cesicat

Centre de Seguretat
de la Informació de Catalunya

Pla nacional de seguretat de la informació de Catalunya

- **Antecedents:**
  - Acord de Govern (GOV/50/2009) d'aprovació del Pla nacional de seguretat de la informació de Catalunya (17-03-2009).
- **Missió:**
  - Garantir una societat de la informació catalana segura per a tots, amb un Centre de Seguretat de la Informació de Catalunya com a eina per a la generació d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui referent nacional i internacional.
- **Objectius estratègics:**
  1. Establiment d'una estratègia nacional de seguretat TIC.
  2. Suport a la protecció de les infrastructures crítiques TIC nacionals.
  3. Promoció d'un teixit empresarial català sòlid en seguretat TIC.
  4. Increment de la confiança i protecció dels ciutadans catalans en la societat de la informació.

Què és el Centre de Seguretat de la Informació de Catalunya?

*"En conseqüència, es considera convenient aprovar un pla de seguretat de la informació a Catalunya, 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."*

DOGC núm. 5351 - 01/04/2009

El Centre de Seguretat de la Informació de Catalunya (**CESICAT**) és l'organisme de suport del Pla nacional d'impuls de la seguretat TIC aprovat pel Govern de la Generalitat de Catalunya el 17 de març de 2009.

cesICAT

Fundació CESICAT: patrons

Generalitat de Catalunya

- Departament de Governació
- Secretaria de Telecomunicacions i Societat de la Informació
- Departament d'Interior
- Departament d'Innovació, Universitats i Empresa
- Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya

- **Agència ACC1Ó**
- **Consorci Administració Oberta de Catalunya**
- **Ajuntament de Reus**
- **Consell de Cambres de Comerç de Catalunya**
- **e-la Caixa**
- **Fundació Barcelona Digital**
- **Universitat Rovira Virgili**

cesICAT

A qui va dirigit?

Ciutadans	• Els **ciutadans i 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.
Professionals i empreses	• Els **professionals i les entitats privades**, amb una atenció especial a les pimes i altres organitzacions de reduïda dimensió.
Administracions públiques	• Les **administracions públiques**, amb una atenció especial als governs locals de Catalunya de petita i mitjana població.
Universitats i centres de recerca	• Les **universitats i els centres de recerca**, amb independència de la seva naturalesa pública o privada.

cesicat

Serveis i activitats: àrees d'actuació

Reactius

Generació d'alertes i advertències

Assistència remota a vulnerabilitats i incidents

Assistència in situ

Anàlisi d'incidents

Preventius

Guies de seguretat

Llistes de configuració segura de sistemes

Ànalisi preventiva de vulnerabilitats externes

Promoció

Difusió de notícies i comunicats

Foment de la formació en seguretat

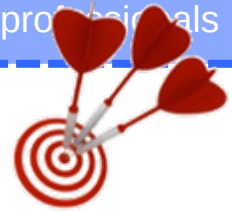
Campanyes de sensibilització

Dinamització

Potenciació del teixit empresarial TIC

Col·laboració amb altres actors de seguretat

Promoció de la certificació de processos i pro[illegible]als



cesicat

Serveis reactius

Generació d'alertes i advertències en seguretat i vulnerabilitats

• Alertes i advertències en seguretat i vulnerabilitats TIC, amb indicadors sobre l'estat global d'alerta de seguretat.

Assistència remota a vulnerabilitats i incidents

• Assistència remota a la gestió de vulnerabilitats i incidents de seguretat TIC tant en el seu tractament com en aspectes de contenció i resol·lució.

Assistència in situ

• Assistència in situ a vulnerabilitats i incidents de seguretat TIC, en relació amb incidències greus o amb major impacte, d'acord amb el definit al pla de resposta a incidents.

Anàlisi d'incidents

•Anàlisi de troballes en relació amb la gestió d'incidents de seguretat TIC, mitjançant eines d'investigació digital i anàlisi forense.

Serveis preventius

Guies de seguretat TIC

• Publicació de guies de seguretat TIC sobre àmbits o tecnologies d'interès adaptades a cada comunitat específica d'usuaris.

Gestió de llistes de configuració segura de sistemes

• Programa continuat per disposar de llistes de configuració segura de sistemes TIC que permetin la revisió o auditoria dels sistemes d'informació.

