EAPC - Gestió de la informació: transparència i protecció de dades

El nou Esquema Nacional de Seguretat i la prevalença de la protecció de dades personals

30-05-2022

La importància de l'Esquema Nacional de Seguretat

El passat 5 de maig va entrar en vigor el nou Esquema Nacional de Seguretat (Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, en endavant, ENS).

L'ENS té per objecte protegir la informació i els serveis oferts, a través de mitjans electrònics, per qualsevol entitat del sector públic en l'exercici de les seves competències. Així mateix, també és aplicable als operadors privats que prestin serveis a les entitats del sector públic per poder materialitzar l'exercici de les seves competències i potestats administratives.

Tenint en compte l'evolució de l'Administració cap a una administració electrònica, la norma que estableix els requisits relatius a la protecció de la informació i serveis oferts per mitjans electrònics és cabdal. En aquest sentit, no és gens estrany que l'article 156.2 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, s'hi refereixi expressament.

El funcionament de l'ENS

El nou ENS, igual que l'anterior, constitueix –essencialment– el marc a partir del qual es determinen les mesures de seguretat que cal aplicar als sistemes d'informació per protegir la informació que s'hi processa, així com els serveis vinculats als referits sistemes.

Per tant, una peça angular de l'ENS són les mesures de seguretat que estableix, incloses en l'annex II.

No obstant això, l'ENS es mostra sensible a l'hora d'exigir el compliment d'aquestes mesures; una sensibilitat que es projecta respecte de dos elements: la importància del sistema i els riscos que pateixen els actius més valuosos per al sistema.

Determinar la importància del sistema s'anomena, en terminologia més tècnica, "categoritzar el sistema". Per establir aquesta categorització del sistema es tenen en compte les informacions i els serveis relacionats amb aquest sistema d'informació (la metodologia que s'ha d'emprar és inclosa en l'annex I de l'ENS). Hi ha tres possibles resultats finals: categoria bàsica, mitjana o alta. Un

cop establerta la categoria del sistema (importància), cal revisar la llista de l'annex II de l'ENS i determinar quines mesures concretes i quins reforços són d'aplicació obligatòria (com més categoria, més requeriments de seguretat).

L'ENS, però, també és sensible als riscos concrets que pateixen els actius més valuosos del sistema. Així, les mesures obligatòries que s'han d'aplicar no seran només les pròpies de la categoria (importància) del sistema, sinó també les que resultin necessàries per mitigar certs riscos sobre actius essencials del mateix sistema.

Per això, també caldrà dur a terme una anàlisi de risc d'aquests actius essencials. En primer lloc, per determinar en quins casos hi ha un risc inacceptable per, en segon lloc, identificar quines mesures poden fer possible la mitigació d'aquests riscos inacceptables.

Llavors, tenint en compte les mesures que són aplicables en atenció a la importància del sistema (categoria) i les indispensables per controlar el nivell de risc dels elements essencials del sistema, sí que es pot confeccionar la declaració d'aplicabilitat o SOA (*Statement of Applicability*, en anglès); és a dir, ja queda definit allò que cal complir.

Finalment cal implantar aquestes mesures i acreditar-ne el compliment mitjançant una auditoria de seguretat externa (sistemes de categoria mitjana o alta).

L'ENS estableix un període màxim de 24 mesos perquè els sistemes d'informació que ja existien prèviament a l'entrada en vigor s'adeqüin a les seves exigències.

L'aplicació de l'ENS a les dades personals

La disposició addicional primera de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, ja va establir que les entitats enumerades en l'article 77 de la mateixa Llei orgànica –sector públic– havien d'aplicar als tractaments de dades personals les mesures de seguretat que corresponguessin de les establertes en l'ENS (una obligació que, en virtut de la mateixa disposició addicional primera, també es traslladaria als tercers que oferissin serveis a les administracions públiques).

Una remissió lògica, ja que l'ENS s'encarrega de protegir el conjunt de la "informació" i, en definitiva, les dades personals són un subconjunt d'aquesta informació.

La prevalença de les dades personals en la determinació de les mesures de seguretat establertes en el nou ENS

L'ENS, en l'article 3, disposa que, sempre que es duguin a terme tractaments de dades personals, caldrà efectuar una anàlisi de risc de conformitat amb l'article 24 del Reglament general de protecció de dades (en endavant, RGPD) –així com les avaluacions d'impacte de protecció de dades quan siguin escaients de conformitat amb l'article 35 del RGPD.

Cal tenir en compte que l'anàlisi de risc de l'àmbit de protecció de dades (art. 24 del RGPD) no és equivalent a l'anàlisi de risc que s'efectua en el marc de l'aplicació de l'ENS mateix. L'anàlisi de risc de protecció de dades fa referència a l'anàlisi dels efectes potencials negatius envers els drets i les llibertats de les persones físiques; en canvi, l'anàlisi de risc de l'ENS (art. 14 de l'ENS) està vinculat a la probabilitat que determinades amenaces es materialitzin en els actius essencials del sistema i l'impacte que aquesta circumstància podria comportar.

Resulta destacable també que el nou ENS no només té present la necessitat que es tingui en compte la visió i l'anàlisi de la protecció de dades personals (mitjançant l'elaboració d'una anàlisi de risc específica), sinó que atorga un nivell de prevalença als seus resultats, de tal manera que

l'article 3.3 indica que "prevalen les mesures a implantar com a conseqüència de l'anàlisi de riscos [de protecció de dades] i, si escau, de l'avaluació d'impacte [...] en cas que resultin agreujades respecte de les establertes en el present Reial decret". Una preponderància que reitera mitjançant la mesura sobre "dades personals":

"Quan el sistema tracti dades personals, el responsable de seguretat ha de recollir 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 són necessaris implementar als sistemes d'acord amb la naturalesa, l'abast, el context i les finalitats d'aquest, així com dels riscos per als drets i les llibertats d'acord amb el que estableixen els articles 24 i 32 del RGPD, i d'acord amb l'avaluació d'impacte en la protecció de dades, si s'ha dut a terme."

En definitiva, l'ENS és especialment rellevant per determinar les mesures de seguretat informàtica que s'han d'aplicar i que serviran per protegir el conjunt d'informació i serveis oferts digitalment per les administracions i entitats del sector públic i, per tant, també, per protegir les dades personals.

En plena coherència amb aquesta circumstància, l'ENS exigeix que, en aquest procés de determinació de les mesures de seguretat que s'han d'aplicar, es prengui en consideració la perspectiva de protecció de dades personals i, fins i tot, li reconeix un rol prevalent.

Així, quan es treballa en el disseny de seguretat informàtica de la informació, sempre cal tenir en compte que s'ha de donar una resposta preferent a les necessitats de protecció de les dades personals.

Xavier Puig Soler

Auditor de Sistemes d'Informació de l'Autoritat Catalana de Protecció de Dades