



**GUIA LEGAL DE SEGURETAT:
Esquema Nacional de Seguretat
Part 1: Guia metodològica**

Índex

3	Presentació
4	Llicència d'ús
5	Introducció
	Audiència
	Abast
	Aspectes legals i normatius
6	Descripció general
	Què és i en què consisteix?
8	Finalitat
9	Casos d'estudi
	Qui ha de complir les normes de l'Esquema Nacional de Seguretat.
	Quin és l'àmbit d'aplicació de l'Esquema Nacional de Seguretat.
10	Quins són els sistemes que han de complir amb l'Esquema Nacional de Seguretat.
	Quins són els terminis per complir amb l'Esquema Nacional de Seguretat.
11	L'establiment de la política de seguretat.
12	La identificació dels sistemes afectats.
	La determinació dels riscos sobre els sistemes afectats.
13	La categorització de seguretat dels sistemes afectats.
15	L'aplicació dels controls de seguretat.
16	L'auditoria de compliment de l'Esquema Nacional de Seguretat.
17	Recomanacions
	Recomanacions per a totes les Administracions públiques.
18	Recomanacions per a les Administracions públiques locals de població reduïda.
19	Glossari de termes
22	Referències i enllaços web.
	Eines
	Eines d'anàlisi de riscos.
	Recursos de suport on-line

Presentació

El Centre de Seguretat de la Informació de Catalunya, CESICAT, és l'organisme executor del Pla nacional d'impuls de la seguretat TIC aprovat pel govern de la Generalitat de Catalunya el 17 de març de 2009. La missió d'aquest pla és la de garantir una Societat de la Informació Segura Catalana per a tots. Amb aquesta finalitat, es crea el CESICAT com a eina per a la generació d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui referent nacional i internacional.

El Pla nacional d'impuls de la seguretat TIC a Catalunya s'estructura al voltant de quatre objectius estratègics principals que seran desenvolupats pel CESICAT:

- Executar l'estratègia nacional de seguretat TIC establerta pel Govern de la Generalitat de Catalunya
- Donar suport a la protecció de les infraestructures crítiques TIC nacionals
- Promocionar un teixit empresarial català sòlid en seguretat TIC
- Incrementar la confiança i protecció de la ciutadania catalana en la societat de la informació

La forma jurídica del CESICAT és la de "fundació del sector públic de l'administració de la Generalitat".

Amb l'objectiu de proporcionar unes bones pràctiques i uns coneixements mínims en seguretat de la informació, com a servei preventiu el CESICAT ofereix l'elaboració d'un conjunt de guies de seguretat adreçades a les diferents comunitats. En particular, la temàtica d'aquesta publicació és la d'establir una guia metodològica per donar a conèixer l'Esquema Nacional de Seguretat.

En aquest sentit, el CESICAT, com a òrgan encarregat d'executar l'estratègia nacional de seguretat TIC i d'acord amb la Disposició addicional 2 de l'Esquema Nacional de Seguretat, establirà una seguit d'actuacions per tal de donar suport a la millor implantació de les mesures de seguretat establertes a l'ENS en l'àmbit de Catalunya. Aquesta guia constitueix la primera actuació del CESICAT complementant-se amb d'altres per facilitar el compliment de la norma i la millora dels nivells de seguretat en l'àmbit de les Administracions públiques de Catalunya.

El contingut de la present guia és titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya i resta subjecta a la llicència de Creative Commons BY-NC-ND. L'autoria de l'obra es reconeixerà mitjançant la inclusió de la següent menció:



Obra titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya.


Llicenciada sota la llicència CC BY-NC-ND.

La present guia es publica sense cap garantia específica sobre el contingut.





L'esmentada llicència té les següents particularitats:


Vostè és lliure de:

 Copiar, distribuir i comunicar públicament la obra.

Sota les condicions següents:

 **Reconeixement:** S'ha de reconèixer l'autoria de la obra de la manera especificada per l'autor o el llicenciador (en tot cas no de manera que suggereixi que gaudeix del seu suport o que dona suport a la seva obra).

 **No comercial:** No es pot emprar aquesta obra per a finalitats comercials o promocionals.

 **Sense obres derivades:** No es pot alterar, transformar o generar una obra derivada a partir d'aquesta obra.

Respecte d'aquesta llicència caldrà tenir en compte el següent:

■ **Modificació:** Qualsevol de les condicions de la present llicència podrà ser modificada si vostè disposa de permisos del titular dels drets.

■ **Altres drets:** En cap cas els següents drets restaran afectats per la present llicència:.

■ Els drets del titular sobre els logotips, marques o qualsevol altre element de propietat intel·lectual o industrial inclòs a les guies. Es permet tan sols l'ús d'aquests elements per a exercir els drets reconeguts a la llicència.

■ Els drets morals de l'autor.

■ Els drets que altres persones poden tenir sobre el contingut o respecte de com s'empra la obra, tals com drets de publicitat o de privacitat.

Avis: En reutilitzar o distribuir la obra, cal que s'esmentin clarament els termes de la llicència d'aquesta obra.

