



Destaquem... Propera edició de la jornada DAT2010, el 29 de juny de 2010

Una vegada més, estem ultimant els detalls de la propera edició del DAT 2010, que aquest any dediquem a l'Esquema Nacional de Seguretat (ENS) i els reptes que suposa, no solament per al desenvolupament del que preveu la Llei 11/2007, sinó també des de la perspectiva de la seva convivència i sincronia amb les mesures de seguretat previstes en el reglament de desplegament de la LOPD.

La data: el proper 29 de juny; en horari de matí i tarda, al CosmoCaixa. Comptarem amb experts que han participat directament en l'elaboració de l'ENS i amb empreses que aportaran la seva visió sobre com adequar-se a l'ENS i les possibles sinergies amb la seguretat LOPD, juntament amb d'altres novetats que concretarem una vegada tancat el programa de la jornada.

Esther Mitjans Perelló
Directora de l'Agència Catalana de Protecció de Dades

Parlem... de l'Esquema Nacional de Seguretat i mesures de seguretat LOPD

La publicació, a primers d'aquest any, del Reial decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'administració electrònica, suposa un canvi rellevant quant a la manera en què el sector públic ha anat organitzant i desplegant la protecció dels mitjans electrònics utilitzats en l'exercici de les seves funcions i competències.

Per què es tracta d'un canvi rellevant? Doncs perquè implica normalitzar, sobre la base d'uns principis bàsics i requisits mínims de seguretat, els controls o mesures de seguretat a implantar en els sistemes d'informació de les administracions públiques; fins ara aquesta qüestió quedava a discreció de cada Administració, tot i que, certament, en relació a les dades de caràcter personal ja es disposava d'un marc comú de protecció de la informació.

En aquest breu article abordarem una petita part del que implica l'entrada en vigor de l'ENS, concretament el diferent enfocament que, per a la determinació dels nivells de seguretat, té l'ENS en relació a l'aplicació dels nivells de seguretat previstos a la normativa de protecció de dades de caràcter personal.

Continguts

Destaquem...	1
Parlem de...	1
Incidents de seguretat relacionats amb la protecció de dades	2
On anar...	2
Tecnologia i protecció de dades	3
Enllacem amb...	3
Butlletí revisió vulnerabilitats	4
Secció responsables de seguretat	5
Esquema Nacional de Seguretat i mesures de seguretat LOPD	6

+info

Incidents de seguretat relacionats amb la protecció de dades

Un hospital britànic perd 2.000 històries clíniques (març 2010)

L'hospital de Haywood de la localitat de Burslem ha perdut les històries clíniques de 2.000 pacients, que havien rebut tractaments de fisioteràpia abans o durant l'any 2006. La direcció d'aquest hospital, propietat de NHS Stoke-on-Trent, ja ha demanat disculpes públicament.

Un portaveu de NHS va manifestar que s'està investigant l'incident, per descobrir què va passar amb aquestes històries clíniques. Una de les possibilitats que s'investiguen és que la documentació hagi estat destruïda per error. Segons el portaveu, els procediments i les mesures de seguretat en el tractament d'aquesta informació s'han endurit, per tal que no es tornin a produir incidents d'aquest tipus.

El coordinador de North Staffordshire HealthWatch ha declarat que s'ha de contactar amb tots els pacients implicats, per informar-los de l'incident.

Font: www.thisisstaffordshire.co.uk

El 80% de les pèrdues de les dades en les empreses les causen els comportaments de risc dels empleats (març 2010)

Un estudi de l'empresa BitDefender, dedicada a la fabricació de programari de seguretat, determina que prop de vuit de cada deu pèrdues de dades sofertes a les empreses tenen l'origen en comportaments insegurs dels seus empleats. Entre aquests comportaments hi ha l'error humà, el robatori o la pèrdua de maquinari, un USB personal infectat o la desactivació de l'antivirus.

