ÍNDEX

RESUM 2
1. OBJECTIU I MOTIVACIÓ 3
2. ÀMBIT I VIGÈNCIA 3
3. COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT 3
4. DESCRIPCIÓ 3
5. CONTROL 5
6. PENALITZACIONS 5
7. DIVULGACIÓ 6
8. REVISIÓ 6
9. GLOSSARI DE TERMES 6
10. DOCUMENTACIÓ REFERENCIADA 6
11. PARAULES CLAU 6
12. HISTÒRIC DEL DOCUMENT 6

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
2.0	CTTI – QSRaP	CTTI - QSRaP	28/1/2009	1/2/2009

Estàndard signat digitalment pel:
Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
2009.01.30 14:19:13 +01'00'

RESPONSABLE DEL DOCUMENT: Silvia Garre (CTTI – Qualitat, Seguretat i Relació amb Proveïdors)

RESUM

1. Objectiu: Establir els requeriments per a gestionar els comptes d'usuari sobre els sistemes d'informació de la Generalitat de Catalunya.

2. Àmbit: Sistemes de tractament d'informació on estiguin definits comptes d'usuari i les corresponents contrasenyes.

4. Descripció:

- Construcció de les contrasenyes
- Confidencialitat de les contrasenyes
- Vigència de les contrasenyes
- Canvi de les contrasenyes
- Entrega de les contrasenyes
- Relatiu als sistemes
- Contrasenyes de comptes amb privilegis d'administració
- Tractament d'incidències

1. OBJECTIU I MOTIVACIÓ

L'objectiu d'aquest document és desenvolupar la guia a aplicar pel tractament de les contrasenyes que s'usen per accedir als sistemes d'informació de la Generalitat de Catalunya.

Per a garantir la protecció i autenticació d'accés als sistemes, és important que les contrasenyes compleixin uns requisits mínims que garanteixin la robustesa del sistema.

2. ÀMBIT I VIGÈNCIA

Aquesta guia va dirigida a tota persona que disposi d'un usuari i la corresponent contrasenya que li permeti identificar-se i accedir a qualsevol sistema d'informació de la Generalitat de Catalunya.

Entrarà en vigor el dia 1 de febrer de 2009.

Aquesta guia romandrà vigent fins la propera versió aprovada de la mateixa.

És d'obligat compliment en l'àmbit dels *Serveis TIC Centrals*.

Es recull com a excepció la norma N10 en l'àmbit del Directori Corporatiu de la Generalitat de Catalunya, mentre s'analitza amb la Secretaria General Funció Pública i Modernització de l'Administració l'impacte i pla d'implantació.

3. COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT

La present guia proporciona cobertura a aspectes recollits en els següents controls de la ISO 27002:2005:

- 11.2.3 Gestió de les contrasenyes d'usuari
- 11.3.1 Ús de les contrasenyes
- 11.5.3 Sistema de gestió de les contrasenyes

4. DESCRIPCIÓ

Construcció de les contrasenyes.

N1. Les contrasenyes hauran de tenir una longitud mínima 8 caràcters.

N2. Han de contenir obligatòriament almenys un caràcter de cada un dels següents grups: numèric, alfabètic (majúscules i minúscules) i, si el sistema ho permet, caràcters especials (*, +, $, &, #, @, -, !, %, ^, *, ;, (,), {, }, [,], <, >, ?, /,_).

N3. No poden ser formades únicament per paraules de diccionari o altres fàcilment predictibles o associables a l'usuari (identificador d'usuari, inicials o nom de l'usuari, noms de família, direccions, matrícules, etc.).

Confidencialitat de les contrasenyes

N4. És responsabilitat de l'usuari mantenir les contrasenyes en secret.

N5. La contrasenya és d'ús exclusiu de l'usuari al qual pertany.

N6. No poden ser escrites ni enviades via correu electrònic sense xifrar.

N7. Si és necessari emmagatzemar les contrasenyes en un registre, aquest ha de ser xifrat i amb l'accés controlat només a les persones autoritzades.

