



Generalitat de Catalunya
Departament de Governació
i Administracions Públiques
**Secretaria de Telecomunicacions
i Societat de la Informació**

Pla nacional d'impuls de la seguretat de les TIC a Catalunya

Index

Index	2
Una Societat de la Informació Segura.....	5
La seguretat TIC a la Cimera Mundial de la Societat de la Informació.....	5
La seguretat TIC a la política de la Unió Europea	8
Actuació de l'Agència Europea de Seguretat de les Xarxes i de la Informació ...	11
Actuació del Grup Directiu de Normalització de Xarxes i de la Informació	12
La política de seguretat TIC a l'Estat espanyol	12
Actuació del Ministeri d'Indústria, Turisme i Comerç i dels seus organismes.....	13
Actuació del Ministeri d'Administracions Públiques.....	18
Actuació del Centre Nacional d'Intel·ligència / Centre Criptogràfic Nacional.....	19
Avaluació actual de l'estat de situació de la seguretat TIC a Catalunya	20
El rol de Catalunya en matèria de seguretat TIC.....	24
La seguretat TIC a l'Estatut d'Autonomia de Catalunya de 2006 (EAC)	24
Bases per a un Pla nacional de seguretat TIC en el Pla de Govern 2007-2010..	27
Actuacions prèvies rellevants en matèria de seguretat TIC a Catalunya	28
El Pla nacional d'impuls de la seguretat de les TIC a Catalunya.....	30
La missió del Pla nacional d'impuls de la seguretat de les TIC a Catalunya.....	30
Els objectius estratègics del Pla nacional d'impuls de la seguretat de les TIC a Catalunya	30
Establiment d'una estratègia nacional de seguretat TIC	31
Suport a la protecció de les infraestructures crítiques TIC nacionals	31
Promoció d'un teixit empresarial català sòlid en seguretat TIC	32
Increment de la confiança i protecció de la ciutadania catalana en la societat de la informació	33
El Centre de Seguretat de la Informació de Catalunya (CESICAT).....	34
Programa d'actuació CESICAT per al període 2009-2013.....	34

Actuació 1.1: Establiment d'una estratègia global de seguretat de la informació per a Catalunya	39
Actuació 1.2: Capacitat de resposta a incidents de seguretat (CSIRT)	40
Abast dels serveis de prevenció i resposta a incidents	43
Servei d'alertes i advertències (reactiu).....	44
Servei de gestió d'incidents (reactiu).....	45
Servei de coordinació a resposta de vulnerabilitats (reactiu)	48
Servei de comunicats (proactiu)	48
Servei d'auditoria (proactiu).....	49
Servei de difusió d'informació de seguretat (proactiu).....	49
Servei de sensibilització en seguretat (gestió de qualitat de la seguretat)	50
Servei de consultoria i assistència en seguretat (gestió de qualitat de la seguretat)	51
Servei d'educació i formació en seguretat (gestió de qualitat de la seguretat)....	51
Actuació 1.3: Anàlisi de riscos amb impacte sobre el desenvolupament de la Societat de la Informació a Catalunya.....	52
Actuació 1.4: Serveis de seguretat TIC gestionada.....	52
Abast dels serveis de seguretat gestionada del CESICAT.....	54
Servei de detecció i prevenció d'intrusions (IDPS).....	54
Servei de gestió de registres de seguretat (SIEM).....	56
Servei de gestió de vulnerabilitats de seguretat (VMS).....	59
Actuació 1.5: Suport i foment de la protecció i l'assegurament del domini .CAT i dels serveis bàsics d'Internet	62
Actuació 2.1: Establiment i seguiment d'un pla de protecció d'infraestructures crítiques en TIC governamentals.....	63
Actuació 2.2: Col·laboració públic-privada en relació amb les infraestructures crítiques TIC no governamentals localitzades en territori català	64
Actuació 3.1: Creació d'una xarxa nacional de PIMEs especialitzades en seguretat TIC	64
Actuació 3.2: Promoció d'una comunitat de desenvolupament d'eines de seguretat TIC	65
Actuació 3.3: Promoció de l'avaluació i certificació de processos de desenvolupament segur del programari	66

Actuació 3.4: Promoció de la certificació dels processos de seguretat: ISO 27000	68
Actuació 3.5: Promoció de la formació i certificació de professionals en seguretat TIC	69
Actuació 3.6: Promoció de la certificació de seguretat de productes: Common Criteria.....	70
Actuació 3.7: Promoció de la recerca i innovació en seguretat TIC	72
Actuació 4.1: Educació en seguretat i confiança en col·lectius amb riscos especials	75
Actuació 4.2: Promoció entre la ciutadania dels instruments de seguretat essencials.....	76
CESICAT – Catàleg de serveis 2009	77

Una Societat de la Informació Segura

La Societat de la Informació, com ha estat reconegut de forma generalitzada, es caracteritza inicialment per l'ús intensiu de les tecnologies per a la creació, distribució i manipulació de la informació com a base per la realització d'activitats productives, de forma que la generació de riquesa es trasllada del sector industrial als sectors de serveis, en una conceptualització de la Societat de la Informació com economia informacional o capitalisme post-industrial.

En un moment posterior, la Societat de la Informació s'ha deixat de considerar un paradigma exclusivament econòmic, sinó que, en termes de la Cimera Mundial de la Societat de la Informació de la Unió Internacional de Telecomunicacions i Nacions Unides (2003-2005), la Societat de la Informació ha esdevingut una plataforma global per a la lliure circulació d'informacions, idees i coneixement, afectada per diverses problemàtiques i reptes, entre ells el de la seguretat i la qualitat TIC.

Així mateix, els darrers temps s'ha anat adquirint consciència de la importància de la infraestructura de xarxes i serveis de comunicacions electròniques que permeten la Societat de la Informació, així com el teixit econòmic i social de la Unió Europea, i que cal reforçar per evitar atacs a la seva seguretat. Com veure'm, la reforma del marc regulatori de les comunicacions electròniques a la Unió Europea consideren a la seguretat com un dels aspectes principals a tractar.

La seguretat TIC a la Cimera Mundial de la Societat de la Informació

Amb la Declaració de Principis de la Cimera Mundial de la Societat de la Informació de Ginebra de 12 de maig de 2004 es declara la superació de la concepció purament econòmica de la Societat de la Informació, refermant la voluntat de construir una Societat de la Informació centrada en la persona, integradora i orientada al desenvolupament, en que tots puguin crear, consultar, utilitzar i compartir la informació i el coneixement, perquè les persones, les comunitats i els pobles puguin emprar de forma plena les seves possibilitats en la promoció del seu desenvolupament sostenible i en la millora de la seva qualitat de vida, sobre la base dels propòsits i principis de la Carta de les Nacions Unides i respectant i defensant plenament la Declaració Universal dels Drets Humans.

En aquest context, els aspectes de confiança i seguretat en la utilització de les TIC han adquirit una elevada importància, com resulta evident, i que es qualifica de principi fonamental d'una Societat de la Informació integradora (apartat 19 de la Declaració de Principis de la Cimera Mundial de la Societat de la Informació).

Aquest principi fonamental es desenvolupa a la secció B.5 de la Declaració, que indica que “el foment d'un clima de confiança, inclús en la seguretat de la informació i la seguretat de les xarxes, l'autenticació, la privacitat i la protecció dels consumidors, és un requisit previ perquè es desenvolupi la Societat de la Informació i per promoure la confiança entre els usuaris de les TIC. Cal fomentar, desenvolupar i posar en pràctica una cultura global de ciberseguretat, en cooperació amb totes les parts interessades i els organismes internacionals especialitzats. Caldria oferir suport a aquests esforços amb una major cooperació internacional [...]” (apartat 35 de la Declaració).

Així mateix, s'indica que cal suportar les actuacions dirigides a “impedir que s'utilitzin les TIC amb finalitats incompatibles amb el manteniment de l'estabilitat i la seguretat internacionals, i que podrien suposar un menyscapse a la integritat de les infraestructures nacionals, i de la seva seguretat. Cal impedir que les tecnologies i els recursos de la informació s'utilitzin per a finalitats criminals o terroristes, respectant sempre els drets humans” (apartat 36 de la Declaració).

Finalment, es reconeix que “l'enviament massiu de missatges electrònics no desitjats (*spam*) és un problema considerable i creixent per als usuaris, les xarxes i Internet en general. Convé adreçar els problemes de la ciberseguretat i *spam* en els plànols nacional i internacional, segons correspongui” (apartat 37 de la Declaració).

En connexió amb la problemàtica de la ciberdelinqüència cal també referir-se a l'apartat 59 de la Declaració, que dintre de les dimensions ètiques de la Societat de la Informació, determina que “tots els actors de la Societat de la Informació han d'adoptar les accions i mesures preventives apropiades, conforme a dret, per impedir la utilització abusiva de les TIC, com els actes il·lícits o d'altre tipus motivats pel racisme, la discriminació racial, la xenofòbia i les formes connexes d'intolerància, l'odi, la violència, tot tipus de maltractament de nens, incloses la pedofília i la pornografia infantil, així com la tracta i l'explotació d'éssers humans”.

Posteriorment, el Compromís de Tunis de 28 de juny de 2006 indica, en el seu apartat 45, que es “subratlla la importància de la seguretat, la continuïtat i l'estabilitat d'Internet, així com la necessitat de protegir Internet i altres xarxes TIC contra les amenaces i en les seves vulnerabilitats”, afirmant “la necessitat d'arribar a una comprensió comuna sobre els assumptes relatius a la seguretat a Internet, així com d'ampliar la cooperació per facilitar l'abast, la recopilació i la disseminació de la informació relativa a la seguretat, i intercanviar bones pràctiques entre totes les parts interessades sobre les mesures per combatre les amenaces contra la seguretat, a nivell nacional i internacional”.

Així mateix, l'apartat 58 del Compromís identifica a la seguretat i protecció d'Internet com un dels elements que han de formar part de les polítiques públiques de governança d'Internet.

De l'agenda de la Declaració de Ginebra i del seu seguiment posterior pel Compromís de Tunis neix una detallada activitat de la Unió Internacional de Telecomunicacions en matèria de ciberseguretat (línia C.5 del Pla d'acció) amb els següents objectius principals:

1. Propiciar la cooperació entre els governs dintre de les Nacions Unides, i amb totes les parts interessades en altre fors apropiats, per augmentar la confiança dels usuaris i protegir les dades i la integritat de la xarxa; considerar els riscos actuals i potencials per a les TIC, i abordar altres qüestions de seguretat de la informació i de les xarxes.
2. Els governs, en cooperació amb el sector privat, han de prevenir, detectar, i respondre a la ciberdelinqüència i a l'ús indegut de les TIC, definint directrius que tinguin en compte els esforços existents en aquests àmbits; estudiant una legislació que permeti investigar i jutjar efectivament la utilització indeguda; promovent esforços efectius d'assistència mútua; reforçant el suport institucional a nivell internacional per a la prevenció, detecció i recuperació d'aquests incidents; i afavorint l'educació i la sensibilització.
3. Els governs i altres parts interessades han de fomentar activament l'educació i la sensibilització dels usuaris sobre la privadesa en línia i els mitjans de protecció de la privadesa.
4. Han de prendre mesures apropiades contra l'enviament massiu de missatges electrònics no sol·licitats (*spam*) a nivell nacional i internacional.
5. Afavorir una avaluació interna de la legislació nacional per superar qualsevol obstacle a l'ús efectiu de documents i transaccions electròniques, inclosos els mitjans electrònics d'autenticació.
6. Continuar enfortint el marc de confiança i seguretat amb iniciatives complementàries i de suport mutu en els àmbits de la seguretat en l'ús de les TIC, amb iniciatives i directrius sobre el dret a la privadesa i a la protecció de dades i dels consumidors.
7. Compartir pràctiques òptimes en l'àmbit de la seguretat de la informació i de la seguretat de les xarxes, i afavorir la seva utilització per totes les parts interessades.
8. Convidar als països interessats a establir punts de contacte per intervenir i resoldre incidents en temps real, i desenvolupar una xarxa cooperativa entre aquests punts de contacte de forma que es comparteixi informació i tecnologies per intervenir en cas d'aquests incidents.

9. Afavorir el desenvolupament de noves aplicacions segures i fiables que facilitin les transaccions en línia.
10. Animar als països interessats perquè contribueixin activament en les activitats en curs de les Nacions Unides tendents a crear confiança i seguretat en la utilització de les TIC.

Aquests objectius principals formen la base principal de l'actuació pública dels Estats en aquesta important matèria, d'acord amb el context regional (en el nostre cas, de la Unió Europea) i de la distribució de competències dintre de cada Estat.

La seguretat TIC a la política de la Unió Europea

La seguretat de les tecnologies de la informació i de les comunicacions ha estat objecte de tractament profund per part de la Unió Europea, mitjançant tres tipus d'iniciatives:

- Mesures específiques per a la seguretat de les xarxes i dels sistemes d'informació.
- Mitjançant el marc reglamentari de les comunicacions electròniques i, en concret, mitjançant la directiva sobre protecció de la vida privada i de les dades personals.
- Lluita contra la ciberdelinqüència.

Així mateix, la Unió Europea ha establert actuacions específiques que, de forma complementària, adrecen la problemàtica de la seguretat TIC, en concret mitjançant:

- Programes dedicats a recerca i desenvolupament, amb actuacions especialment rellevants en els 6è i 7è Programes Marc.
- El programa "Safer Internet", que promou un ús més segur d'Internet, amb una orientació a la protecció de l'usuari final enfront dels continguts no desitjats.
- Implicació en fòrums internacionals que tracten aquestes qüestions, com per exemple l'Organització de Cooperació i Desenvolupament Econòmic (OCDE), el Consell d'Europa (CoE) o Nacions Unides. En concret, la Unió Europea ha participat en el diàleg sobre seguretat TIC dins de la Cimera Mundial de la Societat de la Informació.

La Comunicació de la Comissió al Consell, al Parlament Europeu, al Comitè Econòmic i Social i al Comitè de les Regions, "El paper de l'administració electrònica en el futur d'Europa", COM (2003) 567, de 29 de setembre de 2003, ja reconeix que només és possible oferir serveis públics dins d'un entorn en que existeix confiança, entorn que ha de garantir sempre una interacció i accés segur a empreses i ciutadans.

La protecció de les dades personals, l'autenticació i la gestió d'identitats són qüestions bàsiques en les que cap servei públic pot fallar, de forma que les institucions públiques han de garantir sempre la seguretat de les transaccions i de les comunicacions digitals i la protecció de les dades personals.

Adicionalment, els ciutadans haurien de tenir sempre la possibilitat de controlar l'accés a les seves dades personals i les formes d'emmagatzematge i utilització d'aquestes dades, així com d'accedir a les mateixes.

La mateixa Comunicació indica que les estratègies d'administració electrònica a tots els nivells han de promoure la confiança en els serveis públics, i que cal impulsar la gestió de la identitat dins la Unió Europea, amb especial atenció a la interoperabilitat.

En termes més generals, la Comunicació de la Comissió al Consell, al Parlament Europeu, al Comitè Econòmic i Social i al Comitè de les Regions, "Reptes per a la societat de la informació europea més enllà de 2005", COM (2004) 757, de 19 de novembre de 2004, identifica la necessitat d'establir polítiques relatives a l'ús de les tecnologies de la informació i les comunicacions per cobrir carències en els serveis públics.

Entre d'altres, s'identifiquen els següents problemes a tractar:

- Els problemes de gestió de la identitat.
- El grau insuficient de seguretat i fiabilitat de les xarxes.
- La dificultat de poder enviar documents signats electrònicament en el marc dels procediments telemàtics, especialment en relació amb les PIMES.

Posteriorment, es publica la important Comunicació de la Comissió al Consell, al Parlament Europeu, al Comitè Econòmic i Social i al Comitè de les Regions, "i2010. Una societat de la informació europea pel creixement i l'ocupació", COM (2005) 229, d'1 de juny de 2005 proposa un marc estratègic, anomenat i2010, que promou una economia digital oberta i competitiva i que aposta per les tecnologies de la informació i les comunicacions en tant que impulsores de la inclusió i de la qualitat de vida.

Un dels pilars en els que es basa aquest marc estratègic és la construcció d'un Espai Únic Europeu de la Informació, que es podrà construir si se superen quatre grans reptes plantejats per la convergència digital, entre el que es troba la seguretat d'Internet, per augmentar la confiança.

Aquesta noció es desenvolupa de forma específica a la Comunicació de la Comissió al Consell, al Parlament Europeu, al Comitè Econòmic i Social i al Comitè de les Regions, "Una estratègia per a una societat de la informació segura – Diàleg, associació i potenciació", COM (2006) 251, de 31 de maig de 2006, dins del marc estratègic i2010, que revisa l'estat actual de les amenaces a la seguretat de la societat de la informació i determina noves accions per millorar el nivell general de seguretat de les xarxes i de la informació.

En aquesta Comunicació es reconeix que la seguretat és un repte per tots, incloent-hi a les administracions públiques, que deuen afrontar la seguretat dels seus sistemes, no només per protegir la informació del sector públic, sinó també per donar exemple de bones pràctiques a la resta d'agents.

Un dels mecanismes més importants que s'identifiquen a la citada Comunicació per millorar el nivell de seguretat és el coneixement, especialment en un entorn cada vegada més divers, obert i interoperable, així com generar una cultura de la seguretat generalitzada.

