CESICAT

GUIA LEGAL DE SEGURETAT:
Esquema Nacional de Seguretat
Seu electrònica

Índex

Presentació

El Centre de Seguretat de la Informació de Catalunya (en endavant, 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 del Pla nacional d'impuls de la seguretat TIC a Catalunya és garantir una Societat de la Informació Segura Catalana per a tots, operant un Centre de Seguretat de la Informació de Catalunya, com a eina per a la generació d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui un referent nacional i internacional.
El Pla nacional d'impuls de la seguretat TIC a Catalunya s'estructura al voltant de quatre objectius estratègics principals:

- Execució de l'estratègia nacional de seguretat TIC establerta pel Govern de la Generalitat de Catalunya.
- Suport a la protecció de les infraestructures crítiques TIC nacionals.
- Promoció d'un teixit empresarial català sòlid en seguretat TIC.
- Increment de la confiança i protecció de la ciutadania catalana en la societat de la informació.

Dintre d'aquests objectius estratègics es constitueix la Fundació Pública "Centre de Seguretat de la Informació de Catalunya" com a entitat auxiliar i instrumental del govern de la Generalitat de Catalunya i dels ens que la componen.

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, el CESICAT ofereix com a servei preventiu l'elaboració d'un conjunt de guies de seguretat adreçades a les diferents comunitats. En particular, la temàtica de la present guia és l'establiment d'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 en l'àmbit de Catalunya a la millor implantació de les mesures de seguretat establertes a l'ENS. Aquesta guia constitueix la primera actuació del CESICAT i es complementa amb d'altres per facilitar el compliment d'aquesta norma i la millora dels nivells de seguretat en l'àmbit de les Administracions públiques de Catalunya.

Introducció

Audiència

Aquesta guia està adreçada als responsables jurídics de les Administracions públiques locals 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 estatal 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics (en endavant, la LAECSP) i el seu Reial decret de desplegament, 3/2010, de 8 de gener (en endavant, el RDENS), en relació amb les seus electròniques que han de tenir totes les Administracions públiques territorials i els organismes i entitats de dret públic que en depenen.

Així mateix, es consideren els requisits i les funcions addicionals de la seu electrònica establerts per la Llei catalana 26/2010, del 3 d'agost, de règim jurídic i de procediment de les Administracions públiques de Catalunya (en endavant, la LRJPCAT) i la Llei catalana 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya (en endavant, la LUMESPC).

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?

Com indica l'exposició de motius de la LAECSP, el reconeixement del dret dels ciutadans a comunicar-se per mitjans electrònics amb l'Administració planteja, en primer lloc, la necessitat de definir clarament la "seu" administrativa electrònica amb què s'estableixen les relacions, i la promoció del seu règim d'identificació, autenticació, contingut mínim, protecció jurídica, accessibilitat, disponibilitat i responsabilitat.

La **seu electrònica** és, d'acord amb l'article 10.1 de la LAECSP, l'adreça electrònica disponible per als ciutadans a través de xarxes de telecomunicacions la titularitat, gestió i administració de la qual correspon a una Administració pública, òrgan o entitat administrativa en l'exercici de les seves competències.

Per **adreça electrònica** cal entendre l'identificador d'un equip o sistema electrònic des d'on es proveeix d'informació o serveis en una xarxa de comunicacions (definició i) de l'annex de la LAECSP). Així, la seu electrònica es configura com un tipus de sistema electrònic que l'Administració utilitza per actuar a la xarxa, i principalment, en forma de servidor web accessible des d'Internet. Generalment, l'adreça es farà correspondre amb un espai web, com per exemple www.cesicat.cat (o una part determinada d'aquest, p. ex., seuelectronica.cesicat.cat).

Resulta necessari fer palès que la seu electrònica es troba disponible per als ciutadans, ja que no existeix el requisit legal d'establir una seu electrònica per a les relacions interadministratives. En aquest sentit, el legislador

ha considerat que les administracions s'han de comunicar mitjançant xarxes privades de comunicacions electròniques (articles 20 i 43 de la LAECSP), el que de fet es constitueix com a mesura addicional de seguretat.

Així mateix, no és una seu electrònica l'adreça electrònica web d'una entitat diferent d'una Administració pública, un òrgan o una entitat administrativa en l'exercici de les seves competències, és a dir, que les pàgines web de les entitats públiques empresarials o de les societats mercantils públiques no tenen la consideració legal de seu electrònica.

En tot cas, la seu electrònica ha de **garantir la identificació del titular** de la seu, així com els mitjans disponibles per a la formulació de suggeriments i queixes, i disposar de sistemes que permetin l'establiment de **comunicacions segures** sempre que siguin necessàries. La seu electrònica és, per tant, una adreça electrònica segura i fiable.

Finalitat

La seu electrònica té per **finalitat essencial** ésser l'espai electrònic de relació entre els ciutadans i l'Administració pública, un espai legalment caracteritzat per la responsabilitat del titular respecte de la integritat, veracitat i actualització de la informació i els serveis a què es pugui accedir a través d'aquesta (article 10.2 de la LAECSP); és a dir, és un lloc vàlid i segur per a l'activitat administrativa i de relació amb la ciutadania.

En aquest sentit, la creació de les seus electròniques es realitza amb subjecció als principis de publicitat oficial, responsabilitat, qualitat, seguretat, disponibilitat, accessibilitat, neutralitat i interoperabilitat (article 10.3 de la LAECSP).

Cal recordar que els **principis de responsabilitat i qualitat** diferencien el règim legal de la seu electrònica de les Administracions públiques d'altres règims aplicables a la resta de pàgines web. Aquestes queden subjectes, en particular, a la legislació de serveis de la societat de la informació i del comerç electrònic, que estableix un règim d'exoneració de responsabilitat en alguns casos. En el cas de les seus electròniques de les Administracions públiques, la responsabilitat dels continguts és plena i objectiva, sense que resulti acceptable l'establiment d'un règim d'exoneració de responsabilitat per a l'Administració. Aquest fet es deriva de l'aplicació del principi de legalitat pel que fa al manteniment de la integritat de les garanties jurídiques dels ciutadans davant les Administracions públiques establertes a la Llei 30/1992, de règim jurídic de les administracions públiques i del procediment administratiu comú.