El text complet de la llicència pot ser consultat a <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca>.

Introducció

Audiència

Aquesta guia està adreçada als responsables jurídics de les Administracions públiques catalanes, així com als responsables dels serveis i/o les aplicacions.

Abast

Aquest document presenta les obligacions de seguretat de la informació que ha establert la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics i el seu Reial decret de desplegament 3/2010, de 8 de gener, aplicable a totes les Administracions públiques territorials i als organismes i entitats de dret públic que en depenen.

Aspectes legals i normatius

Aquesta guia incorpora essencialment els aspectes legals de seguretat de la informació prescrits per la legislació d'administració electrònica i s'ha d'entendre sense perjudici d'altres normes aplicables que estableixen obligacions de seguretat de la informació, en particular la legislació de protecció de les dades de caràcter personal. És important notar que els subjectes obligats a donar compliment a ambdues normatives hauran de coordinar-ne el compliment mitjançant documentació conjunta o la implementació de les mesures de seguretat tècniques i/o organitzatives necessàries.

Descripció general

Què és i en què consisteix?

La seguretat de la informació té una importància molt rellevant en la legislació reguladora de l'administració electrònica, com s'ha evidenciat en la Llei bàsica 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

Cal recordar, en primer lloc, que la Llei 11/2007 és una veritable llei d'administració, que **reconeix el dret dels ciutadans a relacionar-se amb les Administracions públiques per mitjans electrònics** i regula els aspectes bàsics de la utilització de les tecnologies de la informació en l'activitat administrativa, en les relacions entre les Administracions públiques i en les relacions dels ciutadans amb aquestes amb la finalitat de garantir-ne els drets, un tractament comú davant les Administracions i la validesa i eficàcia de l'activitat administrativa en condicions de seguretat jurídica.

En aquest sentit, el concepte de seguretat de la informació ja apareix en l'article 1.2, dedicat a l'objecte de la norma, que indica que les Administracions públiques han d'utilitzar les tecnologies de la informació d'acord amb el que disposa aquesta llei i **assegurar la disponibilitat, l'accés, la integritat, l'autenticitat, la confidencialitat i la conservació de les dades, les informacions i els serveis** que gestionin en l'exercici de les seves competències.

També l'article 3 de la Llei 11/2007, que explicita les finalitats de la llei, indica a l'epígraf 3 la voluntat del legislador de **crear les condicions de confiança en l'ús dels mitjans electrònics** i establir les mesures necessàries per a la preservació de la integritat dels drets fonamentals i, en especial, els relacionats amb la intimitat i la protecció de dades de caràcter personal, per **mitjà de**

la **garantia de la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics**, previsió que dota el concepte de seguretat d'un indiscutible protagonisme legal.

En conseqüència, veurem que una part força important de la llei, amb la finalitat de fer efectiva aquesta garantia, tracta aspectes de seguretat en relació amb l'ús intensiu dels elements informàtics per part de les Administracions públiques.

De manera semblant, quan l'article 4 de la Llei 11/2007 institueix els principis legals aplicables a l'administració electrònica, tracta de manera explícita diversos **principis específicament relacionats amb el concepte de seguretat**:

- Principi de **protecció de dades de caràcter personal**, que es plasma en el respecte a aquest dret fonamental en els termes que estableix la Llei orgànica 15/1999, de protecció de les dades de caràcter personal, en les altres lleis específiques que regulen el tractament de la informació i en les seves normes de desplegament, així com en els drets a l'honor i a la intimitat personal i familiar.
- Principi d'**accessibilitat**, a través de sistemes que permetin l'ús dels serveis de manera segura i comprensible i que garanteixin especialment l'accessibilitat universal i el disseny per a tots dels suports, canals i entorns amb la finalitat que totes les persones puguin exercir els seus drets en igualtat de condicions. Aquest principi té impacte en les mesures de seguretat a aplicar donat que no es podrà generar discriminació en l'aplicació.

- Principi de **seguretat en la implantació i utilització dels mitjans electrònics** per part de les Administracions públiques, en virtut del qual s'exigeix almenys el mateix nivell de garanties i seguretat que es requereix per a la utilització de mitjans no electrònics en l'activitat administrativa. Aquest paràmetre constitueix el límit inferior de seguretat a aportar, ja que no resultaria acceptable que el procediment tramitat electrònicament fos menys segur que el procediment tramitat en suport paper i d'altres mitjans tradicionals.

- Principi de **proporcionalitat**, en virtut del qual només s'exigeixen les garanties i mesures de seguretat adequades a la naturalesa i circumstàncies dels diferents tràmits i actuacions. En funció d'aquestes s'estableix el límit superior de seguretat, doncs tampoc no resulta acceptable exigir més seguretat de la necessària, perquè aquesta exigència excessiva constitueix, en si mateixa, una barriera a l'accés dels ciutadans al procediment electrònic.

