IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monogràfic «V Congrés Internet, Dret i Política (IDP). Cara i creu de les xarxes socials»

ARTICLE

Les polítiques públiques en matèria de seguretat a la societat de la informació

Ignacio Alamillo

Data de presentació: setembre de 2009
Data d'acceptació: novembre de 2009
Data de publicació: desembre de 2009

Resum
La majoria dels estats es troben en el procés d'establir una aproximació basada en múltiples participants –a banda dels mateixos governs– i una estructura de governança d'alt nivell per a la implementació de polítiques d'abast nacional.
En aquest sentit, aquests estats han fet avenços importants en el desenvolupament de marcs nacionals de polítiques de seguretat, així com han aprovat mesures per a combatre el cibercrim i han establert equips de resposta a incidències de seguretat informàtica. Aquest article presenta les principals polítiques i actuacions públiques per a la promoció de la seguretat de la informació, i se centra específicament en les actuacions realitzades a Catalunya i a l'Estat espanyol en aquesta matèria.

Paraules clau
polítiques públiques de seguretat, cibercrim, seguretat de la informació

Tema
Protecció de dades

Public Security Policies in the Information Society

Abstract
Most countries are in the process of reaching agreement among multiple participants – apart from the governments themselves – establishing a high level management structure for the implementation of national policies.
Major advances have been made in the development of national frameworks for security policies, measures for combating cybercrime have been approved, and response teams for security issues have been established. This article presents the main public policies and legal proceedings for promoting information security, focussing specifically on legal proceedings which have been carried out in Catalonia and the rest of Spain.

Keywords
public security policies, cybercrime, information security

Subject
Data protection

1. Les polítiques públiques d'impuls genèric de la seguretat de la informació

En aquesta secció presentem les polítiques públiques de seguretat de la informació, des d'una perspectiva genèrica, comuna a tota la problemàtica de la seguretat de la informació.

1.1. Estratègia global de seguretat de la informació

El desenvolupament d'una estratègia global de seguretat de la informació a escala nacional comença a ser una constant entre els estats, política habitualment centrada en la necessitat de desenvolupar eines de recerca i de conscienciació del públic pel que fa al nombre cada vegada més important d'amenaces i vulnerabilitats de la seguretat en línia.

En alguns casos, s'han desenvolupat polítiques nacionals per a coordinar actuacions prèvies individuals que perseguien objectius molt concrets, tractant de crear una política o estratègia global de seguretat, mentre que en altres casos les polítiques nacionals s'han dirigit a la implementació de polítiques d'administració electrònica o, fins i tot, d'iniciatives singulars com les signatures electròniques o les targetes de ciutadans.

La majoria dels estats es troben en fase d'establir algun tipus d'estratègia global de la seguretat de la informació, amb dos trets característics:

- Una aproximació multidisciplinària i amb múltiples participants.
- Una estructura de governança d'alt nivell.

Pel que fa a l'aproximació multidisciplinària i amb múltiples participants de les polítiques nacionals de seguretat de la informació, resulta interessant com la majoria d'iniciatives constaten que la cultura de la seguretat no apareix senzillament a partir de les solucions tecnològiques.

Al contrari, es necessita una aproximació més àmplia, que prengui en consideració també els aspectes socioeconòmics i legals, cosa que imprimeix una dimensió multidisciplinària a les polítiques.

A més, es considera que els governs sols no poden gestionar tots els reptes i qüestions de seguretat, cosa que implica una necessitat d'involucrar el sector privat i la societat civil, efecte que es pot aconseguir amb diferents instruments, com les associacions publicoprivades, el desenvolupament de millors pràctiques, el subministrament de consell i la participació en òrgans comuns.

També és freqüent que els governs acudeixin al sector privat per rebre consultoria sobre desenvolupaments tecnològics i d'implementació global. Alguns estats contracten universitats i experts independents per donar suport en qüestions de política o generen la justificació necessària per a la implementació d'una política concreta.

Com a punt pendent en la majoria dels estats podem trobar la limitada participació de la societat civil en les qüestions de seguretat de la informació, cosa que indica la necessitat de millorar la seva participació.

