


 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008	
	N. versió: 1.0.	Pàg. 1 / 13



Llicència Creative Commons:
Reconeixement – No Comercial – Compartir Igual 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](https://creativecommons.org/licenses/by-nc-sa/2.5/)

ÍNDEX

RESUM.....	2
1 OBJECTIU.....	3
2 ÀMBIT I VIGÈNCIA	3
3 COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT	3
4 DESCRIPCIÓ DELS CONTROLS.....	3
4.1. IN - Instal·lació i manteniment	4
4.2. CN - Configuració	4
4.3. MN - Monitoratge	5
4.4. CA - Control d'accés.....	6
4.5. AU – Auditoria.....	6
4.6. OU - Outsourcing o subcontractació del servei	7
5 CONTROL	7
6 PENALITZACIONS.....	7
7 DIVULGACIÓ	7
8 REVISIÓ	7
9 GLOSSARI DE TERMES	8
10 DOCUMENTACIÓ REFERENCIADA.....	8
11 PARAULES CLAU	8
12 HISTÒRIC DEL DOCUMENT	8
13 ANNEX: Requisits de configuració continguts a la guia Windows Server 2008 Security Guide	9
13.1 Security Settings	9
Recomanacions	11
13.2 Audit Policy	11
13.3 Event Log.....	12
13.4 User Rights Assignments.....	12
13.5 Password Policy.....	13
13.6 Account Lockout Policy.....	13

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA		GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008		
	N. versió: 1.0.		Pàg. 2 / 13

Versió	Redactat / revisat per	Aprovat per	Data aprovació	Data publicació
1.0.	CTTI – Qualitat, Seguretat i Relació amb Proveïdors	Comitè de Direcció del CTTI	22/3/2010	29/3/2010

RESUM

OBJECTIU

Definir els controls a aplicar per a la protecció d'equips instal·lats amb el sistema operatiu *Windows Server 2008*, amb l'objectiu de garantir la confidencialitat, integritat i disponibilitat de la informació i serveis suportats per aquests equips.

ÀMBIT


Aquesta guia va destinada als administradors i responsables de manteniment dels equips *Windows Server 2008* de la Generalitat de Catalunya.

A més d'aquesta guia, s'hauria de complir allò que estigui establert a qualsevol altra guia d'administració de sistemes en general i de Windows en particular, ja que en aquesta guia només s'identifiquen els controls específics per garantir un mínim de seguretat en els equips amb sistema operatiu Windows.

DESCRIPCIÓ

Es recullen els controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació de sistemes basats en *Windows Server 2008*.

Cal remarcar que les configuracions de seguretat indicades en aquesta guia, caldrà provar-les en un entorn de proves abans d'aplicar-les en servidors que estiguin en explotació.

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008	
	N. versió: 1.0.	Pàg. 3 / 13

1 OBJECTIU

Definir els controls per administrar i gestionar la seguretat en els equips amb sistemes operatius *Windows Server 2008*.

Microsoft ha desenvolupat una guia exhaustiva de configuració de seguretat per al Sistema Windows Server 2008 amb recomanacions específiques per a reforçar la seguretat dels Servidors. La present guia fa referència a parts de la guia elaborada per *Microsoft*, i recollida en mode de resum en l'annex.

2 ÀMBIT I VIGÈNCIA

Aquesta guia va destinada als administradors i responsables de manteniment dels equips de processament de la informació instal·lats amb el sistema operatiu *Windows Server 2008* de la Generalitat de Catalunya.

Els controls que s'indiquen en aquesta guia estan orientats a garantir la protecció del sistema independentment dels serveis als quals doni suport el servidor.

A més d'aquesta guia, s'hauria de complir allò que estigui establert a qualsevol altra guia d'administració de sistemes en general i de *Windows* en particular, ja que en aquesta guia s'identifiquen els controls específics per garantir un mínim de seguretat en els equips amb sistema operatiu *Windows*, però no per administrar el sistema en sí.

Entrarà en vigor el dia 30/3/2010.