Finalment, l'article 6 de la Llei 11/2007 reconeix veritables drets dels ciutadans en relació amb la seguretat:

- Dret a la **garantia de la seguretat i confidencialitat de les dades** que figurin en els fitxers, sistemes i aplicacions de les Administracions públiques (important en relació amb el dret dels ciutadans a la **conservació en format electrònic** per part de les Administracions públiques dels documents electrònics que formin part d'un expedient).
- Dret a **obtenir els mitjans d'identificació electrònica necessaris**. Les persones físiques poden utilitzar en tot cas els sistemes de signatura electrònica

del document nacional d'identitat per a qualsevol tràmit electrònic amb qualsevol Administració pública.

- Dret a la **utilització d'altres sistemes de signatura electrònica admesos** en l'àmbit de les Administracions públiques.

Per garantir l'efectivitat d'aquests principis i drets subjectius dels ciutadans, l'article 42 de la Llei 11/2007 ha previst l'existència de l'**Esquema Nacional de Seguretat**, que té per objecte establir la **política de seguretat en la utilització de mitjans electrònics en l'àmbit d'aquesta llei** i està constituït pels **principis bàsics i requisits mínims** que permetin una protecció adequada de la informació.

L'Esquema Nacional de Seguretat ha estat aprovat pel Reial decret 3/2010, de 8 de gener.

Finalitat

Com indica l'exposició de motius del Reial decret 3/2010, la finalitat de l'Esquema Nacional de Seguretat és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per garantir la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics, que permeti als ciutadans i les Administracions públiques l'exercici de drets i el compliment de deures a través d'aquests mitjans.

L'Esquema Nacional de Seguretat persegueix fonamentar la confiança en el fet que els sistemes d'informació presten els serveis i custodien la informació d'acord amb les seves especificacions funcionals, sense interrupcions o modificacions fora de control i sense que la infor-

mació pugui arribar a persones no autoritzades.

En aquest sentit, l'Esquema Nacional de Seguretat defineix la seguretat de la informació com la capacitat de les xarxes o dels sistemes d'informació de resistir, amb un determinat nivell de confiança, els accidents o les accions il·lícites o malintencionades que comprometin la disponibilitat, autenticitat, integritat i confidencialitat de les dades emmagatzemades o transmeses i dels serveis que les xarxes i sistemes esmentats ofereixen o fan accessibles.

Casos d'estudi **Qui ha de complir les normes de l'Esquema Nacional de Seguretat.**

L'Esquema Nacional de Seguretat s'adreça a les Administracions públiques, incloses les entitats següents:

- L'Administració General de l'Estat.
- Les Administracions de les Comunitats Autònomes.
- Les entitats que integren l'Administració local.
- Les entitats de dret públic que estan vinculades a les anteriors o en depenen.

Es poden considerar incloses dintre d'aquest conjunt de destinataris les institucions públiques creades per llei regides de manera subsidiària per la legislació de procediment administratiu.

Quin és l'àmbit d'aplicació de l'Esquema Nacional de Seguretat.

Un dels aspectes més rellevants que cal determinar és l'abast material d'aplicació de l'Esquema Nacional de Seguretat, és a dir, indicar sobre quines activitats de les Administracions públiques recau.

En aquest sentit, cal indicar en primer lloc que la Llei 11/2007 regula els aspectes bàsics de la utilització de les tecnologies de la informació en tres àmbits:

- L'activitat administrativa.
- Les relacions entre les Administracions públiques (o activitat interadministrativa, com per exemple les transmissions de dades emprant xarxes interoperables).

- Les relacions dels ciutadans amb les Administracions públiques (i, en concret, el procediment administratiu electrònic i la participació electrònica).

Per tant, l'Esquema Nacional de Seguretat resultarà d'aplicació a aquestes activitats i als actius involucrats en executar-les. Resten excloses de l'aplicació de l'Esquema Nacional de Seguretat les activitats que les Administracions públiques portin a terme en règim de dret privat.

Quins són els sistemes que han de complir amb l'Esquema Nacional de Seguretat.

Un cop hem determinat les activitats a les quals s'aplica l'Esquema Nacional de Seguretat, cal concretar quins són els sistemes específics sobre els quals s'estableixen els requisits de seguretat.

L'article 5 del Reial decret 3/2010 indica que la seguretat s'entén com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius relacionats amb el sistema d'informació, que és l'objecte principal sobre el qual es construeix l'Esquema Nacional de Seguretat.

En aquest sentit, l'annex IV del Reial decret defineix el sistema d'informació com el conjunt organitzat de recursos perquè la informació es pugui recollir, emmagatzemar, processar o tractar, mantenir, utilitzar, compartir, distribuir, posar a disposició, presentar o transmetre.

Per tant, l'Esquema Nacional de Seguretat, que desplega la Llei 11/2007, s'aplica essencialment als sistemes d'informació que suporten l'activitat administrativa, l'activitat interadministrativa i les relacions amb els ciutadans.

Resten exclosos de l'àmbit d'aplicació de l'Esquema Nacional de Seguretat els sistemes que tracten informació classificada regulada per la Llei 9/1968, de 5 d'abril, de secrets oficials i normes de desplegament, com també els sistemes d'informació que suporten les activitats que les Administracions públiques portin a terme en règim de dret privat.

