGPD) i de **l'avaluació d'impacte en protecció de dades** (en els supòsits d'aplicació art. 35 RGPD).

De les 54 mesures de seguretat mínimes que es consideren en el PCE-Salut, 23 són de categoria mitja, 19 de categoria bàsica i 12 de comuns a totes les categories. També existeixen consideracions per a 11 mesures, que es detallen a continuació en l'apartat III. D'altra banda són 19 les mesures que no s'apliquen de base en el PCE-Salut.

### III. CRITERIS D'APLICACIÓ DE MESURES

- [op.pl.1] Anàlisi de riscos: Cada entitat haurà de realitzar, amb periodicitat anual, una nova iteració de **l'anàlisi de riscos orientat a la pròpia organització** i on es considerin els actius més valuosos de sistema així com les amenaces que es puguin materialitzar sobre aquests actius.
- [op.pl.2] Arquitectura de seguretat: Es construirà un **sistema de gestió de seguretat**, es controlarà la documentació del sistema, es revisarà la política de seguretat de la informació, es planificarà ens anàlisi de riscos i es coordinaran les auditories internes i externes.
- [op.pl.5] Components certificats: **s'exigirà la certificació dels components** als proveïdors **d'equipaments mèdics**.
- [op.acc.5] Mecanismes d'autenticació d'usuaris externs: s'aplicaran **mesures de reforç als accessos de serveis d'història clínica** i relacionats.
- [op.exp.9] Registre de la gestió d'incidents amb l'objectiu **d'aprendre dels incidents registrats** per tal d'obtenir conclusions que permetin millorar la seguretat del sistema i evitar que es repeteixin els mateixos incidents.
- [op.cont.2] Pla de continuïtat: Si els sistemes d'informació que entrin dins l'abast del PCE-Salut estan categoritzats en la dimensió de disponibilitat en nivell ALT, caldrà realitzar un **pla de continuïtat** per aquells serveis que es considerin, per exemple podria ser necessari crear un pla de continuïtat circumscrit a urgències mèdiques.
- [op.mon.3] Vigilància: el **servei de vigilància** serà proporcionat externament per un tercer, que potser el **CERT** el referència o la xarxa nacional de **SOC**.
- [mp.eq.2] Bloqueig del lloc de treball: s'hauran de bloquejar aquells llocs de treball al cap d'un temps prudencial, prestant **especial atenció als llocs de treball mòbil** que estiguin ubicats a zones públiques a l'abats de pacients o visites.
- [mp.eq.4] Altres dispositius connectats a la xarxa: aquesta mesura es focalitzarà especialment a **dispositius mèdics connectats a la xarxa interna** coneguts com *Internet of Medical Things* (IoMT).

## LES PÍNDOLES DEL DPD

- [mp.info.6] **Còpies de seguretat**: s'hauran de realitzar còpies de seguretat efectives i documentades, indicant la freqüència de les còpies, els requisits d'emmagatzematge, el lloc on es realitzaran i les mesures de seguretat de les mateixes.
- [mp.s.4] Protecció davant d'atacs de denegació de servei: es dimensionaran adequadament els components del sistema accessibles a través d'internet i es **desplegaran tecnologies per prevenir els atacs de denegació de servei** coneguts. Es recomana addicionalment implementar sistemes de detecció i tractament d'aquesta tipologia d'atacs.

Podeu consultar el text íntegre del PCE-Salut, així com els cinc annexos sobre anàlisi de riscos, política de seguretat, categorització del sistema, declaració d'aplicabilitat i pla de conscienciació i formació, en el següent enllaç:

**-Guía CCN-STIC 891 sobre Perfil de Cumplimiento Específico para Salud y Prestación Sanitaria a Pacientes (Atención Primaria y Atención Especializada)**

<https://www.ccn-cert.cni.es/es/guias-de-acceso-publico-ccn-stic/7206-ccn-stic-891-perfil-de-cumplimiento-especifico-para-salud-prestacion-sanitaria-a-pacientes-atencion-primaria-y-atencion-especializada/file.html>

**Per qualsevol dubte o aclariment addicional, us podeu adreçar al DPD de Salut:**

[dpd@ticsalutsocial.cat](mailto:dpd@ticsalutsocial.cat)

<https://ticsalutsocial.cat/oficina-dpd/>

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