SOSTIC

# OFICIALÍA MAYOR DEL GOBIERNO DEL ESTADO DE AGUASCALIENTES

**REPORTE:**

## SERVICIO DE ANÁLISIS DE VULNERABILIDADES PARA DETECTAR POSIBLES RIESGOS DE INTRUSIÓN A SERVIDORES ESPECIFICOS DE LA RED GUBERNAMENTAL, EL SERVICIO DE HARDENING Y AUDITORÍA DE SEGURIDAD TENDRÁ COMO OBJETIVO LA REDUCCIÓN DE POSIBLES VULNERABILIDADES, INTRUSIONES NO AUTORIZADAS Y ATAQUES EN UN SERVIDOR BAJO EL SISTEMA OPERATIVO WINDOWS SERVER 2003 CON IIS 6.0.

**SOSTIC S.A. DE C.V.**
**R.F.C. SOS1309231S9**

**DAVID MARTINEZ FLORES**
**REPRESENTANTE LEGAL**

**REFERENCIA: PEDIDO 833/16**

**AGUASCALIENTES, AGUASCALIENTES**

**NOVIEMBRE 2016**

SOSTIC

# LÍNEA BASE DE SEGURIDAD EN EQUIPOS WINDOWS SERVER 2003

**Noviembre 2016**



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

# Contenido





Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 1 Introducción

La presente directriz, establece las políticas, los lineamientos, metodología, formatos y herramientas que conforman la provisión de servicios, para el diseño y la provisión de servicios de Ciberseguridad y Ciberdefensa.

## 2 Objetivos

Establecer una línea base de seguridad para los servidores Windows 2003 que considere los requerimientos mínimos de seguridad que deben ser configurados. Dichos requerimientos deben de cumplirse antes de que el equipo sea entregado al usuario final.

## 3 Alcance

En caso de que algún equipo no cumpla con todos los requerimientos de seguridad establecidos por razones de negocio deberá de establecerse por escrito una carta de aceptación del riesgo donde se mencionen que se está consciente de los riesgos asociados al no cumplimiento de las políticas y deberá asumir la responsabilidad en caso de que se llegue a materializar.



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 4 Política de cuentas de usuario