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:

- 6.2.3 Requeriments de seguretat en els acords amb les terceres parts
- 10.10.1 Registres d'auditoria (logging)
- 10.10.6 Sincronització de rellotges
- 11.4.4 Protecció dels ports de configuració i diagnòstic remot
- 11.5.1 Processos de connexió segurs
- 11.5.3 Sistema de gestió de les contrasenyes
- 11.6.1 Restricció d'accés a la informació
- 12.5.3 Restriccions en els canvis als paquets de programari
- 13.1.1 Notificar dels esdeveniments de seguretat

4 DESCRIPCIÓ DELS CONTROLS

Es presenten a continuació els possibles controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació, així com el compliment de la legislació vigent. Aquests s'agrupen per grups d'accions o procediments operatius orientats a combatre les amenaces a les quals un equip amb *Windows* està exposat. L'aplicació d'un conjunt ampli dels controls d'una manera lògica, ordenada i planificada reduirà progressivament les vulnerabilitats del sistema i, per tant, l'exposició als riscos. Sota la columna "categoria", s'especifiquen els aspectes de seguretat que cada control reforça (confidencialitat– C, integritat– I, disponibilitat– D).

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008	
	N. versió: 1.0.	Pàg. 4 / 13

4.1. IN - Instal·lació i manteniment


OBJECTIUS		
Definir els controls a tenir en compte a l'hora d'instal·lar un nou sistema <i>Windows Server 2008</i> i el seu posterior manteniment.		
CARACTERÍSTIQUES		
Descripció		Categoria
C1. Mantenir els sistemes actualitzats amb els pegats (SP) i les actualitzacions de seguretat que publiqui Microsoft per corregir vulnerabilitats aparegudes en els sistemes <i>Windows Server 2008</i> . Pels sistemes ubicats en l'àmbit dels Serveis TIC Centrals , cal donar compliment a la <i>Norma de gestió de vulnerabilitats de programari base</i> .		I D
C2. No instal·lar programari o paquets innecessaris en el sistema.		C I D
C3. No instal·lar programari o paquets de fonts desconegudes o no fiables.		C I D
C4. Utilitzar el sistema de fitxers NTFS a l'hora de formatar el disc dur.		C I D
C5. Durant la instal·lació inicial del sistema, crear les particions de manera que les dades d'usuaris, el programari que s'instal·larà i el propi sistema operatiu estiguin separats i no s'afectin mútuament. Sobretot cal protegir la partició amb el sistema operatiu.		D
C6. Sempre que tècnicament sigui possible, instal·lar un programari antivirus i mantenir-lo actualitzat de forma contínua. En cas que el sistema serveixi de passarel·la o d'emmagatzemament de fitxers, el control serà d'obligat compliment.		C I D
C7. Caldrà donar compliment a la <i>Norma de còpies de seguretat</i> per a garantir que es realitza còpia de seguretat dels sistemes.		C I D
C8. Netejar els usuaris i grups per defecte que es creen durant la instal·lació. Si no són necessaris pels diferents serveis que s'hagin d'instal·lar, cal eliminar-los o bé inhabilitar-los per evitar forats de seguretat.		C
C9. S'hauran de sincronitzar els rellotges amb servidors NTP corporatius o servidors NTP corporatius intermedis si existeixen i, en tot cas, mantenir els rellotges dels sistemes en hora.		C I

Recomanacions

- R1. Es recomana crear una partició on residiran els fitxers web. S'indicarà al sistema operatiu que aquesta partició no és executable.
- R2. No donar servei de xarxa a un equip fins que no hagi acabat la instal·lació inicial del sistema operatiu i no s'hagin aplicat les mesures de seguretat adequades, incloent els pegats de seguretat necessaris.

4.2. CN - Configuració

OBJECTIUS										
Habilitar i inhabilitar capacitats i característiques del sistema. Configurar varis paràmetres com per exemple signatura digital de dades, noms de comptes d'administrador i convidats, instal·lació de controladors, etc.										
CARACTERÍSTIQUES										
Descripció		Categoria								
C10.Aplicar la configuració recollida en punt 13.1 <i>Security Settings</i> de l'annex d'aquesta guia per configurar diferents aspectes que afecten directament a la seguretat de l'equip.		C I								
C11.Per evitar atacs de denegació de servei contra el servidor <i>Windows Server 2008</i> , cal aplicar els següents paràmetres en la subclau <i>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\</i>		I D								
<table><tr><td>KeepAliveTime</td><td>300,000</td></tr><tr><td>DisableIPSourceRouting</td><td>2</td></tr><tr><td>TcpMaxDataRetransmissions</td><td>3</td></tr><tr><td>PerformRouterDiscovery</td><td>0</td></tr></table>		KeepAliveTime	300,000	DisableIPSourceRouting	2	TcpMaxDataRetransmissions	3	PerformRouterDiscovery	0	
KeepAliveTime	300,000									
DisableIPSourceRouting	2									
TcpMaxDataRetransmissions	3									
PerformRouterDiscovery	0									