En virtut del **principi de seguretat (i de proporcionalitat)**, la seu electrònica exigeix almenys el mateix nivell de garanties i seguretat que es requereix per a la utilització de mitjans no electrònics en l'activitat administrativa, però també les garanties i mesures de seguretat adequades a la naturalesa i les circumstàncies dels diferents tràmits i actuacions. En aquest sentit, l'Esquema Nacional de Seguretat ("ENS") estableix el conjunt de mesures tècniques mínimes que cal aplicar, segons la categorització de la seu electrònica.

Al seu torn, el **principi de disponibilitat** crida a la possibilitat efectiva de l'accés per part dels ciutadans a la seu electrònica que, tot i no haver d'estar legalment operativa tots els dies de l'any (excepte en cas de contenir un registre electrònic), és la condició bàsica i essencial del dret d'accés electrònic, per la qual cosa és imprescindible vetllar perquè es compleixi.

El **principi d'accessibilitat** indica que l'accés a la informació i als serveis per mitjans electrònics s'ha de realitzar a través de sistemes que permetin obtenir-los de manera segura i comprensible, i garantir especialment l'accessibilitat universal i el disseny per a tots els suports, canals i entorns. La finalitat d'aquest principi és permetre que totes les persones puguin exercir els seus drets en igualtat de condicions, incorporant les característiques necessàries per garantir l'accessibilitat d'aquells col·lectius que ho requereixin.

En virtut del **principi de neutralitat** i adaptabilitat al progrés de les tècniques i sistemes de comunicacions electròniques, la seu electrònica ha de permetre garantir la independència en l'elecció de les alternatives tecnològiques per part dels ciutadans i les Administracions públiques, així com la llibertat de desenvolupar i implantar els avenços tecnològics en un àmbit de lliure mercat. A aquests efectes, i arran de l'aprovació de l'Esquema Nacional d'Interoperabilitat, les Administracions públiques han d'utilitzar estàndards oberts així com, si s'escau i de forma complementària, estàndards que siguin d'ús generalitzat per part dels ciutadans.

Finalment, el principi d'interoperabilitat es manifesta en la cooperació en la utilització de mitjans electrònics per part de les Administracions públiques, especialment en el reconeixement mutu dels documents electrònics i dels mitjans d'identificació i autenticació que s'ajustin al que disposa la LAECSP.

Les **funcions principals** de la seu electrònica són les següents:

- Ésser l'espai virtual en el qual es produeix la relació electrònica entre els ciutadans i les Administracions públiques, tant en relació amb el procediment administratiu com en altres respectes, com la participació electrònica.

- Servir de punt d'accés electrònic, fins i tot d'accés electrònic general, a tots els tràmits d'una mateixa Administració pública, o de diverses Administracions públiques (article 8.2.b de la LAECSP).

- Donar accés a informacions administratives i, si es considera oportú, no administratives, així com als serveis i les transaccions electròniques (article 10.5 de la LAECSP). En concret, resulta obligatori publicar de manera segura determinades informacions necessàries per a la relació electrònica procedimental:

  - La relació de sistemes de signatura electrònica avançada admesos (article 15.2 de la LAECSP).

- La relació de segells electrònics d'actuació administrativa automatitzada (article 18.3. de la LAECSP).

- Les disposicions de creació de registres electrònics accessibles des de la seu electrònica (article 25.1 de la LAECSP).

- La relació actualitzada dels documents electrònics normalitzats corresponents als serveis, procediments i tràmits que s'especifiquin d'acord amb el que disposa la norma de creació del registre, formalitzats d'acord amb formats preestablerts (articles 25.2 i 35.1 de la LAECSP).

- La data i hora oficial de la seu electrònica d'accés al registre electrònic, íntegra i visible (article 26.1 de la LAECSP).

- Els mitjans electrònics que els ciutadans poden utilitzar en cada cas en l'exercici del seu dret a comunicar-se amb l'Administració pública (article 27.4 de la LAECSP).

- Les instruccions i circulars i les ordres de servei dels òrgans administratius, si una disposició específica ho estableix o s'estima convenient per raó dels destinataris o dels efectes que es puguin produir (article 7.2 de la LRJPCAT).

- La delegació de competències i l'extinció, per revocació o per qualsevol altra causa, si s'escau (article 8.6 de la LRJPCAT).

- Els convenis subscrits amb altres Administracions públiques a l'efecte del registre de sol·licituds, escrits i comunicacions (article 25.3 de la LRJPCAT).

- La interrupció del servei de registre electrònic, amb indicació del sistema alternatiu de registre que es pot utilitzar mentre duri la interrupció (article 41.9 de la LRJPCAT).

- Els tràmits d'informació pública, llevat que el procediment específic determini una altra cosa (article 52.2 de la LRJPCAT).

- Les convocatòries successives d'un procediment selectiu o de concurrència competitiva de qualsevol tipus (article 58.4.c de la LRJPCAT).

- Les publicacions dels projectes de disposicions reglamentàries (article 67.5 de la LRJPCAT).

- L'organització, de manera que es permeti als ciutadans conèixer l'organització administrativa, les competències de les entitats que integren el sector públic, les autoritats, el personal directiu i el personal a llur servei responsables de la tramitació dels procediments administratius i de la prestació dels serveis públics, i la relació actualitzada dels llocs de treball, de llurs funcions i les taules retributives corresponents (article 10.1.a, en relació amb l'article 11.1 de la LUMESPC).

- Els procediments que són d'interès per als ciutadans i, en particular, els que fan referència als requisits jurídics i tècnics que estableix l'ordenament jurídic per als projectes, les actuacions o les sol·licituds; els procediments administratius que tramiten, tot precisant-ne els terminis i el sentit del silenci; el perfil de contractant; les convocatòries i les resolucions d'ajuts i subvencions; l'accés i la selecció del personal, i el Catàleg de dades i documents interoperables que són en poder de les Administracions públiques (article 10.1.b, en relació amb l'article 11.1 de la LUMESPC).

- L'activitat, incloent-hi les actuacions que porten a terme les entitats que conformen el sector públic i, en particular, la informació relativa als serveis públics prestats, les prestacions previstes, llur disponibilitat i les cartes de serveis, i també la informació relativa als acords que prenen les entitats del sector públic, d'acord amb el que estableix llur normativa reguladora (article 10.1.c, en relació amb l'article 11.1 de la LUMESPC).