Pel que fa a l'estructura de governança d'alt nivell, la majoria dels estats posicionen la seva estructura de governança de la seguretat al més alt nivell. Moltes vegades, trobem una dependència d'aquesta estructura de seguretat de l'oficina del govern o del primer ministre, i de forma més escassa, com sembla que és el cas de l'Estat espanyol, aquesta responsabilitat és repartida entre diferents departaments ministerials.

En tots els casos cal indicar que una aproximació jeràrquica, de dalt a baix, no és suficient, sinó que fa falta 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 requerits.

Més enllà de les fronteres nacionals, es requereix la col·laboració amb les organitzacions internacionals i la resta de governs per a aconseguir l'objectiu de la seguretat, ja que l'activitat individual dels estats no pot donar resposta al repte global de la seguretat de la xarxa Internet, que no té fronteres.

A l'Estat Espanyol, el pla Avança, liderat pel Ministeri d'Indústria, Turisme i Comerç, a través de la Secretaria d'Estat de Telecomunicacions i per a la Societat de la Informació, ha estat un dels instruments importants en relació amb l'estratègia global espanyola de seguretat de la informació, del qual ha sorgit una línia rellevant

de serveis als ciutadans i a les empreses, oferts per l'INTECO.

També cal referir-se a l'actuació del Centre Nacional d'Intel·ligència / Centre Criptològic 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 l'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, i que es presenta posteriorment.

Finalment, en l'àmbit català, és necessari referir-se al Pla nacional de seguretat de la informació de Catalunya, aprovat per acord del Govern de la Generalitat de Catalunya de 17 de març de 2009.

1.2. Conscienciació i formació sobre la seguretat de la informació

Una de les polítiques públiques genèriques més important és aquella que s'orienta a incrementar els nivells de consciència sobre la necessitat de la seguretat de la informació, que l'OCDE anomena la *cultura de la seguretat*.

A aquest aspecte s'han dedicat les importants Directrius de la OCDE per a la seguretat de sistemes i xarxes d'informació: cap a una cultura de la seguretat, de l'any 2002, que substitueixen les Directrius de seguretat dels sistemes d'informació, de l'any 1992.

Les directrius parteixen de la noció d'un important canvi en la computació, que ha passat de sistemes aïllats i xarxes privades a un entorn basat en ordinadors personals, tecnologies convergents, l'ús massiu de xarxes públiques com Internet i la interconnexió de sistemes oberts. En aquest nou context, Internet ha esdevingut part de les infraestructures operatives de sectors estratègics com l'energia, els transports i les finances, i es troba a la base del comerç i el govern electrònics, a més de permetre noves possibilitats als ciutadans.

En contrapartida, han sorgit noves vulnerabilitats i amenaces a la seguretat de la informació i les comunicacions, que cal tractar adequadament, començant per un nivell suficient de coneixement dels nous reptes de seguretat, per a arribar a una cultura de la seguretat que inclogui tots els participants en la societat de la informació.

Els propòsits de les directrius són els següents:

- Promoure una cultura de seguretat entre tots els participants com a mitjà per a protegir els sistemes i xarxes d'informació.
- Incrementar la conscienciació sobre el risc dels sistemes i xarxes d'informació, sobre les polítiques, pràctiques, mesures i procediments disponibles per a poder fer front a aquests riscos, així com sobre la necessitat d'adoptar-los i executar-los.
- Promoure entre tots els participants una confiança més gran en els sistemes i xarxes d'informació, així com en la seva forma d'operació i d'ús.
- Crear un marc general de referència que ajudi els participants en la comprensió dels aspectes de seguretat i respecte als valors ètics en el desenvolupament i execució de polítiques coherents, així com de pràctiques, mesures i procediments per a la seguretat de sistemes i xarxes d'informació.
- Promoure entre tots els participants, quan sigui possible, la cooperació i l'intercanvi d'informació sobre el desenvolupament i l'execució de polítiques de seguretat, així com de pràctiques, mesures i procediments.
- Promoure el coneixement en matèria de seguretat com un objectiu important que s'ha d'assolir entre tots els participants involucrats en el desenvolupament i execució de normes tècniques.