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008	
	N. versió: 1.0.	Pàg. 5 / 13


C12. Inhabilitar els serveis de <i>Netbios</i> . Caldrà validar prèviament que cap aplicació es vegi afectada i requereixi <i>Netbios</i> per funcionar.	D
C13. Cal donar compliment a la <i>Norma de gestió de comptes d'administració de sistemes</i> per garantir la correcta definició i gestió dels comptes amb privilegis d'administració. La configuració està recollida en el punt 13.5 <i>Password Policy</i> de l'annex d'aquesta guia.	C I
C14. Inhabilitar tots aquells serveis que no siguin necessaris o insegurs. Es pot establir la configuració dels serveis del sistema en la següent ubicació de l'editor d'objectes de directiva de grup: <i>Configuración de equipo\Configuración de Windows\Configuración de seguridad\Servicios del sistema\</i>	C I D
C15. Les contrasenyes s'han de guardar de forma xifrada i s'han de modificar els permisos d'accés al fitxer de contrasenyes per evitar que siguin de lectura per a tots els usuaris.	C I
C16. En sistemes ubicats en entorns de producció, només estaran instal·lats aquells llenguatges interpretats necessaris per a l'execució del servei.	I D
C17. Restringir l'accés a les traces per part dels usuaris sense privilegis.	C
C18. No habilitar serveis d'administració del sistema a les interfícies de producció. Consultar l'apartat 2. ÀMBIT I VIGÈNCIA, de la <i>Norma de mesures de seguretat en el nus corporatiu TIC de la Generalitat</i> .	C I D
C19. Modificar els missatges de benvinguda per evitar que es proporcioni informació del sistema. Canviar el tipus de missatge pel següent exemple: "AVÍS ALS USUARIS: L'ús no autoritzat d'aquest sistema no està permès. Les activitats seran registrades". El text cal informar-lo a la configuració de política "Message text for users attempting to log on" de l'àrea "Interactive logon".	C

Recomanacions

- R3. Provar les configuracions de seguretat en un entorn de proves abans d'aplicar-les en servidors que estiguin en explotació.
- R4. Crear configuracions de seguretat a partir de les plantilles base que es puguin reutilitzar per a noves instal·lacions de Windows Server 2008. D'aquesta manera es poden aprofitar les configuracions de seguretat per a altres equips amb les mateixes funcions que s'instal·lin.
- R5. Tots els equips Windows Server 2008 emmagatzemen les plantilles de seguretat en la carpeta %SystemRoot%securitytemplates. Aquesta carpeta no es replica entre els diversos controladors de domini, així que s'haurà de designar una ubicació per a emmagatzemar la còpia mestra de les plantilles de seguretat amb la finalitat d'evitar que es produeixin problemes de control de versió amb les plantilles.
- R6. Crear configuracions a nivell de grup (GPO – Group Policy Object) quan puguin ser aplicades a un grup de servidors. L'avantatge es que es poden aplicar a nivell de *Active Directory*. Un exemple d'aquest tipus de configuracions són les de contrasenyes.
- R7. Quan es requereixi configurar un *Active Directory* existeixen diversos tipus de límits que defineixen el bosc, la topologia del lloc i la delegació de permisos. Aquests límits s'estableixen automàticament, però ha d'assegurar-se que els límits dels permisos incorporin els requisits i les directives de l'organització. Els límits són: límits de seguretat de l'entorn i límits administratius.