- Les entitats locals han de publicar a la seva seu electrònica les actes de les sessions del ple, tenint en compte els principis i les garanties que estableix la normativa de protecció de dades i la de protecció del dret a l'honor i a la intimitat (article 10.2 de la LUMESPC).

- Els drets i les obligacions que estableixen la LUMESPC i la LAECSP, i la previsió per fer efectius els drets i les obligacions esmentats en el marc de llurs serveis i prestacions (disposició addicional quarta de la LUMESPC).

- Donar accés al registre electrònic d'entrada i sortida de documents (articles 24 a 26 de la LAECSP).

- Permetre la publicació dels butlletins oficials (article 11 de la LAECSP).

- Permetre la publicació dels actes i comunicacions del tauler d'anuncis o edictes (article 12 de la LAECSP i article 58.4 de la Llei catalana 26/2010).

- Permetre la comprovació de la integritat dels documents produïts amb codi segur de verificació (article 18.1.b de la LAECSP) i de les còpies autèntiques electròniques imprimibles (article 30.5 de la LAECSP).

- Donar accés a l'estat dels expedients en els quals el ciutadà té la consideració d'interessat (article 37 de la LAECSP i article 13.1.a de la LUMESPC).

- Donar accés als expedients de procediments subjectes a informació pública a tot el personal, llevat de les dades excloses del dret d'accés (article 52.3 de la LRJPCAT).

Oferir als ciutadans un espai personalitzat per a les següents funcions (article 13.1 de la LUMESPC):

- Accedir a l'estat de les relacions i els tràmits que porten a terme electrònicament amb l'Administració corresponent.

- Accedir a la documentació annexada als tràmits i les gestions fets electrònicament.

- Rebre el document acreditatiu de la resolució del procediment iniciat electrònicament.

- Accedir a les notificacions i les comunicacions que els tramet l'Administració.

- Accedir a llur perfil i modificar-lo, si s'escau.

- Posar a disposició del sector públic la informació necessària per resoldre llurs procediments administratius.

- Donar accés als serveis electrònics que presta el sector públic de Catalunya adreçats a les empreses, entenent com a tals les entitats que exerceixen una activitat econòmica, independentment de la seva forma jurídica (article 16 de la LUMESPC).

- Donar accés al Catàleg de dades i documents interoperables de Catalunya (article 21.3 de la LUMESPC).

Totes aquestes funcions requereixen d'unes importants mesures de seguretat, que s'enumeren a la LAECSP i es desenvolupen al Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica, que resulta plenament aplicable a la seu electrònica (article 38 del RDENS).

Així mateix, l'article 32 del RDENS determina requisits per a les notificacions i publicacions electròniques, que resulten aplicables plenament a la seu electrònica quan s'utilitza per realitzar notificacions per compareixença electrònica (article 28.5 de la LAECSP) o publicació d'informacions, per exemple en el tauler d'anuncis electrònic (article 12 de la LAECSP).

Les funcions anteriorment indicades són suportades mitjançant un sistema d'informació de seu electrònica, que és responsable del manteniment de les garanties legals de seguretat, fet que obliga a determinar-ne la categoria de seguretat, d'acord amb l'annex 1 del Reial decret 3/2010, atenent als actius del sistema i de les dimensions de seguretat aplicables als mateixos.

El resultat de la categorització serà diferent en funció del model d'organització de la seu electrònica i de la seva relació amb la resta de serveis d'administració electrònica: per exemple, no rebrà la mateixa valoració un model de seu electrònica única que un model de múltiples seus electròniques, ja que els riscos són diferents en ambdós casos.

Casos d'estudi

La identificació de l'Administració, organisme o entitat de dret públic

Una de les funcions essencials de la seu electrònica és precisament la identificació de l'Administració, organisme o entitat de dret públic. Així ho indica l'article 10.3 de la LAECSP, quan imposa l'obligació de garantir la identitat de l'Administració, organisme o entitat de dret públic titular de la seu electrònica. Sense aquesta garantia es podria donar el cas d'una suplantació de la pròpia Administració pública, de manera que un atacant podria establir relacions amb ciutadans i cometre fraus importants.

De fet, es pot dir que la necessitat de garantir la identitat de l'Administració pública, organisme o entitat de dret públic titular de la seu és possiblement el requisit més important de seguretat de la seu electrònica, i s'ha de valorar des de la perspectiva de la dimensió de l'autenticitat, és a dir, 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.

Tot i que la llei és neutral des de la perspectiva tecnològica, és a dir, tracta de no referir-se a tecnologies concretes, en la majoria de casos el canal electrònic més habitual és Internet i, per tant, el sistema d'informació que dóna suport a la seu electrònica consisteix en un o més servidors web que utilitzen, principalment, el protocol HTTP per a les comunicacions amb els ciutadans.

1.1.1 La identitat web de l'Administració pública

L'article 13.3.a de la LAECSP autoritza a l'Administració pública, organisme o entitat de dret públic a utilitzar sistemes de signatura electrònica basats en certificats de dispositiu segur o un mitjà equivalent que permeti identificar la seu electrònica i establir-hi comunicacions segures, mentre que l'article 17 de la LAECSP estableix de forma obligatòria que les seus electròniques han d'utilitzar, per identificar-se i garantir una comunicació segura, sistemes de signatura electrònica basats en certificats de dispositiu segur o un mitjà equivalent.

Amb l'ús d'aquests certificats, el servidor web passa a fer servir el protocol HTTPS o, més correctament, el protocol SSL/TLS sobre HTTP, que -sempre que estigui ben configurat- aporta un nivell de seguretat que permet la identificació del titular del servidor web que es correspon amb la seu electrònica.

Per tant, el requisit de la identificació de l'Administració pública, organisme o entitat de dret públic es compleix emprant un certificat digital, que es podrà basar en un dispositiu segur o en un mitjà equivalent a un dispositiu segur, fet que ens marca l'existència de tres nivells de seguretat:

- Nivell alt, determinat per la utilització de certificats basats en dispositius segurs.

