



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

Pla Nacional d'impuls de la Seguretat TIC-CESICAT

BDIGITAL 2009

19 de maig del 2009

Necessitat d'una pla nacional d'impuls de la seguretat TIC

EL PAÍS.com | Versión para imprimir

Inprimir

SEGU

Las
seg

CIBER

Las py
en el 9
conias
in



La Agencia Tributaria

Inicio La Agencia Tributaria Sala de prensa **Notas de prensa**

La Agencia Tributaria advierte de un intento de Phishing

30-enero-2007.

La Agencia Tributaria

La Agencia Tributaria advierte de que se ha producido un intento de Phishing suplantando a la AEAT con el fin de pedir los datos de las tarjetas de crédito de algunos contribuyentes.

La mayoría de los ataques buscan burlar los sistemas de seguridad tradicionales, como el escaneo del correo electrónico

tecnología

IA EMPLEO MOTOR
Economía Internet y

Phishing"

✉ | A⁻ A⁺

per semestre

esta técnica de fraude, que
ser comunicaciones seguras
M.



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

Necessitat d'una pla nacional d'impuls de la seguretat TIC

Els estudis mostren les carències en matèria de protecció de la informació, el que farà créixer el volum i gravetat de les incidències en seguretat la informació.

CIUTADÀ

- Increment d'incidències relatives a programari maliciós (77% ordinadors infectats) i correu brossa (80% tràfic fraudulent).
- Augment del nombre i tipologies dels programes fraudulents.
- Enginyeria social com a vector d'atac més freqüent, degut a falta de conscienciació i formació.

PIMES

- Tipus d'atacs semblants als que pateixen els ciutadans.
- Escepticisme envers el problema de la seguretat, degut a la falta de coneixements i a un nombre "petit" d'atacs.
- Desconeixement de les tecnologies de seguretat.
- Problemes per accedir al mercat, per preu i altres factors. Necessitat d'apropar la tecnologia i oferir serveis des del sector públic o tutelats des del sector públic.
- Compliment normatiu insuficient, especialment en LOPD.



Necessitat d'una pla nacional d'impuls de la seguretat TIC

L'aprovació de la llei 11/2007, d'accés electrònic dels ciutadans als serveis públics, obliga a la implantació de mesures de seguretat molt importants a les AA.PP.

ADMINISTRACIONS PÚBLIQUES LOCALS

- 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, en què cal actuar.
- Molt baix nivell d'ús d'eines avançades, com xifratge, sondes, vulnerabilitats... Especialment en governs locals amb poca població (30% dels governs locals de Catalunya tenen menys de 500 habitants).



La seguretat de les TIC a l'Estatut d'Autonomia de Catalunya 2006

- ✓ Competència executiva en xarxes de comunicacions electròniques de la Generalitat de Catalunya (art. 140.7) i dels governs locals de Catalunya (art. 84).
- ✓ Accés a les TIC (art. 53), garantint que les TIC no afectin negativament als drets i garantint la continuïtat de les TIC.
- ✓ Protecció d'infants i joves, i persones grans i grups en risc d'exclusió social, també en el seu ús de la Societat de la Informació (art. 40): *ciberbullying*, continguts nocius...
- ✓ Protecció dels consumidors i dels usuaris, en la seva interacció amb empreses mitjançant xarxes (arts. 49 i 123) i comerç electrònic (art. 112): *phishing*, *pharming*, *spam*, informació mínima sobre seguretat, retenció de dades...
- ✓ Evidentment, les garanties de funcionament de les Administracions Públiques Catalanes també obliguen a la implantació de programes de seguretat de la informació.



Actuacions fetes en matèria de seguretat

- ✓ Oficina de seguretat del CTTI (corporativa)
- ✓ Plans específics: Sanitat
- ✓ Mossos d'Esquadra (Delictes informàtics)
- ✓ CATCERT (Identitat digital)
- ✓ Cambra de comerç de Barcelona (Llibre blanc de seguretat a les empreses)
- ✓ Agència Catalana de Protecció de dades



Pla nacional d'impuls de la seguretat TIC -1

✓ El pla ha estat aprovat pel govern amb data 17 de març

✓ **Missió**

Garantir una Societat de la Informació Segura Catalana per a tots tot generant d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui referent estatal i internacional.

✓ **Objectius estratègics**

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.

Pla nacional d'impuls de la seguretat TIC - 2

1. Establiment d'una estratègia nacional de seguretat TIC

Recerca i conscienciació

Necessitat de desenvolupar **eines de recerca i de conscienciació** del públic en relació amb el nombre cada vegada més important d'amenaques de la seguretat en línia.

Sistema Públic Català de Seguretat de la Informació

Es definirà un sistema públic català de seguretat de la societat de la informació, 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.

Col·laboració i potenciació

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, consums, infants i joves, policies públiques, etc).