4.3. MN - Monitoratge

OBJECTIUS	
Identificar quines accions i activitats dels usuaris que es realitzen en el sistema cal registrar. Especificar les característiques del sistema de registre.	
CARACTERÍSTIQUES	
Descripció	Categoria
C20. Caldrà donar compliment als requeriments de la <i>Norma de gestió de traces</i> per a garantir la traçabilitat i custòdia dels esdeveniments dels sistemes.	C I
C21. Pels sistemes d'àmbit departament / ens, es connectaran a eines de correlació de traces pròpies quan existeixin; de no ser així, caldrà guardar les traces durant un període mínim d'1 any i revisar-les periòdicament per a detectar anomalies o	C I

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008	
	N. versió: 1.0.	Pàg. 6 / 13

incidències en el funcionament del sistema.	
C22. Aplicar la configuració recollida en el punt 13.2 <i>Audit Policy</i> de l'annex d'aquesta guia per a la configuració de quines accions cal registrar en el sistema.	C I
C23. Aplicar la configuració recollida en el punt 13.3 <i>Event Log</i> de l'annex d'aquesta guia per a la configuració del sistema de registre (capacitat i protecció dels fitxers de registre).	C I D
C24. Qualsevol possible incident de seguretat haurà de ser comunicat en la major brevetat possible mitjançant el <i>Procediment de notificació d'incidents de seguretat</i> .	C I D

Recomanacions

- R8. Es recomana, revisar periòdicament les traces per a detectar activitats anòmales que puguin comprometre la seguretat del sistema.
- R9. Definir llistes de control d'accés (System **ACL** o SACL– System Access Control List) que recullin els actius del sistema Windows Server 2008 (ja siguin de sistema o d'informació) als que cal aplicar monitoratge. Són exemples els fitxers executables per evitar que codi maliciós els modifiqui, informació sensible per obtenir un registre d'accés, el registre de configuració del sistema per detectar modificacions per part de codi maliciós, etc.

4.4. CA - Control d'accés


OBJECTIUS	
Proveir als usuaris i grups de privilegis o drets d'accés als sistemes Windows Server 2008.	
CARACTERÍSTIQUES	
Descripció	Categoria
C25. Aplicar la configuració recollida en el punt 13.4 <i>User Rights Assignments</i> de l'annex d'aquesta guia per a la configuració del control d'accés.	C I D
C26. Aplicar la configuració recollida en el punt 13.6 <i>Account Lockout Policy</i> de l'annex d'aquesta guia, per la gestió dels bloquejos dels comptes si per exemple, se supera el número d'intents fallits permesos per accedir al sistema.	C I
C27. No utilitzar aplicacions de connexió remota en les quals la contrasenya viatgi en clar per la xarxa.	C I D
C28. Limitar l'accés als serveis del sistema que no siguin publicats per a tots els usuaris.	C I
C29. Fer un ús adequat dels usuaris, grups, propietat dels fitxers i permisos dels usuaris i grups sobre els fitxers i/o aplicacions, per tal de mantenir la confidencialitat i integritat de les dades que continguin aquests fitxers i/o aplicacions. Sempre caldrà garantir el principi de mínims privilegis.	C I
C30. Inhabilitar l'accés al compte d'invitat.	C I D

4.5. AU – Auditoria

OBJECTIUS	
Controlar la configuració dels diferents sistemes i facilitar les traces del sistema a l'eina centralitzada de gestió de traces.	
CARACTERÍSTIQUES	
Descripció	Categoria
C31. Caldrà facilitar les tasques d'auditoria per part de l'oficina de Seguretat davant la revisió del compliment dels requeriments de seguretat marcats pel CTTI.	C I D

Recomanacions

- R10. Utilitzar l'eina desenvolupada per Microsoft (Microsoft Baseline Security Analyzer-MBSA) per a realitzar comprovacions del nivell de seguretat dels equips amb Windows Server 2008.

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008	
	N. versió: 1.0.	Pàg. 7 / 13

4.6. OU - Outsourcing o subcontractació del servei

OBJECTIUS	
Garantir el compliment de les mesures de seguretat i dels acords de nivell de servei en cas de subcontractació o externalització de l'administració de sistemes <i>Windows Server 2008</i> .	
CARACTERÍSTIQUES	
Descripció	Categoria
C32. Es recollirà contractualment el compliment de les normes i guies que el CTTI tingui per l'entorn <i>Windows Server 2008</i> , així com qualsevol altra norma de gestió o administració que sigui d'aplicació.	C I D
C33. Es garantirà el compliment de la <i>Norma de contractació de tercers</i> .	C I D
C34. Es garantirà la qualitat i el nivell de servei requerit a través d'acords de nivell de servei: <ul style="list-style-type: none"> • Procediments d'escalat d'incidències. • Temps de resolució d'incidències. • Temps de resposta per canvis / noves instal·lacions. • Compliment i actualització dels controls de seguretat. • Gestió de problemes. • Etc. L'incompliment d'acords de nivell de servei haurà de comportar penalitzacions econòmiques al proveïdor.	C I D

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.