- Nivell mitjà, determinat per la utilització de certificats basats en certificats reconeguts o dispositius segurs, preferentment (recomanable en tot cas emprar ambdós o en el seu defecte com a mínim la utilització de certificats basats en certificats reconeguts).

- Nivell baix, determinat per la utilització de certificats que no es basin ni en dispositius segurs ni en un mitjà equivalent i que, de fet, no es podrien fer servir per a la seu electrònica, però sí per a d'altres funcions, com per exemple l'assegurament de les comunicacions entre components purament tècnics, en un entorn tancat de comunicacions electròniques (com succeeix amb l'autenticació electrònica de serveis web remots).

El dubte que es planteja immediatament és la determinació dels casos en què cal fer servir un certificat de seu electrònica de nivell alt o de nivell mitjà ja que, de fet, semblen intercanviables legalment.

Una via per resoldre aquest dubte és precisament aplicar la categorització de sistemes d'informació del RDENS al sistema d'informació que suporta la seu electrònica, des de la perspectiva de la dimensió de seguretat de l'autenticitat, a la qual ens hem referit anteriorment.

Un sistema d'informació de seu electrònica serà de **nivell baix** quant a la **dimensió de seguretat d'autenticitat** si es produeix un perjudici limitat en cas de suplantació de la identitat de la seu electrònica. Per exemple, una seu electrònica d'una Administració pública que només ofereix informació i que no dóna accés al registre electrònic, de manera que no resulta possible fer cap tràmit -sempre que aquesta circumstància sigui coneguda per la ciutadania-, es podria qualificar fàcilment de nivell baix quant a la dimensió d'autenticitat, tot i que, en general, no oferir cap garantia d'autenticació seria, en si mateix, una infracció de la reglamentació.

En segon lloc, un sistema d'informació de seu electrònica serà de **nivell mitjà** quant a la **dimensió de seguretat d'autenticitat** si es produeix un perjudici greu en cas de suplantació de la identitat de la seu electrònica. Per exemple, una seu electrònica d'una Administració amb informacions administratives i tràmits serà, en general, qualificada com a nivell mitjà en la dimensió d'autenticitat.

Finalment, un sistema d'informació de seu electrònica serà de **nivell alt** quant a la **dimensió de seguretat d'autenticitat** si es produeix un perjudici molt greu en cas de suplantació de la identitat de la seu electrònica. Per exemple, una seu electrònica d'accés a un sistema amb molts tràmits electrònics obligatoris i amb informació sensible possiblement seria qualificada de nivell alt en la dimensió d'autenticitat, ja que l'impacte d'una suplantació d'identitat seria molt important i els danys causats podrien ser impossibles de reparar.

En atenció a aquesta anàlisi, es pot indicar, en general, la necessitat de fer servir certificats de seu electrònica de nivell mitjà per a les seus electròniques categoritzades en la dimensió d'autenticitat com a nivell baix o mitjà, i certificats de seu electrònica de nivell alt per a les seus electròniques categoritzades en la dimensió d'autenticitat com a nivell alt.

1.1.2 Certificats de servidor segur i certificats de seu electrònica

Respecte al tipus de certificat, cal dir que no es pot considerar suficient en tots els casos el fer servir un certificat qualsevol que suporti el protocol de comunicació HTTPS, ja que, en no existir normativa homogènia en relació amb la identificació del titular del domini web que se certifica, resultaria possible obtenir un certificat de servidor segur sense garantia real.

Tot i que els certificats de servidor segur emesos per prestadors com l'Agència Catalana de Certificació no pateixen aquesta problemàtica, els ciutadans no sempre estan conscienciats respecte de quina és l'entitat que ha emès el certificat, de manera que la indústria ha creat polítiques més estrictes d'emissió de certificats, amb una garantia més forta d'identitat. Aquestes polítiques són els certificats SSL EV, acrònim que indica que hi ha una "validació ampliada" de les dades d'identitat i que estableixen un protocol d'identificació estricte que necessàriament haurà d'acomplir qualsevol entitat sol·licitant del certificat abans que li sigui atorgat.

Addicionalment a aquests estàndards, que resulten aplicables a qualsevol organització, i dintre de l'Esquema Nacional d'Interoperabilitat, s'ha definit un tipus especial de certificat, precisament per garantir la identificació dels titulars de les seus electròniques, que seria el tipus que es recomana emprar.

L'Agència Catalana de Certificació emet certificats de servidor segur i també certificats de seu electrònica, en aquest cas, de nivell mitjà, en suport programari, i de nivell alt, en suport maquinari segur.1

Un dels reptes que cal considerar és el fet que els sistemes dels ciutadans no sempre incorporen directament els certificats arrel dels prestadors de serveis de certificació,

1- Serà necessari que l'Administració sol·licitant avalui els certificats disponibles en relació amb les seves necessitats, podent referir-se així mateix als criteris establerts pel Ministeri de Presidència en el document "Esquema de identificación y firma electrónica de las Administraciones públicas".

fet que genera falsos avisos de problemes de seguretat. Tot i que els prestadors de serveis de certificació treballen constantment perquè els seus certificats arrel siguin incorporats als sistemes més utilitzats, és recomanable que l'Administració pública estableixi procediments fora de línia per tal d'informar els ciutadans del prestador que emet els certificats i del lloc web on poden obtenir i instal·lar manualment els certificats arrel i incrementar així la seguretat global del sistema.

L'establiment de comunicacions segures

La seu electrònica, com hem indicat anteriorment, és l'espai de relació electrònica amb els ciutadans i, en aquest sentit, l'article 10 de la LAECSP exigeix que la seu electrònica disposi de sistemes que permetin l'establiment de comunicacions segures sempre que siguin necessàries, el que necessàriament ha de considerar els elements següents:

- La identificació dels ciutadans en l'accés a la seu electrònica, quan s'escaigui.
- La confidencialitat de les comunicacions establertes.
- La integritat de les comunicacions portades a terme.

1.1.3 La identificació dels ciutadans en l'accés electrònic a la seu electrònica

La seu electrònica ha de considerar la necessitat d'identificar els ciutadans que hi accedeixen, sempre que resulti necessari per a una finalitat legítima i concreta, com per exemple a efectes de donar-los accés a informació personalitzada, a la carpeta de tràmits, o per poder presentar sol·licituds electrònicament.