N8. Mai no es donarà la contrasenya a un usuari administrador. Aquest disposa de les eines per canviar-la, sense necessitat de conèixer la contrasenya vigent.

N9. No utilitzar en l'àmbit professional les mateixes contrasenyes que es fan servir a nivell particular.

Vigència i canvi de les contrasenyes

N10. Les contrasenyes tindran una vigència màxima de 90 dies. Per entorns no ubicats en l'àmbit dels Serveis TIC Centrals, es podrà especificar un període de temps adequat a les necessitats de l'organització.

Es recomana reduir el temps màxim de vigència de les contrasenyes, en sistemes que estiguin exposats a xarxes públiques o siguin vulnerables a atacs de força bruta per obtenir les contrasenyes. L'antiguitat màxima ha de ser proporcional al risc i confidencialitat de les dades protegides per les contrasenyes.

N11. En els sistemes que tècnicament sigui possible, s'avisarà amb una antelació de cinc dies laborables als usuaris, quan la contrasenya vagi a caducar.

N12. Al realitzar el canvi de les contrasenyes no es podran reutilitzar com a mínim les 10 últimes contrasenyes.

N13. En els sistemes que tècnicament sigui possible, el sistema haurà de validar la qualitat de la contrasenya abans d'acceptar-la.

N14. Caldrà canviar la contrasenya a la primera connexió que realitzi l'usuari al sistema, i sempre que s'hagi produït reinicialització de la contrasenya per part de l'administrador.

N15. Caldrà canviar la contrasenya quan se sospiti que d'altres persones en puguin tenir coneixement.

N16. Quedaran exempts del compliment dels requeriments indicats en aquest apartat (vigència i canvi de contrasenya) els usuaris utilitzats per a tasques automàtiques (execució scripts, transferència de fitxers, etc), així com entorns on l'usuari no pugui realitzar el canvi de contrasenya de forma automàtica. En aquests casos caldrà aplicar controls addicionals:

a) Inhabilitar l'accés a la consola del sistema.

b) Definir els mínims privilegis necessaris tant d'accés com d'execució.

c) Mantenir un registre dels usuaris, indicant la persona o grup responsable dels mateixos.

d) Pels entorns on l'usuari no pugui realitzar el canvi de forma automàtica, el responsable d'aquests haurà de sol·licitar un canvi de contrasenya de forma periòdica mitjançant els canals establerts.

Entrega de les contrasenyes per persones autoritzades

N17. Les contrasenyes s'hauran d'entregar de manera segura als usuaris. No es podran usar missatges de correu electrònic sense xifrar. Son mètodes vàlids per l'entrega: Entrega personal, correu electrònic xifrat, correu postal o missatgeria, correu intern precintat.

Relatiu als sistemes

N18. El nom d'usuari i la contrasenya s'han de transmetre xifrades per la xarxa.

N19. Quan s'introdueixi la contrasenya en els sistemes, mai no ha d'aparèixer de manera visible i llegible a la pantalla.

N20. No està permès incloure contrasenyes sense xifrar dins del codi d'aplicacions o *scripts*. Com a alternativa, es pot emmagatzemar aquestes contrasenyes en fitxers amb accés restringit només als usuaris amb privilegis d'execució.

N21. Els identificadors i contrasenyes per defecte dels sistemes seran canviades o inhabilitades immediatament després de la instal·lació.

N22. S'habilitarà un sistema de protecció de pantalla amb contrasenya que s'activarà després de més de 15 minuts d'inactivitat.

N23. Els comptes d'usuari es bloquejaran després de 5 intents infructuosos d'accés.

N24. Els sistemes no acceptaran contrasenyes en blanc.

Contrasenyes de comptes amb privilegis d'administració

N25. Per a la definició i gestió de les contrasenyes de comptes amb privilegis d'administració, caldrà aplicar les normes indicades en la *Guia de gestió de comptes d'administració de sistemes*.