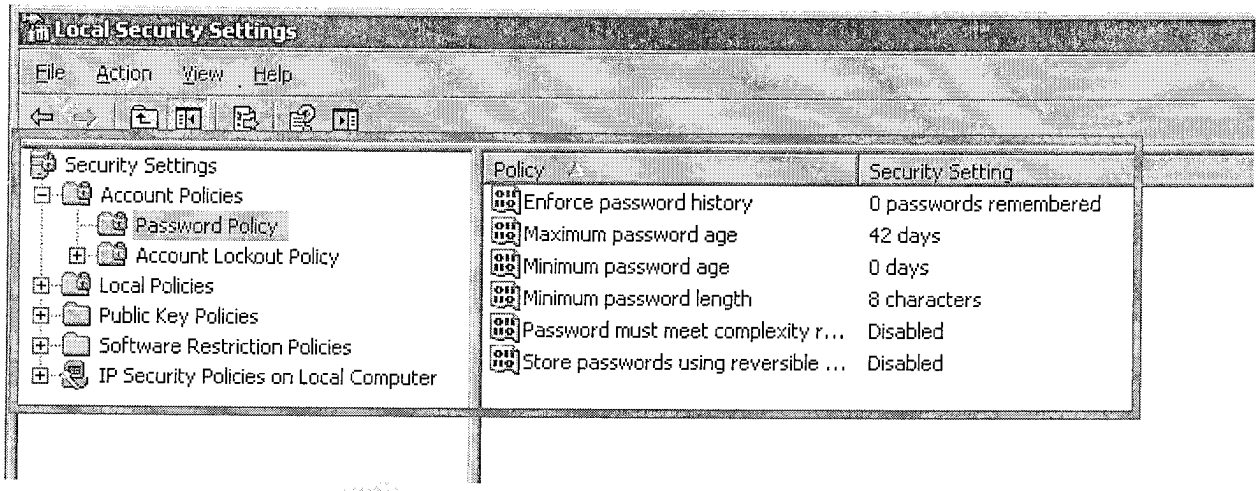



**Figura 1 Configuración actual**

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| **Historial de contraseña** | 24 o más | Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history | Este control define el número de contraseñas únicas que un usuario puede establecer antes de que una contraseña previa pueda ser rehusada. |
| **Tiempo máximo de contraseña** | 90 días o menos. | Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age | Este control define cuantos días puede el usuario usar la misma contraseña antes de que expire. |
| **Tiempo mínimo de contraseña** | 1 o más días. | Computer Configuration\Windows Settings\Security Settings\Account Policies\PasswordPolic | Este control define cuantos días puede el usuario usar la misma contraseña antes de que la pueda cambiar nuevamente. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
Leon, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | y\Minimum password age | |
| **Longitud mínima de contraseña** | Para el perfil Corporativo, el valor recomendado es **8 o más caracteres** Para el perfil SSLF, el valor recomendado es de **12 o más caracteres** | Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length | Este control define el número mínimo de caracteres de una contraseña puede contener. |
| **Complejidad de contraseña** | Enabled | Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements | Este control determina si las nuevas contraseñas definidas por los usuarios satisfagan el nivel de complejidad definido. Esto se cumple requiriendo que la composición de las nuevas contraseñas deberán ser de tal manera que sean mayores a 6 caracteres, que no estén comprometidos o que se un nombre real, que contengan al menos caracteres de 3 diferentes tipos (mayúsculas, minúsculas, dígitos). |
| **Almacenamiento de contraseñas usando cifrado reversible** | Disabled | Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption | El modelo de autenticación de Windows permite el almacenamiento del Hash de la contraseña en lugar de la contraseña actual. El hash de la contraseña no puede ser decodificado para encontrar la contraseña original. En lugar, para autenticar, la contraseña debe de convertirse en hash exactamente del mismo modo y comparada con el hash almacenado. Si los valores concuerdan, la contraseña |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | | presentada es correcta y se otorga el acceso. |
| **Duración del bloqueo de la cuenta de usuario** | 15 o más minutos | Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration | Este control determina el número mínimo de minutos que un usuario puede esperar antes que la cuenta bloqueada se desbloquee. Una vez que los criterios de bloqueo se cumplieron, la cuenta se bloquea. Sin embargo, la cuenta automáticamente se restablecerá una vez después que la duración haya terminado especificado en la "duración del bloqueo de la cuenta de usuario." Si se especifica 0 minutos la cuenta permanece bloqueada hasta que el administrador desbloquee la cuenta de forma manual. |
| **Límite de intentos de bloqueo de cuenta de usuario** | Para un perfil SSLF, el valor recomendado es: **10 intentos de acceso fallidos.** Para un perfil corporativo, el valor recomendado es: **15 intentos de acceso fallidos.** | Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold | Este control define el número de intentos de acceso fallidos antes de que una cuenta de usuario se bloquee. |
| **Restablecer el contador después del bloqueo de la cuenta de usuario** | Valor recomendado es **15 o más minutos.** | Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset | Seguido de un inicio de sesión no exitoso, el sistema incrementa el contador de intentos inválidos para esta cuenta. Este contador continúa incrementándose hasta que el umbral del bloque haya |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | account lockout counter after | alcanzado, o el contador sea restablecido. |
| **Cumplir con las restricciones de inicio de sesión de usuario** | Para el perfil de controlador de dominio corporativo y SSLF, el valor recomendado es: **Enabled** Para el perfil de servidores miembros y miembros SSLF, el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy\Enforce user logon restrictions | Este control define los atributos relacionados a Kerberos de las cuentas de usuario de dominio. Tales como el tiempo máximo de duración de un ticket de usuario y cumplir con los parámetros de inicio de sesión de usuario. |
| **Tolerancia máxima para sincronizar el reloj de una computadora** | Para el perfil de controlador de dominio corporativo y SSLF, el valor recomendado es: **5** Para el perfil de servidores miembros y miembros SSLF, el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy\Maximum tolerance for computer clock synchronization | Este control define la tolerancia máxima para la sincronización de reloj de una computadora. |
| **Vigencia máxima para un ticket de servicio** | Para el perfil de controlador de dominio corporativo y SSLF, el | Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy\Maximum | Este control define la vigencia máxima de minutos que son otorgados a un ticket de sesión que pueden ser usados para acceder a un servicio. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | valor recomendado es: **600**<br>Para el perfil de servidores miembros y miembros SSLF, el valor recomendado es: **Notdefined** | lifetime for service ticket | |
| **Vigencia máxima de renovación de un ticket de usuario** | Para el perfil de controlador de dominio corporativo y SSLF, el valor recomendado es: **7 días**<br>Para el perfil de servidores miembros y miembros SSLF, el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy\Maximum lifetime for user ticket renewal | Este control define el número de días durante el cual un ticket-granting-ticket (TGT) de usuario pueda ser renovado. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 5 Política de auditoría

