Procediment de seguretat de les entitats de registre idCAT:

Requisits i recomanacions

Control documental

Estat formal	**Elaborat per:** Àrea de Qualitat i Procediments	**Aprovat per:** Emma Suevos i Guillamet
Data de creació	25/03/2008	
Control de versions	**Data:**	27/01/2010
	Descripció:	Revisió general
Nivell accés informació	pública	
Títol	Distribució i enviament de certificats des de CATCert	
Fitxer	ER idCAT_PS.doc	
Control de còpies	Només les còpies disponibles a M:\NouPrometeo\Departaments\QualitatProcediments\Elaboracio_Procediments_D1131\Procediments_gestió_interna\Procediments_seguretat_ER_D1133 garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.	
Drets d'autor	Aquesta obra està subjecta a una llicència Reconeixement-No comercial-Sense obres derivades 2.5 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.	

Índex

1. Introducció

Aquest document pretén detallar els objectius de control necessaris per garantir la seguretat del servei de certificació digital, identificant uns mínims que totes les entitats de registre hauran de superar per poder iniciar i dur a terme la seva activitat.

El personal de l'Entitat de Registre T-CAT haurà de conèixer les diferents mesures de seguretat necessàries, per tal de prevenir les exposicions als riscos o robatoris d'informació i de recursos en el tractament de la informació.

En concret es divideixen en 4 àrees d'aplicació:

- Seguretat física
- Seguretat lògica
- Seguretat del personal
- Seguretat de l'arxiu

2. Seguretat física

Aquest apartat contempla les normes i mesures de seguretat física a implantar a les oficines de l'ER-idCAT, on es realitza la petició i aprovació de certificats.

- Les targetes dels operadors hauran d'estar custodiades de forma segura, és a dir, que estiguin sota clau mentre no es facin servir en possessió dels propis operadors.

Subministrament elèctric

- Es recomana que l'ER disposi subministrament elèctric alternatiu, ja que pot causar l'aturada del servei, encara que no és un requeriment obligatori.

Seguretat dels cablejats

- Es recomana que els cables de dades i els de corrent elèctric estiguin separats per evitar possibles interferències.

3. Seguretat del personal

Els procediments descrits en aquest apartat tenen com a objectiu assegurar que el personal de l'ER amb accés als processos crítics gaudeix d'un nivell de confiança i qualificació adequats per portar a terme les tasques que tenen assignades.

La política de contractació i formació del personal garanteix aquest aspecte crucial de la seguretat, ja que no només les accions malintencionades, sinó també els errors humans deguts a una escassa capacitació, poden posar en perill l'operació fiable de la infrastructura.

Tot el personal de l'ER, tant intern com extern, que utilitzi, dissenyi, operi o simplement tingui accés als recursos d'informació del SCD, ha de complir la política i procediments descrits en aquest apartat.

- A la finalització de qualsevol contracte laboral, l'empleat haurà de retornar al Responsable del servei les claus d'accés, les targetes criptogràfiques, codis accés a la sala d'operacions, caixa de seguretat.

- En aquest sentit, el Responsable del servei comunicarà a CATCert per a la revocació dels certificats d'operador corresponents de manera immediata mitjançant la corresponent sol·licitud de revocació.

- En cas que hagi de participar personal extern de l'ens en el servei de certificació digital, caldrà que hagin signat una clàusula de confidencialitat amb l'ens. Es recomana que s'apliquin accions disciplinàries per part de l'ens per aquells empleats que incompleixin les seves obligacions a aquest respecte.

4. Seguretat d'accessos lògics

El control d'accés als recursos de l'ER és imprescindible a l'hora de prevenir accessos no autoritzats, modificacions no autoritzades, destrucció o mal ús dels actius d'informació del SCD.

- Quan un hagi d'abandonar el lloc de treball durant uns minuts o més temps, haurà de bloquejar la pantalla del sistema, de manera que ningú que no sigui un usuari autoritzat pugui accedir a informació confidencial o fer una operació no permesa.

- Durant el procediment de *log-on* a aquestes màquines, no es mostrarà cap ajuda que pugui ser utilitzada per un usuari no autoritzat per tal d'intentar accedir-hi, com podria ser mostrar els noms dels usuaris amb accés a la màquina, mostrar la part de les dades introduïdes per l'usuari que són incorrectes en cas d'error en el *log-on*, o mostrar el darrer nom d'usuari que ha accedit al sistema.

RECOMANACIONS:

- Limitar el nombre d'accessos erronis, de forma que tres intents fallits suposin el bloqueig temporal dels comptes d'usuari.

- Configurar les màquines de manera que després d'un temps d'inactivitat de 15 minuts, les sessions es bloquegin de forma automàtica [1] i sigui necessari introduir l'identificador d'usuari i la paraula de pas.

RECOMANACIONS: Pel que fa a les claus de pas:

- longitud mínima de 8 caràcters.
- període de validesa de 3 mesos.
- contenir caràcters alfanumèrics
- contenir algun caràcter especial
- contenir majúscules i minúscules
- no estar basades en dades que puguin deduir-se d'una persona, ni ser fàcilment deduïbles
- ser fàcils de recordar
- no escriure-les en text clar i, per tant, fer-les accessible a altres persones;
- no compartir-les amb d'altres usuaris.

Números d'identificació personal (PINs)

[1] ISO 17799 9.5.7 Desconnexió automàtica de terminals

- Els PINs o números d'identificació personal que tindrà cada posseïdor d'un certificat digital que l'utilitzi a l'hora d'operar a la web es composarà d'entre 4 i 8 caràcters alfanumèrics.

- Els PINs utilitzats són confidencials, i els usuaris tenen el deure de no revelar-los a terceres persones.

- Quan un usuari oblidi el seu PIN o cregui que aquest s'ha vist compromès, disposa d'un PUK (*Personal Unblocking Key*, Clau de Desblocatge Personal), que li permet assignar un nou PIN al seu certificat.

Si, a més, l'usuari en qüestió no disposés de l'accés al seu PUK pel motiu que fos, seria necessària l'obtenció d'un nou certificat digital. Aquest procediment serà demanar la revocació de l'antic i sol·licitud d'un nou certificat a CATCert.

5. Seguretat d'arxiu

A continuació es detallen les mesures de seguretat, tant per l'arxiu de gestió (temporal) com per l'arxiu central, destinat a guardar la documentació un mínim de 15 anys. Aquests aspectes estaran ampliats al procediment de gestió documental i d'arxiu.

5.1 Arxiu de gestió

- La documentació haurà de ser guardada en un armari o caixa forta tancada, només accessible pel personal de l'ER que tingui un rol dins el servei de certificació digital idCAT.
- És un espai al qual només accedeix el personal autoritzat de l'ER.

5.2 Arxiu central

- Tindrà mesures de control ambiental: temperatura, humitat, sistemes anti-incendis i es troba lluny d'instal·lacions de risc: canonades aigua, quadres elèctrics, etc.
- La transferència a aquest arxiu es farà conforme indiqui el procediment d'arxiu que CATCert farà arribar a l'ER.

6. Referències

Aquestes normatives de seguretat, junt amb els documents relacionats, estan basades en els següents estàndards:

- Política de certificació i Declaració de pràctiques de certificació de CATCert
- Codis de bones pràctiques per la gestió de la seguretat de la informació:
  - UNE-ISO/IEC 27001
  - Criteris de seguretat del MAP
  - ETSI TS 101 456
  - Webtrust 1.0. Programa per Autoritats de Certificació
- Procediment de creació d'entitats de registre T-CAT de CATCert
- Llei 59/2003, de 19 de desembre, de signatura electrònica