Política d'evidència electrònica de la UOC

Document aprovat pel Consell de Direcció de la UOC el dia 8 de febrer de 2016

Índex

1. Introducció

Aquest document conté les normes d'evidència electrònica de documents, comunicacions i altres actes de procediments acadèmics i de gestió electrònics de la Universitat Oberta de Catalunya (UOC).

Aquest document estableix la política d'evidència electrònica de la UOC, d'acord amb els requisits de seguretat i proporcionalitat corresponents als sistemes electrònics de suport a procediments acadèmics i de gestió electrònics, definits en les normes que regulen l'ús dels mitjans electrònics en els serveis públics.

Els continguts d'aquesta política d'evidència electrònica s'han estructurat per a cobrir els controls que preveuen la norma internacional ISO/IEC 27002:2006 – Tecnologia de la Informació: Tècniques de seguretat: Codi de pràctiques per a la gestió de la seguretat de la informació, en especial les seccions 12 i 15.1.3, i la norma britànica BS 10008:2008 – Valor evidencial i admissibilitat legal d'informació electrònica: Especificació.

2. Continguts generals de la política d'evidència electrònica

2.1. Identificació de la política d'evidència electrònica

Aquesta política d'evidència electrònica s'identifica amb el següent identificador d'objecte: 1.3.6.1.4.1.43653.1.7

2.2. Vigència

Aquesta política d'evidència electrònica entra en vigor l'endemà del dia de ser aprovada.

2.3. Àmbit d'aplicació

Aquesta política és aplicable a tots els sistemes d'informació de suport a procediments acadèmics i de gestió electrònics emprats per la UOC.

3. Normes generals d'evidència electrònica

Els sistemes d'informació que gestionin informacions, sigui en format documental, estructurat o de qualsevol altra manera, que hagin de tenir garantit el valor evidencial, han d'implantar els controls següents:

- Captura d'informació, incloent-hi:
    - Procediments per a la generació d'informació.
    - Procediments per a la importació d'informació.
    - Procediments per a la digitalització de documents.
    - Extracció de dades.
    - Captura de metadades.
- Tractament dels objectes digitals automodificables, com, per exemple, els fitxers amb un codi actiu que permeti fer diferents representacions del contingut.
- Tractament dels objectes digitals compostos, com els expedients electrònics, els documents amb un moltes parts o els registres correlats de diaris d'activitat.
- Tractament del control de versions dels objectes digitals.
- Emmagatzematge de la informació, incloent-hi:
    - Procediments per a demostrar que la informació no ha estat alterada.
    - Ús de tecnologia d'emmagatzematge adequada.
    - Implantació de procediments de migració.
    - Ús de formats d'emmagatzematge.
    - Procediments de conversió de fitxers.
- Transferència d'informació, incloent-hi:
    - Procediments de preparació d'objectes digitals, remoció de codi maliciós, ús de tècniques de compressió, ús de xifratge, determinació i verificació de la identitat de les parts, ús de signatures electròniques, conversió a altres formats de fitxers, selecció de canal, procediments d'inici, recepció i control de qualitat d'enviament.
    - Mecanismes i canals de transmissió.
    - Reglamentació jurídica dels sistemes de transmissió, com el correu electrònic o les xarxes interadministratives o interuniversitàries.
- Indexació de la informació.

– Procediments de sortida autenticada de la informació emmagatzemada.

– Gestió de la identitat de les parts referides a la captura i transmissió de la informació evidencial.

– Disposició/destrucció de la informació evidencial.

– Procediments i mesures de seguretat de la informació, incloent-hi:

  - Control d'accés a la informació.
  - Ús del xifratge.
  - Ús de les signatures electròniques.
  - Còpies de rescabalament de la informació.
  - Planificació de continuïtat del negoci.

– Manteniment del sistema.

– Ús de proveïdors externs, incloent-hi:

  - Adequació dels procediments del tercer.
  - Compliment legal.
  - Seguretat en la transferència.

– Prova del sistema d'informació.

– Auditoria interna i externa.

– Millora del sistema.

En particular, aquests controls s'han d'aplicar en els casos següents:

- Publicació amb efecte legal davant de tercers, com, per exemple, el tauler d'anuncis o edictes o el perfil de contractant.
- Comunicació i notificació.
- Expedients electrònics.

4. Normes d'evidència electrònica forense

La gestió de registres de seguretat és una pràctica de seguretat cada vegada més important per a les organitzacions, atès que només l'existència d'una funció de gestió dels registres de seguretat garanteix que es generen i es conserven registres amb prou informació durant els terminis legalment exigibles.

La revisió rutinària dels registres de seguretat permet identificar incidents de seguretat, infraccions de les normatives de seguretat, activitats fraudulentes i problemes operatius poc temps després que s'hagin produït, i ofereix informació molt útil per a investigar i resoldre el problema.

Així mateix, els registres de seguretat són importants per a fer activitats d'auditoria i d'anàlisi forense, ja que permeten oferir suport a les recerques internes, a l'establiment de línies base de seguretat i a la identificació a llarg termini de tendències operatives i problemes continus al llarg del temps.

La UOC, per a garantir el valor evidencial dels seus registres d'activitat, en particular de tots els sistemes de nivell alt en la dimensió de traçabilitat, ha d'implantar un sistema de gestió de registres de seguretat, amb les funcions següents:

- Generació i captura dels registres de seguretat:
    - Interpretació i extracció de dades.
    - Filtratge d'esdeveniments.
    - Agregació d'esdeveniments.
- Emmagatzematge dels registres de seguretat:
    - Rotació de registres de seguretat.
    - Arxivament de registres de seguretat, incloent-hi la retenció i la preservació.
    - Compressió de registres de seguretat.
    - Reducció de registres de seguretat.
    - Conversió de registres de seguretat.
    - Normalització de registres de seguretat.
    - Comprovació d'integritat de registres de seguretat.
- Anàlisi dels registres de seguretat:
    - Correlació d'esdeveniments.
    - Revisió de registres de seguretat.
    - Informes sobre registres de seguretat.
    - Assegurament de prova, particularment mitjançant l'ús de tercers de confiança.

– Disposició (eliminació) dels registres de seguretat.

En sistemes d'informació de nivell alt en la dimensió de traçabilitat, s'han de registrar totes les activitats dels usuaris en els sistema determinades per l'anàlisi de riscos. Aquests registres han de recollir la informació següent:

- Qui fa l'activitat, quan la porta a terme i sobre quina informació.
- L'activitat dels usuaris i, especialment, la dels operadors i administradors del sistema quan puguin accedir a la configuració dels sistema i actuar en el seu manteniment.
- Les activitats realitzades amb èxit i els intents que han fracassat.

A més a més, en aquests sistemes s'han d'establir les mesures de seguretat següents:

- Determinar el període de retenció dels registres.
- Assegurar la data i hora.
- Impedir la modificació i l'eliminació dels registres per part del personal.
- Protegir les còpies de seguretat dels registres, amb els mateixos requisits.

5. Desenvolupament de la política

Aquesta política s'ha de desenvolupar mitjançant els instruments següents, que s'han de publicar en els espais de comunicació de la comunitat:

– Estàndards tècnics de mecanismes d'evidència electrònica.
– Procediments operatius d'evidència electrònica
– Guies i recomanacions d'evidència electrònica.