En aquest context, la Comissió convida als Estats membres a, entre d'altres, les següents accions:

- Promoure campanyes de sensibilització sobre les virtuts, els beneficis i avantatges associades a l'adopció d'unes tecnologies, pràctiques i comportaments efectius en relació amb la seguretat.
- Impulsar el desplegament de serveis d'administració electrònica destinats a comunicar i fomentar les bones pràctiques de seguretat, que després podrien estendre's a altres sectors.
- Combatre el robatori de la identitat i altres atacs contra la privacitat.

Posteriorment, i en el mateix context, cal situar la Comunicació de la Comissió al Consell, al Parlament Europeu, al Comitè Econòmic i Social i al Comitè de les Regions, "Sobre la lluita contra el SPAM, el programari espia i el programari maliciós", COM (2006) 688, de 15 de novembre de 2006, que identifica línies d'actuació per combatre aquestes amenaces a la seguretat.

Les accions que es proposen en aquesta Comunicació inclouen:

- El reforç del dret comunitari.
- L'aplicació del marc regulatori vigent per combatre el problema.
- La cooperació dintre i entre els Estats Membres.
- El diàleg polític i econòmic amb tercers Estats.
- El foment de les iniciatives de la indústria.
- Les activitats de R+D.

La Unió Europea també ha tractat la qüestió de la protecció de les infraestructures crítiques de la informació, per exemple la Comunicació de la Comissió al Consell i al Parlament Europeu, "Protecció de les infraestructures crítiques en la lluita contra el terrorisme", COM (2004) 702, de 20 d'octubre de 2004, o el Llibre Verd sobre un Programa Europeu per a la Protecció de les Infraestructures Crítiques, COM (2005) 576, de 17 de novembre de 2005 i la recent Proposta de Directiva del Consell sobre la identificació i designació de les infraestructures crítiques europees i l'avaluació de la necessitat de millorar la seva protecció, COM (2006) 787, de 12 de desembre de 2006.

Actuació de l'Agència Europea de Seguretat de les Xarxes i de la Informació

També en l'àmbit de la Unió Europea cal esmentar la creació de l'Agència Europea de Seguretat de Xarxes i de la Informació (ENISA), mitjançant el Reglament (CE) 460/2004 del Parlament Europeu i del Consell, amb la finalitat d'impulsar el funcionament del mercat interior prestant assessorament i assistència als Estats membres, els òrgans de la UE i les organitzacions empresarials, amb la finalitat de dotar d'un nivell alt i eficaç de seguretat a las xarxes i a la informació.

L'ENISA actua igualment com centre de competència per als Estats membres i les institucions comunitàries facilitant el intercanvi d'informació i la cooperació.

Algunes activitats rellevants d'ENISA han estat les següents:

- Catàleg de participants en seguretat de la informació.
- Catàleg de Centre de Resposta a Emergències Informàtiques.
- Guies sobre programes de conscienciació de la seguretat.
- Estudi sobre la seguretat de les comunicacions electròniques i l'SPAM.

- Inventari sobre activitats i normes de seguretat.
- Assistència a la Comissió Europea i autoritats d'alguns Estats membres en aspectes sobre seguretat de la informació, nivells d'autenticació, signatura electrònica i altres.

Actuació del Grup Directiu de Normalització de Xarxes i de la Informació

Finalment, cal esmentar la creació l'any 2004 del Network and Information Security Steering Group (NISSG), dependent del Grup Directiu de Normes de Tecnologies de la Informació i les Comunicacions (ICTSB), amb la missió de garantir la implementació dels requisits de normalització de seguretat de la informació identificats al informe especial ETSI SR 002 298, que contenia la resposta del CEN i del ETSI a la "Comunicació de la Comissió al Consell, el Parlament Europeu, al Comitè Econòmic i Social i al Comitè de les Regions: Seguretat de la Informació i les Xarxes: Proposta per a una Aproximació a una Política Europea, i que realitza un estudi i seguiment permanent de la qüestió.

La política de seguretat TIC a l'Estat espanyol

A l'Estat Espanyol, existeixen diverses polítiques per a la promoció de la seguretat TIC:

- El Plan Avanza, liderat pel Ministeri d'Indústria, Turisme i Comerç, a través de la Secretaria d'Estat de Telecomunicacions i Societat de la Informació, és un dels instruments importants en relació amb l'estratègia global espanyola de seguretat de la informació.
- L'actuació del Centre Nacional d'Intel·ligència / Centre Criptogràfic Nacional, dependent del Ministeri de Defensa, en relació amb la política de seguretat d'informació classificada en l'àmbit de la defensa i la seguretat nacional, incloent-hi la participació a la OTAN, i l'operació de l'Esquema Nacional d'Avaluació i Certificació de la Seguretat de la Informació, orientat a la seguretat dels productes, tant d'àmbit militar com civil.
- L'Esquema Nacional de Seguretat, previst a la llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics (la responsabilitat del qual no resulta clara en aquests moments, podent correspondre al Ministeri

d'Administracions Públiques o al Centre Criptogràfic Nacional), que constitueix una evolució de les actuacions del Consell Superior d'Administració Electrònica, només dirigides a les administracions públiques.

Per tant, podem situar en aquests tres departaments (Ministeri d'Indústria, Turisme i Comerç, Ministeri d'Administracions Públiques i Ministeri de Defensa) la direcció actual i la coordinació de la política de seguretat de la informació a l'Estat Espanyol. Així mateix, cal indicar el paper del Ministeri de l'Interior, en relació amb la tasca dels cossos i forces de seguretat de l'Estat, incloent-hi les policies autonòmiques, en la lluita contra la cibercriminalitat i per obtenir un ús més segur de la xarxa Internet.

Actuació del Ministeri d'Indústria, Turisme i Comerç i dels seus organismes

El Ministeri d'Indústria, Turisme i Comerç, a través de la Secretaria d'Estat de Telecomunicacions y per a la Societat de la Informació, ha rebut la direcció estratègica de l'execució del Plan Avanza, aprovat per Acord del Consell de Ministres de 4 de novembre de 2005.

El Plan Avanza té per finalitat el desenvolupament de la Societat de la Informació, dintre d'un escenari temporal 2006-2010, per a la convergència amb Europa i entre Comunitats Autònomes i Ciutats Autònomes, incloent-hi una línia d'actuació específica en matèria de seguretat i confiança.

El Plan Avanza s'estructura en cinc grans àrees d'actuació, una de les quals és l'anomenada "Nou Context Digital" que, en allò que es refereix a la línia de seguretat i confiança ("e-Confiança"), té com objectius els següents:

- Augmentar el grau de conscienciació, formació i sensibilització dels ciutadans, empreses i Administracions Públiques en matèria de seguretat de les tecnologies de la informació i les comunicacions. D'aquesta forma, es pretén disminuir el nombre d'empreses de més de 10 treballadors amb accés a Internet que tenen problemes de seguretat, situant-se en un 10% el 2010, i augmentar el nombre de particulars que prenen precaucions de seguretat; concretament, el 2010 un 60% dels particulars deurà haver instal·lat un programa antivirus.
- Impuls de la identitat digital, considerant que el 2010 el 100% dels ciutadans amb DNI disposaran d'un identificador únic, eficaç i pràctic que pugui ser utilitzat intensivament en tots els àmbits.
- Estimular la incorporació de la seguretat en les organitzacions como factor crític pel increment de la seva competitivitat, desenvolupant les infraestructures de seguretat necessàries i promovent l'adopció de millors

pràctiques, en especial, la certificació de la seguretat de la informació. El 2010, un 95% de les empreses de més de 10 treballadors haurà aplicat precaucions de seguretat.

- Desenvolupar una infraestructura eficaç per a l'execució de la política nacional de seguretat de la informació, coordinant als diferents agents i actuacions, fent un monitoratge de forma contínua de l'estat de la seguretat de la informació, i coordinant la representació internacional en matèria de seguretat de les TIC.

Les mesures previstes pel Plan Avanza per aconseguir aquests objectius són les següents:

- Accions iniciades el 2006:
 - o Mesura SEG.01. Difusió, comunicació i divulgació: Campanyes de sensibilització de gran públic i jornades sectorials per AAPP i PIMEs. Creació de plataformes per a la protecció del menor a Internet, protecció contra el SPAM i contra els fraus a Internet.
 - o Mesura SEG.04. Desenvolupament d'una xarxa de centres de seguretat: Creació de centres de seguretat i establiment dels procediments i protocols que permetin coordinar les seves funcions i actuacions. Creació d'un CERT per a l'Administració, un CERT per a PIMEs i una unitat de lluita contra la violació de la privacitat (SPAM, phishing i altres fraus).
 - o Mesura SEG.06. Impuls per a la implantació de la identitat digital i la signatura electrònica: Potenciar l'ús de la identitat digital i de la signatura electrònica per part dels diferents segments d'usuaris aprofitant especialment l'oportunitat que proporciona el DNI electrònic com infraestructura bàsica de seguretat.
 - o Mesura SEG.08. Extensió de les millors pràctiques associades a la seguretat i autoregulació: Potenciar millors pràctiques en la indústria i, en especial, en sectors crítics i AA.PP. Desenvolupament d'esquemes d'autoregulació, especialment per a la lluita contra el SPAM i per a la protecció dels menors.
 - o Mesura SEG.09/10. Actuacions per a la seguretat de la informació i la confiança: Crear una Comissió per a la seguretat de la informació, amb participació dels Ministeris i les AAPP competents en matèria de seguretat de la informació, així com al sector privat. Realitzar tasques de coordinació entre els diversos agents, impulsant mecanismes de cooperació nacional i internacional, creant espais de discussió i divulgant i entenent millors pràctiques en matèria de seguretat de la informació. Desenvolupar mètriques i metodologies per a l'avaluació dels indicadors d'e-Confiança, realitzant estudis sobre els avenços en

matèria d'ús de les tecnologies de seguretat per part dels diferents segments d'usuaris (ciutadans, empreses, llars, etc.).

- Accions pel període 2007 a 2010:
 - o Mesura SEG.05. Promoció i impuls al desenvolupament i innovació de tecnologies de seguretat: Identificar necessitats i requisits en matèria de seguretat dels diferents usuaris, traslladar a les empreses del sector TIC les esmentades necessitats i crear xarxes de suport a la innovació en tecnologies de seguretat.
 - o Mesura SEG.07. Promoció de la certificació de la seguretat, productes, serveis i processos: Potenciar i promocionar l'avaluació i certificació de la seguretat de les TIC, principalment mitjançant el desenvolupament i la utilització d'un esquema nacional d'avaluació i certificació de la seguretat de les TIC en l'àmbit públic i privat. Promoure a més el seu reconeixement i acreditació internacional.

Per la seva part, el Plan Avanza 2 continua desenvolupant la línia de eConfiança, potenciant la protecció de la privadesa en la Xarxa i la infància, la lluita contra el frau en línia i l'ajuda a la protecció de les infraestructures lògiques, especialment mitjançant INTECO.

Dintre d'aquesta activitat cal inscriure l'activitat de Red.es i RedIRIS, així com de l'INTECO, que veurem a continuació.

Red.es / RedIRIS

Red.es és una entitat pública empresarial adscrita al Ministeri d'Indústria, Turisme i Comerç amb les següents funcions principals:

- Impulsar el desenvolupament de la seguretat de la informació mitjançant l'execució de programes definits en el Plan Avanza per a la convergència amb Europa i entre comunitats autònomes.
- Analitzar la Societat de la Informació a través de l'Observatori de les Telecomunicacions i de la Societat de la Informació.
- Oferir assessorament i suport específic a l'Administració General de l'Estat.
- Gestionar el registre de noms de domini ".es".

En allò relatiu a la seguretat tecnològica i de la societat de la informació, resulta necessari definir un pla estratègic i un model per a la implantació de un Centre Nacional de Seguretat que inclogui la posada en marxa d'un Centre Demostrador de Seguretat per a la PIME amb l'objectiu de: (i) Realitzar proves i comparatives de diversos tipus de productes de seguretat; (ii) Servir de plataforma de proves i suport a altres centres com el Centre de Resposta a Incidents en Tecnologies de la Informació i el Observatori de Seguretat; i (iii) Potenciar l'ús de les tecnologies de Seguretat de la Informació entre les PIMEs espanyoles i impulsar la visibilitat internacional de la tecnologia espanyola de seguretat de la informació.

Per un altra banda, es considera necessari realitzar una recerca sobre usuaris d'Internet que tingui com finalitat l'elaboració d'un estudi sobre incidència i confiança dels usuaris en la xarxa. Amb aquesta es persegueix impulsar el coneixement i el seguiment dels principals indicadors i polítiques públiques relacionats amb la seguretat de la informació i la confiança; la generació d'una base de dades que permeti l'anàlisi i avaluació de la seguretat i la confiança amb una perspectiva temporal, i finalment elaborar i presentar informes en matèria de seguretat, que serveixin de suport a la presa de decisions per part de l'Administració en matèria de seguretat.

Red.es ha d'executar les següents actuacions en matèria de seguretat¹:

- En relació amb el Centre demostrador de seguretat de la informació per a la PIME, la implantació i manteniment d'un Centre Demostrador capaç de realitzar demostracions de seguretat per entorns empresarials, realitzar proves i comparatives de diversos productes de seguretat sobre diversitat de plataformes, aplicacions i canals de comunicació, donar suport a altres centres relacionats amb la seguretat tecnològica i realitzar tasques de difusió que impulsin la visibilitat nacional i internacional de la tecnologia espanyola de seguretat.
- En relació amb la recerca sobre usuaris d'Internet, un estudi sobre incidència i confiança dels usuaris a la xarxa.

Cal indicar que l'activitat de Red.es es realitza en règim de encàrrec de gestió per part de la Secretaria d'Estat de Telecomunicacions i per a la Societat de la Informació del Ministeri d'Indústria, Turisme i Comerç, publicada per Resolució de 1 de febrer de 2007.

¹ Aquestes actuacions han estat assumides íntegrament per l'INTECO, com es veu posteriorment.

Per una altra banda, Red.es gestiona RedIRIS i participa en l'INTECO. RedIRIS és la xarxa nacional de Recerca i Desenvolupament, que presta serveis de seguretat a la comunitat científica, incloent-hi els següents:

- El servei de seguretat de RedIRIS (IRIS-CERT), que té com missió la detecció de problemes que afectin a la seguretat de les xarxes de centres de RedIRIS, així com l'actuació coordinada amb aquests centres per solucionar aquests problemes. També es realitza una tasca preventiva, avisant amb temps de problemes potencials, oferint assessorament als centres, organitzant activitats d'acord amb els mateixos, i altres serveis complementaris.
- Serveis de infraestructura de clau pública (PKI) per a la comunitat RedIRIS, incloent-hi certificats de servidors segurs i certificats de xarxes *grid*.
- Serveis de control d'accés i autorització, mitjançant el programari PAPI.

INTECO

L'Institut de Tecnologies de la Comunicació (INTECO), promogut pel Ministeri d'Indústria, Turisme i Comerç, i participat per Red.es, és una plataforma per al desenvolupament de la Societat de Coneixement mitjançant projectes en l'àmbit de la innovació i la tecnologia, incloent-hi iniciatives de seguretat tecnològica, accessibilitat i inclusió a la societat digital, així com solucions de comunicació per particular i empreses.

L'activitat de l'INTECO en relació amb la seguretat de la informació inclou els següents projectes:

- Centre de Resposta a Incidents en Tecnologies de la Informació per a PIMES, que té com missió principal aconseguir un desenvolupament sòlid del teixit empresarial espanyol mitjançant la provisió a les PIMES de serveis reactius, preventius i formació en matèria de seguretat.
- Centre d'Alerta Ràpida Antivirus, que té com missió principal la conscienciació en matèria de seguretat, oferint des de 2001 alertes, informació, eines de protecció gratuïtes i informes diaris de seguretat sobre els darrers codis maliciosos apareguts a la Xarxa.
- Centre d'Informació per a la Difusió de la Cultura de la Seguretat, que té com missió principal:
 - o La posada en marxa i operació d'un portal de difusió i divulgació d'informació en matèria de la seguretat de la informació.

- L'elaboració de continguts y guies pràctiques en matèria de seguretat de la informació, en col·laboració amb agents rellevants en aquest àmbit.
- Observatori de la Seguretat de la Informació, que té com missió principal analitzar, descriure, assessorar i difondre la cultura de la seguretat i la confiança en la Societat de la Informació, mitjançant la generació de coneixement especialitzat en la matèria, i l'elaboració de recomanacions i propostes que permetin definir tendències vàlides per a la presa de decisions en el àmbit de la seguretat.
 - L'Observatori haurà de ser un centre de referència per a l'anàlisi i el seguiment de la confiança en la Societat de la Informació a Espanya, elaborant, recollint, sintetitzant i sistematitzant indicadors.
 - Per una altra banda, es generarà i difondrà coneixement especialitzat al menys en les següents àrees clau de la seguretat de la informació:
 - Seguretat de signatura electrònica i de la identitat digital.
 - Mesures de protecció enfront a riscos de seguretat de la informació.
 - Tecnologies de gestió dels drets d'autor en l'àmbit digital (DRMs).
 - Altres tecnologies i eines de seguretat disponibles.

Cal indicar que l'activitat del INTECO es realitza en règim de encàrrec de gestió per part de la Secretaria d'Estat de Telecomunicacions i per a la Societat de la Informació del Ministeri de Indústria, Turisme i Comerç, publicada per Resolució de 1 de febrer de 2007.