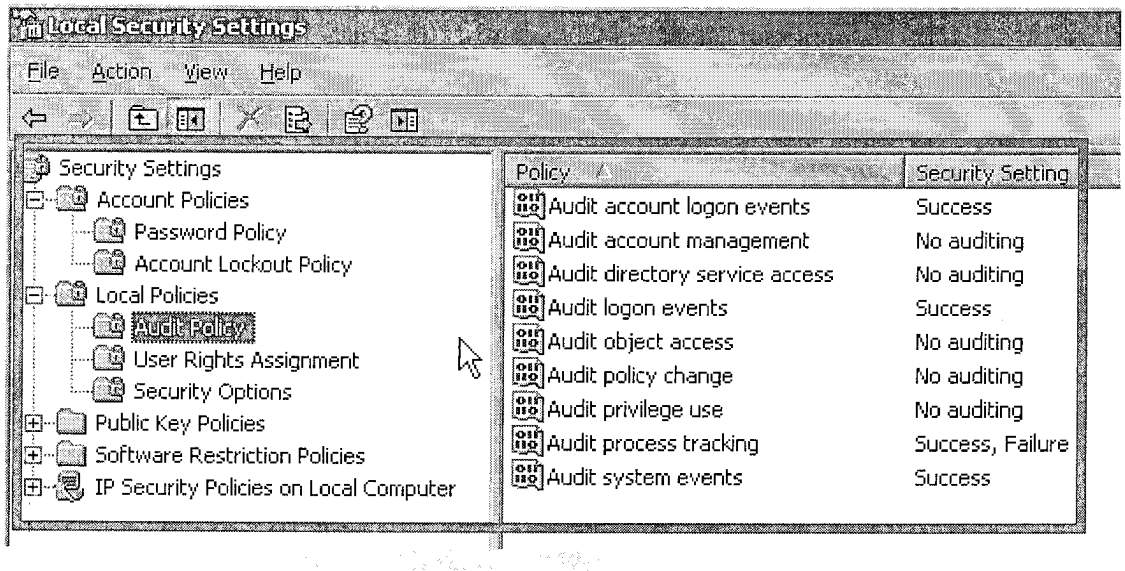



**Figura 2 Configuración actual de políticas.**

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| **Auditoría de los eventos de inicio de sesión a una cuenta de usuario** | El valor recomendado es: **Notdefined.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit account logon events | Auditar los eventos de inicio de sesión de cuenta de usuario creará una entrada al registro de eventos de seguridad cuando ocurra un inicio de sesión interactivo, inicio de sesión de red, proceso batch, o inicio de sesión por servicio. Inicios de sesión fallidos puede mostrar una tendencia de ataques de contraseña; Los eventos de acceso exitosos son importantes para identificar que usuario inició sesión en la computadora en cierto tiempo. Los eventos de inicio de sesión a una cuenta de usuario son generados desde el uso de las cuentas de dominio; esto difiere de los eventos de inicio de sesión |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | | que son generalmente usados por las cuentas locales. |
| **Auditoría de la cuenta de administración** | El valor recomendado es: **Notdefined.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit account management | Este parámetro puede ser usado para crear una entrada al registro de eventos de seguridad cuando ocurren actividades de una cuenta de administración. Ejemplos de actividades de una cuenta de administración incluyen crear o borrar un usuario o un grupo, deshabilitar o habilitar un usuario, renombrar un usuario o un grupo |
| **Auditoría del directorio de acceso a los servicios** | El valor recomendado es: **Notdefined.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit directory service access | Auditar el directorio de acceso a los servicios creará una entrada al registro de eventos de seguridad cuando objetos dentro del directorio activos sean accedidos. Habilitando este control no tiene efecto a menos que los objetos SACL contengan un ACE con banderas de auditoría. Habilitando la auditoria del directorio de acceso a los servicios puede generar una gran cantidad de entradas, y debe ser implementada con cuidado. |
| **Auditoría de eventos de inicios de sesión** | el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit logon events | Los eventos de inicio de sesión identificarán que cuentas acceden a los recursos de la computadora. Estos eventos son generados solamente cuando las credenciales de la máquina local son usadas. Aún si una máquina es miembro de un dominio, es posible iniciar sesión en una computadora usando una cuenta local. |
| **Auditoría de acceso a los objetos** | el valor recomendado | Computer Configuration\Windows Settings\Security | Este control provee capacidades de auditoría a nivel de objeto. Esto es |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | es:<br>**Notdefined** | Settings\Local Policies\Audit Policy\Audit object access | comúnmente usado para objetos del sistema de archivos. Habilitando este control no tiene efectos a menos que los objetos SACL contengan un ACE con banderas de auditoría. |
| **Auditoría del cambio de política** | el valor recomendado es:<br>**Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit object access | Este control define si la auditoría provee capacidades de auditoría a nivel de objeto. Esto es comúnmente usado para objetos del sistema de archivos. Habilitando este control no tiene efectos a menos que los objetos SACL contengan un ACE con banderas de auditoría. |
| **Auditoría del uso de privilegios** | el valor recomendado es:<br>**Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit privilege use | La auditoría del uso del privilegio habilita la auditoría para cualquier aplicación que requiere otorgar un privilegio específico. Si esto se habilita, los eventos se generaran en la bitácora de eventos de seguridad cuando un usuario o proceso intente evitar la seguridad, debugear programas, crear un objeto de token, o generar auditorías de seguridad |
| **Auditar el proceso de seguimiento** | Este valor no se recomienda a menos que sea muy necesario.<br>El valor recomendado es:<br>**Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit process tracking | Cuando esta opción se habilita, un evento se genera cada vez cuando una aplicación o un usuario inician o cambia un proceso. Esto genera rápidamente grandes cantidades eventos en la bitácora y a veces la información no es muy útil, a menos que se busque dar seguimiento a un comportamiento muy específico. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| **Auditar eventos de sistema** | el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit system events | Auditar eventos de sistema es importante. Estos eventos incluyen iniciar o parar servidores, y otros eventos que pueden impactar la computadora, pero no están relacionados con la seguridad directamente. Los eventos de sistema son particularmente útiles cuando son usados durante o después de un incidente. |
| **Auditar: Apagar el sistema inmediatamente si no puede registrar eventos de seguridad** | el valor recomendado es: **Disabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Shut down system immediately if unable to log security audits | Esta configuración causa que el sistema se apague si no puede registrar un evento de seguridad en la bitácora de eventos de seguridad. |
| **Auditar: Forzar las configuraciones de la subcategoría de la política de auditoría (Windows Vista o posterior) para anular las configuraciones de la política de auditoría** | el valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings | Esta configuración provoca que Windows respete las subcategorías de auditoría a favor de las políticas de auditorías de legado. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 6 Política de auditoria detallada