6 PENALITZACIONS

Quan l'explotació / manteniment dels sistemes estigui subcontractat, en cas d'incompliment aplicaran les penalitzacions recollides en el contracte de la prestació del servei.

Si l'administració del sistema recau en personal intern de la Generalitat de Catalunya, l'incompliment d'aquesta guia pot determinar, si 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 ha de ser revisada anualment.

En cas de produir-se una incidència de seguretat relacionada amb aquesta guia, caldrà fer una revisió de compliment i completa.

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008	
	N. versió: 1.0.	Pàg. 8 / 13

9 GLOSSARI DE TERMES

Active Directory: Sistema centralitzat i estandarditzat que automatitza la gestió de la informació en xarxa d'usuaris, la seguretat i els recursos distribuïts, proporcionant interacció amb altres directoris.

LDAP: *Lightweight Directory Access Protocol*. Protocol a nivell d'aplicació que permet l'accés a un servei de directori ordenat i distribuït.

DHCP: *Dynamic Host Configuration Protocol*. Servei que assigna dinàmicament adreces IP als equips que ho sol·liciten. Evita que s'hagin d'assignar manualment les adreces en els equips.

NTP: *Network Time Protocol*. Protocol utilitzat per a sincronitzar els rellotges dels equips en una xarxa.

SDDL: *Security Descriptor Definition Language*. Servei que defineix els elements de cadena per a descriure la informació dels components d'un descriptor de seguretat.

DCOM: *Distributed Component Object Model*. Components software per a comunicar-se amb equips en línia.

SMB: *Server Message Block communications*. Protocol de xarxa que permet compartir recursos entre nodes i també la comunicació entre equips SMB

ACL: *Access Control List*. Comprovació addicional d'accés per a evitar l'accés no autoritzat a equips.

SID: *Security Identifier*. Valor únic assignat pel Controlador de Domini de windows durant el procés de log on, que identifica a cadascun dels sistemes i usuaris.

Hash: Representació d'un password després d'aplicar l'algorisme d'enciptació corresponent.

Serveis TIC Centrals: Serveis TIC Centrals de Caràcter Continuat de la Generalitat de Catalunya, gestionats pel Centre de Telecomunicacions i Tecnologies de la Informació (CTTI).

SP: *Service Pack*. Actualitzacions de programari que distribueix Microsoft per a solucionar vulnerabilitats detectades en el programari del sistema operatiu.

WINS: *Windows Internet Naming Service*. Servei que associa el nom lògic de les estacions de treball amb l'adreça IP associada.

10 DOCUMENTACIÓ REFERENCIADA


- GE-GUI20 Guia de gestió de comptes administrador sistemes
- CT-NOR03 Norma de contractació de tercers
- SC-NOR16 Norma de gestió de traces
- GE-PRO01-01 Procediment de Notificació d'Incidents de Seguretat
- GE-NOR28 Norma de mesures de seguretat en el nus corporatiu TIC de la Generalitat
- Guia del fabricant: <http://technet.microsoft.com/en-gb/library/dd548366%28WS.10%29.aspx>

11 PARAULES CLAU

Windows, administració, usuaris, grups, permisos, pegat de seguretat, W2008, hardenning, protecció.

12 HISTÒRIC DEL DOCUMENT

Versió 1.0.
Versió inicial.

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008	
	N. versió: 1.0.	Pàg. 9 / 13


13 ANNEX: Requisits de configuració continguts a la guia Windows Server 2008 Security Guide

En aquest annex es recullen els requisits de configuració continguts en la guia *Windows Server 2008 Security Guide*. Per a una informació detallada de cada una de les configuracions consultar les dades del fabricant.


S'indiquen com a "Recomanacions" els controls que no són d'obligat compliment.