Actuació del Ministeri d'Administracions Públiques

El Ministeri d'Administracions Públiques impulsa els aspectes de seguretat del procediment administratiu basat en tecnologies de la informació (mitjans electrònics, informàtics i telemàtics) per part de les AA.PP.

En aquest sentit, cal esmentar la tasca que ve realitzant en la difusió de la cultura de la seguretat, mitjançant la important tasca del Consell Superior d'Informàtica, avui Consell Superior d'Administració Electrònica, que ha avançat en la definició inicial del esquema nacional d'avaluació de la seguretat de la informació i en la publicació de criteris i normes de seguretat de la informació en l'àmbit de l'Administració General de l'Estat.

Més recentment, cal considerar la llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, que imposa obligacions concretes de seguretat, identificació i signatura electrònica en l'àmbit de l'anomenada administració electrònica.

Actuació del Centre Nacional d'Intel·ligència / Centre Criptogràfic Nacional

El Secretari d'estat director del Centre Nacional d'Intel·ligència, com a director del Centre Criptogràfic Nacional (CCN), és l'autoritat responsable de coordinar l'acció dels diferents organismes de l'Administració que utilitzen mitjans o procediments de xifra, garantir la seguretat de les tecnologies de la informació en aquest àmbit, informar sobre l'adquisició coordinada del material criptogràfic i formar al personal de l'Administració especialista en aquest camp.

El director del CCN és l'autoritat de certificació de la seguretat de les tecnologies de la informació (<http://www.oc.ccn.cni.es>) i l'autoritat de certificació criptogràfica (<http://www.ccn.cni.es>). Així mateix, és responsable de vetllar pel compliment de la normativa relativa a la protecció de la informació classificada, en els aspectes dels sistemes d'informació i telecomunicacions, d'acord amb l'article 4.e) i f) de la Llei 11/2002, de 6 de maig.

El Centre Criptogràfic Nacional es troba adscrit al Centre Nacional d'Intel·ligència, comparteix amb aquest mitjans, procediments, normativa i recursos. Dins del seu àmbit d'actuació, el Centre Criptogràfic Nacional realitza les següents funcions:

- Elaborar i difondre normes, instruccions, guies i recomanacions per garantir la seguretat dels sistemes de les tecnologies de la informació i les comunicacions de l'Administració. Les accions derivades del desenvolupament d'aquesta funció seran proporcionals als riscos als que estigui sotmesa la informació processada, emmagatzemada o transmesa pels sistemes (<http://www.ccn.cni.es>).
- Formar al personal de l'Administració especialista en el camp de la seguretat dels sistemes de les tecnologies de la informació i les comunicacions.
- Constituir l'organisme de certificació de l'Esquema nacional d'avaluació i certificació de la seguretat de les tecnologies de la informació, d'aplicació als productes i els sistemes en el seu àmbit (<http://www.oc.ccn.cni.es>).
- Valorar i acreditar la capacitat dels productes de xifra i dels sistemes de les tecnologies de la informació, que incloguin mitjans de xifra, per processar, emmagatzemar o transmetre informació de forma segura.

- Coordinar la promoció, el desenvolupament, l'obtenció, l'adquisició i la posada en explotació i la utilització de la tecnologia de seguretat dels sistemes abans esmentats.
- Vetllar pel compliment de la normativa relativa a la protecció de la informació classificada en el seu àmbit de competència (per exemple, informació de seguretat OTAN).
- Establir les necessàries relacions i signar els acords pertinents amb organitzacions similars d'altres Estats, per al desenvolupament de les funcions esmentades.

Dins de les activitats del CCN, cal indicar el CCN-CERT, l'Equip de Resposta a Incidents de Seguretat de la Informació, que té com objectiu principal la millora del nivell de seguretat dels sistemes d'informació a les administracions públiques de l'estat espanyol.

La missió del CCN-CERT és ser el centre d'alerta i resposta a incidents de seguretat, ajudant a les administracions públiques a respondre de forma més ràpida i eficient davant les amenaces de seguretat que afecten als seus sistemes d'informació, a través de dues grans línies d'actuació:

- La prestació de serveis d'informació, como els serveis d'alertes de noves amenaces.
- La realització de tasques de recerca, formació i divulgació de la seguretat de la informació.

Avaluació actual de l'estat de situació de la seguretat TIC a Catalunya

Tot i les polítiques i actuacions abans esmentades, no es pot dir que els nivells de seguretat TIC a Catalunya siguin òptims: més aviat al contrari, la situació només es pot considerar satisfactòriament tractada en pocs casos, especialment en grans entitats, mentre que es pot apreciar una certa desprotecció en molts casos, i en concret en els casos de ciutadans i PIMEs, així com en les administracions públiques amb menys recursos.

En relació amb la seguretat dels ciutadans i ciutadanes, l'estudi² realitzat per l'INTECO durant el segon trimestre del 2007 presenta les següents conclusions:

- La percepció de seguretat personal durant la navegació i ús d'Internet és elevada, tot i que s'ha incrementat sensiblement el volum d'incidències relatives a programari maliciós (malware), i que el correu brossa (spam) afecta al 80% dels usuaris.
- Fins a un 77,1% dels ordinadors dels usuaris presenta algun programari maliciós instal·lat al seu equipament informàtic, en la majoria de casos amb finalitats comercials (troians: 54%, publicitat: 39,1%, eines: 27,3%).
- S'ha confirmat la dada, ja indicada per estudis anteriors, de l'augment del nombre i tipus de programari maliciós, amb una important tendència a la diversificació i a l'especialització en els atacs.
- També es consolida l'ús de tècniques d'enginyeria social com a vector d'atac més freqüent, mitjançant diversos tipus d'enganys als usuaris, sense necessitat de mecanismes tècnics d'infecció i propagació.
- El nivell de seguretat presenta una relació directa amb la formació i l'actitud dels usuaris, especialment amb la prudència en els hàbits d'ús, el que evidencia la necessitat d'una conscienciació i formació més intenses.
- L'estudi recomana centrar els esforços en els següents aspectes:
 - o Potenciar l'ús de mitjans i dispositius de seguretat: programari antivirus, antispam, tallafocs, etc.
 - o Conscienciar i formar adequadament per crear una veritable cultura de seguretat i d'ús responsable en els usuaris.

En relació amb la seguretat de les PIMEs, un altre estudi³ realitzat per l'INTECO durant el 2007 presenta les següents conclusions:

- En general, les PIMEs pateixen un endarreriment tecnològic important en relació amb les gran empreses, que ocasiona que les TIC no siguin emprades de forma particular per als processos productius, sinó només per a tasques col·laterals i poc connectades amb el negoci.

² INTECO, "Segunda Oleada del Estudio sobre Seguridad de la Información y e-Confianza en los Hogares Españoles", Febrer 2008.

³ INTECO, "Estudio sobre Incidencias y Necesidades de Seguridad en las Pequeñas y Medianas Empresas Españolas", Gener 2008.

- Pel que fa a la seguretat de la informació, s'observa un cert escepticisme de les PIMEs als riscos de seguretat TIC, derivat del desconeixement generalitzat dels problemes associats a la tecnologia, excepte en els casos de tecnologia antivirus, tallafocs i antispam, que es coneixen i apliquen més. En concret, les solucions de còpia de seguretat, xifratge o compliment regulatori són poc conegudes i aplicades. Algunes causes són:
 - o Desconeixement de les tecnologies, principalment com a conseqüència de la falta de personal amb una adequada formació i capacitat d'entendre les necessitats tecnològiques de l'empresa.
 - o Falta de conscienciació en relació amb la seguretat de la informació, ja que les PIMEs no tenen percepció de ser objectiu pels atacants amb interès econòmic, el que sense cap dubte les posa en una situació de desprotecció tècnica enfront d'atacs.
 - o Desconfiança en Internet com a mitjà per a la prestació de serveis, causada per la incapacitat de reaccionar enfront de les amenaces sorgides a partir de la connexió a la xarxa.
 - o Falta de recursos en comparació amb les grans empreses, especialment tenint en compte que els costos de determinades solucions resulten massa elevats per a les PIMEs de menys de 50 treballadors, de les quals el 94% tenen menys de 10 treballadors.
- En relació amb el compliment normatiu, ve a passar el mateix: en concret i en relació amb la LOPD, tot i que el grau de declaració de fitxers és elevat (79,2%), existeixen indicadors que demostren que encara no s'ha adoptat realment la mateixa: per exemple, el 56,2% de PIMEs desconeixen les sancions que preveu la LOPD; només el 17,7% realitzen les auditories de seguretat exigides legalment i només un 23,4% disposen de document de seguretat. A més, només un 7,5% de les PIMEs declara que sol·licitaria assessorament legal especialitzat en compliment normatiu de forma freqüent.
- Les mesures d'impuls pel creixement de la seguretat a les PIMEs impliquen necessàriament un apropament de les solucions de seguretat a les PIMEs, posant a la seva disposició personal expert i qualificat que l'ajudi en l'adopció de les mesures de protecció més efectives i, especialment, en l'assessorament pel compliment normatiu.
- L'estudi recomana centrar els esforços en els següents aspectes:
 - o Adaptació, per part dels fabricants, dels productes de seguretat oferts a les PIMEs, seguint criteris com la homogeneïtzació, integració i simplificació del producte mitjançant paquets de serveis específics. Així mateix, caldria oferir contractes dinàmics pels serveis, que redueixin terminis i resultin adaptables a les necessitats puntuals dels clients.
 - o Les PIMEs haurien de delegar la gestió integral de la seguretat dels seus equipaments en proveïdors tecnològics de confiança, el que

aportaria avantatges com la reducció de costos originada per l'optimització del servei i la no necessitat de disposar de personal propi expert de seguretat TIC.

- L'Administració ha de jugar un paper important en quant a la generació d'una cultura de seguretat, així com establir Centres específics que fomentin l'adopció d'eines de seguretat i la prestació de serveis altament especialitzats en seguretat TIC, com a mesura de suport general al sector.

En relació amb la seguretat dels governs locals, un tercer estudi⁴ realitzat per l'INTECO, amb la col·laboració de la Federació Espanyola de Municipis i Províncies i de la Subdirecció General de Coordinació de Recursos Tecnològics del Ministeri d'Administracions Públiques, durant el 2007 presenta les següents conclusions:

- Més del 80% dels ajuntaments de municipis grans i mitjans accedeix a la xarxa a través de banda ampla, mentre que en el grup de petits municipis la proporció es redueix al 50%. Més del 98% de les entitats utilitza programes antivirus i aproximadament el 70%, tallafocs; la primera és pràcticament l'única eina implantada en la majoria de les administracions dels municipis de mida reduïda per protegir-se de possibles incidències de seguretat en la seva informació.
- La implantació de les principals mesures i pràctiques de seguretat mostra un índex mitjà superior al 50% per a tots els governs locals, a excepció dels de municipis amb menys població.
- Una generosa aplicació de la pràctica totalitat de mesures disponibles per part dels governs de municipis grans i mitjans, en contraposició als de les localitats més petites, que fan dependre pràcticament tota la seva seguretat dels antivirus; en aquest grup d'entitats, la mesura de seguretat següent, quant al seu nivell d'implantació (xifratge de comunicacions) difereix amb la primera en 30 punts percentuals (un 94,9% davant d'un 62,7%). Aquestes dades evidencien la necessitat d'impulsar en els petits municipis l'ús de mesures de caràcter proactiu (ex. còpies de suport de dades i del programari).
- La política de "taula buida i pantalla bloquejada" (pràctica considerada pels experts consultats com la més important) està implantada en menys del 36% de les entitats locals espanyoles, si bé la segona més valorada (control del terminal de l'usuari) es troba en més del 90% de les entitats consultades.
- L'estudi recomana centrar els esforços en els següents aspectes:

⁴ INTECO, "Estudio sobre la Seguridad y e-Confianza en el Ámbito de las Entidades Locales", Setembre 2007.

- Cal fer un esforç més gran en formació, en actualització constant i en inversions en nous processos i tecnologies informàtiques (expansió de la signatura digital) per prevenir possibles riscos, en col·laboració amb els principals proveïdors de mesures de seguretat.
- A més, també és imprescindible complementar aquestes actuacions amb la implantació de protocols d'actuació i codis de conducta enfocats al compliment de les pràctiques de seguretat essencials per aconseguir l'objectiu de seguretat.

Les conclusions dels estudis anteriorment ressenyats és força semblant: resulta necessari continuar treballant en la generació de consciència i cultura de seguretat, facilitant eines adequades i vigilant de forma continua l'estat de la seguretat de la xarxa.

El rol de Catalunya en matèria de seguretat TIC

Les necessitats en relació amb la seguretat i la qualitat TIC a Catalunya, que s'han presentat anteriorment, són reals i importants, i cal reconèixer que Catalunya pateix un endarreriment important en relació amb l'actuació pública de l'Estat espanyol i, fins i tot, d'altres Comunitats Autònomes, el que es pot traduir en pèrdua de competitivitat i allunyament d'inversió en el mercat TIC.

En conseqüència, cal actuar de forma decidida i urgent per instaurar una política duradora i un programa d'actuació a curt termini i a mitjà termini que corregeixi aquesta situació, amb base en les competències pròpies de Catalunya, en el context del nou Estatut d'Autonomia de Catalunya del 2006, i alineada amb el Pla de Govern de la Generalitat de Catalunya, amb les actuacions que ja realitzen actualment la Generalitat de Catalunya i la resta de poders públics de Catalunya, el sector privat i la societat civil catalana.

La seguretat TIC a l'Estatut d'Autonomia de Catalunya de 2006 (EAC)

Un dels fonaments important per afirmar la competència de la Generalitat de Catalunya i de la resta d'administracions públiques catalanes en seguretat de la informació deriva del important article 40 de l'EAC ("protecció de les persones i de les famílies).

En aquest sentit, cal partir de l'article 40.1, que exigeix als poders públics "tenir com a objectiu la millora de la qualitat de vida de totes les persones", que evidentment cal

entendre aplicable en el més ampli sentit, i per suposat a la Societat de la Informació, en que les persones desenvolupen una part cada vegada més important de la seva vida.

Respecte als col·lectius a protegir especialment, l'article 40.3 de l'EAC determina que "els poders públics han de garantir la protecció dels infants, especialment contra tota forma d'explotació", incloent-hi les formes d'explotació que es poden produir emprant mitjans electrònics, com per exemple en casos d'assetjament a través de la xarxa (*ciberbullying*) o d'assetjament sexual; previsió estatutària que cal posar en relació amb l'article 142, que estableix les competències de la Generalitat en matèria de joventut.

Així mateix, l'article 40.6 de l'EAC estableix que "els poders públics han de garantir la protecció de les persones grans perquè puguin portar una vida digna i independent i participar en la vida social i cultural", manament estatutari que exigeix adreçar de forma específica els riscos que la gent gran pot patir en les xarxes telemàtiques, per afavorir la seva integració i participació efectiva en la Societat de la Informació, que dependrà, en part, del grau de confiança que en tingui.

Finalment, l'article 40.8 de l'EAC indica que "els poders públics han de promoure la igualtat de totes les persones amb independència de l'origen, la nacionalitat, el sexe, la raça, la religió, la condició social o l'orientació sexual, i també han de promoure l'eradicació del racisme, de l'antisemitisme, de la xenofòbia, de l'homofòbia i de qualsevol altra expressió que atempti contra la igualtat i la dignitat de les persones", obligació estatutària que també cal complir en relació amb les noves formes de discriminació i totes les formes d'atemptats als drets i llibertat que es puguin produir emprant mitjans electrònics, incloent-hi els ciberdelictes.

Per la seva banda, l'article 42.3 de l'EAC ("cohesió i benestar socials") insisteix en l'obligació dels poders públics de "vetllar per la dignitat, la seguretat i la protecció integral de les persones, especialment de les més vulnerables", menció expressa de la seguretat que cal entendre aplicable de forma plena a la seguretat de la Societat de la Informació catalana.

Un altre fonament important en relació amb la competència per actuar en aquesta matèria el trobem en l'article 49.1 de l'EAC ("protecció dels consumidors i usuaris"), quan determina que "els poders públics han de garantir la protecció de la salut, la seguretat i la defensa dels drets i els interessos legítims dels consumidors i usuaris".

Conté aquesta norma una altra referència expressa a la seguretat, que també cal entendre plenament aplicable a la seguretat a la xarxa, en aquest cas amb una especial atenció als consumidors i els usuaris (una part molt important de la ciutadania, en el model econòmic actual), i que s'identifica amb un col·lectiu a protegir de forma específica.

Precisament en relació amb aquest col·lectiu es lliura en l'actualitat una de les batalles importants contra el frau, en concret enfront del robatori d'identitats

financeres (mitjançant el “*phishing*”), el robatori d’informacions comercials sensibles, com les dades de les targetes de pagament, o contra les comunicacions comercials no sol·licitades (“*spam*”).

Cal indicar que l’article 123 de l’EAC determina la competència exclusiva de la Generalitat de Catalunya en matèria de consum, indicant els aspectes de formació i educació, que resulten particularment importants en matèria de seguretat de les TIC.

Respecte al comerç electrònic, a més, cal indicar la competència exclusiva de la Generalitat de Catalunya relativa a la seva ordenació administrativa, d’acord amb l’article 112.1.a) de l’EAC, el que d’acord amb la nova llei d’impuls de la societat de la informació, inclou la declaració de les mesures de seguretat aplicables al comerç electrònic.