En el marc d'aquests objectius generals, es proposen nou principis, complementaris entre si, d'interès polític i tècnic, amb indicació expressa que els esforços per a enfortir la seguretat dels sistemes i xarxes d'informació han de respectar els valors democràtics i en particular garantir fluxos de comunicació lliures i oberts, així com la protecció de les dades de caràcter personal:

1. Conscienciació. Els participants han de ser conscients de la necessitat de disposar de sistemes i xarxes d'informació segurs, i tenir coneixement dels mitjans per a ampliar la seguretat.
2. Responsabilitat. Tots els participants són responsables de la seguretat dels sistemes i xarxes d'informació.
3. Resposta. Els participants han d'actuar de manera adequada i conjunta per a prevenir, detectar i respondre a incidents que afectin la seguretat.

4. Ètica. Els participants han de respectar els interessos legítims de tercers.
5. Democràcia. La seguretat dels sistemes i xarxes d'informació ha de ser compatible amb els valors essencials d'una societat democràtica.
6. Avaluació del risc. Els participants han de dur a terme avaluacions de risc.
7. Disseny i realització de la seguretat. Els participants han d'incorporar la seguretat com un element essencial dels sistemes i xarxes d'informació.
8. Gestió de la seguretat. Els participants han d'adoptar una visió integral de l'administració de la seguretat.
9. Avaluació contínua. Els participants han de revisar i avaluar periòdicament la seguretat dels seus sistemes i xarxes d'informació, i realitzar les modificacions pertinents sobre les seves polítiques, pràctiques, mesures i procediments de seguretat.

Continuant en la seva activitat de promoció de la cultura la seguretat, l'OCDE va preparar el 2003 un pla d'implementació, que identifica aspectes importants respecte als diferents rols o papers dels participants, basant-se en la necessitat d'una cooperació continuada entre els governs, les empreses i la societat civil.

En opinió de l'OCDE, els governs tenen la responsabilitat d'emprendre el lideratge del desenvolupament de la cultura de la seguretat, mitjançant els diversos rols que compleixen en relació amb els sistemes i xarxes de la informació (desenvolupadors de polítiques públiques, propietaris i operadors de sistemes i xarxes).

Durant el procés de desenvolupament de polítiques públiques, els governs han de promoure la seguretat de les xarxes i els sistemes d'informació per a generar confiança en el seu ús i assegurar millor la seguretat global. Tot i ser un procés propi, els governs haurien de desenvolupar aquestes polítiques públiques de forma transparent, mitjançant consultes amb altres governs i amb altres interessats.

Els governs han de desenvolupar polítiques públiques nacionals o regionals sobre seguretat de la informació i garantir la cooperació internacional per a promoure aquesta cultura global de la seguretat, mitjançant instruments com els següents: tÈcniques

- Mesures legals i tÈcniques per a combatre la ciberdelinqüÈncia, consistents en la Convenció del Consell d'Europa, que presentarem posteriorment.
- Equips i recursos personals altament qualificats per a donar suport a la lluita coordinada contra el frau informàtic.
- Institucions preparades per a respondre a atacs i a emergÈncies informàtiques, així com per a intercanviar informació respecte a això, com per exemple els anomenats CERT.
- Mecanismes de cooperació amb el sector privat per a combatre amb més efectivitat els problemes de seguretat.
- Suport a la recerca i el desenvolupament en el camp de la seguretat de les tecnologies de la informació.
- Activitats de conscienciació pública, de formació i educació del públic.
- Subministrament de recursos d'informació al públic sobre la seguretat dels sistemes i xarxes d'informació.

Com a propietaris i operadors de sistemes i xarxes d'informació, els governs comparteixen rol amb les empreses, altres organitzacions i els individus en relació amb l'assegurament de l'ús correcte dels sistemes i xarxes, dintre de la cultura de la seguretat.