Anàlisi preventiva de vulnerabilitats

• Avaluació de forma periòdica i ordinària de l'estat de protecció dels usuaris en relació amb les vulnerabilitats dels seus sistemes d'informació en xarxa.

Accions de Promoció

Difusió de notícies i comunicats en seguretat TIC

• Creació i difusió de comunicats en seguretat TIC, adreçats a comunitats específiques d'usuaris: ciutadania, pimes i governs locals.

Foment de la formació en seguretat de la informació

• Millora de la formació en seguretat dels professionals de les TIC, desenvolupant plans de formació específics en l'àmbit de seguretat TIC per tal de garantir un teixit empresarial dotat de professionals preparats.

Campanyes de sensibilització

• 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.
• Promoció entre la ciutadania dels instruments de seguretat essencials.

Accions de Dinamització

Potenciació del teixit empresarial TIC

- Foment de la demanda amb els mateixos serveis i amb les campanyes de difusió, i dinamitzant l'oferta conjuntament amb el TIC.CAT.
- Creació d'una xarxa nacional de pimes especialitzades en seguretat TIC que prestin serveis de d'aquest àmbit, coordinada pel CESICAT.

Promoció de la certificació de procesos i professionals

- Promoció de la certificació dels processos de seguretat.
- Promoció de la formació i certificació de professionals en seguretat TIC i disciplines relacionades.

Col·laboració amb altres actors de seguretat

- Establiment de lligams i actuacions conjuntes amb proveïdors de serveis, fabricants, organismes rellevants...

cesICAT

Equip de Resposta a Incidents (CESICAT-CERT)

- Pla de resposta a incidents alineat amb les millors pràctiques i estàndards com els de la Carnegie Mellon University (CMU)
- Certificació i acreditació als principals fòrums de resposta a incidents europeus i internacionals tals com TF-CSIRT i FIRST.
- Establiment de lligams de col·laboració en els principals fabricants, proveïdors de servei a Internet, prestadors de serveis de seguretat, organitzacions de resposta:
  - CCN-CERT, ENISA, Microsoft, APWG, ABUSES, CSIRT.ES...
- Integració i col·laboració estreta amb el Cos dels Mossos d'Esquadra (CME) per als incidents de caire il·licit penal.
- Recollida, correlació i explotació de dades d'intel·ligència:
  - Base de dades de coneixement i estratègies de resposta
  - Noves amenaces i bases de dades de vulnerabilitats
  - Laboratori d'investigació i anàlisi amb eines especialitzades d'anàlisi forense, anàlisi de codi maliciós, tractament i correl·lació de dades, etc.

cesICAT

Iniciatives complementaries a l'entorn universitari i de recerca

- esCERT-UPC
  - Àmbit: UPC
  - Serveis: Gestió d'incidents i vulnerabilitats, anàlisi forense, auditories...
  - Altres activitats: Formació, recerca i investigació, certificació digital...
- CESCA-ERIAC
  - Àmbit: Infraestructura dels serveis del CESCA, institucions de l'Anella Científica i proveïdors CATNIX
  - Serveis: Gestió i coordinació d'incidents de seguretat, protecció d'infraestructura, detecció d'intrusions...
  - Altres activitats: Formació i grups de treball
- RedIRIS IRIS-CERT
  - Àmbit: Institucions de la xarxa RedIRIS (inclosa Anella Científica)
  - Serveis: Gestió i coordinació d'incidents. Detecció d'intrusions i anomalies a la xarxa, etc.
  - Altres activitats: Formació, recerca i investigació, certificació digital, coordinació de grups de treball sectorials ...

Que ens pot aportar el CESICAT?