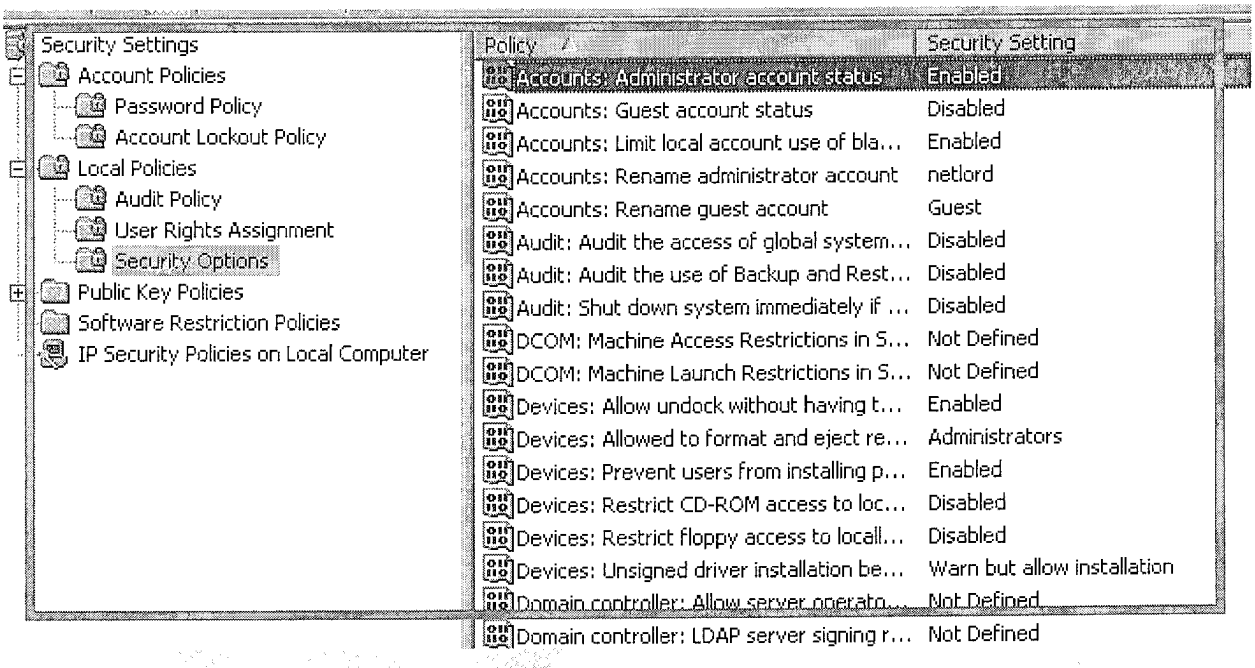



**Figura 3 Políticas que están implementadas.**

Windows server 2003 ha detallado recursos de auditoría que permite a los administradores a afinar su política de auditoría con mucho detalle. Permitiendo que los recursos tradicionales de auditoría señalados en esta sección, es probable que el rendimiento del sistema se pueda ver reducido y que los registros de eventos de seguridad puedan llevar a altos volúmenes de eventos. Dado esto, es recomendable que las políticas detalladas de auditoría en la sección subsecuente sean aprovechadas a favor sobre las políticas presentadas a continuación. Adicionalmente, "Los parámetros de la subcategoría forzar la política de auditoría", el cual se recomienda habilitarlos, causa que Windows que favorezca las subcategorías de auditoría sobre las políticas tradicionales de auditoría. Por las razones antes descritas, este documento no prescribe valores específicos para las políticas de auditoría tradicional.

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| **Política de auditoría: Sistema: Driver de IPsec** | El valor recomendado es: **Success and Failure** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\System\Audit | Este control define si se encuentra activada la auditoría para el protocolo IPSec. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | IPSec Driver\Audit Policy: System: IPsec Driver | |
| **Política de auditoría: Sistema: Cambio del estado de la seguridad** | El valor recomendado es: **Success and Failure** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\System\Audit Security State Change\Audit Policy: System: Security State Change | Este control define si se encuentra activada la auditoria para cambios en el estado de la seguridad en el sistema. |
| **Audit policy:system: Security: system extension** | El valor recomendado es: **Success and Failure** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\System\Audit Security System Extension\Audit Policy: System: Security System Extension | Este control define si se encuentra activada la auditoria para cargar el código de extensión como paquetes de autenticación por el subsistema de seguridad. |
| **Audit policy:system: Security:System integrity** | El valor recomendado es: **Success and Failure** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\System\Audit System Integrity\Audit Policy: System: System Integrity | Este control define si se encuentra activada la auditoría para violaciones a la integridad de la seguridad del subsistema. |
| **Audit policy:Logon-Logoff:Logoff** | El valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Logon/Logoff\Audit Logoff\Audit Policy: Logon-Logoff: Logoff | Este control define si se encuentra activada la auditoría cuando un usuario cierra sesión de un sistema. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
Leon, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| **Audit policy:Logon-Logoff:Logoff** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success and Failure.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Logon/Logoff\Audit Logon\Audit Policy: Logon-Logoff: Logon | Este control define si se encuentra activada la auditoría cuando un usuario inicia sesión en un sistema. |
| **Audit policy:Logon-Logoff:Special Logon** | El valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Logon/Logoff\Audit Special Logon\Audit Policy: Logon-Logoff: Special Logon | Este control define si se encuentra activada la auditoría cuando se usa un inicio de sesión especial. |
| **Audit policy:Objecta ccess:File system** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Failure.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **No auditing** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Object Access\Audit File System\Audit Policy: Object Access: File System | Este control define si se encuentra activada la auditoría cuando se acceden objetos de archivos. |
| **Audit policy:Objecta ccess:Registry** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Failure.** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group | Este control define si se encuentra activada la auditoría cuando se acceden |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **No auditing** | Policy Object\Object Access\Audit Registry\Audit Policy: Object Access: Registry | objetos de registros. |
| **Audit policy:Privileg e use: Sensitive privilege use** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **No auditing.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success and Failure** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Privilege Use\Audit Sensitive Privilege Use\Audit Policy: Privilege Use: Sensitive Privilege Use | Este control define si se encuentra activada la auditoría cuando una cuenta de usuario o un servicio usa privilegios sensibles. |
| **Audit policy:Detailed tracking: Process creation.** | El valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Detailed Tracking\Audit Process Creation\Audit Policy: Detailed Tracking: Process Creation | Este control define si se encuentra activada la auditoría cuando se crea un proceso y el nombre del programa que lo creó. |
| **Audit policy:Policy Change: Audit Policy Change.** | El valor recomendado es: **Success and Failure** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Policy Change\Audit Audit Policy Change\Audit Policy: Policy Change: Audit Policy Change | Este control define si se encuentra activada la auditoría cuando ocurre un cambio en la política de auditoría incluyendo cambios en el SACL. |
| **Audit policy:Account** | Para el perfil SSLF ya sea Controlador de | Computer Configuration\Windows | Este control define si se |