Per evitar aquest tipus d'incidents, l'empresa de seguretat considera que és important que els treballadors estiguin formats i conscienciats sobre els riscos a què s'enfronten.

Malgrat que el nombre d'incidents provocats per atacs de programari maliciós (*malware*) són molt inferiors als provocats pel comportament dels empleats, les conseqüències dels primers són molt més perjudicials.

Segons BitDefender, mentre que la fallada d'un ordinador o l'error humà suposen només la pèrdua de dades, la infecció amb programari maliciós pot provocar la pèrdua

de dades i perjudicar la imatge de l'empresa, per no disposar de les mesures de seguretat necessàries per evitar l'atac.

Des de BitDefender es donen alguns consells bàsics per estar més protegits: que cada equip compti amb una contrasenya personal o un mòdul d'autenticació biomètrica; limitar l'accés dels usuaris a l'antivirus, per evitar que el desactivin per aconseguir que la navegació per Internet sigui més ràpida; i que es facin actualitzacions i còpies de seguretat de la informació periòdicament.

També aconsellen fer auditories periòdiques de seguretat, protegir fortament els servidors web de la companyia i instal·lar un filtre antiinundació (*antispam*) en el servidor de correu de l'empresa.

Font: Portal TIC

Suïssa investiga el banc HSBC pel robatori de les dades de 24.000 clients (març 2010)

Les autoritats suïsses han anunciat l'obertura d'una investigació a la filial del banc britànic HSBC al país, pel robatori de dades d'alguns dels seus clients. La sostracció d'aquestes dades, de la qual es va tenir coneixement el passat mes de desembre, després que França reconegués haver utilitzat aquestes dades per perseguir evasors fiscals, va afectar menys de 10 clients, segons va dir el banc llavors. Ara, però, ha reconegut que el robatori perpetrat per un dels seus empleats implica uns 24.000 clients de l'entitat, que tenien diners en un paradís fiscal abans de 2006.

HSBC aclareix que la informació robada no és vàlida per accedir als comptes dels seus clients. Això no obstant, segons el diari *Financial Times* sí que pot afectar aquells ciutadans de fora de Suïssa que hagin desviat els seus diners al país helvètic, per beneficiar-se del seu règim fiscal més favorable.

L'autor del robatori és un antic empleat de la seu de l'HSBC a Ginebra que va oferir les dades a les autoritats franceses, tot i que assegura que no va rebre diners a canvi. Alemanya també va mostrar interès en aquesta informació.

L'entitat britànica ha assegurat que farà tot el possible perquè situacions d'aquest tipus no es tornin a produir. Les autoritats suïsses, que han obert un procediment formal d'examen administratiu, han avançat que "seguiran de prop aquest procés per confirmar que es compleixi amb tots els requisits legals i de seguretat".

Font: ELPAIS.com

On anar...

Congressos i esdeveniments

Conferència "Privacidad y libertad de expresión en la era de Internet"

11 de maig de 2010. Escuela Universitaria de Ingeniería Técnica de Telecomunicación, Madrid
<http://www.euitt.upm.es/escuela>

Presentació Recomanació 1/2010 sobre l'encarregat del tractament

12 de maig de 2010. Barcelona
http://www.apd.cat/ca/curs_jornada_activitat.php?cat_id=170&curs_id=138

IST Information Security Expo 2010

Del 12 al 14 de maig de 2010. Tòquio (Japó)
<http://www.ist-expo.jp/en/>

The 6th International Security Practice and Experience Conference (ISPEC 2010)

12 i 13 de maig de 2010. Seül (Corea)
<http://cb-lab.sch.ac.kr/ISPEC2010/index.html>

The 2010 International Symposium on Collaborative Technologies and Systems (CTS 2010)

Del 17 al 21 de maig de 2010. Chicago, Illinois (EUA)
<http://cisedu.us/cis/cts/10/main/storageDocs.jsp?doc=/docs/cts/10/workshops/W10.COLSEC.html>

The 5th International Conference on Future Information Technology (FutureTech 2010)