Tractament d'incidències

N26. En cas d'oblit de la contrasenya, o bloqueig per acumulació d'intents fallits d'accés al sistema, es sol·licitarà la reinicialització de la contrasenya mitjançant els procediments establerts, prèvia verificació de la identitat de l'usuari sol·licitant.

Es recomana implementar sistemes de desafiaments pregunta-resposta quan sigui possible per permetre al propi usuari la reinicialització de la contrasenya.

N27. Qualsevol incident de seguretat relacionat amb la gestió de les contrasenyes haurà de ser comunicat en la major brevetat possible mitjançant el *Procediment de notificació d'incidents de seguretat.*

Recomanacions a l'hora d'escollir una contrasenya

R1. Evitar utilitzar paraules de diccionari de qualsevol llenguatge.

R2. No crear noves contrasenyes que simplement incrementin un dígit de la contrasenya actual.

R3. Evitar l'ús de contrasenyes que comencin o acabin amb números, donat que poden ser deduïdes més fàcilment que si els números estan al mig de la contrasenya.

R4. Evitar utilitzar contrasenyes que terceres persones puguin deduir fàcilment de l'entorn de la taula de treball (mascotes, equips d'esports, familiars...)

R5. Evitar utilitzar paraules de la cultura popular.

R6. Utilitzar contrasenyes que requereixen de les dues mans per a introduir-les al teclat.

R7. Utilitzar espais en blanc i caràcters que es generin mitjançant la tecla ALT.

5. CONTROL

Per a l'àmbit dels *Serveis TIC Centrals*, el control del compliment d'aquesta guia es realitzarà mitjançant auditories periòdiques segons s'estableix en el *Pla d'auditories de seguretat*. Per altres àmbits, es recomana realitzar auditories cada 6 mesos.

En el cas que no s'apliqui algun dels controls d'aquesta guia, caldrà justificar i documentar aquestes excepcions. Per a l'àmbit dels *Serveis TIC Centrals*, cada excepció a un control haurà de ser validada prèviament per l'Oficina de Seguretat i autoritzada per Qualitat i Seguretat CTTI.

Caldrà mantenir un registre on quedin recollides totes les excepcions, a disposició de les auditories.

6. PENALITZACIONS

En cas d'incompliment d'aquesta guia per part de personal subcontractat, aplicaran les penalitzacions recollides en el contracte de la prestació del servei.

Si l'incompliment és per part de personal intern de la Generalitat de Catalunya pot determinar, si s'escau, l'aplicació del règim disciplinari corresponent.

7. DIVULGACIÓ

L'àrea de Qualitat, Seguretat i Relació amb Proveïdors del CTTI publicarà aquesta guia al repositori d'estàndards de la intranet del CTTI.

8. REVISIÓ

Aquesta guia es revisarà anualment.

9. GLOSSARI DE TERMES

Desafiaments pregunta – resposta: Conjunt de preguntes a les quals l'usuari ha de respondre en un primer moment d'inicialització. En cas d'oblit de la contrasenya, si l'usuari contesta correctament les preguntes (introduint les mateixes respostes que va donar en el moment de la inicialització), el sistema li permetrà canviar la contrasenya, sense necessitat d'introduir la contrasenya vigent.

Script: conjunt d'instruccions tècniques a executar en un sistema de manera automàtica.

10. DOCUMENTACIÓ REFERENCIADA

- GE-GUI20 Guia de gestió de comptes administració sistemes
- GE-PRO01 Procediment de notificació d'incidents de seguretat

NOTA: Consultar els documents en la seva última versió.

11. PARAULES CLAU

Contrasenya, vigència, xifrar, paraula de pas.

12. HISTÒRIC DEL DOCUMENT

Versió 1.0
Versió inicial

Versió 2.0.
Revisió de continguts. Veure la fitxa de l'estàndard per a més informació.
Aquesta versió unifica la *GE-GUI19-01 Contrasenyes*, amb la *SC-NOR05-01 Contrasenyes* en un sol document. La GE-GUI19-01 passa a ser d'obligatòria implantació en l'entorn dels *Servei TIC Centrals*.