Política d'autenticació 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'autenticació aplicables a 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'autenticació 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'autenticació s'han estructurat per a cobrir els controls que preveu 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 11 i 15.1.3.

2. Continguts generals de la política d'autenticació

2.1. Identificació de la política d'autenticació

Aquesta política d'autenticació s'identifica amb el següent identificador d'objecte: 1.3.6.1.4.1.43653.1.4

2.2. Vigència

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

2.3. Àmbit d'aplicació de la política d'autenticació

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'autenticació

La UOC ha de considerar el sistema d'identificació i autenticació dels usuaris en la seva arquitectura de seguretat i en el disseny dels sistemes d'informació de nivell mitjà, amb una atenció especial a l'autenticació en la producció i gestió de documents electrònics.

Els mecanismes d'autenticació han de comprovar la identitat de l'usuari que intenta accedir a un sistema o a una informació de manera inequívoca i personalitzada en accessos locals i remots, i també ha de desbloquejar el lloc de treball en sistemes de nivell mitjà.

En els sistemes de categoria de seguretat de nivell alt, s'han de definir punts d'accés que exigeixin la renovació de l'autenticació de l'usuari mitjançant una identificació singular, no havent-hi prou amb la sessió establerta.

La fortalesa i la fiabilitat dels mecanismes d'autenticació s'han d'establir segons la sensibilitat de la informació que es vulgui protegir, d'acord amb el que estableixi aquesta política.

Els usuaris s'han d'autenticar per a accedir als sistemes i a la informació que suporten, de manera que els sistemes puguin reconèixer (identificació) i comprovar (autenticació) la identitat de l'usuari que hi accedeix, d'acord amb les normes següents:

- Cada compte ha d'estar associat a un identificador únic. D'aquesta manera, s'ha d'assignar un identificador singular per a cada entitat (usuari o procés) que accedeixi al sistema, de tal manera que es pugui saber qui el rep i quins drets d'accés rep, i també qui ha fet alguna cosa i què ha fet.

- L'usuari ha de reconèixer que ha rebut les informacions d'autenticació, i que coneix i accepta les obligacions que implica la tinença d'aquestes informacions, particularment el deure de custòdia diligent, de protecció de la confidencialitat i d'informació immediata en cas de pèrdua.

- Les pantalles de presentació dels sistemes que siguin prèvies al mecanisme d'autenticació han de mostrar la informació mínima necessària, i no han d'oferir cap informació del sistema operatiu, de l'organització, de la configuració de xarxa, etc.

- L'autenticació d'un usuari s'ha de fer un cop s'hagi introduït tota la informació necessària per a la validació. Si l'autenticació és errònia, el sistema només ha de donar informació anònima de la qual no es pugui interpretar quina ha estat la seqüència del procés que ha fallat.

- Els comptes d'usuari s'han de bloquejar si hi ha més de cinc intents fallits d'autenticació, i s'estableix un temps mínim de reactivació de cent vint minuts.

– Les informacions d'autenticació s'han de canviar amb una periodicitat marcada per la política de l'organització, d'acord amb la categoria del sistema al qual s'accedeix.

– Les informacions d'autenticació s'han de retirar i deshabilitar quan l'entitat (persona, equip o procés) que autentiquen acaben la relació amb el sistema.

– Els comptes s'han d'inhabilitar en els casos següents: quan l'usuari deixa l'organització, quan l'usuari cessa en la funció per a la qual es requeria el compte d'usuari, o quan la persona que va autoritzar el compte dóna una ordre en sentit contrari.

– Els comptes es retindran durant el període necessari per a atendre les necessitats de traçabilitat dels registres d'activitat associats a aquestes necessitats (període de retenció).

– Quan s'interconnecten sistemes en els quals la identificació, l'autenticació i l'autorització tenen lloc en diferents dominis de seguretat, sota responsabilitats diferents, en els casos en què sigui necessari, les mesures de seguretat locals s'han d'acompanyar dels acords de col·laboració corresponents que delimitin mecanismes i procediments per a l'atribució i l'exercici de les responsabilitats de cada sistema.