En sentit similar, d'acord amb el que disposa l'article 30 del Reial decret 3/2010, les Administracions públiques poden determinar els sistemes d'informació als quals no els sigui aplicable l'Esquema Nacional de Seguretat si es tracta de sistemes no relacionats amb l'exercici de drets, el compliment de deures per mitjans electrònics ni l'accés per mitjans electrònics dels ciutadans a la informació i al procediment administratiu.

Quins són els terminis per complir amb l'Esquema Nacional de Seguretat.

La disposició transitòria del Reial decret 3/2010 indica que els sistemes existents a l'entrada en vigor de l'Esquema Nacional de Seguretat s'hi han d'adequar de manera que permetin el compliment del que estableix la disposició final tercera de la Llei 11/2007, de 22 de juny, mentre que els nous sistemes han d'aplicar el que estableix el present Reial decret des que són concebuts. Aquesta previsió legal implica que el calendari d'adequa-

ció dels sistemes existents resta subjecte a l'existència d'un pressupost adequat i suficient per a la implantació de l'administració electrònica, fet que apunta la necessitat de coordinar l'adequació dels sistemes existents amb la planificació de modernització i impuls a l'administració electrònica de cada entitat.

En qualsevol cas, s'ha de tenir en compte que l'apartat segon de la disposició transitòria indica que si al cap de dotze mesos de l'entrada en vigor de l'Esquema Nacional de Seguretat hi ha circumstàncies que impedeixen la plena aplicació del que s'hi exigeix, s'ha de disposar d'un pla d'adequació que estableixi els terminis d'execució, que en cap cas no poden ser superiors a quaranta-vuit mesos des de l'entrada en vigor. Per tant, el termini inicial establert per al compliment de l'Esquema Nacional de Seguretat **finalitzarà el proper gener de 2011** per a tots els sistemes preexistents, si no es disposa d'un pla d'implantació d'acord amb allò exposat anteriorment.

Per complir amb l'Esquema Nacional de Seguretat resulta necessari, com indica l'article 27 del Reial decret 3/2010, aplicar un conjunt de mesures identificades en l'annex II de la norma i considerar els actius del sistema d'informació, la categoria del sistema i les decisions que s'adoptin per gestionar els riscos identificats de manera integrada, quan s'escaigui, amb la reglamentació de seguretat de protecció de dades de caràcter personal.

Per assolir aquest objectiu, resulta necessari aplicar una metodologia que consideri els següents passos:

1. Establir una política de seguretat.

2. Identificar els sistemes afectats.

3. Determinar els riscos sobre els sistemes afectats.

4. Categoritzar els sistemes afectats.

5. Aplicar els controls corresponents, dels previstos a l'annex II de l'Esquema Nacional de Seguretat.

L'establiment de la política de seguretat.

Respecte a l'**establiment de la política de seguretat**, es tracta de redactar i aprovar formalment un document que, d'acord amb el que determina l'article 11 del Reial decret 3/2010, estableixi els principis i requisits mínims de seguretat que a ha de complir l'organització.

Aquesta política de seguretat necessàriament haurà d'adreçar i descriure un conjunt mínim de requisits, en proporció als riscos identificats a cada sistema, que versaran sobre el següents punts:

- a) Organització i implantació del procés de seguretat.
- b) Anàlisi i gestió dels riscos.
- c) Gestió de personal.
- d) Professionalitat.
- e) Autorització i control dels accessos.
- f) Protecció de les instal·lacions.
- g) Adquisició de productes.
- h) Seguretat per defecte.
- i) Integritat i actualització del sistema.
- j) Protecció de la informació emmagatzemada i en trànsit.
- k) Prevenció enfront d'altres sistemes d'informació interconnectats.

- l) Registre d'activitat.
- m) Incidents de seguretat.
- n) Continuitat de l'activitat.
- o) Millora contínua del procés de seguretat.

Aquesta política haurà de coordinar-se amb el Document de Seguretat requerit per la normativa de protecció de dades i recollir en conjunt les polítiques i mesures de seguretat i el tractament de dades al si de l'organització (essent possible que el Document de Seguretat s'integri dins la política global de seguretat o bé que ambdós documents es relacionin).

La identificació dels sistemes afectats.

Respecte a la **identificació dels sistemes afectats**, hem indicat anteriorment que l'Esquema Nacional de Seguretat s'aplica essencialment als sistemes d'informació que ofereixen suport a l'activitat administrativa, l'activitat interadministrativa i les relacions electròniques amb els ciutadans, la qual cosa inclou sistemes com, per exemple, la seu electrònica, el registre electrònic, el sistema de notificació electrònica i les aplicacions de gestió i tramitació o de gestió documental, entre d'altres.

Resulta molt convenient alinear aquesta fase amb l'estratègia i planificació de desplegament de l'administració electrònica i, si s'escau, preparar i aprovar un pla director de seguretat de la informació si l'entitat ho requereix, tenint-ne en compte la rellevància o en cas que gestioni aquesta matèria per tercers (com en el cas de les diputacions).