Del 20 al 24 de maig de 2010. Bussan (Corea)
<http://www.ftg.org/futuretech2010/>

Conferència "Hacia un nuevo y más amplio concepto de seguridad: la seguridad integral"

25 de maig de 2010. Escuela Universitaria de Ingeniería Técnica de Telecomunicación, Madrid
<http://www.euitt.upm.es/escuela>

The International Conference on Practice and Theory in Public Key Cryptography (PKC)

Del 26 al 28 de maig de 2010. París (França)
<http://www.iseclab.org/eurosec-2010/>

Los retos jurídicos de la protección de datos personales en Internet. Jornadas SICARM 2010

Del 19 al 21 de maig de 2010. Múrcia
<http://www.sicarm.es/>

Presentació Recomanació 1/2010 sobre l'encarregat del tractament

25 de maig de 2010. Girona
http://www.apd.cat/ca/curs_jornada_activitat.php?cat_id=170&curs_id=138

The 6th Workshop on RFID Security

Del 7 al 9 de juny. Istanbul (Turquia)
<http://www.projectice.eu/rfidsec10/>

Tecnologia i protecció de dades

La UE vol canvis en el Street View de Google

Les autoritats de protecció de dades de la Unió Europea van demanar a Google que escurés el període d'emmagatzemament de les imatges del seu servei web Street View, per dubtes de privacitat. Els crítics d'aquest servei de Google l'acusen de no enfosquir les imatges delicades i de situar les càmeres de tal manera que els permet observar sobre tanques o murs dins d'una propietat privada.

Google, que actualment manté les dades durant un any, hauria de reduir aquest període a la meitat, segons les autoritats de privacitat de la UE. El grup de treball creu que una retenció màxima de 6 mesos de còpies no modificades de les imatges seria un equilibri adequat entre protecció de la privacitat i la capacitat d'eliminar falsos positius.

http://noticias.lainformacion.com/politica/proteccion-de-datos/proteccion-de-datos-de-la-ue-quiere-cambios-en-el-street-view_lxAHnEdraoTOKFJdSNLRZ2/

L'Audiència Nacional ratifica el criteri de protecció de dades sobre la difusió de dades per eMule

L'Audiència Nacional ha desestimat el recurs contenciós administratiu interposat pel Govern de Cantàbria, contra una resolució de l'Agència Espanyola de Protecció de Dades (AEPD) que sancionava el servei de salut d'aquesta comunitat autònoma, per difondre dades personals a través del programa d'intercanvi d'arxius eMule.

A principis de 2009, l'AEPD va declarar que el servei de salut citat estava cometent una infracció, en constatar l'existència d'un arxiu accessible des del programa eMule que contenia els noms, cognoms, dates de naixement, adreces, telèfons, sexe, i en algun cas dades de salut associades, de 1.748 pacients de diverses localitats.

En aquest cas, els magistrats conclouen que resulta clar que s'ha produït una omisió de mesures de seguretat i que, a més, això ha ocasionat com a resultat la divulgació a Internet de les dades dels pacients.

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/marzo/03_08_2010_NP_AN_EMULE.pdf

Facebook estudia implantar un sistema de verificació d'edat

Facebook està estudiant la possibilitat d'implantar un sistema de verificació d'edat per als usuaris que vulguin unir-se a la xarxa social, després que al febrer va incrementar a 14 anys l'edat mínima per poder-se registrar.

Així ho va assegurar el director de polítiques per Europa de Facebook, Richard Allan, en una trobada amb el director de l'Agència Espanyola de Protecció de Dades (AEPD), Artemi Rallo. Aquesta institució, tal i com ha afirmat en un comunicat, manté contactes periòdics amb Facebook.

Facebook ha assegurat que està duent a terme una anàlisi de diferents opcions per implantar un sistema de verificació de l'edat dels menors i la comprovació del consentiment patern, amb l'objectiu d'instaurar un mecanisme d'acord amb les exigències de les diferents legislacions internacionals.