- Serveis proactius com l'anàlisi de vulnerabilitats externs dels sistemes d'informació de manera periòdica, llistes de configuració segura i guies de seguretat.
- Notificacions i alertes sobre noves amenaces i vulnerabilitats adaptats a la comunitat.
- Resposta a incidents de seguretat de manera remota o in-situ certificada qualitativament per FIRST i TF-CSIRT, en coordinació directa amb els Mossos d'Esquadra i amb contacte directe amb els tercers involucrats.
- Anàlisi d'incidents en un entorn de laboratori amb recursos d'investigació digital i anàlisi forense avançats.
- Catalitzar la certificació dels futurs professionals de la seguretat TIC i l'apropament d'àmbits d'I+D a les empreses.
- Jornades de difusió, conscienciació i formació a diversos col·lectius com els departaments de sistemes d'informació de les organitzacions, alumnes d'estudis relacionats amb les TIC...

cesICAT

L’Esquema Nacional de Seguretat (I)

La finalitat de l’ENS és la creació de les condicions necessàries de confiança en l’ús dels mitjans electrònics, a través de mesures per garantir la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics. L’ENS es defineix a l’article 42.2. de la Llei 11/2007 i es desenvolupa en el Reial Decret 3/2010.

Àmbit subjectiu

L’ENS s’adreça a les administracions públiques, incloent-hi a les següents entitats:

- L’Administració General de l’Estat.
- Les administracions de les Comunitats Autònomes.
- Les entitats que integren l’Administració local.
- Les entitats de dret públic que estan vinculades o depenen de les anteriors.

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

L'Esquema Nacional de Seguretat (II)

Àmbit material

La llei 11/2007 regula els aspectes bàsics de la utilització de les TIC en tres àmbits:

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

Per tant, l'Esquema Nacional de Seguretat **resultarà d'aplicació a aquestes activitats i als actius involucrats en l'execució del mateix.** Resten excloses de l'aplicació de l'Esquema Nacional de Seguretat les activitats que les administracions públiques portin a terme en règim de dret privat.

Termini per al compliment:

L'apartat segon de la disposició transitòria indica que si al cap de dotze mesos de l'entrada en vigor de l'ENS hi ha circumstàncies que impedeixen la plena aplicació del que s'hi exigeix, s'ha de disposar d'un pla d'adequació que marqui els terminis d'execució, els quals en cap cas no poden ser superiors a quaranta-vuit mesos des de la seva entrada en vigor. Per tant, el termini inicial establert pel compliment de l'Esquema Nacional de Seguretat **finalitzarà el proper gener de 2011** per tots els sistemes preexistents.

Els nous sistemes han d'aplicar el que estableix l'ENS des de la seva concepció.

L’Esquema Nacional de Seguretat (III)

Compliment material:

Per complir amb l’Esquema Nacional de Seguretat resulta necessari aplicar un conjunt de mesures identificades en l’annex II de la norma, considerant els actius del sistema d’informació, la categoria del sistema i les decisions que s’adoptin per gestionar els riscos identificats.

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

- Establir una política de seguretat.
- Identificar els sistemes afectats.
- Determinar els riscos sobre els sistemes afectats.
- Categoritzar els sistemes afectats.
- Aplicar els controls i mesures corresponents, dels previstos a l’annex II de l’ENS.

Posicionament de CESICAT respecte L'ENS

CESICAT vol ser el referent de l'aplicació de l'ENS a Catalunya:

- Difusió I explicació de l'ENS a les administracions públiques I empreses consultores
- Formació als responsables de la seva aplicació I a les empreses consultores
- Publicació de guies I exemples d'aplicació de l'ENS
- Punt de trobada I switch de l'ENS a Catalunya
- Suport al teixit empresarial de seguretat per a la seva industrialització
- Assessorament legal I tecnològic

On som?

El CESICAT es troba ubicat a Reus, a l'edifici REDESSA

Adreça:

Edifici Redessa - Reus Desenvolupament Econòmic SA
Camí de Valls, 81-87
Reus 43204

Localització a la xarxa:

http://www.cesicat.cat/onsom.html

Per contactar amb el CESICAT podeu fer-ho per correu a:

info@cesicat.cat
977.010.893

Gràcies per la vostra atenció

info@cesicat.cat

	CESICAT	CESCA	esCERT-UPC	IRIS-CERT
Àmbitd'actuació	Administració Empreses Universitats Ciutadans	InstitucionsA nella	UPC	Institucions RedIRIS
Reactius				
Alertes	✓	✓	✓	✓
Gestió de vulnerabilitats	✓		✓	✓
Assistència in-situ	✓		✓	
Assistènciaremota	✓	✓	✓	✓
Preventius				
Guies de seguretat	✓			
Llistes de configuraciósegura	✓			
Anàlisi de vulnerabilitats	✓		?	?
Promoció				
Difusió de notícies	✓	✓	✓	✓