Llicència Creative Commons:

Reconeixement – No Comercial – CompartirIgual 2.5.

Sou lliure de copiar, distribuir i comunicar públicament l'obra, així com de fer-ne obres derivades**, en les següents condicions:**

Reconeixement. Heu de reconèixer els crèdits de l'obra de la manera especificada per l'autor o el llicenciador.

No comercial. No podeu utilitzar aquesta obra per a finalitats comercials.

Compartir amb la mateixa llicència. Si altereu o transformeu aquesta obra, o en genereu obres derivades, només podeu distribuir l'obra generada amb una llicència idèntica a aquesta.

- Quan reutilitzeu o distribuïu l'obra, heu de deixar ben clar els termes de la llicència de l'obra.
- Alguna d'aquestes condicions pot no aplicar-se si obteniu el permís del titular dels drets d'autor.

Podeu trobar el text legal de la llicència a: Creative Commons Attribution-NonCommercial-ShareAlike 2.5 License

ÍNDEX

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, Oficina Seguretat, Lots	CTTI – Qualtitat, Seguretat i Relació amb Proveïdors	25/2/2009	9/3/2009

Estàndard signat digitalment pel:
Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
2009.02.25 12:48:09 +01'00'

RESPONSABLE DEL DOCUMENT: CTTI – Qualitat, Seguretat i Relació amb Proveïdors

RESUM

1. Objectiu: Establir les pautes per una bona gestió dels comptes que disposen de privilegis d'administració sobre els sistemes d'informació de la Generalitat de Catalunya.

2. Àmbit: Sistemes de tractament d'informació on s'utilitzin comptes d'administració i els usuaris amb privilegis d'administració.

4. Descripció:

- Definició dels comptes
- Accés als sistemes
- Característiques de les contrasenyes
- Auditoria
- Estacions de treball
- Administració remota
- Tractament d'incidències

5. Recomanacions

1. OBJECTIU I MOTIVACIÓ

Els sistemes que processen la informació necessiten per la seva instal·lació i manteniment de comptes amb privilegis d'administració. Es diferencien dels comptes d'usuari del sistema en què tenen capacitat de modificar la configuració del sistema, així com accedir a la informació emmagatzemada.

Dintre de les tasques d'administració dels sistemes es poden definir diferents perfils que permeten realitzar una segregació de funcions, per adequar les necessitats d'accés a la informació i al sistema en funció dels requeriments de cada perfil, aplicant el principi de privilegis mínims. A continuació s'enumeren alguns dels possibles perfils:

- Administradors de domini: Configuració i gestió de les estacions de treball en xarxa d'una organització.
- Administradors de bases de dades: Configuració i manteniment dels sistemes gestors de bases de dades per emmagatzemar i processar informació.
- Administradors de sistemes: Configuració i gestió dels equips de tractament de la informació que donen suport a l'organització.
- Administradors d'estacions de treball: Configuració i manteniment de les estacions de treball dels usuaris.
- Administradors de sistemes d'emmagatzemament: Configuració i manteniment dels sistemes encarregats d'emmagatzemar la informació.
- Administradors d'impressió: Configuració i gestió dels sistemes d'impressió de l'organització.

En ocasions, per a facilitar les tasques d'administració, manteniment o de solució de problemes, s'accedeix de forma remota als sistemes d'informació. Aquest accés tant pot ser efectuat internament com des de l'exterior per personal de terceres parts que proveeixen un servei de manteniment. Cal controlar aquest accés amb privilegis d'administració per a minimitzar el risc al que estan exposats els sistemes i la informació continguda en ells.

Per tot això, la present guia contempla:

- Prevenir l'ús de comptes genèrics d'administració.
- Controlar els drets d'accés als sistemes i a la informació per part dels diferents perfils d'usuari administrador.
- Garantir que les accions dels usuaris administradors es puguin auditar per a detectar activitats il·lícites, que no són pròpies de les tasques d'administració.
- Controlar l'accés de forma remota als sistemes per les tasques d'administració.

2. ÀMBIT I VIGÈNCIA

Aquest guia afecta als sistemes de tractament de la informació que requereixin de comptes d'administració per a la seva configuració i administració, als usuaris que disposin de comptes amb privilegis d'administració, així com a terceres parts que accedeixin remotament a l'administració d'aquests sistemes.

Entrarà en vigor el dia 1/3/2009 tret del control N1 que serà vigent a partir del 31/3/2009.