Més en concret, l’article 53 de l’EAC (“accés a les tecnologies de la informació i de la comunicació”) imposa obligacions d’actuació positiva als poders públics en relació amb les TIC, i en concret, el seu apartat 1 determina que “els poders públics han de facilitar el coneixement de la societat de la informació i han d’impulsar l’accés a la comunicació i a les tecnologies de la informació, en condicions d’igualtat, en tots els àmbits de la vida social, inclòs el laboral; han de fomentar que aquestes tecnologies es posin al servei de les persones i no afectin negativament llurs drets, i han de garantir la prestació de serveis per mitjà de les dites tecnologies, d’acord amb els principis d’universalitat, continuïtat i actualització”.

Com resulta evident del text, l’actuació pública ha de garantir que les tecnologies no afectin negativament els drets de les persones, el que exigeix d’un programa públic de seguretat de la Societat de la Informació que se’n responsabilitzi.

Per una altra banda, el principi de continuïtat imposat per l’EAC obliga a la vigilància i protecció dels elements que componen la infraestructura crítica de les TIC, tant quan aquesta es troba sota responsabilitat de les administracions i, en general, del sector públic, com en mans del sector privat, amb qui cal establir polítiques de col·laboració i suport mutu.

Una altra dimensió d’actuació en matèria de seguretat de les TIC deriva, per connexió, de la resta de competències de la Generalitat de Catalunya i dels governs locals de Catalunya. Aquest és el cas en relació amb les competències de seguretat i protecció civil (article 132 de l’EAC), de seguretat pública (article 164 de l’EAC) i privada (article 163) o energia i, en concret, en matèria de seguretat nuclear, ja que els efectes d’un incident de seguretat de la informació podrien manifestar-se civilment, produint un efecte en cascada, especialment quan els incidents afecten a les infraestructures crítiques TIC que donen suport als sectors governamental i productiu que en depenen.

Aquesta competència en matèria de seguretat TIC sobre infraestructures crítiques es fonamenta, addicionalment, en l'article 140.7 de l'EAC, en relació amb les xarxes de comunicacions electròniques, la seguretat de les quals cal protegir, ja que aquestes xarxes són el factor principal que permet l'existència i la continuïtat de la Societat de la Informació. Com hem vist anteriorment, la política de la Unió Europea en matèria de seguretat TIC es tracta en seu del marc reglamentari de les comunicacions electròniques, en que l'EAC atorga competències executives a la Generalitat de Catalunya.

Finalment, correspon a l'administració pública la competència d'organització i regulació del funcionament administratiu propi, així com el règim jurídic i procediment administratiu (article 159 de l'EAC), en el context de la legislació estatal bàsica, i en matèria TIC, dins del marc de la llei d'accés electrònic dels ciutadans als serveis públics, que tracta extensament les obligacions de seguretat de l'actuació administrativa, incloent-hi aspectes de signatura electrònica, però també la resta d'aspectes de seguretat de la informació.

Bases per a un Pla nacional de seguretat TIC en el Pla de Govern 2007-2010

El Pla de Govern de la Generalitat de Catalunya per al període 2007-2010 preveu diversos objectius que presenten relació i oportunitat relatives a la seguretat TIC.

L'objectiu 1.1.2 preveu potenciar l'existència d'una xarxa d'atenció especialitzada de serveis a les famílies: serveis de formació per a pares, punts de trobada, mediació familiar, casals i esplais per a infants i joves... que hauria de considerar també informació i assistència en relació amb la problemàtica d'ús segur de les xarxes per les famílies, oferint un punt de detecció i suport en cas de problemes de seguretat i confiança, especialment a menors, dintre del concepte de protecció a la infància.

La justificació per aquesta possibilitat neix de l'ús il·lícit de les xarxes per promoure la violència, la xenofòbia, l'homofòbia, malalties com la bulímia i l'anorèxia, l'assetjament moral i sexual, la pornografia infantil i altres, que exigeix una atenció especial per part de les autoritats públiques, i de mecanismes de reacció adequats, propers i efectius.

L'objectiu 3.1.3 considera la necessitat d'establir polítiques de suport a la creació de teixit industrial i de serveis de TIC al país mitjançant, sobretot, la capacitat de compra de l'Administració, que es pot fer mitjançant la creació d'un clúster empresarial de seguretat i qualitat TIC.

També és un objectiu per aquesta legislativa l'actuació en matèria de formació de persones adultes en TIC, el que es refereix a diversos nivells, entre els que podem trobar la formació en les diversos aspectes professionals en TIC, ajudant a incrementar la competitivitat de la indústria TIC catalana.

L'objectiu 3.1.6 persegueix, entre altres aspectes, la promoció d'estàndards de qualitat en els productes i serveis catalans, el que s'ha de projectar en la indústria TIC, a tots els nivells: l'actuació dels professionals i de les empreses, els processos de producció de programari o la prestació de serveis TIC, sempre en connexió amb la seguretat TIC.

Objectiu que lliga amb l'objectiu 3.2.2, relatiu a la formació per al treball al llarg de la vida professional, necessàriament aplicable a la formació continuada en TIC, de forma particularment intensa degut a l'accelerat ritme de canvi tecnològic que exigeix una actualització permanent mitjançant programes de certificació, com a eina per assolir i mantenir els nivells de qualitat necessaris per fer de la indústria TIC catalana un sector competitiu.

En aquest cas, resulta particularment necessari atendre als continguts de l'Acord estratègic per a la internacionalització, la qualitat de l'ocupació i la competitivitat de l'economia catalana, així com al Programa de formació especialitzada i ajustada a les necessitats empresarials de Catalunya, i al Programa de formació en sectors emergents, tot dos impulsats per la Generalitat de Catalunya.

Finalment, l'objectiu 3.4.1 persegueix garantir el suport al naixement i creixement de les PIME i les cooperatives catalanes, així com als sectors industrials davant el repte de la globalització econòmica, amb una política industrial activa que sigui capaç d'orientar el desenvolupament cap a aquells sectors amb més capacitat d'adaptació i que basin la seva competitivitat en la qualitat, la tecnologia i el coneixement, el que connecta amb les necessitats de seguretat TIC identificades en aquest document.

Aquest objectiu s'ha d'aconseguir mitjançant una política activa de clústers, actuant de forma proactiva en suport dels sectors econòmics estratègics i de nous sectors emergents per crear activitat econòmica i ocupació. En aquest sentit, cal impulsar de forma decidida un clúster especialitzat en la seguretat TIC, que permeti el desenvolupament d'un teixit empresarial català preparat per aquests reptes.

Actuacions prèvies rellevants en matèria de seguretat TIC a Catalunya

La Generalitat de Catalunya ha vingut establint una política de seguretat corporativa, els darrers anys, que s'orienta a protegir els sistemes d'informació emprats pels

departaments de l'Administració de la Generalitat de Catalunya i dels ens que en depenen.

Organitzada pel Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya, cal fer esment de l'Oficina de Seguretat de la Informació, unitat adscrita a l'àrea de qualitat, seguretat i relació amb proveïdors, que s'encarrega de vetllar per l'establiment de normatives i estàndards de seguretat, realitzar anàlisis preventius de problemàtiques de seguretat, intervenir en suport del sistemes corporatius i respondre, en general, a qualsevol necessitat de seguretat que si l'hi plantegi.

Així mateix, cal fer esment d'iniciatives d'àmbit mixt, que s'adrecen tant a la protecció corporativa com a la seguretat global de sectors específics. En suposa exemple l'ordre SLT/465/2008, de 27 d'octubre, per la qual es regula el Programa de Seguretat de la Informació en el Departament de Salut, que presenta un indubtable impacte en el sector sanitari.

No es poden oblidar tampoc les iniciatives tecnològiques que ve liderant la direcció general de la policia – mossos d'esquadra en relació amb la lluita contra totes les formes de delinqüència electrònica, mitjançant una unitat especialitzada específicament adreçada a millorar la capacitat de detecció i resposta al delicte amb base tecnològica.

Finalment, i sense perjudici d'altres iniciatives corporatives d'indubtable valor, cal fer esment de la tasca que, en matèria de seguretat de la informació, realitzen l'Agència Catalana de Certificació, organisme adscrit al Consorci Administració Oberta de Catalunya, i l'Agència Catalana de Protecció de Dades, en els àmbits de la identitat digital i la protecció de les dades de caràcter personal, aspectes que presenten íntima relació amb la seguretat.

De forma complementària amb les actuacions en els diferents àmbits corporatius de les Administracions Públiques i de les polítiques i actuacions en matèria de lluita contra la delinqüència electrònica, cal refermar la necessitat de procedir a establir i liderar una actuació pública de caire global a Catalunya, amb la col·laboració de totes les administracions i del sector privat, per coordinar i impulsar totes les actuacions orientades a combatre les problemàtiques abans esmentades i ser referent de país.

El Pla nacional d'impuls de la seguretat de les TIC a Catalunya

La missió del Pla nacional d'impuls de la seguretat de les TIC a Catalunya

La missió del pla nacional de seguretat de les TIC és garantir una Societat de la Informació Segura a Catalunya per a tots i totes, operant un Centre de Seguretat de la Informació de Catalunya, com a eina per a l'execució de les polítiques públiques en seguretat TIC, i la generació d'un teixit empresarial català de suport, aplicacions i serveis de seguretat TIC que sigui referent nacional i internacional.

Els objectius estratègics del Pla nacional d'impuls de la seguretat de les TIC a Catalunya

El Pla s'estructura al voltant de quatre objectius estratègics principals:

1. Establiment d'una estratègia nacional de seguretat TIC.
2. Suport a la protecció de les infraestructures crítiques TIC nacionals.
3. Promoció d'un teixit empresarial català sòlid en seguretat TIC.
4. Increment de la confiança i protecció de la ciutadania catalana en la societat de la informació.

Establiment d'una estratègia nacional de seguretat TIC

El primer objectiu tracta sobre el desenvolupament d'una estratègia global de seguretat de la informació a nivell nacional, política que s'ha de centrar en la necessitat de desenvolupar eines de recerca i de conscienciació del públic en quant al nombre cada vegada més important d'amenaçes i vulnerabilitats de la seguretat en línia, definida per una aproximació multidisciplinària i amb múltiples participants, per una banda, i per una estructura de governança d'alt nivell, per una altra.

Cal definir un *model públic català de seguretat de la societat de la informació* a Catalunya, que adrexi de forma global els reptes que es plantegin en cada moment, que actuï com a interlocutor amb tots els implicats i que tingui una capacitat de resposta real als problemes que es puguin donar, amb un Centre de Seguretat i Resposta a Incidentes com a pal de paller vertebrador del pla nacional de seguretat TIC, que efectuï un anàlisi de risc continuat i vetlli per la integritat i la continuïtat de les xarxes i dels sistemes.

En tot cas, s'ha d'indicar que una aproximació jeràrquica, de dalt a baix, no resulta suficient, sinó que es precisa de la cooperació propera de la indústria i de tots els actors de la societat de la informació, amb el govern com a coordinador dels esforços i activitats requerides. Al contrari, es considera que els governs sols no poden gestionar tots els reptes i qüestions de seguretat, el que implica una necessitat d'involucrar al sector privat i a la societat civil, efecte que es pot aconseguir amb diferents instruments, com les associacions públic-privades, el desenvolupament de millors pràctiques, el subministrament de consell i la participació en òrgans comuns.

Aquest sistema reforçarà iniciatives i programes ja existents, com el sistema públic català de certificació, sota responsabilitat de l'Agència Catalana de Certificació, i l'actuació d'altres òrgans supervisors (comerç, consum, infants i joves, policies públiques, etc).

Suport a la protecció de les infraestructures crítiques TIC nacionals

El segon objectiu estratègic s'orienta a la protecció dels elements que conformen les infraestructures crítiques TIC nacional, incloent-hi les xarxes de comunicacions electròniques, però també els principals elements en que les mateixes es basen, com els sistemes d'energia, i també els principals centres de processament de dades i de prestació de serveis crítics, ja que en aquestes infraestructures d'informació confien els governs, la indústria, els ciutadans i la resta de la societat (com per exemple, l'energia, el subministrament d'aigua, el transport, el sector financer, les telecomunicacions i la salut).

Les conseqüències d'un atac contra els sistemes industrials de control de les infraestructures crítiques podrien ser molt diverses. Es considera que un atac cibernètic causaria poques víctimes o cap, però que podria implicar la pèrdua de serveis d'infraestructura vitals, com per exemple el servei telefònic en què es confia per part dels serveis d'emergència, mentre que atacs contra els sistemes de control d'infraestructures químiques podrien implicar fuites de materials tòxics, que en aquest cas podrien produir víctimes mortals.

D'altra banda, cal indicar que els efectes en cascada poden ser molt danyosos, i provocar grans caigudes dels serveis públics. Alguns supòsits a tractar són els serveis TIC del govern de la Generalitat de Catalunya i dels governs locals de Catalunya, les xarxes dels serveis d'emergències i de protecció civil (a través del número únic 112, Mossos, CECOPALS, bombers, agents rurals, etc.), així com els serveis privats que hi donen suport.

Promoció d'un teixit empresarial català sòlid en seguretat TIC

El tercer objectiu estratègic persegueix la creació d'un teixit empresarial en seguretat TIC a Catalunya, que complementi l'actuació pública en aquesta matèria i potenciï el sector TIC català en un dels mercats emergents.

Aquesta necessitat ha estat manifestada a l'Estudi sobre el Mercat de les TIC a Catalunya⁵ realitzat per la Fundació Observatori de la Societat de la Informació de Catalunya (FOBSIC), que indica com a línia recomanada d'actuació l'impuls a la PIME del sector TIC, emprant la promoció de les certificacions de qualitat i tecnològiques de les empreses del sector mitjançant programes de comunicació de les empreses clients dels beneficis de la certificació, normatives d'obligat compliment en la contractació amb l'administració, suport a programes de formació i certificació en metodologies i processos de prestació de serveis.

En aquest sentit, es promourà la creació d'una xarxa de PIMES per a la prestació de serveis de seguretat i resposta a incidents de seguretat, així com una comunitat en seguretat TIC especialitzada en tots els aspectes de la seguretat, amb una especial atenció a la formació i certificació de professionals, empreses, productes i programari, en aquest cas basant-se en les potencialitats d'un mercat de programari lliure de seguretat, així com de la innovació i la recerca.

Aquesta comunitat s'ha d'emprar com a eina per a la generació de negoci TIC en el territori, i per aquest motiu es considera necessari ubicar-lo en algun espai adient per a aquesta finalitat, com per exemple un parc tecnològic que pugui actuar com a *near-shore* a dintre de Catalunya (en són bons exemples les iniciatives del Camp de

⁵ FOBSIC i Penteo Research, "El Mercat de les Tecnologies de la Informació i la Comunicació a Catalunya: 2007-2010", Març del 2008.

Tarragona o Lleida), com també es recull de l'esmentat Estudi sobre el Mercat TIC a Catalunya.

Increment de la confiança i protecció de la ciutadania catalana en la societat de la informació

El quart objectiu estratègic s'adreça a vetllar per la confiança i la protecció dels ciutadans i ciutadanes en el seu ús de la societat de la informació, amb una atenció especial als col·lectius amb més riscos, com per exemple els infants i els joves, mitjançant l'establiment de programes de conscienciació i suport específicament adreçat a aquests col·lectius.

També s'actuarà en suport de la lluita contra totes les formes de delinqüència informàtica, de forma coordinada amb els agents competents, reforçant les capacitats de detecció i denúncia d'il·lícits de tota mena, filtratge de continguts i anàlisi forense d'evidències electròniques.

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

Per a la consecució dels objectius del Pla nacional d'impuls de la seguretat TIC a Catalunya, la Secretaria de Telecomunicacions i Societat de la Informació de la Generalitat de Catalunya ha d'impulsar la creació del Centre de Seguretat de la Informació de Catalunya (CESICAT), que s'ha de responsabilitzar de l'establiment i seguiment dels programes d'actuació corresponents, sota la direcció estratègica de la Direcció General de la Societat de la Informació, el suport del Centre de Telecomunicacions i Tecnologies de la Informació, i amb la participació directa en el Centre dels governs locals de Catalunya, del sector privat i de la societat civil.

El CESICAT abordarà un programa plurianual d'actuació, dotat inicialment de pressupost públic de la Generalitat de Catalunya, però amb un model de finançament que garanteixi la seva continuïtat mitjançant la prestació de serveis.

Programa d'actuació CESICAT per al període 2009-2013

A continuació es presenta el programa inicial d'actuació del Centre de Seguretat de la Informació de Catalunya, amb 16 línies d'actuació estructurades per objectius estratègics:

1. Objectiu 1: Estratègia nacional de seguretat TIC.

- a. [Actuació 1.1] Establiment d'una estratègia global de seguretat de la informació per a Catalunya: model català de seguretat de la societat de la informació. Qui és qui en seguretat de la informació a Catalunya. Interlocució amb tots els sectors afectats i amb els organismes implicats sectorialment.

- b. [Actuació 1.2] Creació i operació d'un servei de resposta a incidents de seguretat (CSIRT) per a Catalunya, de caràcter universal (administracions públiques, universitats, empreses, ciutadans), que a més actuarà com a catalitzador de la comunitat en seguretat TIC.
 - 1) Serveis reactius.
 - 2) Serveis proactius.
 - 3) Serveis de gestió de la qualitat de la seguretat.

- c. [Actuació 1.3] Anàlisi de riscos amb impacte sobre el desenvolupament de la Societat de la Informació a Catalunya.