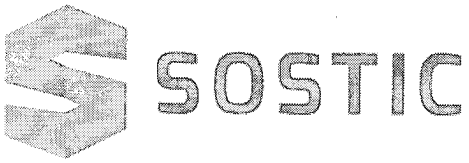
Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| **Management:Computer account management.** | dominio o Servidor miembro el valor recomendado es: **Success and Failure.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success** | Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Account Management\Audit Computer Account Management\Audit Policy: Account Management: Computer Account Management | encuentra activada la auditoría cuando ocurre un evento de una cuenta de administrador tales como: crear, cambiar, renombrar, borrar, deshabilita o habilitar. |
| **Audit policy:Account Management:Other account management events.** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success and Failure.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Account Management\Audit Other Account Management Events\Audit Policy: Account Management: Other Account Management Events | Este control define si se encuentra activada la auditoría cuando ocurre un evento de una cuenta de administrador. |
| **Audit policy:Account Management:Security Group Management** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success and Failure.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Account Management\Audit Security Group Management\Audit Policy: Account Management: Security Group Management | Este control define si se encuentra activada la auditoría cuando ocurre un evento del grupo de seguridad tales como: crear, cambiar, renombrar, borrar, deshabilitar o habilitar. |
| **Audit policy:Account Management:User account Management** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success and Failure.** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group | Este control define si se encuentra activada la auditoría cuando ocurre un evento |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06



| | | | |
|---|---|---|---|
| | Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success** | Policy Object\Account Management\Audit User Account Management\Audit Policy: Account Management: User Account Management | de una cuenta de administrador tales como: crear, cambiar, renombrar, borrar, deshabilitar o habilitar. |
| **Audit policy:DS Access: Directory Service Access** | Para el perfil SSLF y Corporativo de servidor miembro el valor recomendado es: **No auditing** Para el perfil SSLF de controlador de dominio, el valor recomendado **es Success and Failure.** Para el perfil corporativo de Controlador de dominio es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\DS Access\Audit Directory Service Access\Audit Policy: DS Access: Directory Service Access | Este control define si se encuentra activada la auditoría cuando se accede a un objeto AD DS. |
| **Audit policy:DS Access: Directory Service Changes** | Para el perfil SSLF y el corporativo de servidor miembro el valor recomendado es: **No auditing** Para el perfil SSLF de controlador de dominio, el valor recomendado **es Success and Failure.** Para el perfil corporativo de Controlador de dominio es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\DS Access\Audit Directory Service Changes\Audit Policy: DS Access: Directory Service Changes | Este control define si se encuentra activada la auditoría cuando ocurran cambios en el directorio activo en los servicios de dominio (AD DS). |
| **Audit policy:AccountLogon:Credential validation** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success and Failure.** Para el perfil corporativo ya sea | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Account Logon\Audit Credential | Este control define si se encuentra activada la auditoría para reportar los resultados de las pruebas de |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | Controlador de dominio o Servidor miembro el valor recomendado es: **Success** | Validation\Audit Policy: Account Logon: Credential Validation | validación ingresadas por una solicitud de un inicio de sesión de una cuenta de usuario. |

Windows server 2003 ha detallado recursos de auditoría que permite a los administradores a afinar su política de auditoría con mucho detalle. Permitiendo que los recursos tradicionales de auditoría señalados en esta sección, es probable que el rendimiento del sistema se pueda ver reducido y que los registros de eventos de seguridad puedan llevar a altos volúmenes de eventos. Dado esto, es recomendable que las políticas detalladas de auditoría en la sección subsecuente sean aprovechadas a favor sobre las políticas presentadas a continuación. Adicionalmente, "Los parámetros de la subcategoría forzar la política de auditoría", el cual se recomienda habilitarlos, causa que Windows que favorezca las subcategorías de auditoría sobre las políticas tradicionales de auditoría. Por las razones antes descritas, este documento no prescribe valores específicos para las políticas de auditoría tradicional.

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| **Política de auditoría: Sistema: Driver de IPsec** | El valor recomendado es: **Success and Failure** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\System\Audit IPSec Driver\Audit Policy: System: IPsec Driver | Este control define si se encuentra activada la auditoría para el protocolo IPSec. |
| **Política de auditoría: Sistema: Cambio del estado de la seguridad** | El valor recomendado es: **Success and Failure** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy | Este control define si se encuentra activada la auditoria para cambios en el estado de la seguridad en el sistema. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto. Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | Object\System\Audit Security State Change\Audit Policy: System: Security State Change | |
| **Audit policy:system: Security: system extension** | El valor recomendado es: **Success and Failure** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\System\Audit Security System Extension\Audit Policy: System: Security System Extension | Este control define si se encuentra activada la auditoria para cargar el código de extensión como paquetes de autenticación por el subsistema de seguridad. |
| **Audit policy:system: Security:Syste m integrity** | El valor recomendado es: **Success and Failure** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\System\Audit System Integrity\Audit Policy: System: System Integrity | Este control define si se encuentra activada la auditoría para violaciones a la integridad de la seguridad del subsistema. |
| **Audit policy:Logon-Logoff:Logoff** | El valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Logon/Logoff\Audit Logoff\Audit Policy: Logon-Logoff: Logoff | Este control define si se encuentra activada la auditoría cuando un usuario cierra sesión de un sistema. |
| **Audit policy:Logon-Logoff:Logoff** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success and Failure.** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy | Este control define si se encuentra activada la auditoría cuando un |