La determinació dels riscos sobre els sistemes afectats.

Respecte a la **determinació dels riscos sobre els sistemes afectats**, d'acord amb l'article 6 del Reial decret 3/2010, l'anàlisi i gestió de riscos és part essencial del procés de seguretat i s'ha de mantenir permanentment actualitzada, de manera que la gestió de riscos permeti el manteniment d'un entorn controlat, minimitzant els riscos fins a nivells acceptables.

La reducció d'aquests nivells s'ha de realitzar mitjançant el desplegament de mesures de seguretat adequades, que s'han de determinar analitzant la naturalesa de les dades i els tractaments i els riscos a què estiguin exposades, previsió que concreta l'aplicació dels principis de seguretat i proporcionalitat de la Llei 11/2007.

En el mateix sentit, l'article 13 del Reial decret 3/2010 exigeix que cada organització que elabori i implanti sistemes per al tractament de la informació i les comunicacions realitzi la seva pròpia gestió de riscos, que s'ha de fer per mitjà de l'anàlisi i el tractament dels riscos als quals està exposat el sistema, utilitzant alguna metodologia reconeguda internacionalment, com per exemple MAGERIT, OCTAVE o CRAMM (a l'apartat 9 d'aquesta guia es recull una eina com a referència per a la gestió de riscos).

La realització d'una anàlisi de riscos exigeix prèviament la **identificació dels actius** que formen els sistemes d'informació afectats, que en la conceptualització de l'Esquema Nacional de Seguretat són els components

o funcionalitats d'un sistema d'informació susceptibles de ser atacats de manera deliberada o accidental amb conseqüències per a l'organització.

És molt important retenir que les mesures adoptades per mitigar o suprimir els riscos han d'estar justificades i, en tot cas, hi ha d'haver una proporcionalitat entre aquestes i els riscos existents.

Un cop realitzat l'anàlisi de riscos, es disposa d'un **catàleg d'actius i amenaces** sobre els mateixos, generalment amb una valoració qualitativa (risc alt, risc mitjà, etc.) o quantitativa (general, en forma de percentatge de freqüència previsible d'ocurrència). A partir d'aquesta anàlisi podem establir la categoria de seguretat del sistema i, en conseqüència, seleccionar els controls mínims a aplicar.

La categorització de seguretat dels sistemes afectats.

Respecte a la **categorització dels sistemes** afectats, cal dir que la categoria d'un sistema d'informació, en matèria de seguretat, ha de modular l'equilibri entre la importància de la informació que utilitza, els serveis que ofereix i l'esforç de seguretat requerit, en funció dels riscos als quals està exposat, sota el criteri del principi de proporcionalitat.

La determinació de la categoria s'efectua en funció de la valoració de l'impacte que tindria un incident que afectés la seguretat de la informació o dels serveis amb perjudici per a les anomenades dimensions de la seguretat d'un actiu, que són les següents:

- a) La disponibilitat, que és la propietat o característica dels actius de permetre a les entitats o processos autoritzats de tenir-hi accés quan ho requereixen.
- b) L'autenticitat, que és la propietat o característica consistent en el fet que una entitat és qui diu que és o bé que garanteix la font de la qual procedeixen les dades.
- c) La integritat, que és la propietat o característica consistent en el fet que l'actiu d'informació no ha estat alterat de manera no autoritzada.
- d) La confidencialitat, que és la propietat o característica consistent en el fet que la informació ni es posa a disposició, ni es revela a individus, entitats o processos no autoritzats.
- e) La traçabilitat, és la propietat o característica d'identificar les actuacions realitzades de manera que permetin identificar l'estat d'un servei i/o producte i puguin ser imputades a l'entitat que les executi.

La valoració de les conseqüències d'un impacte negatiu sobre la seguretat de la informació i dels serveis l'ha d'efectuar el responsable de cada informació o servei, atenent la seva repercussió en la capacitat de l'Administració per a l'assoliment dels seus objectius, la protecció dels seus actius, el compliment de les seves obligacions de servei i el respecte de la legalitat i els drets dels ciutadans.

La categoria del sistema s'estableix en dues passes:

1. En primer lloc, es determina el nivell de seguretat d'un actiu per a cada dimensió de seguretat.
2. En segon lloc, es determina la categoria de seguretat del sistema d'informació.

Pel que fa a la **determinació del nivell de seguretat d'un actiu**, una informació o un servei es poden veure afectats en una o més de les dimensions de seguretat descrites anteriorment. Cada dimensió de seguretat afectada s'ha d'adscriure a un dels nivells següents: BAIX, MITJÀ o ALT.

a) Nivell BAIX: s'utilitza quan les conseqüències d'un incident de seguretat que afecti alguna de les dimensions de seguretat suposin un perjudici limitat sobre les funcions de l'organització, els seus actius o els individus afectats.

S'entén per perjudici limitat:

1r La reducció de manera apreciable de la capacitat de l'organització per atendre eficaçment les seves obligacions corrents, encara que aquestes se segueixin portant a terme.