13.1 Security Settings

Paràmetre	Valor
Account settings	
A1. Administrator account status	Enabled
A2. Guest account status	Disabled
A3. Limit local account use of blank passwords to console logon only	Enabled
Audit Settings	
A4. Audit the access of global system objects	Disabled
A5. Audit the use of Backup and Restore privilege	Enabled
Device Settings	
A6. Allowed to format and eject removable media	Administrators
Domain controller	
A7. LDAP server signing requirements	Require signature
A8. Refuse machine account password changes	Disabled
Domain Member Settings	
A9. Digitally encrypt or sign secure channel data (multiple related settings)	Enabled
A10. Digitally encrypt secure channel data (when possible)	Enabled
A11. Digitally sign secure channel data (when possible)	Enabled
A12. Disable machine account password changes	Disabled
A13. Maximum machine account password age	45 days
A14. Require strong session key	Enabled
Interactive logon	
A15. Do not display last user name	Enabled
A16. Do not require CTRL+ALT+DEL	Disabled
A17. Message text for users attempting to log on and Message title for users attempting to log on	User-defined text "AVÍS ALS USUARIS: L'ús no autoritzat d'aquest sistema no està permès. Les activitats seran registrades"
A18. Number of previous logons to cache (in case domain controller is not available)	0
A19. Prompt user to change password before expiration	5 days
Microsoft network client	
A20. Digitally sign communications (always)	Enabled
A21. Digitally sign communications (if server agrees)	Enabled
A22. Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server	
A23. Amount of idle time required before suspending session	15 minutes
A24. Digitally sign communications (always) This setting is configured to Disabled for print servers.	Enabled
A25. Digitally sign communications (if client agrees)	Enabled
Network access	
A26. Allow anonymous SID /Name translation	Disabled
A27. Do not allow anonymous enumeration of SAM accounts	Enabled

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008	
	N. versió: 1.0.	Pàg. 10 / 13

A28. Do not allow anonymous enumeration of SAM accounts and shares	Enabled
A29. Do not allow storage of credentials or .NET Passports for network authentication	Enabled
A30. Let Everyone permissions apply to anonymous users	Disabled
A31. Named Pipes that can be accessed anonymously	COMNAP, COMNODE, SQL\QUERY, SPOOLSS, LLSRPC, netlogon, lsarpc, samr, browser
A32. Remotely accessible registry paths	System\CurrentControlSet\Control\Product Options; System\CurrentControlSet\Control\Server Applications; Software\Microsoft\Windows NT\CurrentVersion
A33. Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog
A34. Restrict anonymous access to Named Pipes and Shares	Enabled
A35. Shares that can be accessed anonymously	None
A36. Sharing and security model for local accounts	Classic - Local users authenticate as themselves
Network security	
A37. Do not store LAN Manager hash value on next password change	Enabled
A38. LAN Manager authentication level	Send NTLMv2 responses only. Refuse LM & NTLM
A39. LDAP client signing requirements	Negotiate signing
A40. Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled all settings
A41. Minimum session security for NTLM SSP based (including secure RPC) servers	Enabled all settings
Recovery console	
A42. Allow automatic administrative logon	Disabled
A43. Allow floppy copy and access to all drives and all folders	Disabled

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008	
	N. versió: 1.0.	Pàg. 11 / 13


Shutdown	
A44. Allow system to be shut down without having to log on	Disabled
A45. Clear virtual memory pagefile	Disabled
System cryptography	
A46. Force strong key protection for user keys stored on the computer	User must enter a password each time they use a key
A47. Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled
System objects	
A48. Default owner for objects created by members of the Administrators group	Object creator
A49. Require case insensitivity for non-Windows subsystems	Enabled
A50. Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled
System settings	
A51. Optional subsystems	None
A52. Use Certificate Rules on Windows Executables for Software Restriction Policies	Enabled
User Account Control	
A53. Admin Approval Mode for the Built-in Administrator account	Disabled
A54. Allow UIAccess applications to prompt for elevation without using the secure desktop	Enabled
A55. Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent
A56. Behavior of the elevation prompt for standard users	Automatically deny elevation requests
A57. Detect application installations and prompt for elevation	Enabled
A58. Only elevate executables that are signed and validated	Disabled
A59. Only elevate UIAccess applications that are installed in secure locations	Enabled
A60. Run all administrators in Admin Approval Mode	Enabled
A61. Switch to the secure desktop when prompting for elevation	Enabled
A62. Virtualize file and registry write failures to per-user locations	Enabled