SOSTIC

| | | | |
|---|---|---|---|
| | Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success** | Configuration\System Audit Policies - Local Group Policy Object\Logon/Logoff\Audit Logon\Audit Policy: Logon-Logoff: Logon | usuario inicia sesión en un sistema. |
| **Audit policy:Logon-Logoff:Special Logon** | El valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Logon/Logoff\Audit Special Logon\Audit Policy: Logon-Logoff: Special Logon | Este control define si se encuentra activada la auditoría cuando se usa un inicio de sesión especial. |
| **Audit policy:Objecta ccess:File system** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Failure.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **No auditing** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Object Access\Audit File System\Audit Policy: Object Access: File System | Este control define si se encuentra activada la auditoría cuando se acceden objetos de archivos. |
| **Audit policy:Objecta ccess:Registry** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Failure.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Object Access\Audit Registry\Audit Policy: Object Access: Registry | Este control define si se encuentra activada la auditoría cuando se acceden objetos de registros. |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | recomendado es: **No auditing** | | |
| **Audit policy:Privileg e use: Sensitive privilege use** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **No auditing.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success and Failure** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Privilege Use\Audit Sensitive Privilege Use\Audit Policy: Privilege Use: Sensitive Privilege Use | Este control define si se encuentra activada la auditoría cuando una cuenta de usuario o un servicio usa privilegios sensibles. |
| **Audit policy:Detailed tracking: Process creation.** | El valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Detailed Tracking\Audit Process Creation\Audit Policy: Detailed Tracking: Process Creation | Este control define si se encuentra activada la auditoría cuando se crea un proceso y el nombre del programa que lo creó. |
| **Audit policy:Policy Change: Audit Policy Change.** | El valor recomendado es: **Success and Failure** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Policy Change\Audit Audit Policy Change\Audit Policy: Policy Change: Audit Policy Change | Este control define si se encuentra activada la auditoría cuando ocurre un cambio en la política de auditoría incluyendo cambios en el SACL. |
| **Audit policy:Account** | Para el perfil SSLF ya sea Controlador | Computer Configuration\Windows | Este control define si se encuentra activada |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| **Management:Computer account management.** | de dominio o Servidor miembro el valor recomendado es: **Success and Failure.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success** | Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Account Management\Audit Computer Account Management\Audit Policy: Account Management: Computer Account Management | la auditoría cuando ocurre un evento de una cuenta de administrador tales como: crear, cambiar, renombrar, borrar, deshabilita o habilitar. |
| **Audit policy:Account Management:Other account management events.** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success and Failure.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Account Management\Audit Other Account Management Events\Audit Policy: Account Management: Other Account Management Events | Este control define si se encuentra activada la auditoría cuando ocurre un evento de una cuenta de administrador. |
| **Audit policy:Account Management:Security Group Management** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success and Failure.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Account Management\Audit Security Group Management\Audit Policy: Account Management: Security Group Management | Este control define si se encuentra activada la auditoría cuando ocurre un evento del grupo de seguridad tales como: crear, cambiar, renombrar, borrar, deshabilitar o habilitar. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Seccion, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| **Audit policy:Account Management:User account Management** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success and Failure.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Account Management\Audit User Account Management\Audit Policy: Account Management: User Account Management | Este control define si se encuentra activada la auditoría cuando ocurre un evento de una cuenta de administrador tales como: crear, cambiar, renombrar, borrar, deshabilitar o habilitar. |
| **Audit policy:DS Access: Directory Service Access** | Para el perfil SSLF y Corporativo de servidor miembro el valor recomendado es: **No auditing** Para el perfil SSLF de controlador de dominio, el valor recomendado **es Success and Failure.** Para el perfil corporativo de Controlador de dominio es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\DS Access\Audit Directory Service Access\Audit Policy: DS Access: Directory Service Access | Este control define si se encuentra activada la auditoría cuando se accede a un objeto AD DS. |
| **Audit policy:DS Access: Directory Service Changes** | Para el perfil SSLF y el corporativo de servidor miembro el valor recomendado es: **No auditing** Para el perfil SSLF de controlador de dominio, el valor recomendado **es Success and Failure.** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\DS Access\Audit Directory Service Changes\Audit Policy: DS Access: Directory Service Changes | Este control define si se encuentra activada la auditoría cuando ocurran cambios en el directorio activo en los servicios de dominio (AD DS). |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | Para el perfil corporativo de Controlador de dominio es: **Success** | | |
| **Audit policy:AccountLogon:Credential validation** | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success and Failure.** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Success** | Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Account Logon\Audit Credential Validation\Audit Policy: Account Logon: Credential Validation | Este control define si se encuentra activada la auditoría para reportar los resultados de las pruebas de validación ingresadas por una solicitud de un inicio de sesión de una cuenta de usuario. |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 7 Bitácora de eventos