- d. [Actuació 1.4] Prestació de serveis de seguretat gestionada per a entitats i col·lectius específics, principalment del sector públic català i PIMES.
 - 1) Servei de detecció i prevenció d'intrusions (IDPS).
 - 2) Servei de gestió de registres (SIEM).
 - 3) Servei de gestió de vulnerabilitats (VMS).

- e. [Actuació 1.5] Suport i foment de la protecció i l'assegurament del domini .CAT i als serveis bàsics d'Internet emprats pels ciutadans (e-mail, web, ftp, altres) quan els proveïdors operen a Catalunya.

2. Objectiu 2: Suport a la protecció de les infraestructures crítiques TIC nacionals.

En col·laboració amb els òrgans competents en matèria de seguretat pública i protecció de les infraestructures crítiques, i dintre de l'àmbit de les competències en TIC de la STSI, s'estima necessari adreçar les següents actuacions:

- a. [Actuació 2.1] Establiment i seguiment d'un pla de protecció d'infraestructures crítiques en TIC governamentals.

- 1) Comunicacions electròniques dels governs.
 - 2) Centres de processament de dades.
 - 3) Coordinació amb òrgans competents, catalans i espanyols, en particular el Centre d'Emergències de Catalunya (CECAT) i el Centre Nacional de Protecció d'Infraestructures Crítiques espanyol.
- b. [Actuació 2.2] Establiment d'una col·laboració públic-privada en relació amb les infraestructures crítiques TIC no governamentals localitzades en territori català, amb un catàleg d'interdependències i mesures de protecció mútua.
3. **Objectiu 3: Promoció d'un teixit empresarial català sòlid en seguretat TIC**, com a eina de política industrial pròpia sobre el sector, especialment adreçada a PIMEs, microPIMEs i professionals autònoms/empresaris individuals⁶ que formen el Mercat TIC Català.
- a. [Actuació 3.1] Creació d'una xarxa nacional de PIMEs especialitzades en seguretat TIC, que prestin serveis de resposta immediata, coordinada i suportada, fins i tot financerament, pel Centre de Seguretat de la Informació de Catalunya.
- b. [Actuació 3.2] Promoció d'una comunitat de seguretat TIC, basada principalment en programari lliure sota el control d'una comunitat de desenvolupadors, dirigida pel Centre de Seguretat de la Informació de Catalunya⁷.
- 1) Productes d'anàlisi de riscos.
 - 2) Productes d'avaluació i seguiment de seguretat.
 - 3) Productes de xifratge.
 - 4) Productes de control parentiu sobre continguts.

⁶ Aquesta política industrial s'ha de coordinar amb altres instruments ja existents, com per exemple el Pla PIMESTIC.

⁷ Es pot proposar l'alliberament de tecnologies de servidor i client ja existents a la Generalitat de Catalunya i als governs locals de Catalunya per formar un nucli inicial que doti a la comunitat de desenvolupadors.

- 5) Productes antivirus, antispam, antiespia, etc.
 - 6) Altres.
- c. [Actuació 3.3] Promoció de l'avaluació i certificació de processos de desenvolupament segur del programari.
- 1) Web segura: OWASP.
 - 2) Codificació segura de programari.
- d. [Actuació 3.4] Promoció de la certificació dels processos de seguretat: ISO 27000.
- e. [Actuació 3.5] Promoció de la formació i certificació de professionals en seguretat TIC i disciplines relacionades.
- 1) Processos de seguretat: ISO 27000.
 - 2) Gerència de seguretat: CISM.
 - 3) Seguretat tècnica: CISSP.
 - 4) Continuitat de negoci: BCP.
 - 5) Bon govern de les TIC: CGEIT.
 - 6) Auditoria de TIC: CISA, COBIT.
- f. [Actuació 3.6] Promoció de la certificació de seguretat de productes: Common Criteria.
- 1) Selecció i avaluació de perfils de seguretat.
 - 2) Producció de perfils de seguretat.
 - 3) Especial atenció als productes adquirits pel govern de la Generalitat de Catalunya i els governs locals de Catalunya.
- g. [Actuació 3.7] Promoció de la recerca i innovació en seguretat TIC.

- 1) Càtedra en seguretat TIC amb alguna Universitat catalana o Centre de recerca especialitzat.
- 2) Publicacions conjuntes Universitat-Empresa-CESICAT.
- 3) Subvencions per a programes de recerca en seguretat TIC (doctorats, etc), i per a publicacions de prestigi.

4. Objectiu 4: Increment de la **confiança i protecció de la ciutadania catalana en la societat de la informació**.

a. [Actuació 4.1] Educació en seguretat i confiança, especialment adreçada als sectors amb més risc, com per exemple els infants i els joves, les persones grans o els consumidors i usuaris.

- 1) Presència els principals portals públics i privats adreçats a públic català, i altres eines sota la filosofia Web 2.0 (e-Catalunya, YouTube).
- 2) Publicació de guies, recomanacions, materials didàctics.
- 3) Actuacions específiques, com actes de sensibilització.

b. [Actuació 4.2] Promoció entre la ciutadania dels instruments de seguretat essencials

- 1) En col·laboració amb l'entitat pública de certificació de Catalunya, foment de l'extensió de l'ús dels certificats electrònics.
- 2) Eines de vigilància i monitoratge instal·lades als ordinadors dels ciutadans – amb el seu consentiment – per detectar amenaces de forma proactiva.
- 3) Eines de còpia de seguretat, xifratge i altres.

Actuació 1.1: Establiment d'una estratègia global de seguretat de la informació per a Catalunya

La primera actuació, i una de les més importants i duradores del pla nacional de seguretat TIC, és l'establiment d'una estratègia continuada i global en relació amb la seguretat de la informació per a Catalunya, i es justifica en la necessitat de realitzar un seguiment ordinari de l'evolució de la problemàtica de la seguretat TIC, per poder donar suport al disseny de polítiques del Govern de la Generalitat de Catalunya i dels governs locals de Catalunya, de forma coordinada.

Els objectius principals de l'estratègia global de seguretat de la informació per a Catalunya són els següents:

1. Prevenir atacs informàtics contra les infraestructures crítiques de Catalunya.
2. Reduir el grau de vulnerabilitat de Catalunya als atacs informàtics.
3. Minimitzar els danys i el temps de recuperació en cas d'atac informàtic.
4. Millorar la capacitat de resposta global de la societat catalana en relació amb els incidents de seguretat.

Es tracta d'una actuació realitzada pel personal del CESICAT, a partir del coneixement de l'entorn i del sector, a partir de la qual s'obtenen lliuraments com els següents:

1. Base de dades sobre actors en seguretat de la informació a Catalunya ("qui és qui" en seguretat), amb la finalitat de coordinar les diferents actuacions del Govern i del CESICAT, i d'informar al públic de les iniciatives existents.
2. Definició d'un model català de seguretat de la informació, en especial alineat amb les polítiques de l'Estat en la matèria, com per exemple l'Esquema Nacional de Seguretat previst per la Llei estatal 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics. Model que es basa en la col·laboració pública i privada, en que han de participar el govern de la Generalitat de Catalunya, els governs locals de Catalunya i la societat civil, mitjançant els corresponents mecanismes de participació.
3. Interlocució i participació en grups de treball, dintre i fora de Catalunya, sobre la seguretat de la informació, per contribuir a formar les polítiques de país.

4. Realització d'anàlisis estratègics, tàctics i de risc sobre l'evolució de la problemàtica de seguretat de la informació, en connexió amb les actuacions de suport a la protecció d'infraestructures crítiques TIC catalanes.
5. Coordinació amb els òrgans competents per raó de la matèria, en totes les actuacions connectades amb els aspectes de seguretat de la informació, com per exemple, els diferents departaments competents, el Cos de Mossos d'Esquadra o l'Agència de Protecció de Dades, entre d'altres.

Actuació 1.2: Capacitat de resposta a incidents de seguretat (CSIRT)

Aquesta actuació consisteix en la formació de capacitat de resposta a incidents de seguretat, mitjançant un CSIRT, que és un equip d'experts en seguretat de les TIC dedicat, de forma principal, a donar resposta a incidents de seguretat informàtica, mitjançant la prestació d'una sèrie de serveis adreçats a ocupar-se d'aquests incidents i ajuda als seus usuaris a recuperar el funcionament ordinari en cas de patir un incident (serveis reactius).

De forma complementària, amb l'objectiu de mitigar els riscos i reduir el nombre d'actuacions de resposta, resulta habitual oferir serveis preventius i educatius (divulgació), publicant avisos sobre vulnerabilitats de programari i maquinari, i informant sobre el programari maliciós i virus que aprofiten aquestes deficiències, de forma que els usuaris puguin corregir els seus sistemes de forma adequada.

La llista de serveis que es considera pot prestar un CSIRT és la següent⁸:

- Serveis reactius, incloent-hi:
 - o Alertes i advertències.
 - o Gestió d'incidents, incloent-hi:
 - Tractament d'incidents.
 - Anàlisi d'incidents.

⁸ Basada en la llista de serveis d'un CSIRT, identificada pel CERT/CC. SEI. Universitat Carnegie Mellon.

- Resposta a incidents *in situ*.
 - Suport en la resposta a incidents.
 - Coordinació de la resposta a incidents.
 - Gestió de vulnerabilitats, incloent-hi:
 - Tractaments de vulnerabilitats.
 - Anàlisis de vulnerabilitats.
 - Coordinació de la resposta a vulnerabilitats.
 - Gestió d'artefactes, incloent-hi:
 - Anàlisi d'artefactes.
 - Resposta a artefactes.
 - Coordinació de la resposta a artefactes.
- Serveis proactius, incloent-hi:
- Comunicats.
 - Observatori de tecnologia.
 - Avaluacions o auditories de la seguretat.
 - Configuració i manteniment de la seguretat.
 - Desenvolupament d'eines de seguretat.
 - Serveis de detecció d'intrusos.
 - Difusió d'informació relacionada amb la seguretat.
- Serveis de gestió de la qualitat de la seguretat, incloent-hi:
- Anàlisi de riscos.
 - Continuitat del negoci i recuperació després de desastres.
 - Sensibilització.
 - Consultoria de seguretat.
 - Educació i formació.
 - Avaluació o certificació de productes.

Resulta important identificar els serveis bàsics que presta un CSIRT, per diferenciar-los d'altres iniciatives del programa i, en particular, dels serveis de seguretat gestionada del CESICAT (SOC).

En aquest sentit, els serveis que es consideren bàsics per a un CSIRT d'aproximació generalista⁹ i que es consideren dintre de l'actuació inicial del CSIRT del CESICAT són els següents:

- Serveis reactius:
 - o Alertes i advertències.
 - o Gestió d'incidents, incloent-hi:
 - Suport en la resposta a incidents.
 - Coordinació de la resposta a incidents.
 - Resposta a incidents *in situ*.
 - Anàlisi d'incidents.
 - o Gestió de vulnerabilitats, en forma de coordinació de la resposta a vulnerabilitats.

- Serveis proactius:
 - o Comunicats.
 - o Auditoria.
 - o Difusió d'informació relacionada amb la seguretat.

- Serveis de gestió de la qualitat de la seguretat:
 - o Sensibilització.
 - o Consultoria de seguretat, en particular en relació amb el desenvolupament de polítiques de seguretat.

⁹ Organizational Models for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon Software Engineering Institute. 2003.

- Educació i formació.

El CSIRT del CESICAT es conceptualitza com un servei universal, adreçat a tots els sectors de Catalunya, amb actuació directa en el cas del sector públic, i indirecta, mitjançant un esquema de col·laboració amb altres agents especialitzats, en el cas del sector privat (inclou ciutadans, empreses i altres organitzacions del sector privat).

En aquest concepte generalista i ampli de CSIRT, s'opta per la prestació a un col·lectiu el més ampli possible, del conjunt de serveis bàsics identificats anteriorment, mentre que altres serveis més avançats, i adreçats a comunitats específiques d'usuaris, es consideren en relació amb l'actuació dels serveis de seguretat gestionada del CESICAT (punt 1.4).

Abast dels serveis de prevenció i resposta a incidents

El CSIRT oferirà nou serveis, agrupats en tres categories:

- Serveis reactius. Es tracta de serveis que són activats per un esdeveniment o sol·licitud, com un informe d'un sistema que ha estat compromès, programari maliciós de difusió àmplia, vulnerabilitats de programari o algun altre esdeveniment detectat per un sistema de detecció d'intrusos o d'auditoria. Els serveis reactius són la part nuclear del treball del CSIRT.

El CESICAT prestarà tres serveis reactius:

- Servei d'alertes i advertències.
- Servei de gestió d'incidències.
- Servei de gestió de vulnerabilitats.

- Serveis proactius. Es tracta de serveis que ofereixen informació i assistència per ajudar a preparar, protegir i assegurar els sistemes dels usuaris en anticipació a atacs, problemes o esdeveniments. Aquests serveis redueix directament el nombre d'incidents futurs de seguretat.

El CESICAT prestarà tres serveis proactius:

- Servei de comunicats.
 - Servei d'auditoria.
 - Servei de difusió d'informació relacionada amb la seguretat.
- Serveis de gestió de la qualitat de la seguretat. Aquests serveis ofereixen suport a serveis ja existents i suficientment establerts, que són independents de la gestió d'incidents, i que tradicionalment han estat executats per altres àrees de l'organització, com per exemple el departament TIC, d'auditoria o de formació. El CSIRT ha d'ajudar en aquests serveis, amb la seva experiència, per incrementar la seguretat global de l'organització, identificant riscos, amenaces i debilitats del sistema. Aquests serveis són normalment proactius però contribueixen indirectament a reduir el nombre d'incidents.

El CESICAT prestarà tres serveis de gestió de la qualitat de la seguretat:

- Servei de sensibilització en seguretat.
- Servei de consultoria de seguretat.
- Servei d'educació i formació.

Servei d'alertes i advertències (reactiu)

El servei d'alertes i advertències consisteix en la disseminació d'informació descriptiva d'atacs d'intrusió, vulnerabilitats de seguretat, virus informàtics i altre programari maliciós, i en oferir recomanacions sobre actuacions a curt termini per tractar amb la problemàtica concreta derivada d'aquestes amenaces.

L'alerta, advertència o el consell concret s'envia en reacció al problema conegut, per notificar als usuaris del servei i per oferir una guia inicial per protegir els sistemes dels usuaris o per recuperar-los en cas d'haver estat afectats per l'amenaça.

La informació de les alertes i advertències pot haver estat creada pel CSIRT o ser redistribuïda de proveïdors tecnològics, altres CSIRTs o experts de seguretat, o fins i tot obtinguda d'altres usuaris.

En concret, en el cas del CESICAT, s'espera obtenir una part important de la informació de les següents fonts:

- Serveis de Seguretat Gestionada del CESICAT.

- CSIRT del Centre Criptogràfic Nacional, de l'Institut Tecnològic de Lleó (INTECO), d'entitats financeres i operadors de serveis de comunicacions electròniques.
- Pàgines web de seguretat.
- Proveïdors tecnològics, com Microsoft, CISCO... i altres fonts.
- Serveis de seguretat de les AAPP catalanes, com el del Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya, o l'Institut Municipal d'Informàtica de Barcelona i d'altres governs locals.

Servei de gestió d'incidents (reactiu)

El servei de gestió d'incidents consisteix en la recepció, selecció i resposta a sol·licituds i informes sobre incidents i esdeveniment de seguretat, i planteja diferents actuacions, en atenció al grau d'intensitat en la participació del CSIRT.

També es preveu la possibilitat de rebre informes d'usuaris en relació amb continguts potencialment delictius o que suposin infracció de la normativa administrativa de seguretat de consumidors, infants, joves, etc. (actuació 4.3 del programa CESICAT).

Les activitats de resposta als incidents previstes pel CESICAT, de menys a més intensitat d'actuació, són les següents:

- Suport en la resposta a incidents.
- Coordinació de la resposta a incidents.
- Suport a incidents *in situ*.
- Anàlisi d'incidents.

Suport en la resposta a incidents

El suport en la resposta a incidents consisteix en l'assistència remota als usuaris que han patit incidents o atacs de seguretat, mitjançant telèfon, correu electrònic o documentació estàndard. Es pot tractar d'assistència tècnica referida a la interpretació de les dades recollides, d'oferir informació de contacte amb terceres organitzacions, o de subministrar informació sobre estratègies de mitigació o recuperació de l'incident.

Es tracta d'una actuació de baixa intensitat, sense presència del personal del CESICAT a les instal·lacions de l'usuari, que resulta més efectiu quan l'usuari disposa de personal amb capacitat per procedir a la resposta, amb suport extern especialitzat.

Coordinació de la resposta a incidents

La coordinació de la resposta a incidents consisteix en actuar com intermediari entre totes les parts involucrades en un incident de seguretat, com la víctima, altres llocs afectats per l'atac i altres llocs que necessitin assistència en l'anàlisi de l'atac. També pot incloure als proveïdors de serveis Internet o TIC de l'usuari afectat, o altres CSIRTs.

Les tasques de coordinació de la resposta a incidents poden incloure la recollida d'informació de contacte, la notificació a llocs atacats o dels que s'origina l'atac, obtenció d'estadístiques sobre el nombre de llocs afectats, i el suport en el intercanvi i anàlisi de dades.

Així mateix, es pot oferir suport a les funcions d'assessoria jurídica, de personal i de relacions públiques de l'usuari, en relació amb els efectes de l'incident, i la coordinació amb les policies, en funció de la rellevància de l'incident, en especial en els casos de descobriment d'actuacions que suposin una presumpta infracció administrativa o penal.