Recomanacions

R1. Shut down system immediately if unable to log security audits	Enabled
R2. Allow undock without having to log on	Disabled
R3. Prevent users from installing printer drivers	Enabled
R4. Restrict CD-ROM access to locally logged-on user only	Disabled
R5. Restrict floppy access to locally logged-on user only	Disabled
R6. Require Domain Controller authentication to unlock workstation	Enabled
R7. Require smart card	Disabled
R8. Smart card removal behavior	Lock workstation
R9. Disconnect clients when logon hours expire	Enabled
R10. Force Logoff when Logon Hours expire	Enabled

13.2 Audit Policy

Paràmetre	Valor
A63. Audit account logon events	Success Failure

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008	
	N. versió: 1.0.	Pàg. 12 / 13


A64. Audit account management	Success Failure
A65. Audit logon events	Success Failure
A66. Audit object access	Failure
A67. Audit policy change	Success
A68. Audit privilege use	Failure
A69. Audit process tracking	No auditing
A70. Audit system events	Success

13.3 Event Log

Paràmetre	Valor
A71. Maximum application log size	20.480KB
A72. Maximum security log size	20.480KB
A73. Maximum system log size	20.480KB
A74. Retain Application Log	365
A75. Retain Security Log	365
A76. Retain System Log	365

13.4 User Rights Assignments

Paràmetre	Valor
A77. Access this computer from the network	Administrators, Authenticated Users, Domain Controllers
A78. Act as part of the operating system	No one
A79. Adjust memory quotas for a process	Administrators, Network Service, Local Service
A80. Allow log on locally	Administrators
A81. Allow log on through Terminal Services	Administrators
A82. Back up files and directories	Administrators
A83. Bypass traverse checking	Authenticated Users
A84. Change the system time	Local Service Administrators
A85. Create a pagefile	Administrators
A86. Create a token object	No one
A87. Create global objects	Administrators, SERVICE
A88. Create permanent shared objects	No one
A89. Debug programs	No one
A90. Deny access to this computer from the network	ANONYMOUS LOGON; Guests; Support_388945a0; all NON-Operating System service accounts
A91. Deny logon as a batch job	Guests; Support_388945a0
A92. Deny logon as a service	No one
A93. Deny logon locally	Guests; Support_388945a0
A94. Deny logon through Terminal Services	Guests
A95. Enable computer and user accounts to be trusted for delegation	Administrators
A96. Force shutdown from a remote system	Administrators
A97. Generate security audits	NETWORK SERVICE, LOCAL SERVICE
A98. Impersonate a client after authentication	Administrators, SERVICE
A99. Increase scheduling priority	Administrators
A100. Load and unload device drivers	Administrators
A101. Lock pages in memory	No one

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI41-01
	PROTECCIÓ DE SISTEMES WINDOWS 2008	
	N. versió: 1.0.	Pàg. 13 / 13

A102. Log on as a batch job	Not defined
A103. Log on as a service	NETWORK SERVICE
A104. Manage auditing and security log	Administrators
A105. Modify firmware environment values	Administrators
A106. Perform volume maintenance tasks	Administrators
A107. Profile single process	Administrators
A108. Profile system performance	Administrators
A109. Remove computer from docking station	Administrators
A110. Replace a process level token	LOCAL SERVICE, NETWORK SERVICE
A111. Restore files and directories	Administrators
A112. Shut down the system	Administrators
A113. Synchronize directory service data	No one
A114. Take ownership of files or other objects	Administrators

13.5 Password Policy

Els valors de configuració dels paràmetres han estat adequats als valors definits per la *Guia de gestió de comptes administrador de sistemes*.

Paràmetre	Valor
A115. Enforce password history	10 passwords remembered
A116. Maximum password age	45 days
A117. Minimum password age	0 days
A118. Minimum password length	14 characters
A119. Password must meet complexity requirements	Enabled
A120. Store password using reversible encryption	Disabled

13.6 Account Lockout Policy

Paràmetre	Valor
A121. Account lockout duration	0 minutes
A122. Account lockout threshold	3 invalid login attempts
A123. Reset account lockout counter after	0 minutes