En general, a causa del volum dels sistemes dels governs en relació amb el territori nacional, haurien de ser un model i exemple d'operació segura, per a guiar la resta d'organitzacions i ciutadans, mitjançant l'establiment de millors pràctiques i altres tÈcniques de millora organitzativa, mentre que, en particular, cal considerar la capacitat d'adquisició de tecnologia que tenen els governs com un mecanisme per a influir en la millora de la seguretat dels productes oferts al mercat.

L'anàlisi realitzat per l'OCDE a finals de 2004 sobre les activitats governamentals en relació amb la seguretat de la informació i, en particular, sobre el marc normatiu en suport de la seguretat, ha mostrat que una sÈrie important d'estats identifiquen la signatura electrònica i la certificació digital com a aspecte essencial de la seva estratÈgia legal en suport de la seguretat.

Addicionalment, s'identifiquen com a elements importants la protecció de dades personals i les mesures d'inspecció i de control sobre les comunicacions electròniques.

Respecte als programes de sensibilització sobre la seguretat de la informació, l'ENISA ha publicat un interessant document, dirigit a ajudar els estats membres de la Unió a

preparar aquest tipus de programa, en quÈ exposa els beneficis principals que té:

1. Representar un punt de referÈncia i un motor per a una sÈrie d'activitats de sensibilització, formació i educació relacionades amb la seguretat de la informació, algunes de les quals ja poden existir, però possiblement hagin de ser objecte d'una coordinació i optimització més grans.
2. Transmetre les directrius o pràctiques recomanades importants que siguin necessàries per a protegir els recursos d'informació.
3. Facilitar informació general i específica sobre els riscos i controls de la seguretat de la informació a les persones que hagin de conÈixer-la.
4. Informar les persones de les seves responsabilitats en relació amb la seguretat de la informació.
5. Estimular les persones a adoptar les directrius o pràctiques recomanades.
6. Crear una cultura de seguretat més arrelada, amb una comprensió i un compromís d'ampli abast amb la seguretat de la informació.
7. Contribuir a potenciar la coherÈncia i eficàcia dels controls de la seguretat de la informació i fomentar l'adopció de controls eficaços respecte al cost que té.
8. Contribuir a reduir el nombre i l'abast de les infraccions de la seguretat, i disminuir així el cost directament (per exemple, danys produïts per virus) i indirectament (per exemple, reducció de la necessitat d'investigar i solucionar les infraccions). Aquests són els principals avantatges financers del programa.

Els darrers estudis mostren que els estats ja estan activament involucrats en iniciatives per a incrementar la conscienciació pública en relació amb la cultura de la seguretat, iniciatives que inclouen presentacions públiques i la distribució de materials informatius.

Per exemple, a l'Estat espanyol es poden esmentar diverses iniciatives en aquest sentit, incloent-hi el projecte de divulgació de l'estat de la seguretat FARO, d'ASIMELEC, la campanya itinerant (o *road-show*) EXPOSEC per a presentar aspectes de seguretat, també realitzada per ASIMELEC en col·laboració amb el Ministeri d'Indústria, Turisme i Comerç, la constant tasca divulgadora de les Cambres de Comerç, en particular mitjançant Camerfirma, o l'actuació de la societat civil, per exemple, mitjançant el Fòrum de les EvidÈncies Electròniques, que genera discussió en línia i reunions periòdiques amb tots els actors en relació amb aspectes relatius a la seguretat de la informació, com la generació de proves electròniques amb reconeixement judicial.

Els actes públics tracten una important diversitat d'assumptes de seguretat, qüestions molt generals o més específiques com la gestió de risc, l'autenticació electrònica, les signatures electròniques o les infraestructures de clau pública (PKI). El públic destinatari d'aquests esdeveniments també és variable: des del públic en general fins a experts que treballen en el sector privat i el sector públic. En particular, molts governs fan de forma regular esdeveniments interns per a formar el seu personal (per exemple, el Centre Criptològic Nacional té una important activitat en aquest sentit), amb una incipient tendÈncia a obrir aquests actes al sector privat i als ciutadans, que pot ser una manera d'arribar a aquests destinataris de forma més efectiva.