4. Autenticació basada en contrasenya

En general, l'ús de la contrasenya es considera un mecanisme només vàlid per a la comprovació prèvia de la identitat d'un usuari que ha d'accedir a un document, sense perjudici de la possibilitat d'ús de la contrasenya per a determinades actuacions, segons el que s'estableix en la *política de signatura electrònica*.

Es considera més idoni l'ús de sistemes d'autenticació robusta, com es disposa a la secció següent.

En tot cas, l'ús d'aquests mecanismes es limita a sistemes de categoria de seguretat corresponents a nivells baix i mitjà. En el nivell mitjà, a més a més, l'ús d'aquests mecanismes s'hauria de fer, preferentment, en combinació amb un segon factor d'autenticació.

4.1. Generació i distribució de contrasenyes

Les contrasenyes inicials dels usuaris han de ser sempre diferents i aleatòries, de manera que no es pugui utilitzar la mateixa contrasenya per defecte.

La distribució de les contrasenyes s'ha de fer separadament de la comunicació de l'identificador associat, garantint en tot el procés la confidencialitat i la integritat de les contrasenyes.

4.2. Canvi de contrasenyes

L'administrador, si cal que faci el canvi d'una contrasenya (per exemple, perquè l'usuari l'ha oblidat), ha d'identificar de manera inequívoca i fefaent l'usuari que la sol·liciti i la hi ha de comunicar per un mitjà que garanteixi la seva identitat (per exemple, mitjançant el correu electrònic personal).

En els casos en què no sigui possible la identificació inequívoca de l'usuari que sol·licita la reinicialització o el canvi de la contrasenya, l'administrador ha de poder requerir la confirmació (telefònica, per correu electrònic, etc.) de la sol·licitud al superior jeràrquic o funcional del sol·licitant.

Opcionalment, per a la identificació inequívoca del sol·licitant en el procediment de reinicialització o de canvi de la contrasenya, els sistemes o administradors han de poder establir mecanismes de desafiament/resposta partint d'informacions particulars o personals prèviament acordades amb l'usuari sol·licitant.

Sempre que les contrasenyes siguin iniciades o canviades pels administradors, s'ha de forçar l'usuari a canviar la contrasenya en el primer accés.

S'ha de forçar el canvi de les contrasenyes que no s'hagin canviat en un període de més de cent vuitanta dies.

S'han d'oferir mecanismes que permetin a l'usuari fer el canvi de contrasenya en qualsevol moment. Aquests mecanismes han de complir les normes següents:

- Les contrasenyes no s'han de visualitzar a la pantalla mentre s'introdueixen.
- S'ha de demanar la contrasenya antiga abans de continuar el procés de canvi de contrasenya.
- S'ha de demanar la confirmació de la nova contrasenya abans de fer el canvi (per a evitar possibles errors d'escriptura).
- No s'ha de permetre la reutilització de les dues darreres contrasenyes que l'usuari hagi fet servir.
- S'ha de comprovar que la sintaxi de la nova contrasenya és correcta abans de fer el canvi.

Qualsevol identificador i contrasenya establerts per defecte en la instal·lació d'una aplicació, d'un programa o d'un sistema, s'ha de canviar.

4.3. Sintaxi de les contrasenyes

Les contrasenyes han de tenir com a mínim 8 caràcters.

La sintaxi de les contrasenyes ha de complir les normes següents:

- Hi ha d'haver, com a mínim, lletres (majúscules i minúscules) i xifres.

- No s'ha de poder endevinar amb tècniques basades en el diccionari i en regles, per la qual cosa no es poden fer servir paraules que estiguin relacionades amb l'usuari (domicili, data de naixement, DNI, etc.).

4.4. Transmissió de les contrasenyes

En general, es recomana utilitzar serveis criptogràfics per a protegir les contrasenyes mentre es transmeten, fins i tot en els accessos locals de la intranet. Aquests serveis han de complir la *política de seguretat criptogràfica*.

