**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 - QSRaP | CTTI – QSRaP | 20/04/2009 | 18/05/2009 |
| 2.1. | CTTI – QSRaP | CTTI – QSRaP | 27/07/2009 | 31/07/2009 |

Estàndard signat digitalment pel: Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2009.07.27 11:58:25 +02'00'

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

## RESUM

### OBJECTIU

Definir els controls a aplicar per a la protecció d'equips instal·lats amb el sistema operatiu *Windows 2003*, 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 2003* 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 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 2003*.

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.

## 1 OBJECTIU

Definir els controls per administrar i gestionar la seguretat en els equips amb sistemes operatius *Windows 2003*.

Microsoft ha desenvolupat una guia exhaustiva de configuració de seguretat pel Sistema Windows 2003 amb recomanacions específiques per a reforçar la seguretat dels Servidors, aquesta guia fa referència a parts de la guia elaborada per *Microsoft*, i recollida en mode de resum en l'annex.

Els administradors poden definir, provar, revisar i implantar configuracions de seguretat que permeten inhabilitar serveis no necessaris en les instal·lacions de *Windows 2003*. Permet l'aplicació de les configuracions en grups de servidors o bé a nivell individual. Així mateix, permet fer marxa enrere en cas de què sorgeixin problemes en la implantació d'una configuració.

## 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 2003 d*e la Generalitat de Catalunya.

Els equips instal·lats amb *Windows 2003* poden estar destinats a la realització de diferents tasques:

- Servidor d'aplicacions
- Servidor web
- Controlador de domini
- Servidor d'infraestructura (*DHCP*, *WINS*)
- Servidor de fitxers
- Servidor d'impressió
- Servidor de serveis de certificació

Els controls que s'indiquen en aquesta guia estan orientats a garantir la protecció del sistema indiferentment dels serveis als que 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 18 de maig 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*.

## 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).

### *4.1. IN - Instal·lació i manteniment*

| **OBJECTIUS** | |
|---|---|
| Definir els controls a tenir en compte a l'hora d'instal·lar un nou sistema *Windows 2003* 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 *Windows 2003*. Pels sistemes ubicats en l'àmbit dels Serveis TIC Centrals, cal donar compliment a la *Norma de gestió de vulnerabilitats de programari base*. | 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 *Norma de còpies de seguretat* 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 què 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 *Security Settings* de l'annex d'aquesta guia per configurar diferents aspectes que afecten directament a la seguretat de l'equip. | C I |
| C11. Per a evitar atacs de denegació de servei contra el servidor *Windows 2003*, cal aplicar els següents paràmetres en la subclau *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters*<br><br>EnableICMPRedirect: 0<br>SynAttackProtect: 1<br>EnableDeadGWDetect: 0<br>KeepAliveTime: 300,000 | I D |

| | | | |
|---|---|---|---|
| | DisableIPSourceRouting | 2 | |
| | TcpMaxConnectResponseRetransmissions | 2 | |
| | TcpMaxDataRetransmissions | 3 | |
| | PerformRouterDiscovery | 0 | |
| C12. Inhabilitar els serveis de *Netbios*. Caldrà validar prèviament que cap aplicació es vegi afectada i requereixi *Netbios* per a funcionar. | | | D |
| C13. Cal donar compliment a la *Norma de gestió de comptes d'administració de sistemes* per a garantir la correcta definició i gestió dels comptes amb privilegis d'administració. La configuració està recollida en el punt 13.6 *Password Policy* 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: *Configuración de equipo\Configuración de Windows\Configuración de seguridad\Servicios del sistema* | | | 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 *Norma de mesures de seguretat en el nus corporatiu TIC de la Generalitat.* | | | 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 2003. 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 2003 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 limitis 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 *Norma de gestió de traces* per a | C I |

| | |
|---|---|
| garantir la traçabilitat i custòdia dels esdeveniments dels sistemes. | |
| 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 incidències en el funcionament del sistema. | C I |
| C22. Aplicar la configuració recollida en el punt 13.3 *Audit Policy* 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 13.4 *Event Log* 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 *Procediment de notificació d'incidents de seguretat.* | 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 (SACL – System Access Control List) que recullin els actius del sistema Windows 2003 (ja siguin de sistema o d'informació) als que cal aplicar monitoratge. Exemples són 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 2003. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C25. Aplicar la configuració recollida en el punt 13.5 *User Rights Assignments* 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 13.7 *Account Lockout Policy* 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. Utilitzar les protocols segurs com sftp o ssh. | 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 a 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 2003.

