Consorci
Administració Oberta
de Catalunya

Procediment de seguretat de les Entitats de Registre

Generalitat de Catalunya

LOCALRET

Realitzat per: Consorci AOC

Versió: 01

Data: 20/07/2022

Índex

1 Introducció

1.1 Objecte

Aquest document té per objecte establir els requisits mínims per garantir la seguretat del Servei de Certificació Digital (SCD), identificant les condicions de seguretat que totes les Entitats de Registre han de complir per iniciar i dur a terme la seva activitat d'acord amb la Declaració de Pràctiques de Certificació (DPC) i la Política de Certificació (PC) corresponent.

El Procediment de seguretat comprèn en 4 àmbits d'aplicació:

- Seguretat física
- Seguretat lògica
- Seguretat del personal
- Seguretat d'arxiu

1.2 Àmbit subjectiu

Les Entitats de Registre (ER) han de complir l'establert en el present document; aquestes són: els Ens Subscriptors, les Entitats de Registre de T-CAT (ER T-CAT) i les Entitats de Registre de ciutadania (ER idCAT).

El personal de l'ER ha de conèixer les mesures de seguretat enumerades en el Procediment de seguretat, per tal de prevenir les exposicions als riscos o robatoris d'informació i de recursos en el tractament de la informació.

1.3 Marc legal

Totes les actuacions del personal de les ER de l'ens subscriptor de certificats electrònics envers la seguretat en l'exercici de les funcions i activitats relacionades amb la prestació del SCD han d'estar subjectes i regulades per la normativa vigent en matèria de serveis de confiança, de seguretat i la DPC i les PC del Consorci AOC.

La relació detallada de la normativa està al punt 7 d'aquest Procediment de seguretat.

1.4 Responsabilitats

El responsable del servei a l'entitat és el responsable de la supervisió i aplicació d'aquest document. L'ER ha de garantir que les mesures de seguretat previstes en aquest document es duen a terme correctament.

2 Seguretat física

Els requisits de seguretat física estableixen mecanismes amb la finalitat d'impedir la intrusió de personal no autoritzat a las àrees restringides (intern i/o extern), en compliment del previst a la DPC.

Ofereixen protecció envers agents o circumstàncies que suposin un risc per a la informació, el personal, o el servei que es proporciona, com per exemple: incendis, inundacions o talls del subministrament elèctric.

Aquests requisits, que han de garantir la seguretat de l'entorn i s'han d'implantar a les oficines on es realitza l'emissió i gestió dels certificats, són:

- **Espais**:
  - Els locals on es tractin les dades han de disposar de mitjans mínims de seguretat: extintors, alarmes, sales amb clau i sistemes de control d'accés físic, en virtut del previst a la normativa[1].
  - Restringir l'accés als locals al/s responsables del servei i membres del personal, autoritzats pels anteriors i sota la seva responsabilitat.
  - Disposar d'un registre d'accessos als espais on es conserva la documentació (sol·licituds/revocacions, etc.).

    Si la documentació es guarda en format electrònic, s'ha de disposar d'un sistema que garanteixi l'accés exclusiu de les persones que ho requereixin en l'exercici de les funcions que tenen encomanades com a ens subscriptor i que permeti la traçabilitat dels accessos a la informació.
  - Disposar de subministrament elèctric alternatiu, per garantir el servei davant de possibles talls elèctrics
- **Custòdia de certificats**:
  - Desar el material sensible (targetes criptogràfiques i els certificats generats pendents de lliurar) en un espai d'accés restringit.
  - Disposar, com a mínim, d'un armari amb clau.
  - Custodiar de manera diligent les targetes dels operadors per ells mateixos.
  - Custodiar les targetes emeses fins que no s'han enviat als titulars, de manera que s'impedeixi l'accés a persones no autoritzades.
  - Guardar la sol·licitud d'emissió o revocació del certificat electrònic en paper en armaris tancats amb clau.
- **Eliminació i esborrat**:
  - Esborrar de forma segura la informació que continguin els suports que ja no es necessitin o es vulguin eliminar per qualsevol raó, de manera que la informació no sigui recuperable.
  - Destruir els plàstics de manera diligent.
  - Eliminar amb destructora de paper (o mecanisme similar) les informacions en paper que tinguin informació confidencial i s'hagin de retirar. Aquest requisit,

[1] DPC, PC, ENI, NTI, Normes ISO, etc., així com la normativa en matèria de protecció contra incendis.

només per la informació que no sigui necessari conservar durant 15 anys des de la data de caducitat del certificat.