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

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

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:

- 6.2.1 Identificació dels riscos relacionats amb terceres parts
- 8.1.1 Rols i responsabilitats
- 10.1.3 Segregació de funcions
- 10.2.1 Prestació del servei
- 10.10.1 Registre d'activitats

- 10.10.2 Monitoratge de l'ús dels sistemes
- 10.10.4 Traces d'administradors i operadors
- 11.1.1 Política de control d'accés
- 11.2.1 Registre d'usuaris
- 11.2.2 Gestió de privilegis
- 11.4.2 Autenticació d'usuari per les connexions externes.
- 11.5.1 Processos de connexió segurs
- 11.5.2 Identificació i autenticació d'usuaris
- 11.5.3 Sistema de gestió de contrasenyes
- 11.6.1 Restricció d'accés a la informació
- 12.1.1 Anàlisis i especificació dels requeriments de seguretat

4. DESCRIPCIÓ

Definició dels comptes

N1. L'accés als sistemes pels usuaris amb privilegis d'administració es realitzarà de la següent manera:

a) Per sistemes Linux (i arquitectures similars) i sempre que tècnicament sigui possible, s'accedirà al sistema mitjançant un compte unipersonal sense privilegis. Caldrà configurar l'eina *sudo* per poder realitzar un escalat de privilegis basats sempre en el principi de mínims privilegis necessaris.

b) Per a sistemes Windows s'accedirà directament amb comptes unipersonals amb els mínims privilegis necessaris.

N2. Sempre que tècnicament sigui possible, no s'utilitzaran els comptes genèrics d'administrador definits en els sistemes[1]. En el seu lloc s'utilitzaran els comptes amb privilegis d'administració unipersonals.

N3. Sempre que tècnicament sigui possible, es reanomenarà el compte per defecte d'administració dels sistemes.

N4. Es guardarà la contrasenya del compte genèric administrador de forma segura. L'accés a aquesta informació serà restringit i només conegut pel responsable del sistema.

N5. Només s'utilitzarà la informació guardada en cas de no poder accedir al sistema amb els comptes personals i prèvia autorització del responsable del sistema.

N6. En cas de no existir un compte d'administració genèric en el sistema, es guardarà de forma segura l'identificador i contrasenya de com a mínim un compte amb privilegis d'administració sobre el sistema.

N7. S'establiran els procediments necessaris per garantir que sempre que hi hagi alguna modificació sobre l'identificador o contrasenya, s'actualitzi també la còpia guardada dels mateixos.

N8. S'eliminaran els comptes amb privilegis d'administració que estiguin inactius o bé en desús.

N9. Caldrà definir un procediment d'alta, baixa i modificació d'usuaris amb privilegis d'administració. Aquest caldrà que contempli les autoritzacions i el registre de les operacions.

N10. Caldrà mantenir un llistat actualitzat amb els usuaris amb privilegis d'administració sobre els sistemes. Aquest llistat haurà d'estar a disposició de les auditories o a petició del CTTI.

Accés als sistemes

N11. Existirà una segregació de funcions dintre de les tasques d'administració dels sistemes, evitant sempre que sigui possible que recaigui en una sola persona la completa administració d'un sistema. S'assignaran els privilegis mínims necessaris per a executar les tasques en cada cas.

N12. Quan sigui necessari accedir puntualment a un sistema amb privilegis d'administració per tasques puntuals i d'una duració concreta caldrà l'autorització del responsable del servei. Es crearà un compte

[1] Comptes impersonals amb privilegis d'administració com *root* o *Administrador*.

amb privilegis d'administració que tindrà data d'expiració i serà eliminat una vegada finalitzades les tasques.

N13. Quan un usuari que tingui privilegis d'administració sobre un sistema causi baixa o canviï les seves funcions deixant de tenir privilegis d'administració sobre el sistema, es donarà de baixa el compte de l'usuari. Si l'usuari utilitza el compte genèric d'administrador, es canviarà la contrasenya d'aquest compte.

N14. En cap cas, es podran incloure comptes amb privilegis d'administració en sistemes de *SSO*.

Característiques de les contrasenyes

N15. La contrasenya dels diferents comptes que tingui un usuari administrador no podrà ser la mateixa.

N16. La contrasenya dels diferents comptes que tingui un usuari administrador haurà de ser diferent de la contrasenya que faci servir com a usuari no administrador.

N17. La gestió de la contrasenya del compte d'usuari es realitzarà complint les normes indicades en la *Guia de contrasenyes*.

N18. Sempre que tècnicament sigui possible, la longitud mínima de les contrasenyes pels comptes amb privilegis d'administració serà de 14 caràcters. En cap cas podrà ser menys de 8 caràcters.

N19. Les contrasenyes dels comptes amb privilegis d'administració tindran una vigència màxima de 45 dies.

N20. Les contrasenyes dels comptes genèrics d'administració s'han de canviar almenys un cop l'any.

N21. Si el sistema ho permet, s'activarà la detecció automàtica de contrasenyes poc segures, per evitar que siguin establertes contrasenyes dèbils. Es podran utilitzar diccionaris de contrasenyes prohibides, polítiques de contrasenyes o altres eines que en garanteixin la robustesa.

N22. A l'instal·lar nous sistemes es canviaran els valors per defecte, establint unes contrasenyes segures pels comptes genèrics d'administrador evitant que quedi en blanc o amb una contrasenya dèbil.