Per altra banda, la preparació i distribució gratuïta de recomanacions, millors pràctiques i guies generals és una manera molt important de vehicular les polítiques de conscienciació de la seguretat.

A més, en diversos estats existeix la tendÈncia de redactar millors pràctiques i guies en qüestions tÈcniques i operatives com per exemple l'autenticació en línia, les signatures electròniques, les xarxes sense fil, les xarxes d'igual a igual (*peer-to-peer*), la gestió del risc i la resposta a incidents.

1.3. Anàlisi i gestió de risc

L'anàlisi i la gestió de risc és també una política genÈrica important a diversos estats, incloent-hi l'Estat espanyol.

Les iniciatives en relació amb l'anàlisi i la gestió de risc inclouen casos com el desenvolupament de metodologies (França, amb EBIOS, o Espanya, amb MAGERIT), o normes i guies (Noruega, el Japó o els EUA). Algunes iniciatives es completen amb una xarxa específica d'usuaris, com succeeix a França, per a l'intercanvi d'informació i per A continuar el desenvolupament de la metodologia.

Altres iniciatives inclouen la creació i el subministrament d'eines automàtiques per a l'assistÈncia en la realització de les anàlisis de risc, com és el cas de l'eina PILAR, del Centre Criptològic Nacional, o de les eines del mÈtode britànic CRAMM.

Cal indicar que l'ús de les tÈcniques i eines d'anàlisi i gestió de risc no és limitat a les tecnologies de la informació, sinó que es comença a utilitzar en àrees com els desastres naturals, el sector de les telecomunicacions i, de forma més genÈrica, per a la protecció de les infraestructures crítiques.

Així mateix, en alguns estats, com Àustria, l'anàlisi de risc forma part dels processos de supervisió i control dels prestadors de serveis de certificació de signatura electrònica, mentre que a Finlàndia s'ha utilitzat com a eina per als projectes de cooperació financera liderats pel govern.

1.4. Avaluació de la seguretat de la informació en productes i serveis

Amb una orientació més particular als productes, ja és consolidada la política dels estats de fomentar la qualitat i la seguretat dels productes mitjançant la certificació conforme amb metodologies formals. Cada vegada són més els estats que exigeixen certificacions de seguretat als productes que han d'adquirir per a la realització de les seves tasques.

La manera d'implementar aquesta avaluació i certificació de la seguretat de la informació és la creació d'un esquema nacional d'avaluació, que permet 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.

Un 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 mateix 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 o laboratori 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, creat pel Reial decret 421/2004, ha estat nomenat l'òrgan competent de certificació de l'esquema nacional d'avaluació i certificació de la

seguretat de les tecnologies de la informació, mentre que l'Institut Nacional de TÈcnica Aeroespacial (INTA) actua com a laboratori d'avaluació autoritzat per a productes que tractin informació classificada i no classificada, i l'empresa APPLUS actua com a laboratori d'avaluació autoritzat per a productes que tractin informació no classificada, i ENAC, com a entitat d'acreditació.

1.5. Recerca i desenvolupament en seguretat de la informació

La recerca i el desenvolupament en matÈria de seguretat de la informació és una de les polítiques més habituals dels estats avançats en la cultura de la seguretat, especialment per l'impacte posterior en la competitivitat de les empreses productores de tecnologies de seguretat, que comercialitzen els seus productes en el mercat global.

En aquest sentit, des d'una perspectiva de política de la Unió Europea, la Resolució del Consell de 22 de març de 2007, sobre una estratÈgia per a una societat de la informació segura a Europa, considera que els recursos destinats a recerca i desenvolupament (R+D) i innovació, tant a escala nacional com comunitària, constitueixen un dels elements fonamentals per a reforçar el nivell de seguretat de les xarxes i de la informació dels nous sistemes, aplicacions i serveis.

En conseqüÈncia, es considera important intensificar l'esforç a escala europea en els àmbits de la recerca i la innovació en relació amb la seguretat, en particular mitjançant el setÈ Programa marc i el Programa marc per a la competitivitat i la innovació.