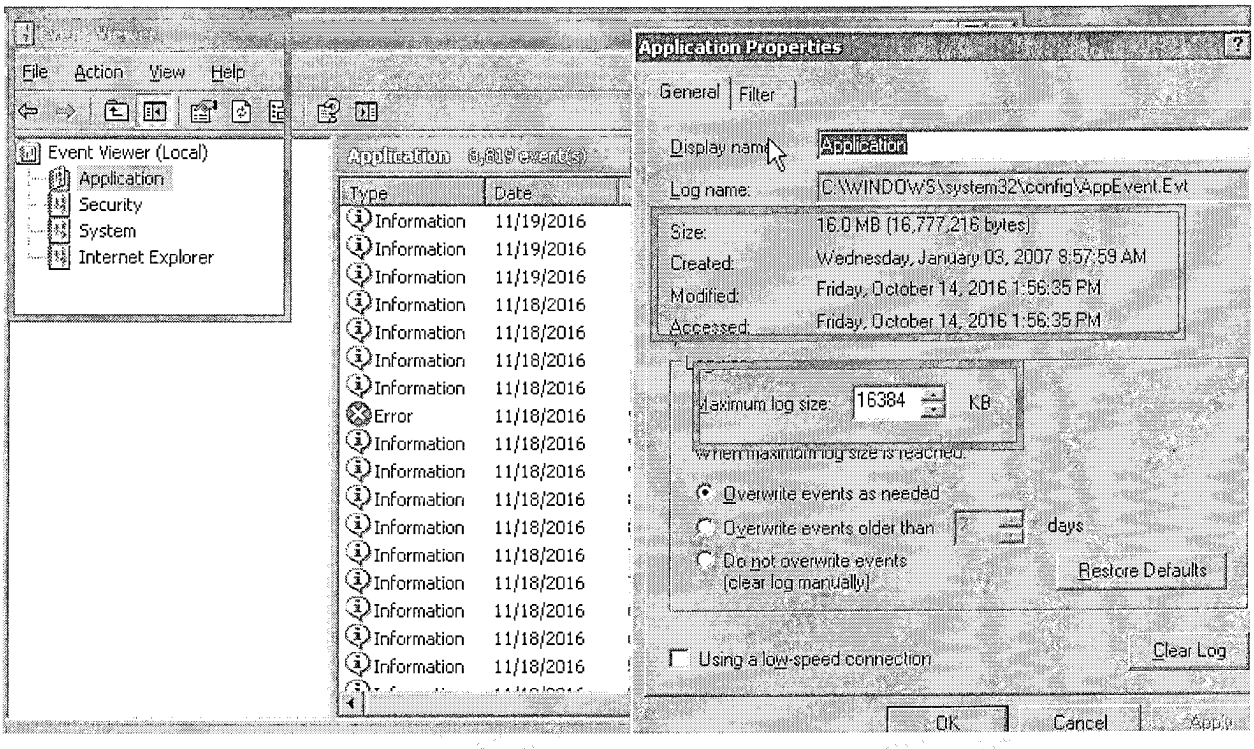



**Figura 4 Bitácoras de eventos.**

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| **Application:Maximum Log Size (KB)** | El valor recomendado es: **32768KB o mayor** | Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Application\Application: Maximum Log Size (KB) | Este control define el tamaño máximo del archivo de la bitácora en Kilobytes. |
| **Application:Retain Old Events** | El valor recomendado es: **Deshabilitado** | Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Application\Application: Retain old events | Este control determina el comportamiento de la Bitácora de eventos cuando la bitácora alcanza su tamaño máximo. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| **Security:Maximum Log Size(KB)** | El valor recomendado es: **81920 o mayor** | Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Security\Security: Maximum Log Size (KB) | Este control determina el tamaño máximo del archivo de bitácoras en Kilobytes. |
| **Security:Retain Old Events** | El valor recomendado es: **Deshabilitado** | Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Security\Security: Retain old events | Este control determina el comportamiento de la Bitácora de eventos cuando la bitácora alcanza su tamaño máximo. |
| **System:Maximum Log Size (KB)** | El valor recomendado es: **32768KB o mayor** | Computer Configuration\Administrative Templates\Windows Components\Event Log Service\System\System: Maximum Log Size (KB) | Este control define el tamaño máximo del archivo de la bitácora en Kilobytes. |
| **System:Retain Old Events** | El valor recomendado es: **Deshabilitado** | Computer Configuration\Administrative Templates\Windows Components\Event Log Service\System\System: Retain old events | Este control determina el comportamiento de la Bitácora de eventos cuando la bitácora alcanza su tamaño máximo. |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 8 Firewall de Windows