3 Seguretat lògica

Els requisits de seguretat lògica determinen com han de ser les comunicacions i les operacions de les estacions de treball des d'on es porten a terme les tasques relatives al servei d'ER.

En el cas dels Ens Subscriptors, el responsable d'aplicar aquestes mesures és el Consorci AOC.

Aquests requisits, que s'estableixen en aplicació del previst a l'Esquema Nacional de Seguretat (ENS), són:

- Disposar d'un sistema anti-virus i anti-malware a les estacions de treball.
- Mantenir constantment actualitzades les estacions de treball amb les darreres actualitzacions de seguretat publicades pels fabricants del Sistema Operatiu i del programari instal·lat.
- Establir un sistema que permeti la identificació inequívoca i personalitzada de tot usuari que intenti accedir a l'estació de treball i la deguda autenticació per a verificar la identitat de l'usuari.
- Accedir a les webs pròpies del servei amb certificat electrònic donat d'alta a l'aplicació. Aquest certificat és personal i intransferible.
- Custodiar el certificat de forma diligent i per part del titular, per evitar que altres persones suplantin la seva identitat, signin documents en el seu nom, o accedeixin a missatges confidencials o sistemes d'informació d'accés restringit.
- En els casos en què els treballadors s'hagin d'absentar del seu lloc de treball mentre estiguin connectats a l'aplicatiu del SCD, bloquejar els ordinadors amb salvapantalles protegits per paraula de pas, per tal d'evitar que es pugui veure la informació que hi ha al terminal o que alguna altra persona pugui manipular la màquina.

Sense perjudici de l'anterior, amb la finalitat d'incrementar les garanties de seguretat lògica, es formulen les següents **recomanacions**:

- Disposar d'un sistema antivíric instal·lat a tots els equips del personal.
- Per evitar costos innecessaris i incompatibilitats, el programari utilitzat pot ser l'antivirus corporatiu de cada ens.

  És important que aquest antivirus no obligui instal·lar cap component de control de Navegació Web. Si el programari corporatiu té aquests components, s'han de deshabilitar en cas d'instal·lació.
- Actualitzar automàticament la protecció, a diari i a temps real, de forma que estigui permanentment activa.
- En el cas de les ER T-CAT, abstenir-se d'instal·lar programari que la doti de funcionalitats diferents al seu objectiu principal de servei de certificació T-CAT.

Tot i això, està permesa la instal·lació de programari que millori la seguretat de l'ER (es recomana la instal·lació d'un programa antivíric) o programari necessari per alguna tasca relacionada amb el servei de certificació T-CAT.

4 Seguretat del personal

Aquests requisits, tenen com a objectiu assegurar que el personal de l'ER amb accés als processos crítics compta 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 han de garantir aquest aspecte crucial de la seguretat, ja que no només les accions malintencionades poden posar en perill l'operació fiable de la infraestructura, sinó també els errors humans deguts a una escassa capacitació.

Tot el personal de l'ER, 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.

Els requisits són:

- **Qualificació**:
  - Garantir que el personal que intervé en el SCD està qualificat, garanteix un nivell de confiança i té l'experiència necessària per a la prestació dels serveis.
- **Baixes de personal**: el Responsable del servei ha de dur a terme les següents actuacions:
  - Assegurar-se el retorn de les claus d'accés (PIN i PUK) i les targetes criptogràfiques T-CAT a la finalització de qualsevol contracte laboral.
  - Eliminar o modificar els codis d'accés a espais segurs, caixa forta o aplicacions relacionades amb el servei del SCD.
  - En el cas de baixa temporal d'algun operador, obtenir la targeta per la seva correcta custòdia.
  - En cas de cessament de la relació laboral, sol·licitar al Consorci AOC la revocació immediata dels certificats mitjançant el formulari corresponent.
  - Actualitzar la fitxa del servei derivat de la situació anterior.
- **Personal extern**: en cas que participi personal extern de l'ens en el SCD, a més dels requisits en cas de baixa de personal intern, el responsable del servei ha de:
  - Signar una clàusula de confidencialitat amb l'ens.
  - Comunicar-ho al Consorci AOC per a la seva aprovació.