Addicionalment, cal fer esforços per a implantar mesures destinades a la difusió i promoció de l'explotació comercial dels resultats, inclosa l'avaluació de la utilitat per a la comunitat en conjunt, cosa que contribuirà a millorar la capacitat dels proveïdors europeus per a subministrar solucions de seguretat que responguin a les necessitats específiques del mercat europeu.

La majoria dels estats reconeixen la importància de les activitats de recerca i desenvolupament per a la seguretat de la informació, ja que són la clau per a produir solucions innovadores que puguin fer front als requisits presents i futurs de la seguretat de la informació. Com s'ha avançat, la inversió en recerca i desenvolupament en seguretat de la informació es percep com un element que contribueix a l'increment global d'innovació i competitivitat dels estats.

Tot i això, els estudis mostren que pocs estats han establert programes específics de recerca en seguretat de la informació amb fons públics, mentre que la majoria dels estats financen la recerca en seguretat dintre de programes més amplis de recerca, habitualment relatius als aspectes computacionals (per exemple, criptografia) i tecnològics, sense que es considerin de forma general els aspectes socials, legals i econòmics de la seguretat de la informació.

De forma general, aquestes tasques de recerca i desenvolupament són realitzades per les universitats, habitualment per instituts específicament creats per a tractar la qüestió de la seguretat de la informació i, amb menys freqüÈncia, en cooperació amb la indústria. També és notable que la cooperació internacional en matÈria de recerca i desenvolupament de la seguretat de la informació resulta limitada.

Com a exemples de les activitats en aquesta àrea, es poden esmentar els següents:

- El projecte dels Països Baixos SENTINEL, amb l'objectiu de desenvolupar aplicacions segures per a sistemes d'usuari, administració electrònica i comerç electrònic, que presenta una interessant aproximació multidisciplinària.
- El projecte Oppidum (França) i l'IKT SoS (Noruega).
- El projecte Seguretat 2020 (Espanya) i els projectes espanyols de recerca específica, dintre de línies d'abast tecnològic més ampli (un cas similar a Àustria, Dinamarca, Alemanya, Corea, el Regne Unit o els EUA).

En alguns casos, les tasques de recerca són suportades o realitzades per organitzacions governamentals amb responsabilitats de seguretat de la informació, com l'Oficina Federal Alemanya de Seguretat de la Informació, l'AgÈncia Coreana de Seguretat de la Informació, l'Establiment Públic Canadenc de Seguretat de les Comunicacions o la Divisió de Ciberseguretat del Departament d'Interior dels EUA. Aquestes tasques de recerca persegueixen el desenvolupament de noves solucions, com per exemple RFID,

biometria o tecnologia sense fil, o solucionar necessitats o problemes immediats.

En altres casos, els estats faciliten la participació de la indústria i d'altres institucions independents de recerca en les seves iniciatives de recerca en seguretat de la informació, com és el cas d'Espanya, Alemanya, els Països Baixos o Àustria.

2. El Pla nacional de seguretat de la informació de Catalunya

El 17 de març de 2009, per acord de govern 50/2009, publicat en el DOGC 5351, d'1 d'abril, es va aprovar el Pla nacional de seguretat de la informació de Catalunya, ateses les competències de la Generalitat de Catalunya en societat de la informació i, en concret, en l'accés a les tecnologies de la informació i la comunicació (TIC), en comerç electrònic i consum, i en administració electrònica, arran del qual es creï, si escau, un centre de seguretat de la informació de Catalunya (CESICAT), per tal que desenvolupi els objectius estratègics del Pla.

2.1. La seguretat TIC a l'Estatut d'autonomia de Catalunya de 2006 (EAC)

Un dels fonaments importants per a afirmar la competència de la Generalitat de Catalunya i de la resta d'administracions públiques catalanes en seguretat de la informació deriva de l'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 descomptat a la societat de la informació, en què les persones desenvolupen una part cada vegada més important de la seva vida.

Respecte als col·lectius que s'han de 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 (ciberassetjament o *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 a afavorir la seva integració i participació efectiva en la societat de la informació, que dependrà, en part, del grau de confiança que hi 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 a 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».