D'altra banda, Rallo va animar la companyia a continuar treballant amb l'objectiu de millorar la seva adequació als requisits legals en relació a la presència de menors a Internet, cosa a la qual el representant de Facebook es va comprometre.

L'AEPD també va instar Facebook a reduir la quantitat d'informació dels perfils accessibles a través de buscadors d'Internet, de tal manera que es pugui accedir únicament a les dades del propietari del perfil i no a d'altres informacions de tercers, com per exemple la seva llista d'amics.

UN NOU FORMULARI DE DENÚNCIA

Així mateix, l'AEPD també va preguntar respecte de la forma en què s'atenen les reclamacions i l'exercici de drets, tant d'usuaris como de no usuaris de Facebook, principalment quan les seves dades les publiquen terceres persones.

La xarxa social compta amb un sistema de denúncia, a través del servei d'ajuda. Tot i això, Allan va afirmar que a l'actualitat Facebook està treballant en l'elaboració d'un formulari específic de denúncies, adreçat tant als membres de la xarxa social com als que no en són.

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/marzo/100316_NP_FACEBOOK_WEB.pdf

Enllacem amb...

<http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt>

Els dies 15 i 16 d'abril es va reunir a Granada el Grup Internacional de Protecció de Dades i Telecomunicacions (IWGDPT), conegut pel sobrenom de *grup de Berlín*. És un grup de treball creat l'any 1983, que es reuneix cada sis mesos, i aplega experts i professionals que tracten qüestions relacionades amb les tecnologies de la informació i la comunicació i la protecció de dades i la privacitat.

Hi són representades tant autoritats de control com organitzacions internacionals i el sector privat, tot i que fonamentalment és una reunió d'autoritats de privacitat i protecció de dades.

Com a resultat d'aquestes reunions, es publiquen documents que pretenen avançar-se als problemes que afecten l'esfera de la privacitat i les dades personals derivades de l'ús de les tecnologies.

El grup de Berlín es va crear per iniciativa del Comissionat de Protecció de Dades de Berlín, que és qui el lidera i presideix. Per aquest motiu, la documentació i informació relacionada amb aquest grup la trobarem al lloc web d'aquesta institució, on podrem accedir a la majoria de documents de treball i posicions comunes adoptades des dels seus inicis. És molt recomanable per conèixer quins són els nous riscos detectats per aquest grup d'experts, i quines recomanacions fan per reduir-los o eliminar-los.

L'Agència Catalana de Protecció de Dades participa en les reunions del grup de Berlín des de l'any 2004.

Butlletí revisió vulnerabilitats

Rogues¹ i falsos antivirus

User Protection, Paladin, Dr. Guard... la llista podria seguir infinitament, segons el nom que l'atacant li vulgui posar. Si bé poden variar a l'hora d'infectar l'equip, tots tenen una cosa en comú: són falsos antivirus, que es fan passar per eines legítimes.



El que interessa destacar d'aquests programes maliciosos és el seu bon disseny, que és força treballat i convincent i que recorda el robot i el disseny d'eines d'ESET: només cal compararlos:



Si l'ordinador està infectat amb algun d'aquests falsos antivirus, es pot eliminar utilitzant alguna eina d'ESET, que és un antivirus de prestigi, o bé amb els programes gratuïts Malwarebytes i SuperAntiSpyware, que són eines de protecció contra programes espia (*spyware*) i programari maliciós (*malware*) i que funcionen molt bé.

Si en algun moment s'ha comprat la llicència que ofereixen aquests programes fraudulents, és recomanable posar-se en contacte amb l'entitat bancària per informar de la situació i, si és possible, cancel·lar el pagament. Hi ha la possibilitat, a més, que la informació de la targeta hagi estat robada.

Font: INTECO

¹ El *rogue software* (es podria traduir com a "programari bandit") és un tipus de programa informàtic malintencionat, que té com a objectiu principal fer creure que un ordinador està infectat per algun tipus de virus i induir a fer un pagament per eliminar-lo.