D'acord amb l'article 13.2 de la LAECSP, els ciutadans poden utilitzar els sistemes següents de signatura electrònica per relacionar-se amb les Administracions públiques, d'acord amb el que cada Administració determini:

a) En tot cas, els sistemes de signatura electrònica incorporats al document nacional d'identitat, per a persones físiques.

b) Sistemes de signatura electrònica avançada, inclosos els basats en un certificat electrònic reconegut, admesos per les Administracions públiques.

c) Altres sistemes de signatura electrònica, com la utilització de claus concertades en un registre previ com a usuari, l'aportació d'informació coneguda per les dues parts o altres sistemes no criptogràfics, en els termes i les condicions que es determinin en cada cas.

En relació amb la identificació dels ciutadans en l'accés a la seu electrònica, el que caldrà avaluar per tal de categoritzar el sistema és l'aplicació a la qual accedeix el ciutadà, de manera que si, per exemple, accedeix al registre electrònic, l'avaluació de les necessitats de seguretat es farà en relació amb el sistema d'informació del registre electrònic.

Pel que fa a la pròpia seu, considerada com el lloc d'accés a la resta d'aplicacions d'administració electrònica, cal tenir en compte que només s'ha d'exigir la identificació en els casos estrictament necessaris, en aplicació dels principis de protecció de dades de caràcter personal, de seguretat i de proporcionalitat. Així, no resulta acceptable

enregistrar dades personals de navegació o altres dades dels ciutadans sense cap motiu legítim i específic, excepte si aquestes dades es troben dissociades de la identitat dels ciutadans i s'utilitzen per a finalitats legítimes, com per exemple l'avaluació de la usabilitat de la seu electrònica.

Des d'aquesta perspectiva, podem considerar que la categorització de seguretat de la seu electrònica en relació amb la identificació dels ciutadans s'ha de realitzar a partir de la categorització prèvia dels sistemes d'informació als quals dóna accés la seu electrònica, i només en el cas que l'autenticació es delegui a la seu electrònica.

Si apliquem els criteris de categorització del RDENS en relació amb la dimensió d'autenticitat referida a la identificació dels ciutadans en l'accés a la seu electrònica, i amb una especial atenció a la protecció de les dades de caràcter personal, podem fer les indicacions següents:

- Un sistema d'informació de seu electrònica serà de **nivell baix** quant a la **dimensió de seguretat d'autenticitat** si es produeix un perjudici limitat en cas de suplantació de la identitat dels ciutadans. Per exemple, la suplantació de la identitat d'un ciutadà li podria representar un perjudici menor únicament si el mecanisme d'identitat utilitzat es pot fer servir per a actuacions que no tinguin conseqüències jurídiques. Així, si el ciutadà disposa d'un mecanisme d'autenticació per accedir a informació no personal o a informació personal de molt baixa sensibilitat (per exemple, un espai on s'accedeixi exclusivament a material merament informatiu), es podria considerar la categorització del sistema com a nivell baix.

- En segon lloc, un sistema d'informació de seu electrònica serà de **nivell mitjà** quant a la **dimensió de seguretat d'autenticitat** si es produeix un perjudici greu en cas de suplantació de la identitat dels ciutadans. Per exemple, una seu electrònica d'una Administració que permeti l'accés a informacions de caràcter personal o exercir el dret a la presentació de sol·licituds, recursos administratius o altres documents amb efectes legals serà, en general, qualificada com a nivell mitjà en la dimensió d'autenticitat, ja que la divulgació per part de l'Administració de dades personals a una persona no autoritzada pot suposar l'incompliment material de la legislació de protecció de dades de caràcter personal, a més de produir-li perjudicis greus al ciutadà. Així mateix, la realització de tràmits administratius fraudulentament pot produir molt fàcilment un perjudici significatiu al ciutadà, especialment si parlem d'una sol·licitud amb notificació electrònica, cas en el qual el suplantador podria realment substituir al ciutadà, que haurà d'actuar davant de l'Administració per impugnar el procediment administratiu, amb la dificultat que comporta.

- Finalment, un sistema d'informació de seu electrònica serà de **nivell alt** quant a la **dimensió de seguretat d'autenticitat** si es produeix un perjudici molt greu en cas de suplantació de la identitat dels ciutadans. Per exemple, una seu electrònica d'accés a un sistema amb informacions personals especialment sensibles, com per exemple dades de salut, possiblement seria qualificada de nivell alt en la dimensió d'autenticitat, ja que l'impacte d'una suplantació d'identitat implicaria la infracció amb caràcter greu de la legislació de protecció de dades personals, a banda de causar un perjudici greu i de difícil o impossible reparació

al ciutadà, ja que un cop produïda la divulgació no autoritzada de dades personals ja no es pot reparar el dany.

En atenció a aquesta anàlisi, es pot indicar, en general, la necessitat de fer servir sistemes d'identitat digital o signatura electrònica de ciutadà per a l'accés autenticat a les seus electròniques, emprant qualsevol sistema de signatura electrònica legalment previst per a l'accés a la seu electrònica de nivell baix, certificats reconeguts per a l'accés a la seu electrònica de nivell mig i dispositius segurs certificats per a l'accés a la seu electrònica de nivell alt.

1.1.4 La confidencialitat de les comunicacions establertes

La seu electrònica també ha de permetre garantir la confidencialitat de les comunicacions establertes, especialment en aplicació del principi del secret de les comunicacions i la protecció de dades de caràcter personal, ja que els ciutadans remeten les seves informacions a l'Administració mitjançant els mecanismes de comunicació de la seu electrònica.

L'article 17 de la LAECSP indica que les seus electròniques han d'utilitzar, per identificar-se i garantir una comunicació segura, sistemes de signatura electrònica basats en certificats de dispositiu segur o mitjà equivalent. Com hem vist anteriorment, això implica l'ús de protocols SSL/TLS (o d'altres de similars i equivalents) per a les comunicacions mantingudes mitjançant la seu.

Com en el cas de la identitat de la seu electrònica, cal determinar el tipus del certificat que cal emprar per garantir la confidencialitat de les informacions intercanviades entre els ciutadans i l'Administració.