Es tracta d'una actuació d'intensitat moderada, sense presència del personal del CESICAT a les instal·lacions de l'usuari, i més orientada a oferir una resposta global a incidents que afecten a múltiples usuaris, més enllà del suport a la resposta puntual en un usuari concret.

Suport a incidents in situ

El suport a incidents *in situ* consisteix en l'assistència directa, en les instal·lacions de l'usuari afectat per un incident, per ajudar-lo a recuperar-se del mateix, en els casos en que l'usuari no disposi d'un equip total o parcialment dedicat a tasques de recuperació, com a part normal de la seva feina de TIC. El personal del CSIRT

desplaçat a l'usuari analitza físicament els sistemes afectats, recull les dades tècniques de l'incident i efectua la seva reparació i recuperació.

Es tracta d'una actuació d'intensitat elevada, amb presència del personal del CESICAT a les instal·lacions de l'usuari, molt orientada a ajudar a un usuari concret, freqüentment amb pocs recursos especialitzat en TIC.

Aquesta activitat s'ha de veure complementada per la xarxa nacional de resposta a incidències de seguretat (actuació 3.1), per evitar sobrecarregar innecessàriament els recursos del CESICAT, el que impediria assolir altres objectius i suposaria un risc.

Anàlisi d'incidents

L'activitat d'anàlisi d'incidents consisteix en l'examen de tota la informació disponible, i de les evidències electròniques i artefactes relatius a un incident de seguretat, amb l'objectiu de identificar l'àmbit de l'incident, l'extensió de dany causat per l'incident, la seva naturalesa i les estratègies de resposta i recuperació.

El CSIRT pot emprar els resultats dels anàlisi de vulnerabilitats per entendre la problemàtica de seguretat, i oferir la resposta més actualitzada i efectiva possible en relació amb un sistema específic. Hi ha dues activitats importants relacionades amb l'anàlisi d'incidents que cal considerar:

- Recol·lecció d'evidències forenses¹⁰, que consisteix en la recol·lecció, preservació, documentació i anàlisi d'evidències de sistemes que han estat compromesos, per determinar els canvis en els sistemes afectats i assistir en la reconstrucció de la seqüència d'esdeveniments que han generat l'incident. Aquesta tasca s'ha de fer d'acord amb les normes judicials, mitjançant una cadena de custòdia que preservi el valor probatori de les evidències, amb personal preparat per actuar com a pèrit en el procediment judicial corresponent.
- Seguiment i rastreig, que implica determinar des de quin lloc s'ha produït una intrusió o fins quin lloc ha pogut accedir, així com tractar de determinar-ne la

¹⁰ Vegeu, entre altres recursos, la guia NIST SP800-86, sobre integració de tècniques forenses en el procediment de resposta a incidents, d'agost del 2006, o la guia NIST SP800-101, sobre anàlisi forense de telèfons mòbils, de maig del 2007.

identitat, el que exigeix disposar de procediments i acords de col·laboració amb les policies i els prestadors de serveis d'Internet, i processos ràpids d'actuació judicial, per sol·licitar i obtenir les autoritzacions judicials oportunes per a determinats tipus d'actuacions.

L'activitat de recol·lecció d'evidències forenses, i en part l'activitat de seguiment i rastreig, moltes vegades en pot realitzar a distància, però també poden exigir el desplaçament de personal del CESICAT a les instal·lacions de l'usuari. En aquest cas, es tracten de forma global dintre de l'activitat de suport a incidents *in situ*.

Servei de coordinació a resposta de vulnerabilitats (reactiu)

El servei de gestió de vulnerabilitats implica rebre informació i informes sobre vulnerabilitats de maquinari i programari, analitzar la seva naturalesa, mecànica de funcionament i efectes, i desenvolupar estratègies de resposta per detectar-les i reparar-les.

En el cas del CSIRT del CESICAT, el servei de gestió de vulnerabilitats es limita a la coordinació de la resposta a vulnerabilitats, que consisteix en la notificació, als usuaris del CSIRT, de la vulnerabilitat, compartint informació sobre com reparar o mitigar la vulnerabilitat. El CSIRT també verifica que l'estratègia de resposta a vulnerabilitats hagi estat executada amb èxit.

El servei implica comunicació amb els proveïdors de tecnologia, altres CSIRTs, experts tècnics, usuaris i les persones que inicialment varen descobrir o informar sobre la vulnerabilitat. Les activitats concretes a realitzar en el servei inclouen:

- Subministrar informes de vulnerabilitats.
- Coordinar la difusió programada dels documents, informes, pegats o altres solucions.
- Sintetitzar l'anàlisi tècnica realitzada pels diferents actors.
- Mantenir un arxiu o base de coneixement, pública o privada, d'informació de vulnerabilitats i de les corresponents estratègies de resposta.

Servei de comunicats (proactiu)

El servei de comunicats consisteix en la creació i difusió de alertes d'intrusions possibles, advertències relatives a vulnerabilitats i consells de seguretat, per informar als usuaris sobre problemàtiques de seguretat que es poden produir a mitjà o a llarg termini.

Els comunicats permeten als usuaris protegir els seus sistemes i les seves xarxes enfront de noves amenaces abans que aquestes puguin ser explotades per atacants.

Servei d'auditoria (proactiu)

El servei d'auditoria consisteix en realitzar anàlisis, revisions i auditories relatives a l'estat de seguretat dels usuaris, d'acord amb estàndards generalment acceptats.

Les auditories podran tractar sobre els següents aspectes:

- Revisions d'infraestructura: configuracions de maquinari i programari, adreçadors, tallafocs, servidors i dispositius de sobretaula, garantint que compleixen amb les millors pràctiques i polítiques de seguretat.
- Revisió de millors pràctiques: comprovació que les pràctiques de seguretat es troben alineades amb les millors pràctiques.
- Escaneigs: emprant escàners de vulnerabilitats o de programari maliciós per determinar els sistemes que resulten vulnerables.
- Proves de penetració: comprovant la seguretat d'un lloc mitjançant atacs a les xarxes i els sistemes corresponents.

Caldrà valorar els permisos i les autoritzacions necessàries per dur a termini algunes d'aquestes actuacions, tot i que algunes activitats d'escaneig i de penetració poden resultar útils practicades d'ofici, per conscienciar els usuaris de les debilitats dels sistemes.

Servei de difusió d'informació de seguretat (proactiu)

El servei de difusió d'informació de seguretat consisteix en produir, traduir, adaptar i localitzar informació general o específica de seguretat, que sigui completa i fàcilment accessible pels usuaris, amb l'objectiu d'incrementar el nivell de seguretat global.

Aquesta informació pot incloure:

- Guies per informar al CSIRT d'incidències, vulnerabilitats, etc., i la informació de contacte corresponent.
- Arxius d'alertes, advertències i altres anuncis.
- Documentació sobre les millors pràctiques actuals.
- Guies generals sobre seguretat de la informació.
- Polítiques, procediments i llistes de control.
- Informació de desenvolupament i distribució de pegats.
- Enllaços a proveïdors.
- Estadístiques i tendències sobre denúncies d'incidents de seguretat.

La informació de seguretat pot haver estat creada pel CSIRT o ser redistribuïda de proveïdors tecnològics, altres CSIRTs o experts de seguretat, o fins i tot obtinguda d'altres usuaris.

Com succeeix amb les alertes i advertències, molta d'aquesta informació provindrà de les següents fonts:

- CSIRT del Centre Criptogràfic Nacional, de l'Institut Tecnològic de Lleó (INTECO), d'entitats financeres i operadors de serveis de comunicacions electròniques.
- Pàgines web de seguretat.
- Proveïdors tecnològics, com Microsoft, CISCO... i altres fonts.
- Serveis de seguretat de les AAPP catalanes, com el del Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya, o l'Institut Municipal d'Informàtica de Barcelona i d'altres governs locals.

Servei de sensibilització en seguretat (gestió de qualitat de la seguretat)

El servei de sensibilització en seguretat consisteix en un programa estructurat d'actuació adreçada a conscienciar al públic i, en particular, als usuaris del CSIRT, de la necessitat i la importància de la seguretat de la informació, amb l'objectiu de

reduir el nombre d'atacs i incrementar la probabilitat de detecció i denúncia d'atacs, el que contribueix a reduir el temps de resposta i recuperació i els danys.

Es desenvoluparan recursos d'informació, en diversos formats i adreçats a públics diversos, incloent-hi articles, pòsters, cartes, llocs web que expliquin les millors pràctiques i ofereixin consells.

També es realitzaran seminaris i altres esdeveniments públics per informar sobre els darrers desenvolupaments en seguretat i noves amenaces a les organitzacions.

Servei de consultoria i assistència en seguretat (gestió de qualitat de la seguretat)

El servei de consultoria i assistència en seguretat consisteix en oferir suport específic per ajudar a les organitzacions amb les seves necessitats en seguretat de la informació, incloent-hi:

- La preparació de recomanacions o la identificació de requisits per a l'adquisició, instal·lació o configuració segura de sistemes, dispositius de xarxa, programari o processos de negoci de l'organització.
- L'assistència en el desenvolupament de polítiques i pràctiques de seguretat.
- El suport legal necessari per suportar la funció de seguretat, i garantir el compliment normatiu.

Servei d'educació i formació en seguretat (gestió de qualitat de la seguretat)

El servei d'educació i formació en seguretat consisteix en un programa estructurat d'informació i de formació específica de seguretat de la informació, mitjançant seminaris, tallers, cursos i materials docents.

Les matèries consideraran aspectes com la denúncia d'incidents, mètodes de resposta adequats, eines de gestió d'incidències, de prevenció d'atacs, etc.

Actuació 1.3: Anàlisi de riscos amb impacte sobre el desenvolupament de la Societat de la Informació a Catalunya

Aquesta actuació, de caràcter permanent i continuat durant tot el programa del CESICAT, consisteix en la realització d'una anàlisi de riscos TIC que presentin impacte possible sobre el desenvolupament de la Societat de la Informació a Catalunya.

Es tracta, en aquest cas, d'una funció de recopilació i anàlisi d'informacions en relació amb la seguretat, tant de fonts internes como externes – públiques o de pagament – amb la finalitat de disposar de coneixement sobre les principals amenaces TIC que poden afectar a Catalunya.

L'anàlisi de riscos ha de servir per garantir no només el correcte funcionament de les xarxes i sistemes TIC, és a dir, minimitzar les fallades com es contempla en aquesta iniciativa, sinó també per establir prioritats en relació amb les comunicacions entre els operatius de protecció civil en cas d'una gran emergència.

Els resultats d'aquesta anàlisi de risc seran comunicats de forma periòdica al govern de la Generalitat de Catalunya i als governs locals de Catalunya, per a l'establiment de mesures correctives, i serviran per informar les polítiques d'actuació general dels òrgans competents.

Actuació 1.4: Serveis de seguretat TIC gestionada

Aquesta actuació consisteix en la prestació de serveis de seguretat gestionada (freqüentment anomenats "Centre d'operacions de seguretat" o "SOC", en el seu acrònim anglès), que permeten a una organització delegar les funcions de gestió de la seguretat, total o parcialment, al CESICAT.

Un Centre d'operacions de seguretat ofereix una visió en temps real de l'estat de seguretat d'una xarxa i dels sistemes que la componen: analitza, descobreix i prioritza esdeveniments de seguretat, determina possibles amenaces als actius, avaluant-ne el risc i realitza actuacions per a solucionar les problemàtiques detectades, mitjançant alertes, recomanacions o intervencions directes (per

exemple, aplicant pegats sobre programari), en funció del contracte amb el seu client.

Les necessitats de negoci que justifiquen l'existència dels serveis de seguretat gestionada són les següents:

- Reducció del risc i del temps de caiguda dels sistemes i les xarxes.
- Prevenció i control de les amenaces.
- Reducció dels costos administratius en la gestió de la seguretat, especialment quan el Centre d'operacions de seguretat presta serveis a diferents usuaris, de la mateixa o de diferents organitzacions.
- Establiment de procediments efectius d'escalat de problemes de seguretat.
- Suport a la funció d'auditoria i de compliment normatiu.
- Resposta a incidents i recuperació dels efectes del mateixos. Aquesta necessitat s'ha presentat a l'actuació 1.2.

El Centre d'operacions de seguretat rep informació dels sistemes dels usuaris, com els sistemes de detecció d'intrusos, tallafocs, adreçadors, antivirus, gestió de vulnerabilitats, gestió d'accés o aplicacions de bases de dades i de negoci, l'agrega en un únic sistema i la correlaciona, de forma que pugui conèixer l'estat de seguretat de la xarxa i els sistemes, i detectar problemes que requereixen la seva actuació.

A diferència del servei de resposta a incidències de seguretat informàtica, el Centre d'operacions de seguretat ofereix solucions integrals de protecció per a l'organització usuària del mateix, de forma que aquesta organització pot subcontractar una part més o menys important de la seva operació de seguretat.

Els serveis de seguretat gestionada inclouen una àmplia varietat, des de serveis més genèrics i externs, poc intrusius, fins a serveis molt lligats a la infraestructura del client. Alguns serveis típics de seguretat gestionada són els següents:

- Protecció enfront programari maliciós (virus, programari espia, altres).
- Prevenció i detecció d'intrusos, en relació amb xarxes amb fils, xarxes sense fils, comportament de xarxes o sistemes concrets.
- Gestió de vulnerabilitats.
- Gestió de registres de seguretat.

- Inspecció i control d'accés i transmissió de continguts.
- Filtratge i neteja de correu electrònic (SPAM i altres).
- Resposta a incidents, incloent-hi l'anàlisi forense.

Abast dels serveis de seguretat gestionada del CESICAT

El CESICAT oferirà tres serveis de seguretat TIC gestionada:

- Servei de detecció i prevenció d'intrusos (IDPS).
- Servei de gestió de registres de seguretat (SIEM).
- Servei de gestió de vulnerabilitats (VMS).

L'equip professional de seguretat gestionada del CESICAT es dedica al monitoratge i supervisió de la seguretat de les xarxes i els sistemes (equipaments, servidors, aplicacions i altres), oferint suport a l'operació diària dels mateixos, amb una orientació pràctica i emprant eines específiques (com sistemes de detecció i prevenció d'intrusos, sistemes d'obtenció i correlació d'esdeveniments de seguretat, sistemes d'informació de seguretat, de gestió de vulnerabilitats, etc).

El servei de resposta a incidents, que ja s'ha exposat a l'actuació 1.2, també resulta aplicable als usuaris dels serveis de seguretat gestionada, ja que s'intervé directament quan es detecta una incidència, així com a instància d'un usuari.

Servei de detecció i prevenció d'intrusions (IDPS)

La gestió de processos de detecció i prevenció d'intrusions¹¹ és una pràctica de seguretat que s'orienta al tractament rutinari de problemes relacionats amb incidents de seguretat; és a dir, infraccions o amenaces d'infracció immediata de les polítiques i normes de seguretat de la informació, com per exemple programari maliciós, atacants que persegueixen obtenir accés no autoritzat a sistemes o usuaris autoritzats que abusen dels seus privilegis.

¹¹ Vegeu, entre altres recursos, la guia NIST SP-800-94, de febrer del 2007.

La gestió de detecció i prevenció d'intrusos es basa en tecnologies que automatitzen aquests processos, que freqüentment es diferencien en sistemes de detecció d'intrusions (IDS) i sistemes de prevenció d'intrusions (IPS).

Les utilitats principals de les tecnologies de detecció i prevenció d'intrusions són les següents:

1. Identificació d'incidents, mitjançant diverses tècniques, i la seva notificació als responsables de seguretat de la informació:
 - Detecció basada en signatures, que són patrons corresponents a amenaces conegudes.
 - Detecció basada en anomalies, mitjançant perfils de comportaments habituals dels sistemes i les xarxes sobre els que es produeixen desviacions.
 - Detecció basada en l'anàlisi protocol·lària completa, mitjançant perfils generals de protocols benignes sobre els que es produeixen desviacions.
2. Prevenir infraccions de seguretat per part d'usuaris, especialment quan els mateixos són conscients de l'existència de sistemes de detecció i prevenció d'intrusions.
3. Identificació de problemes de qualitat de la seguretat, com per exemple polítiques de seguretat inconsistents.
4. Documentació de les amenaces actuals a l'organització, mitjançant tractaments dels registres de seguretat.

Les funcions clau dels sistemes de detecció i prevenció d'intrusions són les següents:

1. Enregistrament local d'informació de seguretat, que després es pot tractar mitjançant sistemes de gestió de registres de seguretat (SIEM).
2. Notificació dels esdeveniments més importants identificats als responsables de seguretat.
3. Generació d'informes de seguretat.
4. Reacció davant incidents concrets, per exemple, parar l'atac (acabant la connexió de xarxa o la sessió d'usuari que s'utilitza en l'atac, bloquejant

l'accés a la destinació de l'atac, o fins i tot bloquejant tots els accessos a un sistema atacat), modificar l'entorn de seguretat (configurant els tallafocs) o modificar el contingut de l'atac (removent continguts maliciosos adjunts a missatges).