2n El patiment d'un dany menor per part dels actius de l'organització.

3r L'incompliment formal d'alguna llei o regulació, que tingui un caràcter reparable.

4t Causar un perjudici menor a algun individu, que, tot i ser molest, pugui reparar-se fàcilment.

5è Altres de naturalesa anàloga.

Per exemple, es podria considerar que l'absència de disponibilitat d'un registre electrònic d'ús opcional genera un perjudici limitat, doncs les sol·licituds es poden tramitar a través del registre presencial.

b) Nivell MITJÀ: s'utilitza quan les conseqüències d'un incident de seguretat que afecti alguna de les dimensions de seguretat suposin un perjudici greu sobre les

funcions de l'organització, els seus actius o els individus afectats.

S'entén per perjudici greu:

1r La reducció significativa de la capacitat de l'organització per atendre eficaçment les seves obligacions fonamentals, encara que aquestes se segueixin portant a terme.

2n El patiment d'un dany significatiu per part dels actius de l'organització.

3r L'incompliment material d'alguna llei o regulació, o l'incompliment formal que no tingui un caràcter reparable.

4t Causar un perjudici significatiu a algun individu, de reparació difícil.

5è Altres de naturalesa anàloga.

Per exemple, es podria considerar que l'incident de seguretat mencionat anteriorment implicaria un perjudici greu quan, a més de reduir la disponibilitat del registre electrònic, afectés la informació i el funcionament d'un dels servidors (fent necessari, per exemple, reinstal·lar-ne el sistema operatiu) que empra l'entitat per emmagatzemar els documents rebuts, doncs suposa el patiment d'un dany significatiu per part dels actius de l'organització.

c) Nivell ALT: s'utilitza quan les conseqüències d'un incident de seguretat que afecti alguna de les dimensions de seguretat suposin un perjudici molt greu sobre les funcions de l'organització, els seus actius o els individus afectats.

S'entén per perjudici molt greu:

1r L'anul·lació de la capacitat de l'organització per atendre alguna de les seves obligacions fonamentals i que aquestes se segueixin portant a terme.

2n El patiment d'un dany molt greu, fins i tot irreparable, per part dels actius de l'organització.

3r L'incompliment greu d'alguna llei o regulació.

4t Causar un perjudici greu a algun individu, de reparació difícil o impossible.

5è Altres de naturalesa anàloga.

Per exemple, es podria considerar que l'esborrat total dels documents electrònics de les aplicacions administratives genera un perjudici molt greu.

Quan un sistema utilitzi informacions i presti serveis diferents, la categoria del sistema en cada dimensió ha de ser la més alta de les establertes per a cada informació i servei.

Pel que fa a la **determinació de la categoria de seguretat d'un sistema d'informació**, l'Esquema Nacional de Seguretat estableix tres categories:

a) Un sistema d'informació és de categoria ALTA si alguna de les seves dimensions de seguretat assoleix el nivell ALT.

b) Un sistema d'informació és de categoria MITJANA si alguna de les seves dimensions de seguretat assoleix el nivell MITJÀ i cap assoleix un nivell superior.

c) Un sistema d'informació és de categoria BÀSICA si alguna de les seves dimensions de seguretat assoleix el nivell BAIX i cap assoleix un nivell superior.

Com es pot veure, l'Esquema Nacional de Seguretat aposta per tractar la seguretat dels sistemes d'informació en funció del nivell de seguretat dels actius que componen o gestionen els esmentats sistemes.

L'aplicació dels controls de seguretat.

Un cop s'ha determinat la categoria de seguretat del sistema afectat (per exemple, la seu electrònica), cal procedir a seleccionar i a aplicar els controls de seguretat que resultin apropiats, d'entre els que preveu l'annex II del Reial decret 3/2010.

La selecció de les mesures de seguretat apropiades de les contingudes en l'annex II s'ha de fer d'acord amb les dimensions de seguretat i els seus nivells i, per a determinar les mesures de seguretat, d'acord amb la categoria del sistema.

Aquests controls s'agrupen en les següents categories:

a) Marc organitzatiu, constituït pel conjunt de mesures relacionades amb l'organització global de la seguretat. Consta de 4 controls.

b) Marc operacional, format per les mesures que s'han de prendre per protegir l'operació del sistema com a conjunt integral de components per a un fi. Consta de 36 controls.

c) Mesures de protecció, que se centren a protegir actius concrets, segons la seva naturalesa i la qualitat exigida pel nivell de seguretat de les dimensions afectades. Consta de 40 controls.

Per exemple, si considerem que el sistema de gestió documental tracta documents vitals per al manteniment del funcionament dels serveis públics essencials, hauríem establert que aquest sistema és de nivell alt, i per tant, en matèria de mecanismes d'autenticació aplicarem el control op.acc.5 en la configuració més segura, fet que implica la suspensió dels autenticadors després d'un període definit sense utilitzar-los, la prohibició de l'ús de claus concertades, l'exigència de l'ús de dispositius físics personalitzats o biometria o l'ús preferent de productes certificats.