Si apliquem els criteris de categorització del RDENS en relació amb la dimensió de confidencialitat referida a la identificació dels ciutadans en l'accés a la seu electrònica, i amb una especial atenció a la protecció de les dades de caràcter personal, podem fer les indicacions següents:

- Un sistema d'informació de seu electrònica serà de **nivell baix** quant a la dimensió de **seguretat de confidencialitat** si es produeix un perjudici limitat en cas de divulgació no consentida d'informació dels ciutadans. Per exemple, en cas que les informacions que es remeten no siguin particularment sensibles, com el nom i cognoms, però sense el NIF o dades com un número de targeta de pagament, es podria qualificar la seu electrònica con a nivell baix.

- En segon lloc, un sistema d'informació de seu electrònica serà de **nivell mitjà** quant a la **dimensió de seguretat de confidencialitat** si es produeix un perjudici greu en cas de divulgació no consentida d'informació dels ciutadans. Per exemple, una seu electrònica d'una Administració que permeti l'accés a informacions de caràcter personal o exercir el dret a la presentació de sol·licituds, recursos administratius o altres documents amb efectes legals serà, en general, qualificada com a nivell mitjà en la dimensió de confidencialitat. La divulgació per part de l'Administració de dades personals a una persona no autoritzada —un tercer que intercepta les comunicacions de la seu electrònica— pot suposar l'incompliment material de la legislació

de protecció de dades de caràcter personal, en tot cas. El robatori de dades personals sensibles, com el número de la targeta de pagament, pot produir molt fàcilment un perjudici significatiu al ciutadà, en forma de possibles fraus de tercers o de venda d'informació personal a tercers, generalment en un context d'activitat criminal.

- Finalment, un sistema d'informació de seu electrònica serà de **nivell alt** quant a la **dimensió de seguretat de confidencialitat** si es produeix un perjudici molt greu en cas de divulgació no consentida d'informació dels ciutadans. Per exemple, una seu electrònica d'accés a un sistema amb informacions personals especialment sensibles, com per exemple dades de salut, possiblement seria qualificada de nivell alt en la dimensió de confidencialitat. L'impacte d'una intercepció de les comunicacions implicaria la infracció amb caràcter greu de la legislació de dades personals, a banda de causar un perjudici greu i d'impossible reparació al ciutadà, ja que un cop produïda la divulgació no autoritzada de dades personals ja no es pot reparar el dany.

En atenció a aquesta anàlisi, es pot indicar, en general, la necessitat de fer servir certificats de seu electrònica de nivell mitjà per a les seus electròniques categoritzades en la dimensió de confidencialitat com a nivell baix o mitjà i certificats de seu electrònica de nivell alt per a les seus electròniques categoritzades en la dimensió de confidencialitat com a nivell alt.

La publicació electrònica segura de continguts

La seu electrònica és el lloc on es publiquen les informacions administratives, els butlletins oficials i el tauler d'anuncis, amb subjecció als principis de responsabilitat i seguretat, fet que exigeix mantenir-ne la integritat i autenticitat. Si apliquem els criteris de categorització del RDENS en relació amb la dimensió d'integritat referida a les informacions publicades a la seu electrònica, podem fer les indicacions següents:

- Un sistema d'informació de seu electrònica serà de **nivell baix** quant a la **dimensió de seguretat d'integritat** si es produeix un perjudici limitat en cas de modificació fraudulenta de la informació de la seu electrònica. Per exemple, en cas d'informacions administratives de caire general, de matèries no cobertes per la publicitat oficial i, en especial, d'informacions no administratives, es podria qualificar la seu electrònica com a nivell baix.

- En segon lloc, un sistema d'informació de seu electrònica serà de **nivell mitjà** quant a la **dimensió de seguretat d'integritat** si es produeix un perjudici greu en cas de modificació fraudulenta de la informació de la seu electrònica. Per exemple, una seu electrònica d'una Administració que publiqui informacions administratives subjectes a publicitat oficial a la seu o informacions referides al procediment administratiu serà qualificada, en general, com a nivell mitjà en la dimensió d'integritat, ja que la modificació o l'esborrament no autoritzats de la publicació suposa l'incompliment material de la legislació administrativa. En particular, les informacions publicades al tauler d'anuncis o al perfil del contractant de l'Administració s'haurien de considerar de nivell mitjà quant a la dimensió d'integritat.

Finalment, un sistema d'informació de seu electrònica serà **nivell alt** quant a la **dimensió de seguretat d'integritat** si es produeix un perjudici molt greu en cas de modificació fraudulenta de la informació de la seu electrònica. Per exemple, una seu electrònica de publicació d'un butlletí oficial editat exclusivament en format electrònic hauria de ser qualificada com a nivell alt quant a la dimensió d'integritat.

En atenció a aquesta anàlisi, es pot indicar, en general, la necessitat d'aplicar mesures com la signatura electrònica de les informacions publicades, el segellament de data i hora o la protecció dels registres de publicació, com a mesures destacades dins les determinades específicament pel RDENS.

La disponibilitat de la seu electrònica

La seu electrònica, com s'ha indicat anteriorment, és el mecanisme de suport a la relació electrònica del ciutadà amb l'Administració pública i és el punt d'accés a la informació administrativa, el registre electrònic, el tauler d'anuncis i altres elements, per la qual cosa resulta imprescindible considerar els requisits de disponibilitat de la seu electrònica. D'acord amb el RDENS, la disponibilitat es defineix com la propietat dels actius consistent en la capacitat d'accés als mateixos quan es requereix.

Si apliquem els criteris de categorització del RDENS en relació a la dimensió de disponibilitat referida a la seu electrònica, podem fer les indicacions següents:

Un sistema d'informació de seu electrònica serà de **nivell baix** quant a la **dimensió de seguretat de disponibilitat** si es produeix un perjudici limitat i reparable en cas d'impossibilitat d'accés a la seu electrònica. Per exemple, es podria qualificar la seu electrònica com a nivell baix en el cas de seus electròniques purament informatives o que només suporten tràmits que es poden realitzar a través d'altres canals o d'altres seus.

En segon lloc, un sistema d'informació de seu electrònica serà de **nivell mitjà** quant a la **dimensió de seguretat de disponibilitat** si, en cas d'impossibilitat d'accés a la seu electrònica, es produeix un perjudici greu o la capacitat de la seu es veu reduïda significativament. Per exemple, una seu electrònica d'una Administració que suporti tràmits que només es poden realitzar electrònicament s'hauria de qualificar de nivell mitjà.