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

Comunicacions electròniques crítiques

Millora de la protecció dels elements que conformen les **infraestructures crítiques TIC nacionals**, incloent-hi les xarxes de comunicacions electròniques.

Sistemes electrònics de control industrial (SCADA)

Les conseqüències d'un atac contra els sistemes industrials de control de les infraestructures crítiques podrien ser molt diverses, però els efectes en cascada poden ser molt danyosos, i provocar grans **caigudes dels serveis públics**.

Línies prioritàries d'actuació

Alguns supòsits a tractar seran 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), així com els serveis privats que hi donen suport.



3. Promoció d'un teixit empresarial català sòlid en seguretat TIC

Política industrial
en seguretat TIC

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.

Generació de
negoci privat i
retorn social

Creació de la xarxa de PIMEs per a la **prestació de serveis de seguretat i resposta a incidents de seguretat**, així com una comunitat empresarial especialitzada en tots els aspectes de la seguretat TIC, amb línies de formació i certificació professional.

Comunitat basada
en programari
lliure

Aposta per l'ús de **programari lliure de seguretat**, liderat per una comunitat específica, ubicada a un *near-shore* a Catalunya (exemple: Parc Tecnològic de la Universitat Rovira i Virgili – líder estatal en recerca sobre seguretat de la informació).



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

Atenció a
col·lectius de risc

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.

Suport a la lluita
contra la
delinqüència
informàtica

Suport a 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.

Laboratori de detecció i anàlisi de programari maliciós, recerca i devolució d'informació robada i generació de prova electrònica.



Què és el CESICAT?

L'execució del Plan Nacional exigeix disposar d'un organisme executor que aglutini les iniciatives existents, públiques i privades.

Centre de Seguretat de la Informació de Catalunya (CESICAT)

- La fórmula jurídica escollida és la Fundació amb participació pública i privada
- La seu serà Reus
- Participació: Generalitat, AOC, Ajuntament de Reus, Cambres de comerç, URV, Bdigital, e.La Caixa



Són destinataris dels serveis els col·lectius següents:

1. **Els ciutadans i les ciutadanes de Catalunya**, amb una atenció especial als col·lectius amb més riscos de seguretat de la informació, com són els infants, joves, gent gran i altres col·lectius de recent incorporació a la xarxa.
2. Els **professionals i les entitats privades**, amb una atenció especial a les PIME i altres organitzacions de reduïda dimensió.
3. Les **Administracions Públiques**, amb una atenció especial als governs locals de Catalunya de petita i mitjana població.
4. Les **Universitats i els centres de recerca**, amb independència de la seva naturalesa pública o privada.

CESICAT – Catàleg d'actuacions i serveis 2009 a 2012 (selecció)

El Centre de Seguretat de la Informació de Catalunya abordarà un programa inicial de 23 actuacions, que dóna resposta a les necessitats mínimes inicials identificades.

1. Estratègia nacional de seguretat de la informació.

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

3. Promoció d'un teixit català sòlid en seguretat TIC.

4. Confiança i protecció de la ciutadania en la Societat de la Informació.

01. Difusió de notícies i comunicats en seguretat TIC.
02. Pla de conscienciació de la seguretat en PIME.
05. Guies de seguretat TIC.
07. Base de coneixement de vulnerabilitats i estratègies de resposta.
08. Assistència remota a vulnerabilitats i incidents.
10. Xarxa catalana de seguretat TIC.
11. Coordinació amb tercers. Catàleg d'actors en seguretat TIC.
12. Anàlisi d'incidents de seguretat TIC.
14. Anàlisi preventiva de vulnerabilitats externes.
16. Programes de gestió de la seguretat TIC.
18. Assessoria legal sobre seguretat TIC, informàtica forense i altres.
20. Guies legals sobre seguretat TIC.
21. Estudi sobre requisits de protecció de les xarxes públiques de comunicacions electròniques, considerades com infraestructures crítiques.

CESICAT – Exemples de serveis

- ✓ Jornades i sessions de formació en mesures de seguretat.
- ✓ Anàlisi trimestral de vulnerabilitats externes: permet detectar possibles punts d'entrada des de l'exterior als sistemes (ports de xarxa i aplicacions).
- ✓ Anàlisi trimestral de vulnerabilitats d'aplicació web: permet detectar problemes de programació en les aplicacions web de les pàgines web.
- ✓ Informació preventiva sobre amenaces de dia zero (possibles atacs a partir de la data de publicació de programari).
- ✓ Detecció ràpida d'incidents de seguretat i comunicació d'alertes de seguretat als beneficiaris.
- ✓ Suport en remot a la contenció i recuperació d'incidents de seguretat.
- ✓ Activació, coordinació i supervisió de la resposta a incidents patits pels beneficiaris.