L'auditoria de compliment de l'Esquema Nacional de Seguretat.

Una de les necessitats importants en relació amb la seguretat és el manteniment permanent, per a la qual cosa l'article 34 de l'Esquema Nacional de Seguretat estableix l'obligació de sotmetre els sistemes d'informació a una auditoria regular ordinària, almenys cada dos anys, que verifiqui el compliment dels requeriments corresponents per a la categoria del sistema, identificats d'acord amb la metodologia presentada anteriorment.

Aquesta auditoria, per tant, té la finalitat de determinar en quin grau es pot considerar que els controls de seguretat són efectius, aspecte clau per a una seguretat realment efectiva.

En sentit similar, amb caràcter extraordinari, s'ha de realitzar l'auditoria esmentada sempre que es produeixin modificacions substancials en el sistema d'informació, que puguin repercutir en les mesures de seguretat requerides.

L'informe d'auditoria, per a la realització del qual s'han d'utilitzar els criteris, mètodes de treball i conducta generalment reconeguts i la normalització nacional i internacional aplicables en aquest tipus d'auditories de sistemes d'informació, ha de dictaminar sobre el grau de compliment dels controls, identificar-ne les deficiències i suggerir les possibles mesures correctores o complementàries necessàries, així com les recomanacions que es considerin oportunes. Igualment, ha d'incloure els criteris metodològics d'auditoria utilitzats, l'abast i l'objectiu de l'auditoria i les dades, fets i observacions en què es basin les conclusions formulades.

Recomanacions **Recomanacions per a totes les Administracions públiques.**

Per complir suficientment amb l'Esquema Nacional de Seguretat, es poden realitzar les següents recomanacions:

1. Alinear la implantació de les mesures de seguretat previstes en l'Esquema Nacional de Seguretat amb l'estratègia de desplegament de l'administració electrònica, en relació amb els sistemes d'informació nous, que consideri també els sistemes antics que es vegin afectats pel procés de modernització.

2. Alinear les mesures de protecció previstes en l'Esquema Nacional de Seguretat amb les mesures de seguretat previstes al Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, ja que certament una gran part dels sistemes d'informació dintre de l'àmbit d'aplicació de l'Esquema Nacional de Seguretat també gestionen dades de caràcter personal.

En aquest sentit, resulta molt recomanable crear una única estructura documental que demostrï el compliment dels requisits de seguretat i que tracti de manera coherent i integrada ambdues reglamentacions.

3. Realitzar un pla director d'adequació dels sistemes existents, en especial els que ofereixen suport a les noves aplicacions d'administració electrònica, però que no es veuen afectats per polítiques de modernització, per complir amb el principi de tractament integral de la seguretat.

4. Redactar la política de seguretat de l'Administració i desplegar-la mitjançant un cos normatiu ben documentat, alineat amb les millors pràctiques identificades en les normatives internacionals, com per exemple la ISO 27000, i amb una orientació a la futura certificació del procés de seguretat de la informació.

Recomanacions per a les Administracions públiques locals de població reduïda.

En el cas d'aquestes Administracions, es poden realitzar les següents recomanacions addicionals:

1. Adherir-se a la política de seguretat de la Diputació provincial o del Consell comarcal al qual pertanyin, especialment en relació amb els serveis que els mateixos li ofereixin, com per exemple la seu electrònica o d'altres en l'àmbit de l'administració electrònica.

2. Adherir-se a les iniciatives en matèria de seguretat TIC endegades per la Generalitat de Catalunya (mitjançant el Consorci d'Administració Oberta Electrònica de Catalunya), la Diputació provincial o els Consells Comarcals per tal de garantir els nivells de seguretat de caràcter tècnic requerits per l'Esquema Nacional de Seguretat.

3. Potenciar l'ús de les infraestructures i els serveis comuns, que faciliten el compliment dels principis bàsics i els requisits mínims exigits.

Glossari de termes

Actiu. Component o funcionalitat d'un sistema d'informació susceptible de ser atacat de manera deliberada o accidental amb conseqüències per a l'organització. Inclou: informació, dades, serveis, aplicacions (programari), equips (maquinari), comunicacions, recursos administratius, recursos físics i recursos humans.

Anàlisi de riscos. Utilització sistemàtica de la informació disponible per identificar els perills i estimar els riscos.

Auditoria de la seguretat. Revisió i examen independents dels registres i activitats del sistema per verificar la idoneïtat dels controls del sistema, assegurar que es compleixen la política de seguretat i els procediments operatius establerts, detectar les infraccions de la seguretat i recomanar modificacions apropiades dels controls, la política i els procediments.

Autenticitat. Propietat o característica consistent en el fet que una entitat és qui diu que és o bé que garanteix la font de la qual procedeixen les dades.

Categoria d'un sistema. És un nivell, dins de l'escala bàsica-mitjana-alta, amb què s'adjectiva un sistema a fi de seleccionar les mesures de seguretat necessàries per a aquest. La categoria del sistema recull la visió holística del conjunt d'actius com un tot harmònic, orientat a la prestació d'uns serveis.