Sense perjudici de l'anterior, amb la finalitat d'incrementar les garanties de seguretat del personal, es formulen les següents **recomanacions**:

- En el cas del personal extern, aplicar accions disciplinàries per part de l'ens per aquells empleats que incompleixin les seves obligacions a aquest respecte.

- En el cas de baixa llarga del personal, valorar l'actuació més adient per aquell certificat: suspensió, revocació, etc.

5 Seguretat d'arxiu

Els requisits de seguretat d'arxiu s'estableixen en el Procediment d'Arxiu de les ER (publicat a la web del servei).

6 Auditories de control

El Consorci AOC auditarà el compliment, per part de les ER, dels requisits de seguretat i altres cada 24 mesos, com a mínim, per comprovar que compleixen els requisits de seguretat i d'operació necessaris per ser usuari de SCD.

A més, el Consorci AOC pot realitzar auditories de seguiment sota el seu propi criteri en qualsevol moment a causa d'una sospita d'incompliment d'alguna mesura de seguretat.

7 Referències

Aquest Procediment de seguretat, junt amb els documents relacionats, es basa en la següent normativa i estàndards:

- Declaració de pràctiques de certificació, Polítiques de certificats del Consorci AOC i Condicions específiques de prestació dels serveis.
- Reglament (UE) núm. 910/2014 del Parlament Europeu i del Consell de 23 de juliol de 2014 relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i per la que es deroga la Directiva 1999/93/CE.
- Directiva (UE) 2016/1148 del Parlament Europeu i del Consell de 6 de juliol de 2016 relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i sistemes d'informació a la Unió.
- Llei 6/2020 d'11 de novembre, Reguladora de determinats aspectes dels serveis electrònics de confiança.
- Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- UNE-EN-ISO 19011:2011 Directrices para la auditoria de los sistemas de gestión.
- UNE-EN-ISO/IEC 17065:2012 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment-Requirements for conformity assessment bodies assessing Trust Services Providers.
- Normatives incendis.
- Qualsevol altra relacionada amb la prestació de serveis de confiança.

8 Glossari

Declaració de pràctiques de certificació (DPC): és el document que estableix les condicions en què es gestionen les Entitats de Certificació i el cicle de vida dels certificats emesos per aquestes Entitats de Certificació.

Entitat de registre (ER): és un ens o departament que col·labora amb el Consorci AOC en la prestació de serveis de certificació a les administracions públiques catalanes.

Les ER passen a formar part de la jerarquia d'entitats de certificació de les entitats públiques de Catalunya i es regeixen per la regulació dels serveis de certificació així com tots els procediments operatius, de seguretat i d'arxiu.

En funció dels certificats que expedeixen, les ER poden ser T-CAT o idCAT, segons els emetin per a les administracions públiques o als ciutadans, respectivament.

Ens subscriptor: és l'organització que subscriu els serveis de certificació del Consorci AOC, és a dir, l'organització que sol·licita certificats al Consorci AOC o a les seves ER.

Fitxa d'entitat de registre: és el document on consten les dades de la mateixa entitat.

Fitxa de subscriptor: és el document mitjançant el qual l'ens comunica a l'ER les seves dades i les de les persones que intervindran en el procés de sol·licitud, gestió i distribució de certificats electrònics.

PIN i PUK: són els codis secrets necessaris per operar amb les targetes T-CAT.

El PIN és el codi d'ús de la targeta i el PUK, el codi de desbloqueig en cas de tres intents erronis amb el PIN (tant el PIN com el PUK permeten tres intents respectivament).

Polítiques de Certificació (PC): document que defineix els conceptes bàsics sobre la infraestructura de certificació i els criteris per a la gestió específica de cada família de certificats emesos per l'Entitat de Certificació del Consorci AOC.

Responsable del servei: és la persona responsable de l'ER. Entre les seves funcions es responsabilitza de lliurar els certificats electrònics als titulars, de fer-los signar la documentació legal, d'arxivar-la convenientment i també d'informar-los de les seves obligacions i responsabilitats als sol·licitants.

SCD: acrònim de "Servei de Certificació Digital" del Consorci AOC.

Titular del certificat: és la persona llur nom consta en el certificat, en el cas dels certificats personals, d'entitat o d'infraestructura, o a qui es va emetre un certificat, en el cas dels de dispositiu.