Últims virus detectats

Trojan.W32/Koobface.AL (Perillositat: 1 - Mínima)

Troià que afecta la plataforma Windows i que modifica el registre de Windows per executar-se en cada inici de sessió.

Trojan.W32/Bckdr.RBN (Perillositat: 1 - Mínima)

Troià per a plataforma Windows, que és capaç de robar dades bancàries i enviar-les a un servidor d'Internet.

Trojan.W32/Wisp (Perillositat: 2 - Baixa)

Troià que roba informació sensible i permet a un atacant obtenir accés no autoritzat a l'equip infectat.

Trojan.W32/Agent.MSI (Perillositat: 1 - Mínima)

Troià per a la plataforma Windows, que disminueix el nivell de seguretat del navegador.

Trojan.W32/Scar.AYWK (Perillositat: 1 - Mínima)

Troià que permet la connexió a l'equip infectat mitjançant una porta del darrere, controlada per un servidor IRC.

Trojan.W32/Mdrop.CLF (Perillositat: 1 - Mínima)

Troià per a la plataforma Windows, que modifica valors de l'Internet Explorer i es comunica amb servidors d'Internet.

Trojan.W32/Trjan_0014b0851 (Perillositat: 1 - Mínima)

Troià per a la plataforma Windows que, entre altres modificacions de la configuració de seguretat de l'equip, s'afegeix a la llista d'aplicacions que el tallafocs permet accedir a Internet.

Trojan.W32/Agent.MSB (Perillositat: 1 - Mínima)

Troià per a plataforma Windows, que modifica el registre del sistema i es comunica amb servidors a Internet.

Worm.W32/P2PShared.AV @ MM + P2P + Altres (Perillositat: 2 - Baixa)

Cuc que es propaga per xarxes d'intercanvi d'arxius P2P, correu electrònic i deixant còpies de si mateix en dispositius extraïbles. Monitoritza les recerques que l'usuari fa a Internet, per modificar els resultats de cerca i incloure-hi publicitat.

FraudTool.W32/Antivirus7 @ Altres (Perillositat: 1 - Mínima)

Eina de frau que mostra falses anàlisis de seguretat del sistema que informen de fixers infectats amb codi maliciós. A més, informa que l'usuari pot eliminar aquest codi maliciós del seu equip registrant el programa, per a la qual cosa se li demanen diners.

Trojan.W32/Hupigon.CW (Perillositat: 1 - Mínima)

Troià per a la plataforma Windows, que crea nous fixers en l'equip compromès i es connecta amb llocs remots per descarregar nou programari maliciós (*malware*).

Trojan.W32/Inject.JDT (Perillositat: 1 - Mínima)

Troià per a la plataforma Windows, que es connecta amb llocs maliciosos per obtenir instruccions d'atacants remots.

Trojan.W32/Sykipot (Perillositat: 1 - Mínima)

Troià que es propaga aprofitant una vulnerabilitat no solucionada d'algunes versions d'Internet Explorer.

Trojan.W32/FraudPack.AOIP (Perillositat: 1 - Mínima)

Troià per a plataforma Windows, que modifica el registre del sistema per carregar en memòria i descarrega altre programari maliciós.

Trojan.W32/Mdrop.CLD (Perillositat: 1 - Mínima)

Troià per a la plataforma Windows, que s'executa automàticament i té la funcionalitat de crear fixers d'execució per lots (*batch*).

Font: INTECO

Secció responsables de seguretat

Nom i cognoms
Eulàlia Brugués

Lloc que ocupa
Cap del Departament de Sistemes
d'Informació

Entitat
Ajuntament de Sant Joan Despí

En quin àmbit desenvolupes la teva activitat com a responsable de seguretat?

Desenvolupo la meva activitat com a responsable de seguretat en l'àmbit dels sistemes d'informació, informàtica i telecomunicacions de l'Ajuntament de Sant Joan Despí.