Confidencialitat. Propietat o característica consistent en el fet que la informació ni es posa a disposició ni es revela a individus, entitats o processos no autoritzats.

Disponibilitat. Propietat o característica dels actius consistent en el fet que les entitats o processos autoritzats hi tenen accés quan ho requereixen.

Signatura electrònica. Conjunt de dades en forma electrònica, consignades juntament a altres o associades amb aquestes, que es poden utilitzar com a mitjà d'identificació del signant.

Gestió d'incidents. Pla d'acció per atendre les incidències que es donin. A més de resoldre-les, ha d'incorporar mesures de desenvolupament que permetin conèixer la qualitat del sistema de protecció i detectar tendències abans que es converteixin en grans problemes.

Gestió de riscos. Activitats coordinades per dirigir i controlar una organització respecte als riscos.

Incident de seguretat. Esdeveniment inesperat o no desitjat amb conseqüències en detriment de la seguretat del sistema d'informació.

Integritat. Propietat o característica consistent en el fet que l'actiu d'informació no ha estat alterat de manera no autoritzada.

Mesures de seguretat. Conjunt de disposicions encaminades a protegir-se dels riscos possibles sobre el sistema d'informació, amb la finalitat d'assegurar-ne els objectius de seguretat. Es pot tractar de mesures de prevenció, de dissuasió, de protecció, de detecció i reacció, o de recuperació.

Política de signatura electrònica. Conjunt de normes de seguretat, d'organització, tècniques i legals per determinar com es generen, verifiquen i gestionen signatures electròniques, incloses les característiques exigibles als certificats de signatura.

Política de seguretat. Conjunt de directrius plasmades en un document escrit que regeixen la manera com una organització gestiona i protegeix la informació i els serveis que considera crítics.

Principis bàsics de seguretat. Fonaments que han de regir tota acció orientada a assegurar la informació i els serveis.

Procés. Conjunt organitzat d'activitats que es porten a terme per produir un producte o servei; té un principi i fi delimitats, implica recursos i dóna lloc a un resultat.

Procés de seguretat. Mètode que se segueix per assolir els objectius de seguretat de l'organització. El procés es dissenya per identificar, mesurar, gestionar i mantenir sota control els riscos a què s'enfronta el sistema en matèria de seguretat.

Requisits mínims de seguretat. Exigències necessàries per assegurar la informació i els serveis.

Risc. Estimació del grau d'exposició al fet que una amenaça es materialitzi sobre un o més actius i causi danys o perjudicis a l'organització.

Seguretat de les xarxes i de la informació. Capacitat de les xarxes o dels sistemes d'informació de resistir, amb un determinat nivell de confiança, els accidents o les accions il·lícites o malintencionades que comprometin la disponibilitat, autenticitat, integritat i confidencialitat de les dades emmagatzemades o transmeses i dels serveis que les xarxes i sistemes esmentats ofereixen o fan accessibles.

Serveis acreditats. Serveis prestats per un sistema amb autorització concedida per l'autoritat responsable per tractar un tipus d'informació determinada, en unes condicions precises de les dimensions de seguretat, d'acord amb el seu concepte d'operació.

Sistema de gestió de la seguretat de la informació (SGSI). Sistema de gestió que, basat en l'estudi dels riscos, s'estableix per crear, implementar, fer funcionar, supervisar, revisar, mantenir i millorar la seguretat de la informació. El sistema de gestió inclou l'estructura organitzativa, les polítiques, les activitats de planificació, les responsabilitats, les pràctiques, els procediments, els processos i els recursos.

Sistema d'informació. Conjunt organitzat de recursos perquè la informació es pugui recollir, emmagatzemar, processar o tractar, mantenir, utilitzar, compartir, distribuir, posar a disposició, presentar o transmetre.

Traçabilitat. Propietat o característica consistent en el fet que les actuacions d'una entitat poden ser imputades exclusivament a aquesta entitat.

Vulnerabilitat. Una debilitat que pot ser aprofitada per una amenaça.

Referències i enllaços web

A la web s'hi pot trobar informació rellevant, relacionada amb la matèria desenvolupada en aquesta guia:

Centre de Seguretat de la Informació de Catalunya (CESICAT).

<http://www.cesicat.cat>

Centro Criptológico Nacional del Centro Nacional de Inteligencia (CCN-CERT).

<http://www.ccn-cert.cni.es>

Normativa:

Llei 11/2007 d'accés electrònic dels ciutadans als Serveis Públics

Esquema Nacional de Seguretat

Eines

Eines d'anàlisi de riscos.

El "Centro Criptológico Nacional" ofereix a les Administracions l'eina PILAR d'anàlisi i gestió de riscos d'un sistema d'informació, d'acord amb la metodologia MAGERIT.

Recursos de suport en línia

De moment, no existeixen recursos en línia significatius de suport a l'Esquema Nacional de Seguretat més enllà de la informació recollida als enllaços dels apartats 8 i 9.



Centre de Seguretat de la
Informació de Catalunya

www.cesicat.cat