Finalment, un sistema d'informació de seu electrònica serà de **nivell alt** quant a la **dimensió de seguretat de disponibilitat** si, en cas d'impossibilitat d'accés a la seu electrònica, es produeix un perjudici molt greu o s'incompleix greument alguna normativa. Per exemple, una seu electrònica que suporti processos o serveis que afectin a mesures crítiques de protecció civil (incendis, inundacions...) podria ser qualificada de nivell alt.

En atenció a aquesta anàlisi, es pot indicar, en general, la necessitat d'aplicar mesures específiques de l'ENS, com el dimensionament i la gestió correctes de la capacitat dels sistemes, l'anàlisi d'impacte, el pla de continuïtat, proves periòdiques o mitjans alternatius, entre d'altres.

Recomanacions

Recomanacions per a totes les Administracions públiques

Per complir els requisits de seguretat de la seu electrònica, es poden realitzar les recomanacions següents:

1.En relació amb la identificació electrònica de l'Administració pública, organisme o entitat de dret públic, és necessari dotar a la seu electrònica d'un certificat electrònic específic de seu electrònica, de nivell mig per a seus electròniques de categoria de seguretat baixa o mitjana, i de nivell alt per a seus electròniques de categoria de seguretat alta (d'acord amb la classificació de certificats realitzada a l'apartat 5.1.1 de la present guia).
Es recomana que l'Administració estableixi procediments per tal d'informar els ciutadans del prestador que emet els certificats i del lloc web on poden obtenir i instal·lar manualment els certificats arrel, principalment en relació amb els serveis de l'Agència Catalana de Certificació.

2.En relació amb la identificació electrònica dels ciutadans en l'accés a la seu electrònica, cal exigir la identificació en els casos estrictament necessaris, en aplicació dels principis de protecció de dades de caràcter personal, de seguretat i de proporcionalitat.
És necessari fer servir sistemes d'identitat digital o signatura electrònica de ciutadà per a l'accés autenticat a les seus electròniques, emprant qualsevol sistema de signatura electrònica legalment previst per a l'accés a la seu electrònica de nivell baix, certificats reconeguts per a l'accés a la seu electrònica de nivell mig i dispositius segurs certificats per a l'accés a la seu electrònica de nivell alt.

3.En relació amb la confidencialitat de les comunicacions establertes a través de la seu electrònica, és necessari fer servir certificats de seu electrònica de nivell mitjà per a les seus electròniques categoritzades en la dimensió de confidencialitat, com a nivell baix o mitjà, i certificats de seu electrònica de nivell alt per a les seus electròniques categoritzades en la dimensió de confidencialitat com a nivell alt.

4.En relació amb la publicació segura de continguts a la seu electrònica, és necessari aplicar mesures com la signatura electrònica de les informacions publicades, el segellament de data i hora o la protecció dels registres de publicació, en funció de la categoria de seguretat de la informació i de la seva naturalesa.

5.En relació amb la disponibilitat de la seu electrònica, és necessari aplicar mesures com el dimensionament i la gestió correctes de la capacitat dels sistemes, l'anàlisi d'impacte, el pla de continuïtat, proves periòdiques, mitjans alternatius o d'altres, en funció de la categoria de seguretat del servei.

Les **mesures de seguretat recomanables per a una seu electrònica** de nivell baix, d'acord amb l'annex II del RDENS, són les següents:

- Política de seguretat [org.1].
- Normativa de seguretat [org.2].
- Procediments de seguretat [org.3].
- Procés d'autorització [org.4].
- Anàlisi de riscos [op.pl.1].
- Arquitectura de seguretat [op.pl.2].
- Adquisició de nous components [op.pl.3].
- Identificació [op.acc.1].
- Requisits d'accés [op.acc.2], excepte en relació amb la disponibilitat.
- Procés de gestió de drets d'accés [op.acc.4], excepte en relació amb la disponibilitat.
- Mecanismes d'autenticació [op.acc.5], excepte en relació amb la disponibilitat.
- Accés local [op.acc.6], excepte en relació amb la disponibilitat.
- Accés remot [op.acc.7], excepte en relació amb la disponibilitat.
- Inventari d'actius [op.exp.1].
- Configuració de seguretat [op.exp.2].
- Manteniment [op.exp.4].
- Protecció contra codi perjudicial [op.exp.6].
- Protecció de claus criptogràfiques [op.exp.11].
- Àrees separades i amb control d'accés [mp.if.1].
- dentificació de les persones [mp.if.2].
- Condicionament dels locals [mp.if.3].
- Energia elèctrica [mp.if.4], només en relació amb la disponibilitat.
- Protecció contra incendis [mp.if.5], només en relació amb la disponibilitat.
- Registre d'entrada i sortida d'equipament [mp.if.7].
- Deures i obligacions [mp.per.2].
- Conscienciació [mp.per.3].
- Formació [mp.per.4].
- Acceptació i posada en producció [mp.sw.2].
- Perímetre segur [mp.com.1].
- Protecció de l'autenticitat i de la integritat [mp.com.3]

- Etiquetatge [mp.si.1].
- Custòdia [mp.si.3].
- Transport [mp.si.4].
- Acceptació i posada en servei [mp.sw.2]
- ades de caràcter personal [mp.info.1].
- Qualificació de la informació [mp.info.2], només en relació amb la confidencialitat.
- Signatura electrònica [mp.info.4], només en relació amb la integritat i l'autenticitat.
- Neteja de documents [mp.info.6], només en relació amb la confidencialitat.
- Protecció de serveis i aplicacions web [mp.s.2].