### *4.6. OU - Outsourcing o subcontractació del servei*

| **OBJECTIUS** |
|---|
| Garantir l'acompliment de les mesures de seguretat i dels acords de nivell de servei en cas de subcontractació o externalització de l'administració de sistemes *Windows 2003*. |

| CARACTERÍSTIQUES | |
|---|---|
| **Descripció** | **Categoria** |
| C32. Es recollirà contractualment el compliment de les normes i guies que el CTTI tingui per l'entorn *Windows 2003* així com qualsevol altra norma de gestió o administració que sigui d'aplicació. | C I D |
| C33. Es garantirà el compliment de la *Norma de contractació de tercers*. | C I D |
| C34. Es garantirà la qualitat i el nivell de servei requerit a través d'acords de nivell de servei:<br>• Procediments d'escalat d'incidències.<br>• Temps de resolució d'incidències.<br>• Temps de resposta per canvis / noves instal·lacions.<br>• Compliment i actualització dels controls de seguretat.<br>• Gestió de problemes.<br>• Etc.<br>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 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 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 completesa.

## 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.

*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.

*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

- http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx
- http://www.microsoft.com/spain/technet/security/topics/serversecurity/tcg/tcgch03n.mspx
- http://www.microsoft.com/spain/technet/security/prodtech/windowsserver2003/w2003hg/s3sgch02.msp
- http://www.microsoft.com/spain/technet/security/topics/serversecurity/tcg/tcgch06n.mspx
- http://www.microsoft.com/spain/technet/security/topics/serversecurity/tcg/tcgch07n.mspx
- http://www.microsoft.com/spain/technet/security/topics/serversecurity/tcg/tcgch09n.mspx
- http://www.microsoft.com/spain/technet/security/topics/serversecurity/tcg/tcgch10n.mspx

## 11 PARAULES CLAU

Windows, administració, usuaris, grups, permisos, pegat de seguretat, W2003, hardenning, protecció.

## 12 HISTÒRIC DEL DOCUMENT

Versió 1.0
Versió inicial.

Versió 2.0
Versió revisada de l'estandard. Veure la fitxa de l'estàndard per a més informació.

Versió 2.1.
Correcció d'un error en la numeració dels controls de l'annex (punt 13).

## 13 ANNEX: Requisits de configuració continguts a la guia Windows 2003 Security Guide

En aquest annex es recullen els requisits de configuració continguts en la guia *Windows 2003 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 Member Settings | |
| A7. Digitally encrypt or sign secure channel data (always) | Enabled |
| A8. Digitally encrypt secure channel data (when possible) | Enabled |
| A9. Digitally sign secure channel data (when possible) | Enabled |
| A10. Disable machine account password changes | Disabled |
| A11. Maximum machine account password age | 45 days |
| A12. Require strong (Windows 2000 or later) session key | Enabled |
| Interactive logon | |
| A13. Display user information when the session is locked | User display name, domain and user names |
| A14. Do not display last user name | Enabled |
| A15. Do not require CTRL+ALT+DEL | Disabled |
| A16. Number of previous logons to cache (in case domain controller is not available) | 0 |
| A17. Prompt user to change password before expiration | 5 days |
| Microsoft network client | |
| A18. Digitally sign communications (always) | Enabled |
| A19. Digitally sign communications (if server agrees) | Enabled |
| A20. Send unencrypted password to third-party SMB servers | Disabled |
| Microsoft network server | |
| A21. Amount of idle time required before suspending session | 15 minutes |
| A22. Digitally sign communications (always).<br>A23. The Microsoft **network server: Digitally sign communications (always)** setting is configured to **Disabled** for print servers. | Enabled |
| A24. Digitally sign communications (if client agrees) | Enabled |
| Network access | |
| A25. Allow anonymous SID/name translation | Disabled |
| A26. Do not allow anonymous enumeration of SAM accounts | Enabled |
| A27. Do not allow anonymous enumeration of SAM accounts and shares | Enabled |
| A28. Do not allow storage of credentials or .NET Passports for network authentication | Enabled |
| A29. Let Everyone permissions apply to anonymous users | Disabled |
| A30. Named Pipes that can be accessed anonymously | COMNAP, COMNODE, SQL\QUERY, SPOOLSS, LLSRPC, netlogon, lsarpc, |