Desenvolupes en exclusiva l'activitat de responsable de seguretat?

La qüestió de la seguretat física de les dades és una tasca del Departament de SI.

Els tècnics del departament són els encarregades de revisar la seguretat de les còpies i d'establir els nivells de seguretat d'accés a la informació, segons el nivell que correspongui a cada usuari de la xarxa municipal. No hi ha, però, una persona que desenvolupi en exclusiva l'activitat de responsable de seguretat física i/o jurídica de les dades de caràcter personal.

Quina és la principal dificultat que trobes per desenvolupar les funcions de responsable de seguretat?

La complexitat per donar compliment a tots els requisits que marca la llei.

La manca de conscienciació en temes de tractament i seguretat de dades de caràcter personal dins de l'organització.

En relació a la protecció de dades, quina responsabilitat et requereix més dedicació?

El procés de recollida de dades i els procediments de la declaració de fitxers. També el seguiment del compliment de la llei en el si de l'organització.

Mantens contacte amb l'APDCAT per resoldre qüestions o plantejar dubtes que et puguin sorgir en el dia a dia?

Des de la meua experiència com a coordinadora de la seguretat de les dades de caràcter personal a l'Ajuntament de Sant Joan Despí, puc assegurar que l'APDCAT realitza una tasca important, oferint suport i solucions davant qualsevol dubte o qüestió sobre aquest tema, d'una manera pràctica, propera i entenedora.

Esquema Nacional de Seguretat i mesures de seguretat LOPD

Ramon Miralles. Coordinador d'Auditoria i Seguretat de la Informació
Agència Catalana de Protecció de Dades

L'Esquema Nacional de Seguretat és resultat del que preveu la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, que al seu art. 42.2 estableix quin serà l'objecte i contingut de l'ENS.

L'ENS té per objecte establir la política de seguretat en la utilització de mitjans electrònics en l'àmbit de la Llei 11/2007, i està constituït per principis bàsics i requisits mínims que han de garantir una adequada protecció de la informació.

Per una altra banda, una part important de la regulació del dret fonamental a la protecció de dades de caràcter personal està constituïda per la implantació de mesures de seguretat, tant tècniques com organitzatives, en els fitxers i tractaments de dades de caràcter personal.

El principi de seguretat de l'art. 9 de la LOPD és un requisit de legalitat en el tractament de les dades personals, que es concreta en les mesures de seguretat previstes en el títol VIII del Reial decret 1720/2007, que aprova el reglament de desplegament de la LOPD.

Per tant, el fet que el sector públic compti amb una regulació comuna i obligatòria, basada en uns requisits mínims de seguretat de la informació, no és una novetat, tot i que es tracti d'una protecció centrada en aquella informació relacionada amb el tractament de dades de caràcter personal. En el cas de les administracions públiques, això implica referir-se quasi al 100% de la informació que utilitzen en el desenvolupament de les seves activitats.

L'ENS no és aliè a l'existència d'unes obligacions en matèria de seguretat de la informació, derivades del tractament de dades de caràcter personal. Així, en l'exposició de motius, quan s'aborda la concepció d'activitat integral de la seguretat, s'afegeix que la informació tractada en els sistemes electrònics als quals es refereix l'ENS ha d'estar protegida tenint en compte els criteris que estableix la LOPD; i, ja a la part dispositiva, l'art. 27.2 preveu que quan un sistema

d'informació tracta dades de caràcter personal li és d'aplicació el que disposa la LOPD i la seva normativa de desplegament, sens perjudici dels requisits que estableix l'ENS.

El que sí que planteja l'ENS és una manera diferent, en relació a la LOPD, de determinar quines mesures de seguretat cal aplicar en cada cas. En el context de la LOPD, allò que és prioritari protegir és la dada i, per tant, la protecció sempre gira a l'entorn de salvaguardar la informació personal; per a l'ENS, en canvi, la seguretat s'aplica a l'ús dels mitjans electrònics, una perspectiva més àmplia, si es vol, que inclou com a objecte de protecció les dades, les informacions i els sistemes; per tant, les previsions de l'ENS evidencien que allò que li resulta prioritari protegir és l'ús dels sistemes de informació.

