ÍNDEX

Versió	Redactat / revisat per	Aprovat per	Data aprovació	Data publicació
1.0.	CTTI – Qualitat i Seguretat	Comitè de Direcció del CTTI	26/05/2006	01/06/2006

RESPONSABLE DEL DOCUMENT: Silvia Garre (CTTI – Qualitat i Seguretat)

1 OBJECTIU

L'objectiu principal d'aquest procediment és establir un mecanisme per notificar a l'oficina de seguretat qualsevol incidència, deficiència o debilitat de seguretat detectada. L'oficina de seguretat, a partir de la informació proporcionada, serà l'encarregada de decidir la importància de l'incident i les accions a prendre.

Aquest procediment aplica, però no està limitat, a les següents situacions:

- Risc potencial d'incident (usuaris sense contrasenyes, sistemes antivirus que no s'actualitzen periòdicament, sistemes amb programari no actualitzat...)
- Intents (encara que fallits) d'obtenir accés a sistemes o dades de forma no autoritzada, modificar configuracions del maquinari...
- Interrupcions de servei no planificades
- Ús incorrecte dels sistemes (usuaris que comparteixen contrasenyes, màquines amb programari sospitós (sniffers, eines d'escaneig de xarxa...), informació indeguda emmagatzemada als sistemes...)
- Infeccions d'una o vàries màquines a l'hora per virus, troians, cucs...

2 ÀMBIT I VIGÈNCIA

Aquest document va dirigit a:

- Tots els components de l'oficina de seguretat
- Tots els components de l'equip de seguretat del CTTI
- Tots els components de cada un dels equips de seguretat de Serveis Centrals
- Coordinadors, gestors tecnològics i caps de projecte del CTTI
- SAU primer nivell
- Equips de suport a usuaris

Entrarà en vigor el dia 1 de Juny de 2006.

Aquest procediment romandrà vigent fins la propera versió aprovada del mateix.

3 DESCRIPCIÓ

a) Quan es detecti qualsevol incident o anomalia de seguretat, s'haurà de notificar el més ràpid possible per a què l'oficina de seguretat pugui prendre mesures. Quan més ràpid es notifiqui l'incident, més probabilitats hi ha de què la investigació portada a terme doni resultats positius.

b) Per fer la notificació, s'ha d'omplir el *Formulari de notificació d'incidents de seguretat*. És important donar la màxima informació i que aquesta sigui el més acurada possible. A més d'informar sobre l'incident, s'ha d'informar sobre com s'ha detectat, el seu abast, el tipus de màquines afectades (si són ordinadors personals o servidors), la importància dels serveis compromesos...

> **Atenció**: A l'hora de notificar un possible incident de seguretat, és important que la informació proporcionada sigui el més acurada possible, però s'ha d'evitar incloure informació sensible o confidencial com ara contrasenyes. Aquesta informació serà comunicada directament a l'oficina de seguretat per altres medis com telèfon o correu electrònic només si es sol·licitada.

La informació de contacte de la persona que notifica la incidència també és molt important, en cas que l'oficina de seguretat necessiti contactar per a obtenir més informació.

c) Formes de notificació: existeixen dues formes de notificar els incidents.

- L'habitual serà fer-ho mitjançant un correu al SAU en el que s'inclourà el formulari de notificació d'incidents complimentat:

sau.ctti@gencat.net

El títol del correu serà **INCIDENT DE SEGURETAT** per tal de facilitar la feina de selecció pel personal del SAU i que aquests la puguin prioritzar.

- Si no es pot utilitzar el correu, hi ha un número de telèfon disponible. Si la incidència es notifica per telèfon, es farà arribar el formulari complimentat per fax:

Núm. Telèfon	900 701 444
Núm. Fax	93 484 20 50

d) L'oficina de seguretat és responsable d'investigar tots els possibles incidents que li siguin comunicats, per ordre de criticitat, enviar una contestació a la persona que hagi enviat la notificació i decidir quines mesures s'han de prendre per a corregir-les.

4 DIVULGACIÓ

El CTTI publicarà aquest procediment a la seva intranet.

Quan apliqui, l'oficina de seguretat serà responsable de la distribució d'aquest procediment en l'entorn de Serveis Centrals de la Generalitat de Catalunya.

5 REVISIÓ

Aquest procediment ha de ser revisat com a mínim anualment.

6 GLOSSARI DE TERMES

Incidència: Qualsevol anomalia que no forma part de l'operativa normal d'un servei i que causi o pugui causar una interrupció o reducció del servei o afectar a la seva qualitat.

7 DOCUMENTACIÓ REFERENCIADA

- GE-FOR01 Formulari de Notificació d'Incidents de Seguretat.

8 PARAULES CLAU

Incident, incidència, notificació.

9 HISTÒRIC DEL DOCUMENT

Versió 1.0

Dates d'inici de cada fase:

Detecció de necessitat	*Fase de treball*	*Fase de discussió*	*Fase d'aprovació*	*Fase de difusió*	*Fase de suport*
06/02/2006	06/03/2006	03/04/2006	27/04/2006	01/06/2006	01/09/2006

Equip de treball: Qualitat i Seguretat: Silvia Garre, Josep Mangas, Oficina Seguretat (Indra)
Equip de discussió:
CTTI – Innovació i Tecnologia: Emili Platel, Joan Pérez, Marc Sunyer, Llorenç Coma, Llorenç Franco, Albert Haro
Indra - Marc Autó, Jordi Tarré
Òrgan aprovador: Comitè de Direcció del CTTI
Equip de suport: Oficina Seguretat