| | |
|---|---|
| | samr, browser |
| A31. Remotely accessible registry paths | System\CurrentControlSet\Control\Product Options;<br>System\CurrentControlSet\Control\Server Applications;<br>Software\Microsoft\Windows NT\CurrentVersion |
| A32. Remotely accessible registry paths and sub-paths | System\CurrentControlSet\Control\Print\Printers<br>System\CurrentControlSet\Services\Eventlog<br>Software\Microsoft\OLAP Server<br>Software\Microsoft\Windows NT\CurrentVersion\Print<br>Software\Microsoft\Windows NT\CurrentVersion\Windows<br>System\CurrentControlSet\Control\ContentIndex<br>System\CurrentControlSet\Control\Terminal Server<br>System\CurrentControlSet\Control\Terminal Server\UserConfig<br>System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration<br>Software\Microsoft\Windows NT\CurrentVersion\Perflib<br>System\CurrentControlSet\Services\SysmonLog |
| A33. Restrict anonymous access to Named Pipes and Shares | Enabled |
| A34. Shares that can be accessed anonymously | None |
| A35. Sharing and security model for local accounts | Classic—local users authenticate as themselves |
| Network security | |
| A36. Do not store LAN Manager hash value on next password change | Enabled |
| A37. LAN Manager authentication level | Send NTLMv2 response only\refuse LM & NTLM |
| A38. LDAP client signing requirements | Negotiate signing |
| A39. Minimum session security for NTLM SSP based (including secure RPC) clients | Enabled all settings |
| A40. Minimum session security for NTLM SSP based (including secure RPC) servers | Enabled all settings |
| Recovery console | |
| A41. Allow automatic administrative logon | Disabled |
| A42. Allow floppy copy and access to all drives and all folders | Disabled |
| Shutdown | |
| A43. Allow system to be shut down without having to log on | Disabled |

| | |
|---|---|
| A44. Clear virtual memory page file | Disabled |
| System cryptography | |
| A45. Force strong key protection for user keys stored on the computer | User must enter a password each time they use a key |
| A46. Use FIPS compliant algorithms for encryption, hashing, and signing | Enabled |
| System objects | |
| A47. Default owner for objects created by members of the Administrators group | Object creator |
| A48. Require case insensitivity for non-Windows subsystems | Enabled |
| A49. Strengthen default permissions of internal system objects (e.g. Symbolic Links) | Enabled |
| System settings | |
| A50. Optional subsystems | None |
| A51. Use Certificate Rules on Windows Executables for Software Restriction Policies | Enabled |
| A52. Terminal Services Encryption | High |
| A53. Turn off Windows Error Reporting | Enabled |

**Recomanacions**

| | |
|---|---|
| R10. Shut down system immediately if unable to log security audits | Enabled |
| R11. Allow undock without having to log on | Disabled |
| R12. Prevent users from installing printer drivers | Enabled |
| R13. Restrict CD-ROM access to locally logged-on user only | Disabled |
| R14. Restrict floppy access to locally logged-on user only | Disabled |
| R15. Unsigned driver installation behavior | Warn but allow installation |
| R16. Require Domain Controller authentication to unlock workstation | Enabled |
| R17. Require smart card | Disabled |
| R18. Smart card removal behavior | Lock workstation |
| R19. Disconnect clients when logon hours expire | Enabled |
| R20. Force Logoff when Logon Hours expire | Enabled |