A la pràctica, aquesta visió diferent no té perquè donar resultats divergents o contradictoris, però indubtablement sí que suposa afegir una major complexitat a la gestió de la seguretat de la informació.

A títol d'exemple, aquesta manera diversa de definir la seguretat pot donar lloc a la paradoxa que a unes determinades dades els siguin d'aplicació les mesures de seguretat de nivell bàsic, segons la LOPD, i alhora, d'acord amb els requisits de seguretat de l'ENS, aquell sistema amb dades de nivell bàsic s'hagi de qualificar de categoria alta.

L'ENS busca l'alineació de la seguretat amb l'assoliment dels objectius que tenen les organitzacions vinculades al sector públic i, per tant, una qüestió essencial és garantir l'ús dels sistemes en condicions òptimes de seguretat.

D'aquesta manera, quan l'annex I de l'ENS aborda el mètode de determinació de la categoria dels sistemes, ho fonamenta en la repercussió que l'incident de seguretat pot tenir en elements tan crítics per a les organitzacions com assolir els seus objectius funcionals, protegir els actius al seu càrrec o complir amb les obligacions diàries de servei.

L'ENS busca l'alineació de la seguretat amb l'assoliment dels objectius que tenen les organitzacions vinculades al sector públic i, per tant, una qüestió essencial és garantir l'ús dels sistemes en condicions òptimes de seguretat.

D'aquesta manera, quan l'annex I de l'ENS aborda el mètode de determinació de la categoria dels sistemes, ho fonamenta en la repercussió que l'incident de seguretat pot tenir en elements tan crítics per a les organitzacions com assolir els seus objectius funcionals, protegir els actius al seu càrrec o complir amb les obligacions diàries de servei.

Certament, també es fonamenta la determinació de la categoria dels sistemes d'informació en qüestions connectades amb el dret fonamental a la protecció de dades de caràcter personal, com són el respecte a la legalitat vigent o el respecte als drets de les persones. En definitiva, com veurem, a l'ENS les mesures de seguretat a implantar es vinculen a la categoria del sistema d'informació, mentre que a la LOPD es vinculen al tipus de dades tractades.

L'annex I descriu el mètode a seguir per determinar la categoria dels sistemes, ja que per concretar els controls previstos a l'annex II (mesures de seguretat) s'han de catalogar en una de les 3 possibles categories previstes a l'ENS: bàsica, mitjana o alta. La determinació de la categoria es basa a valorar quin impacte tindria sobre l'organització un incident de seguretat que afectés la informació o els sistemes.

S'entén que les conseqüències d'un incident poden afectar la capacitat de l'organització per:

- Assolir els seus objectius
- Protegir els actius al seu càrrec
- Complir amb les seves obligacions diàries de servei
- Respectar la legalitat vigent
- Respectar els drets de les persones

La categorització dels sistemes s'ha d'aplicar tant als sistemes utilitzats per a la prestació dels serveis d'administració electrònica, com als que serveixen de suport al procediment administratiu general (sistemes de gestió interna).

Per determinar la categoria del sistema d'informació, primer cal concretar l'impacte de l'incident. Per fer-ho, s'ha de tenir en compte com afecta 5 dimensions de seguretat:

- Disponibilitat [D]
- Autenticitat [A]
- Integritat [I]
- Confidencialitat [C]
- Traçabilitat [T]

A l'annex IV de l'ENS trobarem les definicions d'aquestes dimensions:

- Disponibilitat: propietat o característica dels actius consistent que les entitats o processos autoritzats hi tinguin accés quan ho requereixin.
- Autenticitat: propietat o característica consistent que una entitat és qui diu ser o bé queda garantida la font de la qual procedeixen les dades.
- Integritat: propietat o característica consistent que l'actiu d'informació no ha estat alterat de manera no autoritzada.
- Confidencialitat: propietat o característica consistent que la informació ni es posa a disposició, ni es revela a individus, entitats o processos no autoritzats.
- Traçabilitat: propietat o característica consistent que les actuacions d'una entitat poden ser imputades exclusivament a aquesta entitat.