Els tipus principals de sistemes de detecció i prevenció d'intrusions són els següents:

1. Sistemes basats en xarxa, que analitzen el tràfic de les xarxes (segments concrets de xarxa o dispositius concrets) cercant activitats sospitoses. Resulta habitual instal·lar-los a prop de tallafocs o adreçadors exteriors, de servidors de xarxa privada virtual o de servidors d'accés remot.
2. Sistemes sense fils, que analitzen el tràfic de xarxes sense fils, en relació amb els protocols concrets d'aquesta tecnologia.
3. Analitzadors de comportament de xarxa, que analitzen el tràfic de les xarxes per identificar amenaces que generen fluxos anòmals de missatges, com atacs distribuïts de denegació de servei, determinades formes de programari maliciós com els cucs, o infraccions de política de seguretat. Habitualment s'instal·len a les xarxes internes de les organitzacions.
4. Sistemes basats en ordinador (servidor o client), que analitzen el comportament d'un ordinador concret cercant activitat sospitosa. Aquests sistemes poden analitzar els registres del sistema, els processos actius en l'ordinador, les aplicacions, l'activitat del sistema de fitxers i altres. Resulta habitual instal·lar-los en els ordinadors més importants, com els servidors accessibles públicament per la xarxa Internet o els servidors amb informacions sensibles.

El servei ofert pel CESICAT abastarà les anteriors activitats, en funció de les necessitats de cada usuari, amb aportació de les eines necessàries en cada cas, d'acord amb l'anàlisi realitzada per a cada usuari del servei.

Servei de gestió de registres de seguretat (SIEM)

La gestió de registres de seguretat¹² és una pràctica de seguretat cada vegada més important per a les organitzacions, ja que només l'existència d'una funció de gestió

¹² Vegeu, entre altres recursos, la guia NIST SP 800-92, de setembre del 2006.

dels registres de seguretat garanteix que es generen i conserven registres amb suficient informació durant els terminis legalment exigibles.

La revisió rutinària dels registres de seguretat permet identificar incidents de seguretat, infraccions de les normatives de seguretat, activitat fraudulenta i problemes operatius poc temps després de la seva producció, oferint informació molt útil per a la seva investigació i resolució.

Així mateix, els registres de seguretat són importants per realitzar activitats d'auditoria i d'anàlisi forense, el que permet oferir suport a les recerques internes, a l'establiment de línies base de seguretat i a la identificació a llarg termini de tendències operatives i problemes continuats al llarg del temps.

Per una altra banda, s'ha anat incrementant el nombre de lleis i altres normes jurídiques que imposen obligacions de generació i retenció d'evidències forenses en demostració de l'activitat de les organitzacions, com la normativa sobre protecció de dades personals, la normativa administrativa, financera o de serveis de la societat de la informació.

La gestió de registres de seguretat presenta reptes importants, que cal adreçar:

1. Generació i emmagatzematge dels registres de seguretat:

- Moltes fonts de registres de seguretat.
- Inconsistències en els continguts i formats dels registres de seguretat.
- Asincronia de les marques de temps. Possibles problemes per no emprar segellament criptogràfic de data i hora.

2. Protecció dels registres de seguretat:

- Autenticitat dels registres de seguretat.
- Captura indesitjada d'informació sensible (contrasenyes d'usuaris, continguts de comunicacions...), que pot generar problemes legals.
- Accés no autoritzat a registres de seguretat (atac extern, però també intern).

- Alteració o destrucció, accidental o incidental, dels registres de seguretat.
- Disponibilitat dels registres de seguretat (problemes d'espai, temps d'accés...), especialment en cas d'accions antigues. Lliga amb les requisits de retenció d'informacions imposats per la legislació.

3. Anàlisi dels registres de seguretat:

- Baixa prioritat en la revisió dels registres de seguretat, en comparació amb altres activitats de seguretat (com gestió de vulnerabilitats).
- Revisions efectuades per personal insuficientment format i entrenat.
- Absències d'eines per assistir els responsables de les revisions, especialment per identificar patrons de comportament fraudulent.
- Consideració dels registres de seguretat com a eina reactiva, de baix valor en altres casos.

Les funcions clau d'un sistema de gestió de registres de seguretat són les següents:

1. Generació i captura dels registres de seguretat:

- Interpretació i extracció de dades.
- Filtrat d'esdeveniments.
- Agregació d'esdeveniments.

2. Emmagatzematge dels registres de seguretat:

- Rotació de registres de seguretat.
- Arxiu de registres de seguretat, incloent-hi la retenció i la preservació.
- Compensió de registres de seguretat.
- Reducció de registres de seguretat.
- Conversió de registres de seguretat.
- Normalització de registres de seguretat.
- Comprovació d'integritat de registres de seguretat.

3. Anàlisi dels registres de seguretat:

- Correlació d'esdeveniments.
- Revisió de registres de seguretat.
- Informes sobre registres de seguretat.

4. Disposició (eliminació) dels registres de seguretat.

En conseqüència amb el que s'ha exposat, es considera molt important ajudar a les organitzacions a establir programes de gestió de registres de seguretat, amb els següents continguts:

1. Determinació de les prioritats de la gestió de registres de seguretat de forma adequada i horitzontal a tota l'organització.
2. Establiment polítiques i pràctiques en relació amb la gestió de registres de seguretat.
3. Creació i manteniment d'una infraestructura de gestió segura de registres de seguretat, amb una organització i unes funcions adequades a les necessitats.
4. Formació i suport adequats al personal amb responsabilitats sobre la gestió de registres de seguretat.

El servei ofert pel CESICAT abastarà les anteriors activitats, en funció de les necessitats de cada usuari, amb aportació de les eines necessàries en cada cas, d'acord amb l'anàlisi realitzada per a cada usuari del servei.

Servei de gestió de vulnerabilitats de seguretat (VMS)

La gestió de vulnerabilitats de seguretat¹³ és una pràctica de seguretat orientada a la reducció proactiva de l'explotació de vulnerabilitats de productes de tecnologies de la informació que s'utilitzen en les organitzacions, el que redueix el nombre d'incidents de seguretat i, per tant, el cost.

¹³ Vegeu, entre altres recursos, la guia NIST SP 800-40v2, de novembre del 2005.

Algunes vulnerabilitats es poden fixar mitjançant l'aplicació de pegats o actualitzacions de l'aplicació que les pateixen, mentre que altres s'han d'adreçar mitjançant altres remeis, com canvis en la configuració dels sistemes i de les aplicacions, formació adequada dels usuaris de les aplicacions o fins i tot mitjançant la progressiva substitució dels programes que ja no disposen de manteniment.

L'actualització periòdica del programari es considera una de les millors pràctiques per garantir la seguretat informàtica, però cada vegada resulta més difícil per a les organitzacions fer el seguiment i aplicació dels pegats i les actualitzacions del programari, especialment en el programari que suporta operacions crítiques.

Aquesta situació aconsella que les organitzacions implementin programes sistemàtics, mesurables i documentats per a la gestió de vulnerabilitats, sota la responsabilitat d'un equip concret, freqüentment amb suport extern especialitzat.

Algunes de les funcions d'un equip de gestió de vulnerabilitats són les següents:

1. Inventariar els recursos TI de l'organització per determinar quin maquinari i programari (sistemes operatius i aplicacions) s'utilitzen.
2. Monitorar fonts d'informació de seguretat per conèixer anuncis de vulnerabilitats, remeis basats en pegats i altres solucions, i amenaces emergents corresponents al programari emprat per l'organització.
3. Establir prioritats en relació amb l'ordre de solució de les vulnerabilitats.
4. Crear una base de solucions a aplicar a l'organització.
5. Realitzar proves de remeis basats en pegats i altres solucions en dispositius TI que empen configuracions normalitzades.
6. Supervisar l'aplicació de les solucions a les vulnerabilitats.
7. Distribuir informació sobre vulnerabilitats i els seus remeis als administradors locals.
8. Realitzar la instal·lació automàtica de pegats en dispositius TI emprant eines especialitzades.
9. Configurar l'actualització automàtica de les aplicacions, quan sigui possible i apropiat.
10. Verificar el remeis a les vulnerabilitats mitjançant escanejors de xarxa i de sistema.

11. Formar als administradors en l'aplicació de remeis per a les vulnerabilitats.

Els programes de gestió de vulnerabilitats consten dels següents elements:

1. Establiment de l'equip responsable de la gestió de vulnerabilitats.
2. Utilització d'eines automàtiques d'actualització de pegats per facilitar-ne la instal·lació als sistemes afectats per vulnerabilitats.
3. Determinació de les fases d'aplicació del programa de gestió de vulnerabilitats.
4. Assessorament i mitigació dels riscos associats amb les eines automàtiques d'actualització de pegats.
5. Anàlisi de l'ús de configuracions normalitzades dels sistemes TI.
6. Mesura de l'efectivitat del programa de gestió de vulnerabilitats.

El servei ofert pel CESICAT abastarà les anteriors activitats, en funció de les necessitats de cada usuari, amb aportació de les eines necessàries en cada cas, d'acord amb l'anàlisi realitzada per a cada usuari del servei.

Actuació 1.5: Suport i foment de la protecció i l'assegurament del domini .CAT i dels serveis bàsics d'Internet

Aquesta actuació consisteix en un programa especial d'actuació que ha d'oferir suport particular als serveis bàsics d'Internet, quan els proveïdors operen a Catalunya, amb especial atenció al domini .CAT.

Tot i que la responsabilitat de la seguretat dels serveis Internet prestats a Catalunya és dels operadors, es considera necessari establir un diàleg amb els principals operadors, analitzar conjuntament les principals problemàtiques de seguretat TIC i establir actuacions de suport i foment que ajudin als operadors a millorar els seus nivells de seguretat, segons s'escaigui.

Les actuacions a valorar es podran referir a la millora dels serveis de correu electrònic lliure d'SPAM i programari maliciós, seguretat del DNS, tècniques per prevenir la pesca pirata i altres, mitjançant l'avaluació de tècniques de seguretat proposades com Sender ID, DKIM, l'ús de filtres.

S'impulsarà l'establiment d'un programa de col·laboració per a l'intercanvi d'informació sobre incidents de seguretat, i de suport des del servei de resposta a incidents de seguretat descrit a la línia 1.2 del programa CESICAT.

Actuació 2.1: Establiment i seguiment d'un pla de protecció d'infraestructures crítiques en TIC governamentals

Aquesta actuació té per objectiu la millora dels nivells de seguretat de les TIC propietat del govern de la Generalitat de Catalunya i dels governs locals de Catalunya, avaluant la seva importància, per determinar la consideració d'infraestructura crítica i dissenyant un pla per assolir el nivell de protecció corresponent a aquesta consideració.

En l'àmbit de la Generalitat de Catalunya, es catalogaran i revisaran els sistemes de comunicacions electròniques propietaris, així com els centres de processament de dades, i es coordinaran les actuacions amb els òrgans competents en aquesta matèria, en especial el Centre Nacional de Protecció d'Infraestructures Crítiques espanyol, adscrit al Ministeri de l'Interior i el Centre d'Emergències de Catalunya (CECAT).

Les actuacions seran efectuades per la Direcció General d'Infraestructures de Telecomunicacions i el Centre de Telecomunicacions i Tecnologies de la Informació, amb el suport del CESICAT.

En l'àmbit dels governs locals de Catalunya, el CESICAT oferirà el suport necessari per a la identificació de les infraestructures crítiques TIC, l'establiment de plans d'assegurament i la implantació i seguiment de mesures de seguretat per a les esmentades infraestructures.

Actuació 2.2: Col·laboració público-privada en relació amb les infraestructures crítiques TIC no governamentals localitzades en territori català

Aquesta actuació resulta complementària a l'actuació 2.1 del programa CESICAT, centrant-se en l'establiment d'una col·laboració entre el sector públic i el sector privat, per a la millora de la seguretat de les infraestructures crítiques TIC propietat del sector privat que estiguin ubicades en territori català.

En cas de fallida dels serveis, també s'hauria de prioritzar la recuperació de les xarxes i sistemes de què depenen els serveis d'emergència i contemplar la possibilitat d'ampliar el tractament especial que contempla aquesta actuació a infraestructures crítiques que no estiguin localitzades en territori català sempre que sigui tècnica i normativament viable (força fonts d'informació emprades durant la resolució d'una emergència resideixen en servidors web externs, com les fitxes de substàncies perilloses que manté el govern basc, per exemple). Caldria, doncs, definir servidors crítics o d'especial interès per a la protecció civil, i avaluar altres línies d'actuació complementàries.

En aquest cas, el CESICAT realitzarà actuacions de conscienciació de les parts, constituirà una mesa de diàleg permanent en aquesta matèria, i oferirà suport per a la realització dels plans i actuacions que es determinin necessaris per les parts a la mesa.

Actuació 3.1: Creació d'una xarxa nacional de PIMEs especialitzades en seguretat TIC

Aquesta actuació consisteix en la creació d'una xarxa catalana de PIMEs que garanteixi l'existència de punts suficient d'atenció i suport a ciutadans, entitats, empreses i administracions públiques a la totalitat del territori nacional.

Es tracta de complementar l'actuació de l'equip de resposta a incidents de seguretat del CESICAT, de forma que es pugui garantir, mitjançant la col·laboració amb el sector privat, la resposta real a qualsevol incidència de seguretat.

Com s'ha exposat en l'actuació 1.2 del programa, el CESICAT prestarà serveis universals de resposta a incidents de seguretat de la informació, mitjançant diversos instruments i actuacions, i d'acord amb una política de selecció d'incidents en atenció a la seva gravetat, però no podrà atendre a totes les incidències possibles, precisament degut a la seva orientació de servei universal.

Amb la creació d'aquesta xarxa de col·laboradors, el CESICAT pretén oferir una garantia d'assistència *in situ* realista, per part del sector privat, degudament coordinat i, en funció de l'anàlisi de mercat que es realitzi, finançada parcialment pel Centre.

Així mateix, amb la xarxa de col·laboradors, el CESICAT contribueix a l'aparició de serveis privats que puguin prestar assistència més continuada als diferents col·lectius, potenciant l'oferta de serveis TIC catalana i actuant directament, d'acord amb el principi de subsidiarietat, en els col·lectius que queden exclosos del mercat.

La xarxa de col·laboradors estarà formada per PIMEs homologades pel CESICAT, amb la voluntat de garantir un suficient nivell de seguretat, qualitat i temps de resposta màxim garantit en la prestació del servei, i l'establiment d'un marc tarifari consistent per a tot el territori.

Actuació 3.2: Promoció d'una comunitat de desenvolupament d'eines de seguretat TIC

Aquesta actuació consisteix en la promoció, per part del CESICAT, d'una comunitat de desenvolupament d'eines de seguretat TIC, basada principalment en programari lliure, que permeti a les PIMEs catalanes accedir al mercat de solucions de seguretat sense les barreres de cost dels programaris subjectes a llicència comercial¹⁴.

Existeixen excel·lents productes de seguretat TIC en el món del programari lliure, que es poden potenciar perquè serveixin de base a la implantació de seguretat per part d'empreses, administracions públiques i ciutadans, amb el suport de PIMEs

¹⁴ El fet que les solucions promogudes siguin principalment de programari lliure en cap cas implica una renúncia a l'ús d'eines sota llicència per part del CESICAT o dels seus col·laboradors.

d'orientació generalista a la informàtica de gestió, o d'orientació més especialitzada a la seguretat TIC.

Aquestes solucions poden resultar adequades per a moltes entitats, públiques i privades, quan el corresponent procés d'anàlisi de risc no ho desaconselli, i per tant impulsar l'adopció d'aquestes eines pot ajudar al mercat a oferir nous serveis, i als clients a incorporar solucions de seguretat sense que el factor preu de llicència sigui una barrera.

En aquest sentit, cal esmentar que algunes Universitats catalanes han produït eines de seguretat TIC, que es poden reutilitzar, compartir o fomentar per tal de crear oferta de qualitat en relació amb la seguretat.

Per una altra banda, el foment d'una comunitat de desenvolupament d'eines de seguretat TIC pot ajudar a incrementar el coneixement de les eines i metodologies, així com la qualitat, constituint al CESICAT en centre d'excel·lència referent.

Algunes de les eines que s'identifiquen com possible objecte de treballa de la comunitat són:

- Eines d'anàlisi de risc, basades en metodologies ja existents (MAGERIT, OCTAVE) o *ad hoc*, específiques d'un sector concret.
- Eines d'avaluació i seguiment de la seguretat (com, per exemple, OSSIM).
- Eines de xifratge.
- Eines de control parentiu.
- Eines contra el programari maliciós.

Caldrà avaluar en cada cas l'oportunitat i l'interès, per a la societat catalana, de fomentar el desenvolupament d'uns tipus o altres d'eines, en funció de l'anàlisi de risc corresponent (actuació 1.1 i 1.3 del programa CESICAT).

Actuació 3.3: Promoció de l'avaluació i certificació de processos de desenvolupament segur del programari

Aquesta actuació consisteix en la promoció de l'avaluació i la certificació dels processos de desenvolupament segur del programari, l'anomenada "garantia del programari" (*software assurance*, en anglès), com a línia d'actuació a mig i llarg termini que, a través de la millora de la qualitat del programari, ajudi a reduir el volum de vulnerabilitats del mateix.

Algunes línies a fomentar són les següents:

- Web segura: Seguretat en el desenvolupament d'aplicacions web, principalment d'acord amb les recomanacions de la Fundació OWASP.
- Codificació segura: Seguretat en el desenvolupament d'aplicacions emprant llenguatges Java, C, C++, etc. d'acord amb els estàndards de bones pràctiques d'entitats com el Carnegie Mellon CyLab, SEI o altres.