S'ha de prohibir d'una manera expressa l'enviament de contrasenyes en text net per canals i mitjans de transmissió oberts o d'accés públic (tots excepte els accessos locals de la intranet).

4.5. Emmagatzematge de les contrasenyes

Les contrasenyes no s'han de visualitzar a la pantalla mentre s'introdueixen en el procés d'autenticació.

Les contrasenyes no s'han d'escriure en documents personals de cap mena de suport, com ara papers, agendes electròniques, fitxers de text, etc.

Les contrasenyes no s'han d'emmagatzemar en text net, sinó que s'han d'emmagatzemar codificades o xifrades amb el màxim nivell de restricció d'accés possible, de manera que se'n pugui garantir la confidencialitat i la integritat.

Es recomana evitar que es puguin localitzar per defecte, en el sistema de fitxers, els que emmagatzemin contrasenyes, i també evitar denominacions de fitxer que permetin inferir aquest tipus de continguts.

Es recomana no incloure contrasenyes en mecanismes o seqüències d'autenticació d'accés automàtic a sistemes. En cas que aquests mecanismes siguin necessaris, les contrasenyes utilitzades s'han d'emmagatzemar en:

- Fitxers codificats i amb accés restringit.

– Dins del mateix codi de l'aplicació, amb la contrasenya distribuïda entre diverses variables per a dificultar que es pugui descobrir.

S'han d'establir procediments auditables de generació, emmagatzematge, gestió i canvi de les contrasenyes dels identificadors d'administració i dels identificadors pertanyents a mecanismes o seqüències d'autenticació d'accés automàtic als sistemes. Aquests procediments han de garantir la confidencialitat, la integritat i la disponibilitat d'aquestes contrasenyes.

5. Autenticació robusta

Sempre que sigui possible, en sistemes de categoria de seguretat de nivell mitjà, s'han de fer servir mecanismes d'autenticació robusta de manera complementària o substitutiva de l'autenticació basada en la contrasenya o en altres mètodes menys segurs.

En sistemes de nivell alt, la UOC ha de fer servir, necessàriament, mecanismes d'autenticació robusta, i en cap cas es poden utilitzar sistemes basats en contrasenyes.

Els mecanismes d'autenticació robusta s'han de basar en sistemes criptogràfics aprovats, d'acord amb el que disposa la *política de seguretat criptogràfica*, i, en particular, en certificats digitals de nivell 3 o superior en sistemes de nivell baix o nivell mitjà, i en certificats digitals de nivell 4 en sistemes de nivell alt, segons el que s'estableix en la *política de certificació de clau pública*.

Els certificats que cal emprar per a l'autenticació han de ser, en general, els següents:

– Protecció de la identitat web: certificats de seu electrònica, almenys de nivell mitjà[1] en seus de nivell baix o mitjà, i de nivell alt[2] en béns d'equipament criptogràfics en nivell alt.

– Actuacions acadèmiques i de gestió electròniques:
  - Actuació manual: certificat personal d'identificació de nivell 3 o 4.
  - Actuació automàtica: segell electrònic de nivell mitjà o alt.

– Actuació d'intercanvi de dades o d'accés a dades amb administracions públiques:
  - Els certificats admesos per cada organisme que cedeix dades a la UOC o hi dóna accés.

– Actuació dels ciutadans:
  - El certificat d'autenticació incorporat en el DNI electrònic.

[1] Aquests certificats estan en suport lògic o programari.

[2] Aquest certificats estan en dispositius criptogràfics robusts.

- Tots els certificats admesos per a aquest ús d'acord amb la *política de certificació* de la UOC, de nivell 3 o superior.

6. Desenvolupament de la política

Aquesta política s'ha de portar a terme mitjançant els instruments següents:

- Estàndards tècnics de mecanismes d'autenticació.
- Guies i recomanacions d'autenticació.
- Procediments operatius d'autenticació.