Auditoria

N23. S'activaran mecanismes d'auditoria que permetin registrar les accions realitzades pels comptes amb privilegis d'administració. Com a mínim s'han de registrar les accions de connexió i desconnexió, escalat i modificació de privilegis. Si en algun cas, no és possible activar l'auditoria de les accions indicades, el responsable del sistema haurà de determinar quin és l'impacte real (en entorn de PRE) i argumentar les raons que impossibiliten l'activació de les traces especificades, per tal que a través de petició del responsable del servei, sigui aprovada l'excepció des de l'OS.

N24. Quan tècnicament sigui possible, la configuració i administració dels serveis d'auditoria serà restringida a un usuari o rol específic diferent dels operadors i administradors del sistema.

N25. S'auditaran periòdicament les traces de seguretat del sistema per a verificar les accions realitzades després d'habilitar els mecanismes d'auditoria, amb l'objectiu de detectar que no s'inhabilitin aquests mecanismes.

N26. S'auditaran periòdicament les traces generades de les activitats dels comptes amb privilegis administratius per a detectar activitats indegudes.

N27. Es realitzaran auditories periòdicament per a detectar l'existència de comptes amb privilegis d'administració que estiguin inactius o bé en desús.

Estacions de treball

N28. Els usuaris de les estacions de treball no coneixeran la contrasenya del compte d'administrador de l'equip. Si l'usuari ha de realitzar accions que requereixin permisos especials, l'administrador li proporcionarà un compte d'accés amb els permisos específics, diferent del compte d'accés habitual.

Administració remota

N29. L'administració remota dels sistemes no estarà permesa, excepte amb autorització expressa del responsable del servei.

N30. L'eina d'administració remota disposarà d'un sistema d'autenticació per a garantir el control d'accés al sistema remot.

N31. Es garantirà que la comunicació amb el sistema per la seva administració és xifrada, evitant que un tercer pugui desxifrar la comunicació en cas d'interceptar-la.

N32. Per a la comunicació, s'aplicarà el nivell de xifrat màxim que permeti el programari d'administració remota.

N33. Quan una tercera part necessiti l'accés en sistemes per a tasques d'administració, es recolliran de forma contractual les responsabilitats de la tercera part en l'accés, garantint la protecció de la informació tractada pel sistema. Veure "*Guia de contractació de tercers*".

N34. Els comptes amb privilegis d'administració es bloquejaran després de 3 intents fallits d'autenticació a un sistema de forma remota.

N35. Estaran inhabilitades les funcionalitats de redirigir la impressió, redirigir les unitats de fitxers i les utilitats de copiar i enganxar en el porta-retalls[2] de l'equip que s'estigui administrant de forma remota.

N36. No es podrà guardar la contrasenya de forma automàtica per a l'administració remota d'un sistema en cas que el programari d'administració ho permeti. Cada connexió requerirà que s'introdueixi de nou.

Tractament d'incidències

N37. Qualsevol incident de seguretat relacionat amb la gestió dels comptes d'administració de sistemes haurà de ser comunicat en la major brevetat possible mitjançant el *Procediment de notificació d'incidents de seguretat.*

Recomanacions

R1. Donat que les contrasenyes pels comptes d'administració han de tenir una longitud considerable es recomana utilitzar frases que siguin fàcils de recordar. La contrasenya podria ser generada amb la inicial de cada una de les paraules de la frase. Per exemple: "*setze jutges d'un jutjat mengen fetge d'un penjat*" es convertiria en la contrasenya "*!sjdujmfdup@06!*" després d'afegir-hi caràcters numèrics i especials.

R2. Per a usuaris amb privilegis administratius sobre sistemes crítics, seria recomanable disposar d'un mecanisme d'autenticació de dos factors. És a dir, a més de la contrasenya, utilitzar altres sistemes d'autenticació com poden ser targes (*smart card*).

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 autoritzada prèviament per l'Oficina de Seguretat.

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

[2] Traducció al català de *clipboard*.

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 Relacions amb Proveïdors del CTTI publicarà aquesta guia al repositori d'estàndards de la intranet del CTTI.

8. REVISIÓ

Aquesta guia es revisarà anualment.

En cas de produir-se una incidència de seguretat relacionada amb aquesta norma, caldrà fer una revisió de compliment i completesa

9. GLOSSARI DE TERMES

Sudo: Paquet de programari que permet l'execució d'un programa binari o d'un shell script com un usuari diferent. El root ha de configurar aquest paquet per tal d'identificar quin usuari pot executar què programa binari o shell script com quin altre usuari.

SSO: Single Sign On. Procés d'autenticació d'usuari que permet que una vegada s'ha autenticat correctament un usuari contra el sistema, permet accedir a múltiples sistemes sense necessitat d'autenticar-se de nou.

10. DOCUMENTACIÓ REFERENCIADA

- GE-GUI19 Guia de contrasenyes.
- GE-GUI18 Guia de contractació de tercers.
- GE-PRO01 Procediment de notificació d'incidents de seguretat

11. PARAULES CLAU

Administrador, compte, contrasenya, privilegis, administració

12. HISTÒRIC DEL DOCUMENT

Versió 1.0
Versió inicial.

Versió 2.0 – 25/3/2009
Revisió del contingut. Per més informació consultar la fitxa de l'estàndard.