En relació amb les anteriors línies, es considera important abordar tasques relatives a:

- Divulgació de metodologies, millors pràctiques, conscienciació d'usuaris.
- Formació en metodologies¹⁵.
- Suport a la certificació de processos.
- Suport a la realització de proves de qualitat de programari segur.

Actuació 3.4: Promoció de la certificació dels processos de seguretat: ISO 27000

Aquesta actuació consisteix en la promoció de la certificació dels processos de seguretat, principalment al voltant de la norma internacional ISO 27000, que ajuda a les organitzacions a establir formalment el procés de seguretat de la informació, seleccionar una sèrie de controls mínims de seguretat, aplicar-los i, posteriorment, certificar el seu compliment.

La certificació de processos de seguretat amb ISO 27000 aporta a les empreses i administracions pública que l'aplica una visió integral de la seguretat integrada en la gestió ordinària i, per tant, contribueix a l'adopció de seguretat en el dia a dia.

¹⁵ En col·laboració amb entitats especialitzades.

El serveis a oferir són els següents:

- Divulgació de la norma, dels seus beneficis i com adoptar-la.
- Formació sobre la norma¹⁶.
- Suport a la certificació de processos i de professionals.

Actuació 3.5: Promoció de la formació i certificació de professionals en seguretat TIC

Aquesta actuació consisteix en la promoció del sector professional i de PIME que dona suport al mercat, en relació amb totes les qüestions de seguretat TIC, com a pressupost perquè el mercat pugui oferir els serveis corresponents als seus clients.

En aquest cas, es manifesta que la falta de formació adequada dels professionals pot ser una barrera per a l'adopció efectiva de seguretat per part de les empreses. En aquest sentit, la certificació dels professionals resulta un element clau per aconseguir un programa realment efectiu de seguretat TIC per a Catalunya.

Per una altra banda, l'Estudi sobre el Mercat TIC a Catalunya realitzat per la Fundació Observatori de la Societat de la Informació a Catalunya (FOBSIC) posa de manifest la necessitat d'incrementar el nombre de professionals certificats, que s'identifica com un dels àmbits d'actuació recomanats¹⁷ per l'esmentat informe.

Algunes de les certificacions de seguretat TIC que es promouran són les següents:

- Certificació sobre processos de seguretat: ISO 27000.
- Certificació sobre gerència de seguretat: CISM.

¹⁶ En col·laboració amb entitats especialitzades.

¹⁷ En concret, l'àmbit d'actuació recomanat número 3, sota el títol "Millora de la capacitat professional TIC", identifica "actuacions per facilitar l'existència de professionals TIC capacitats a les empreses del sector TIC català, i la contínua adequació dels perfils professionals a les necessitats canviants de les empreses catalanes".

- Certificació sobre seguretat tècnica: CISSP.
- Certificació sobre continuïtat de negoci: BCP.
- Certificació sobre bon govern de les TIC: CGEIT.
- Certificació sobre auditoria de TIC: CISA, COBIT.

Les actuacions a realitzar inclouen les següents:

- Determinació de les certificacions professionals de seguretat més demandades pel sector TIC català.
- Divulgació dels beneficis de les certificacions professionals.
- Formació de professionals¹⁸.
- Suport a la certificació de professionals.

Actuació 3.6: Promoció de la certificació de seguretat de productes: Common Criteria

Aquesta actuació consisteix en la promoció de la certificació de productes de seguretat, d'acord amb la norma ISO 15408, coneguda com a Criteris Comuns.

La certificació de seguretat és un procediment legal en virtut del qual un prestador o fabricant pot acreditar el compliment dels requisits establerts per una norma concreta o especificació tècnica, que normalment desenvolupa una norma jurídica que defineix requisits o recomanacions de caire tècnic. Aquesta certificació s'obté dintre de l'Esquema Nacional d'Avaluació i Certificació de la Seguretat.

La certificació pot ser obligatòria per poder prestar el servei o subministrar el producte, o voluntària. En aquest segon cas, l'obtenció del certificat aporta el benefici de no haver d'acreditar cada vegada que el servei o el producte compleix els requisits tècnics exigits.

¹⁸ En col·laboració amb entitats especialitzades.

Un esquema nacional d'avaluació i certificació de la seguretat de les tecnologies de la informació és l'organització sistemàtica de les funcions d'avaluació i certificació de la seguretat dins d'un país concret, sota l'autoritat d'un consell de direcció o d'una entitat de certificació de la seguretat, amb l'objecte d'assegurar que es mantenen uns alts nivells de competència i d'imparcialitat i que s'aconsegueix la coherència global del sistema.

Els esquemes nacionals es creen a l'empara de l'Acord de reconeixement mutu sobre els certificats d'avaluació de la seguretat de les tecnologies de la informació, de 26 de novembre de 1997, aprovat pel grup d'alts funcionaris en seguretat dels sistemes d'informació de la Comissió Europea, d'acord amb el mandat contingut al punt tercer de la Recomanació del Consell 95/144/CE, de 7 d'abril de 1995.

Inicialment centrat en la certificació de producte d'acord amb els criteris d'avaluació de la seguretat de les tecnologies de la informació (ITSEC) de 1991, actualment els estats signataris de l'Acord també han acollit els anomenats criteris comuns per a l'avaluació de la seguretat de les tecnologies de la informació (Common Criteria o CC, ISO 15408), mitjançant la modificació de l'Acord de 1997, així com la signatura de l'Acord sobre el reconeixement dels certificats de criteris comuns en el camp de la seguretat de la tecnologia de la informació de 23 de maig de 2000.

L'esquema nacional d'avaluació i certificació de la seguretat de les tecnologies de la informació funciona de la manera següent:

- L'esquema nacional és dirigit per un únic organisme de certificació, d'acord amb una política establerta pel propi organisme de certificació o per un consell de direcció de l'esquema nacional, que han de crear i fer complir els reglaments operatius de l'esquema nacional.
- L'organisme de certificació ha de ser un organisme independent, declarat competent per una norma legal o administrativa, o bé acreditat per una entitat d'acreditació nacional. En qualsevol cas, ha de complir els requisits EN 45011 o Guia ISO 65 o els requisits descrits a l'annex C de l'Acord ITSEC.
- L'organisme autoritza la participació dels serveis d'avaluació de l'esquema, en controla el funcionament i l'activitat d'avaluació, examina tots els informes d'avaluació, elabora un informe de certificació respecte a cada avaluació i publica els certificats i els informes de certificació, així com una llista de productes certificats.
- El servei d'avaluació, a més de ser autoritzat per l'organisme de certificació, ha de ser prèviament acreditat per una entitat d'acreditació

nacional, excepte si ha estat creat i declarat competent per una norma legal o administrativa. En qualsevol cas, ha de complir els requisits EN 45001 o Guia ISO 25.

El Centre Criptològic Nacional ha estat nomenat pel Reial decret 421/2004 l'òrgan competent de certificació de l'esquema nacional d'avaluació i certificació de la seguretat de les tecnologies de la informació.

Les actuacions a realitzar inclouen les següents:

- Selecció i avaluació de perfils de seguretat, en atenció a les prioritats identificades.
- Producció de perfils de seguretat, en funció de les necessitats principals dels governs catalans.
- Es prestarà particular atenció als productes adquirits pel govern de la Generalitat de Catalunya i els governs locals de Catalunya, com a forma d'adopció de productes segurs.

Actuació 3.7: Promoció de la recerca i innovació en seguretat TIC

Aquesta actuació consisteix en la promoció de la recerca i el desenvolupament en matèria de seguretat de la informació, que és una de les polítiques més habituals dels Estats avançats en la cultura de la seguretat, especialment pel impacte posterior en la competitivitat de les empreses productores de tecnologies de seguretat, que comercialitzen els seus productes en el mercat global.

A Catalunya disposem de diversos grups de recerca en aquesta matèria, dels quals tres són grups consolidats de recerca (CRISES – Universitat Rovira i Virgili¹⁹, KISON – Universitat Oberta de Catalunya, i ISG – Universitat Politècnica de Catalunya), amb els quals es poden establir relacions de col·laboració o programes de recerca.

¹⁹ A més, CRISES lidera el projecte ARES – Advanced Research on Information Security and Privacy, finançat dintre del programa CONSOLIDER INGENIO 2010.

Algunes de les propostes²⁰ en recerca en seguretat TIC que el CESICAT pot promoure, de forma coordinada amb les actuacions del Pacte Nacional per a la Recerca i la Innovació (PNRI) de Catalunya²¹, són les següents:

1. Criptografia, a partir de la seva consideració com un dels elements fonamentals de la seguretat de la informació. La necessitat de continuar els esforços de recerca en aquesta àrea deriva de l'aparició constant de noves amenaces als mecanismes ja existents, així com de l'aparició de tecnologies i escenaris emergents. Un exemple pràctic de l'impacte d'aquesta problemàtica és la posada en risc del valor de les signatures electròniques en que es basa, de forma cada vegada més important, en el comerç electrònic i en l'administració electrònica.

Dintre d'aquesta proposta, caldria treballar aspectes com el desenvolupament de noves funcions de resum criptogràfic (*hash functions*), d'algorismes de xifra basats en corrents de dades eficients i segurs (*stream cipher*), d'algorismes criptogràfics d'alta velocitat (aplicables en entorns de comunicacions de sistemes de control de processos amb elevats volums de transmissions de dades), criptografia de baix consum d'energia (per dispositius RFID, per exemple), criptografia per a computació ubiqua (*pervasive computing*), seguretat a llarg termini (aplicable a arxius de llarga durada de documents autèntics, per exemple) i per a obtenir més privacitat efectiva i possibilitats d'exercici en l'entorn electrònic dels drets de les persones, com el vot electrònic.

2. Seguretat de la infraestructura d'adreçament i gestió de noms d'Internet. La necessitat d'actuar en aquestes àrees deriva del disseny inicialment insegur de la xarxa Internet, el que obliga a continuar treballant en trobar solucions eficients a aquesta problemàtica. Pel que fa a la seguretat en l'adreçament, cal treballar en la seguretat dels diferents tipus de protocols emprats (com IGP, EGP o BGP). En relació amb la gestió de noms, cal adreçar les diferents problemàtiques referides a la seguretat del DNS, mitjançant eines específiques, polítiques de seguretat adequades i més recerca aplicada als

²⁰ Overview of Current Developments in Network and Information Security Technologies. ENISA/TD/ST/D(2007)0006. European Network and Information Security Agency. 2007.

²¹ En aquest sentit, el Document de Bases del Comitè Permanent d'experts del Pacte Nacional per a la Recerca i la Innovació recull de forma expressa la necessitat d'impulsar la recerca sobre la seguretat de la informació, dintre de l'eix de focalització en recerca capdavantera – punt 12: la transversalitat de les TIC.

nous tipus d'atacs a la infraestructura global de DNS, com els atacs distribuïts de denegació de servei i altres.

3. Seguretat en el negoci electrònic. Lluita contra les comunicacions comercials no sol·licitades (SPAM), amb una orientació global de recerca relativa a tots els aspectes d'aquesta problemàtica de seguretat: en particular, pesca pirata (*phishing*), enverinament de pàgines, el robatori d'identitat (*identity theft*) i la suplantació d'identitat (*spoofing*). S'ha de treballar tant en les noves eines de protecció del correu electrònic i dels clients web, com en totes les qüestions relatives a mitigar l'enginyeria social com a vector d'atac.
4. Seguretat en entorns de-perimetrals. Els nous entorns de negoci, basats en xarxes obertes, un elevat grau de mobilitat dels usuaris, externalització de serveis o integració de processos de negoci mitjançant serveis web, genera nous reptes de seguretat. S'ha de potenciar la recerca en tots els aspectes de la seguretat d'extrem final (*endpoint security*), així com altres tècniques emergents de seguretat de-perimetral.
5. Computació fiable (*trusted computing*). Es considera també necessari fomentar la recerca en dispositius i polítiques de seguretat relatius a computació fiable, que cada vegada s'utilitzen més en els escenaris de descàrregues segures, actualització de programari, comunicacions segures, emmagatzematge segur, identificació fiable de perifèrics, signatures electròniques o control d'accés.
6. Biometria. Es tracta d'una tecnologia relativament nova, que es pot emprar en gran quantitat d'aplicacions, tant en governs com en la indústria, i que planteja reptes que encara exigeixen recerca, tant en els seus aspectes tecnològics (reducció de la taxa de falsos negatius i falsos positius), com organitzatius (registre de les dades biomètriques), com ètics i legals (especialment en relació amb la protecció de les dades personals).

Les actuacions a realitzar inclouen les següents:

- Creació d'una càtedra en seguretat TIC amb alguna Universitat catalana o Centre de recerca especialitzat.
- Publicacions conjuntes Universitat-Empresa-CESICAT.

- Subvencions per a programes de recerca en seguretat TIC (doctorats, etc), i per a publicacions de prestigi.

Actuació 4.1: Educació en seguretat i confiança en col·lectius amb riscos especials

Aquesta actuació consisteix en educar i formar amb particular intensitat a determinats col·lectius, que presenten riscos particulars, com poden ser els infants, els adolescents, la gent gran o les persones sense feina, que també es relacionen amb la xarxa, i que sovint es troben afectats per amenaces i atacs concrets.

En aquest sentit, des del CESICAT s'abordaran programes específics de conscienciació i educació a aquests públics, de forma coordinada amb altres organismes i entitats²² que ja dediquen recursos a aquesta tasca. La noció en aquest cas és potenciar les actuacions d'aquestes entitats, i contribuir amb programes propis del CESICAT.

Les actuacions a realitzar, moltes vegades en règim de col·laboració amb altres entitats, inclouen les següents:

- Presència als principals portals públics i privats adreçats a públic català, i altres eines sota la filosofia Web 2.0 (e-Catalunya, YouTube).
- Publicació de guies, recomanacions, materials didàctics específics per a cada col·lectiu identificat.
- Actuacions específiques, com actes de sensibilització adreçats a aquests col·lectius.

²² Resulta obligat esmentar la feina que des de fa temps realitza el cos dels Mossos d'esquadra, el programa Internet Segura, auspiciat per IQUA, el programa Protegelos, el programa Pantallas Amigas, auspiciat entre d'altres per la Fundació Esplai, i altres moltes bones iniciatives, tot i que encara es considera necessari incidir en aquesta problemàtica.

Actuació 4.2: Promoció entre la ciutadania dels instruments de seguretat essencials

Aquesta actuació consisteix en la promoció de l'ús d'instruments de seguretat essencials entre la ciutadania, com a programa específic de conscienciació i sensibilització, per incrementar l'autoprotecció dels equips de ciutadans, PIMEs i altres petites organitzacions.

Les actuacions a realitzar són les següents:

- En col·laboració amb l'entitat pública de certificació de Catalunya, foment de l'extensió de l'ús dels certificats electrònics.
- Difusió, formació i, eventualment, subministrament d'eines de vigilància i monitoratge instal·lades als ordinadors dels ciutadans – amb el seu consentiment – per detectar amenaces de forma proactiva.
- Difusió, formació i, eventualment, subministrament d'eines de còpia de seguretat, xifratge i altres que es considerin necessàries.

CESICAT – Catàleg de serveis 2009

A continuació es presenta el catàleg de serveis que prestarà el CESICAT durant el 2009:

Unitat de prevenció i resposta a incidents de seguretat TIC:

- Servei de prevenció i formació en seguretat TIC [actuacions 1.1, 1.2, 4.1, 4.2].
 - o Difusió de comunicats en seguretat TIC, de forma preventiva.
 - o Programes de conscienciació en seguretat.
 - o Guies de seguretat TIC.
 - o Programa de gestió de llistes de configuració segura de sistemes TIC.
 - o Cursos de seguretat de la informació (EAPC, Universitats, altres).
 - o Tallers pràctics sobre eines, metodologies i altres.
 - o Servei d'alertes i advertències sobre seguretat i vulnerabilitats TIC.

- Servei de resposta a vulnerabilitats i a incidències sobre seguretat TIC: denegacions de servei, programari maliciós, accés no autoritzat, ús incorrecte de sistemes o combinacions dels anteriors [actuació 1.2].
 - o Assistència remota (contenció, solució i recuperació).
 - o Assistència *in situ* (anàlisi forense, contenció, solució i recuperació).
 - o Coordinació amb tercers.
 - o Anàlisi d'incidentes (en laboratori).
 - o Base de coneixement de vulnerabilitats i estratègies de resposta.

Unitat de serveis professionals en seguretat TIC:

- Servei d'anàlisi preventiva en seguretat TIC [actuació 1.4].
 - o Superfície.
 - o Penetració.
 - o Infraestructura.
 - o Millors pràctiques.

- Servei de consultoria de seguretat TIC.
 - o Anàlisi de riscos [actuacions 1.1 i 1.3].
 - o Programes de gestió de la seguretat [actuacions 1.1, 2.1 i 2.2].
 - o Suport a la adquisició i gestió d'infraestructura de seguretat.

- Servei d'assessorament jurídic especialitzat en seguretat TIC [actuació 1.1, 1.2, 1.3, 2.1, 2.2, 4.1].
 - o Aspectes jurídics dels programes de seguretat: laborals, penals, administratius. Tractament d'evidències electròniques (aspectes legals d'informàtica forense).
 - o Guies i recomanacions legals.
 - o Protocols de col·laboració amb policies i organismes responsables de seguretat nacional i infraestructures crítiques.

Altres actuacions

- Memòria anual del CESICAT.
- Informes sobre l'estat de seguretat TIC a Catalunya (per col·lectius específics).