Les **mesures de seguretat recomanables per a una seu electrònica de nivell mitjà**, d'acord amb l'annex II del RDENS, són les següents:

- Totes les mesures de seguretat de nivell baix.
- Requisits addicionals d'anàlisi de riscos [op.pl.1].
- Dimensionament/gestió de capacitats [op.pl.4], només en relació amb la disponibilitat.
- Segregació de funcions i tasques [op.acc.3], excepte en relació amb la disponibilitat.
- Requisits addicionals dels mecanismes d'autenticació [op.acc.5], excepte en relació amb la disponibilitat.
- Requisits addicionals d'accés local [op.acc.6], excepte en relació amb la disponibilitat.
- Requisits addicionals d'accés remot [op.acc.7], excepte en relació amb la disponibilitat.
- Gestió de la configuració [op.exp.3].
- Gestió de canvis [op.exp.5].
- Gestió d'incidències [op.exp.7].
- Registre de la gestió d'incidències [op.exp.9].
- Requisits addicionals de protecció de claus criptogràfiques [op.exp.11].
- Contractació i acords de nivell de servei [op.ext.1].
- Gestió diària [op.ext.2].
- Anàlisi d'impacte [op.cont.1], només en relació amb la disponibilitat.
- Requisits addicionals d'energia elèctrica [mp.if.4], només en relació amb la disponibilitat.
- Protecció contra inundacions [mp.if.6], només en relació amb la disponibilitat.
- Caracterització del lloc de treball [mp.per.1].
- Requisits addicionals per al lloc de treball ordenat [mp.eq.1].
- Protecció de la confidencialitat [mp.com.2].
- Requisits addicionals en protecció de l'autenticitat i la integritat [mp.com.3].
- Criptografia [mp.si.2].
- Esborrament i destrucció [mp.si.5].
- Mitjans alternatius [mp.eq.9], només en relació amb la disponibilitat.
- Desenvolupament d'aplicacions [mp.sw.1].
- Requisits addicionals d'acceptació i posada en producció [mp.sw.2].
- Requisits addicionals de qualificació de la informació [mp.info.2], només en relació amb la confidencialitat.
- Xifrat de la informació [mp.info.3] pel que fa a la confidencialitat.
- Requisits addicionals de signatura electrònica [mp.info.4], només en relació amb la integritat i l'autenticitat.
- Còpies de seguretat [mp.info.9], només en relació amb la disponibilitat.
- Protecció contra la denegació de servei [mp.s.8], només en relació amb la disponibilitat.

Les **mesures de seguretat recomanables per a una seu electrònica de nivell alt**, d'acord amb l'annex II del RDENS, són les següents:

- Totes les mesures de seguretat de nivell baix i nivell mitjà.
- Requisits addicionals d'anàlisi de riscos [op.pl.1].
- Components certificats [op.pl.5].
- Requisits addicionals dels mecanismes d'autenticació [op.acc.5], excepte en relació amb la disponibilitat.
- Requisits addicionals de l'accés local [op.acc.6], excepte en relació amb la disponibilitat.
- Registre de l'activitat dels usuaris [op.exp.8], només en relació amb la traçabilitat.
- Protecció dels registres d'activitat [op.exp.10], només en relació amb la traçabilitat.
- Mitjans alternatius [op.ext.9].
- Pla de continuïtat [op.cont.2], només en relació amb la disponibilitat.
- Proves periòdiques [op.cont.3], només en relació amb la disponibilitat.
- Detecció d'intrusió [op.mon.1].
- Sistema de mètriques [op.mon.2].
- Instal·lacions alternatives [mp.if.9], només en relació amb la disponibilitat.
- Personal alternatiu [mp.per.9], només en relació amb la disponibilitat.
- Requisits addicionals d'acceptació i posada en producció [mp.sw.2].
- Requisits addicionals de signatura electrònica [mp.info.4], només en relació amb la integritat i l'autenticitat.
- Segells de temps [mp.info.5], només en relació amb la traçabilitat.
- Requisits addicionals per a criptografia [mp.si.2.] pel que fa a la integritat i la confidencialitat.
- Requisits addicionals pel que fa al perímetre segur [mp.com.1].
- Requisits addicionals pel que fa a la protecció de la confidencialitat [mp.com.2], respecte de la dimensió de confidencialitat.
- Requisits addicionals pel que fa a l'autenticitat i integritat [mp.com.3].
- Segregació de xarxes [mp.com.4].
- Mitjans alternatius [mp.com.9]
- Requisits addicionals de protecció contra la denegació de servei [mp.s.8], només en relació amb la disponibilitat.
- Mitjans alternatius [mp.s.9], només en relació amb la disponibilitat.

Recomanacions per a les Administracions públiques locals de població reduïda

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

1.Adherir-se a la política de seguretat de la Diputació Provincial o del Consell Comarcal als quals 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 les 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, de la política i dels 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 que necessita. La categoria del sistema recull la visió holística del conjunt d'actius com un tot harmònic, orientat a la prestació d'uns serveis.

Certificat electrònic: Un certificat electrònic serveix per identificar una persona física o jurídica i la clau pública assignada per a poder realitzar processos de signatura i/o xifratge. Cada certificat està identificat per un número de sèrie únic i té un període de validesa que està inclòs en el certificat.
D'una manera més formal, segons la Llei, 59/2003, de signatura electrònica, un certificat electrònic és un document signat electrònicament per un prestador de serveis de certificació que vincula unes dades de verificació de signatura (clau pública) a un signant i en confirma la identitat. Actualment s'han desenvolupat diversos tipus específics de certificats per tal d'identificar serveis prestats per mitjans electrònics (com per exemple, la seu electrònica).

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 format electrònic, 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 produeixin. 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 que amenacen el sistema d'informació, amb la finalitat d'assegurar 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 les signatures electròniques, incloent-hi 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 els 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 es basa en l'estudi dels riscos i que 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

Consorci Administració Oberta de Catalunya

Informació i guia d'implementació de la seu electrònica:

https://www.aoc.cat/index.php/ezwebin_site/Inici/SERVEIS/Serveis-comuns-d%27Administraci%C3%B3-electr%C3%B2nica/SEU-e

Agència Catalana de Certificació (CATCert).

http://www.catcert.cat

Eines

Certificats de seu electrònica

L'Agència Catalana de Certificació subministra certificats de seu electrònica de nivell mitjà i de nivell alt a les Administracions Públiques catalanes, a les universitats i centres de recerca i al Parlament de Catalunya.

Podeu trobar més informació a l'adreça:

http://www.catcert.cat/web/cat/1_4_1_0_2_cataleg.jsp

cesicat

Centre de Seguretat de la
Informació de Catalunya

www.cesicat.cat