### *13.3 Audit Policy*

| Paràmetre | Valor |
|---|---|
| A54. Audit account logon events | Success Failure |
| A55. Audit account management | Success Failure |
| A56. Audit logon events | Success Failure |
| A57. Audit object access | Failure |
| A58. Audit policy change | Success |
| A59. Audit privilege use | Failure |
| A60. Audit process tracking | No auditing |
| A61. Audit system events | Success |

### *13.4 Event Log*

| Paràmetre | Valor |
|---|---|
| A62. Maximum application log size | 16.384KB |
| A63. Maximum security log size | 81.920KB |
| A64. Maximum system log size | 16.384KB |
| A65. Prevent local guests group from accessing application log | Enabled |
| A66. Prevent local guests group from accessing security log | Enabled |
| A67. Prevent local guests group from accessing system log | Enabled |
| A68. Retention method for application log | As needed |
| A69. Retention method for security log | As needed |
| A70. Retention method for system log | As needed |

### *13.5 User Rights Assignments*

| Paràmetre | Valor |
|---|---|
| A71. Access this computer from the network | Administrators, Authenticated Users, Domain Controllers |
| A72. Act as part of the operating system | No one |
| A73. Adjust memory quotas for a process | Administrators, Network Service, Local Service |
| A74. Allow log on locally | Administrators |
| A75. Allow log on through Terminal Services | Adminstrators |
| A76. Back up files and directories | Administrators |
| A77. Bypass traverse checking | Authenticated Users |
| A78. Change the system time | Local Service Administrators |
| A79. Create a pagefile | Administrators |
| A80. Create a token object | No one |
| A81. Create global objects | Administrators, SERVICE |
| A82. Create permanent shared objects | No one |
| A83. Debug programs | No one |
| A84. Deny access to this computer from the network | ANONOYMOUS LOGON; Guests; Support_388945a0; all NON-Operating System service accounts |
| A85. Deny logon as a batch job | Guests; Support_388945a0 |
| A86. Deny logon as a service | No one |
| A87. Deny logon locally | Guests; Support_388945a0 |
| A88. Deny logon through Terminal Services | Guests |
| A89. Enable computer and user accounts to be trusted for delegation | Administartors |
| A90. Force shutdown from a remote system | Administrators |
| A91. Generate security audits | NETWORK SERVICE, LOCAL SERVICE |
| A92. Impersonate a client after authentication | Administrators, SERVICE |
| A93. Increase scheduling priority | Administrators |
| A94. Load and unload device drivers | Administrators |
| A95. Lock pages in memory | No one |
| A96. Log on as a batch job | Not defined |
| A97. Log on as a service | NETWORK SERVICE |
| A98. Manage auditing and security log | Administrators |
| A99. Modify firmware environment values | Administrators |
| A100. Perform volume maintenance tasks | Administrators |
| A101. Profile single process | Administrators |
| A102. Profile system performance | Administrators |
| A103. Remove computer from docking station | Administrators |
| A104. Replace a process level token | LOCAL SERVICE, NETWORK SERVICE |
| A105. Restore files and directories | Administrators |
| A106. Shut down the system | Administrators |
| A107. Synchronize directory service data | No one |
| A108. Take ownership of files or other objects | Administrators |

### *13.6 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 |
|---|---|
| A109. Enforce password history | 10 passwords remembered |
| A110. Maximum password age | 45 days |
| A111. Minimum password age | 0 days |

| | |
|---|---|
| A112. Minimum password length | 14 characters |
| A113. Password must meet complexity requirements | Enabled |
| A114. Store password using reversible encryption | Disabled |

### *13.7 Account Lockout Policy*

| Paràmetre | Valor |
|---|---|
| A115. Account lockout duration | 15 minutes |
| A116. Account lockout threshold | 3 invalid login attempts |
| A117. Reset account lockout counter after | 15 minuts |