El mètode de catalogació previst a l'annex I implica que primer cal determinar el nivell requerit per a cada dimensió de seguretat de la informació o del sistema (un sistema o informació es pot veure afectat per un incident, en 1 o diverses dimensions).

Cada dimensió que es pugui veure afectada s'ha d'adscriure a un dels nivells següents (si una dimensió no està afectada no se li assigna cap nivell):

- BAIX: les conseqüències suposen un perjudici limitat sobre les funcions de l'organització, els seus actius o els individus afectats.
- MITJÀ: les conseqüències suposen un perjudici greu sobre les funcions de l'organització, els seus actius o els individus afectats.
- ALT: les conseqüències suposen un perjudici molt greu sobre les funcions de l'organització, els seus actius o els individus afectats.

Segons l'ENS, s'ha d'entendre per:

- Perjudici limitat:
 1. Es redueix de forma apreciable la capacitat de l'organització per atendre eficaçment les seves obligacions operatives (encara que se segueixin desenvolupant).
 2. Els actius pateixen un dany menor.
 3. Hi ha incompliment formal d'alguna llei o regulació, que pugui ser esmenat.
 4. Es causa un perjudici menor a algun individu, que pugui ser fàcilment reparable (tot i que pugui causar alguna molèstia).
 5. Altres de naturalesa anàloga.
- Perjudici greu:
 1. Es redueix de forma significativa la capacitat de l'organització per atendre eficaçment les seves obligacions fonamentals (encara que se segueixin realitzant).
 2. Els actius pateixen un dany significatiu.
 3. Hi ha incompliment material d'alguna llei, regulació, o incompliment formal no esmenable.
 4. Es causa un perjudici significatiu a algun individu, de difícil reparació.
 5. Altres de naturalesa anàloga.
- Perjudici molt greu:
 1. Queda anul·lada la capacitat de l'organització per atendre alguna de les seves obligacions fonamentals, que impedeix que se segueixin realitzant.
 2. Els actius pateixen un dany molt greu o irreparable.
 3. Hi ha incompliment greu d'alguna llei o regulació.
 4. Es causa un perjudici greu a algun individu, de difícil o impossible reparació.
 5. Altres de naturalesa anàloga.

Quan un sistema tracti diferents informacions o presti diferents serveis, el nivell del sistema en cada dimensió serà el major dels establerts per a cada informació o servei.

Per últim, una vegada determinat el nivell per a cada dimensió de seguretat, s'ha de determinar la categoria del sistema: BÀSICA, MITJANA O ALTA. La categoria del sistema serà la que correspongui al nivell més exigent d'alguna de les dimensions per les quals es pugui veure afectat; per tant, si per alguna de les dimensions es considera que és d'aplicació el nivell alt, el sistema serà de categoria alta. Òbviament, la determinació d'una categoria concreta per a un sistema no modifica el nivell de seguretat definit per a cada dimensió.

Cal tenir present que el model proposat per l'ENS implica disposar d'un inventari de tots els actius relacionats amb els sistemes d'informació, i que un dels punts de partida és la necessitat de realitzar una anàlisi de riscos, tal i com preveu l'art. 13 (anàlisi i gestió dels riscos). És a dir que cada organització està obligada a fer la gestió de riscos, tot i que el nivell de formalització i profunditat pot variar d'acord de la categoria del sistema.

L'ENS aporta una visió àmplia de la seguretat de la informació. A la pràctica planteja la implantació d'un sistema de gestió de la seguretat de la informació, amb molts elements en comú amb l'UNE-ISO/IEC 27001 i, en conseqüència, amb els controls previstos a la ISO/IEC 27002.