Aquesta norma conté 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 que s'ha de 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 contra el robatori d'identitats financeres (mitjançant la pesca electrònica o *phishing*), el robatori d'informacions comercials sensibles, com les dades de les targetes de pagament, o contra les comunicacions comercials no sol·licitades (correu brossa o *spam*).

Cal indicar que l'article 123 de l'EAC determina la competència exclusiva de la Generalitat de Catalunya en matèria de consum, i indica 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, 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, l'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, cosa que exigeix un programa públic de seguretat de la societat de la informació que se'n responsabilitzi.

Per 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 és 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, i produir un efecte en cascada, especialment quan els incidents afecten 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 què 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.

2.2. 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.

2.2.1. 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 escala nacional, política que s'ha de centrar en la necessitat de desenvolupar eines de recerca i de conscienciació del públic quant al nombre cada vegada més important d'amenaces 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 l'altra.

Cal definir un model públic català de seguretat de la societat de la informació a Catalunya, que adreci de forma global els reptes que es plantegin a 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 incidents com a pal de paller vertebrador del Pla nacional de seguretat TIC, que efectuï una 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 fa falta 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 requerits. Al contrari, es considera que els governs sols no poden gestionar tots els reptes i qüestions de seguretat, cosa que implica una necessitat d'involucrar el sector privat i la societat civil, efecte que es pot aconseguir amb diferents instruments, com les associacions publicoprivades, el desenvolupament de millors pràctiques, el subministrament de consell i la participació en òrgans comuns.

Aquest sistema reforçarà iniciatives i programes que ja existeixen, 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.).

2.2.2. 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 nacionals, incloent-hi les xarxes de comunicacions electròniques, però també els principals elements en quÈ 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 confien els 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 casos que s'han de 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.

2.2.3. 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 Catalunya,[1] 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; en concret, el Tecnoparc de Reus.

2.2.4. 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, i es reforçaran les capacitats de detecció i denúncia d'il·lícits de tota mena, filtratge de continguts i anàlisi forense d'evidències electròniques.

Citació recomanada

ALAMILLO, Ignacio (2009). «Les polítiques públiques en matèria de seguretat a la societat de la informació» A: «V Congrés Internet, Dret i Política (IDP). Cara i creu de les xarxes socials» [monogràfic en línia]. *IDP. Revista d'Internet, Dret i Política*. Núm. 9. UOC. [Data de consulta: dd/mm/aa].

<http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_alamillo/n9_alamillo_cat>

ISSN 1699-8154

1. FOBSIC i Penteo Research (març, 2008). «El Mercat de les Tecnologies de la Informació i la Comunicació a Catalunya: 2007-2010».

Sobre l'autor

Ignacio Alamillo

Consultor sÈnior en seguretat de la informació (Direcció General de la Societat de la Informació, Secretaria de Telecomunicacions i Societat de la Informació, Generalitat de Catalunya).

Llicenciat en Dret. Advocat de l'Il·lustre Col·legi de Madrid. Director de l'àrea d'assessorament i investigació de l'AgÈncia Catalana de Certificació (desembre 2002 -febrer 2008). Director de l'àrea de consultoria i serveis legals de l'AgÈncia de Certificació Electrònica - Punt Directe (juliol 1997 - desembre 2002). Membre del grup directiu europeu de Seguretat de Xarxes i de la Informació i del grup directiu de la Iniciativa Europea de Normalització de la Signatura Electrònica, que assessoren la Comissió Europea. Membre del Consell de Certificació d'ASIMELEC. Ha estat membre del grup directiu europeu de la Iniciativa Europea de Normalització de la Signatura Electrònica, i del grup d'Infraestructura de Seguretat de Signatura Electrònica de l'Institut Europeu de Normes de Telecomunicacions. Autor d'*ABC de la firma electrónica*, coautor de quatre llibres sobre aspectes jurídics de la societat de la informació, nombrosos articles i ponÈncies en signatura electrònica i el terreny d'aplicació que té.

ASTREA, La Infopista Jurídica, S.L.

Blondel, 21

25002 Lleida, España