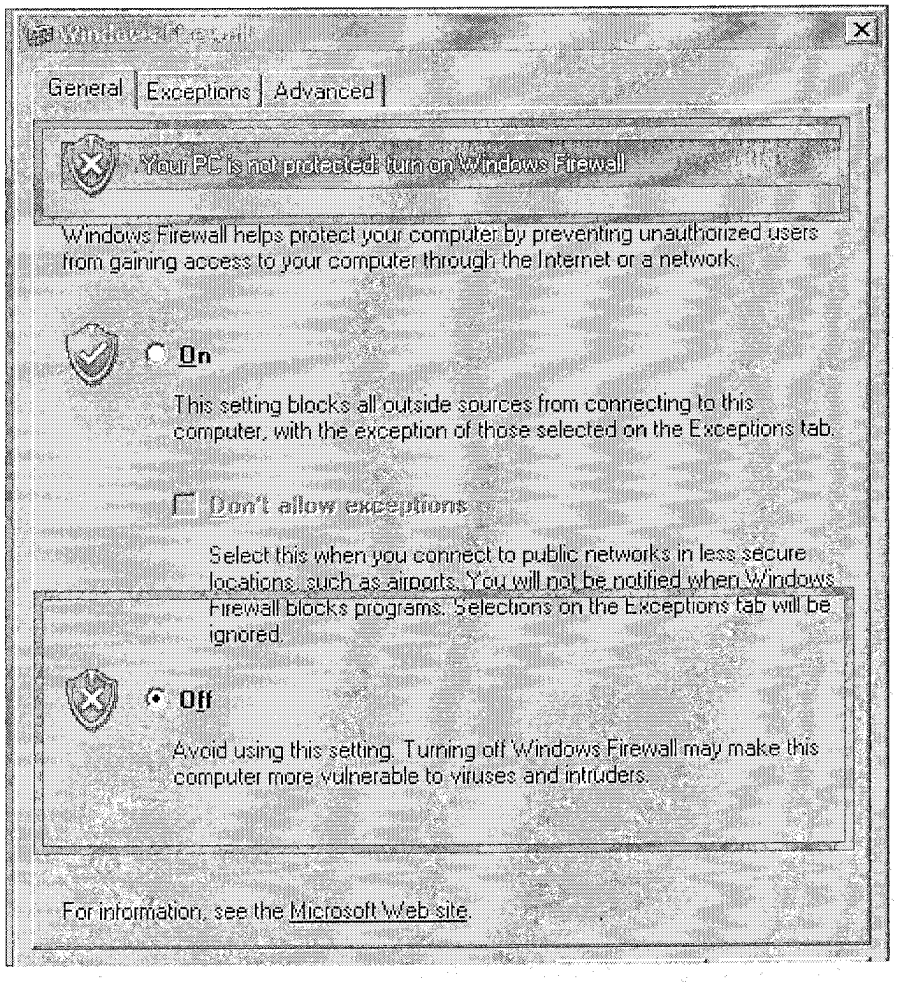



**Figura 5 Firewall deshabilitado**



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

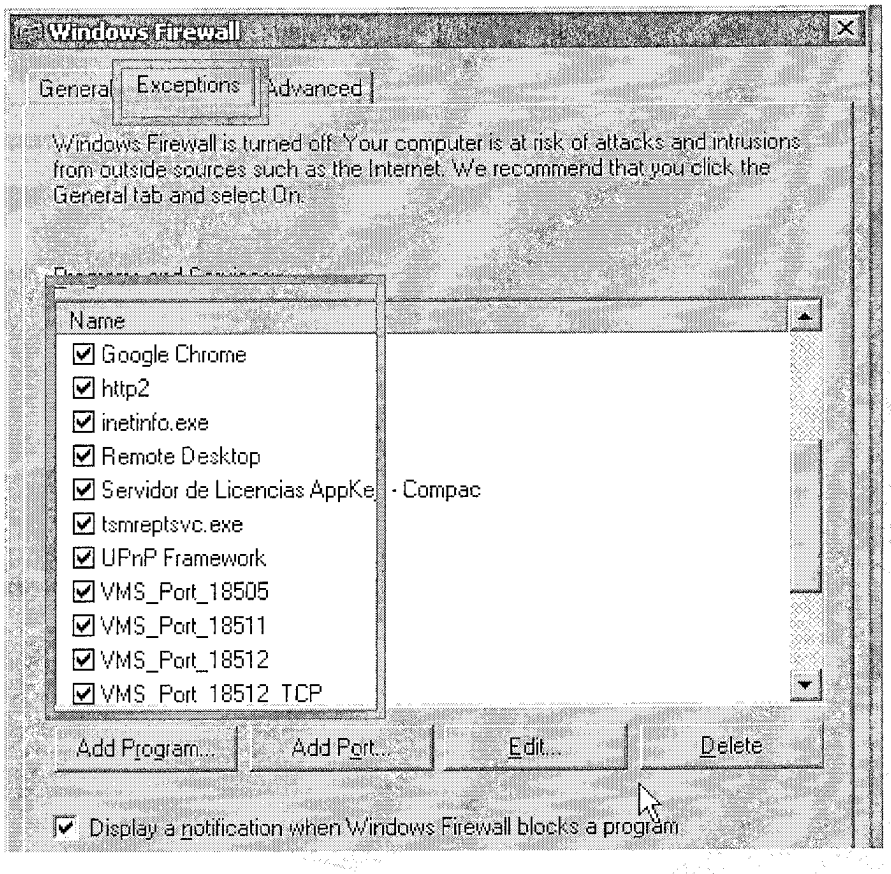



**Figura 6 excepciones de Firewall**

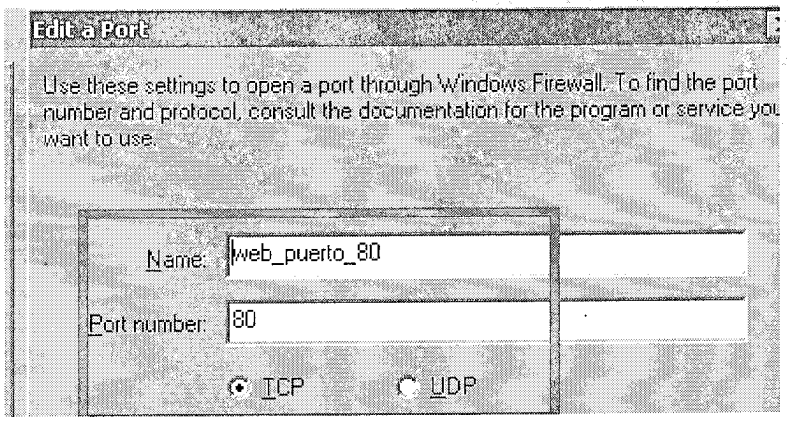



**Figura 7 Excepción del puerto 80.**



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Seccion, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
Leon, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

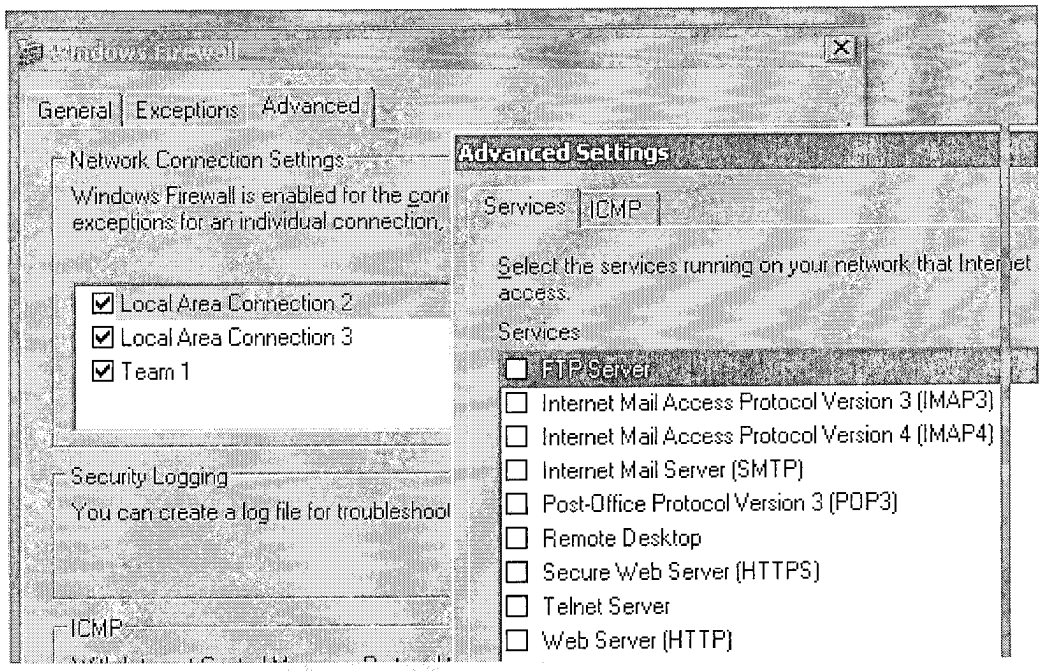



**Figura 8 Firewall configurado en Local Área Conecction 2.**

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| Windows Firewall:Allow ICMP exceptions (Domain) | El valor recomendado es: **Disabled** | Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\Windows Firewall: Allow ICMP exceptions (Domain) | Este control define los tipos de mensaje del protocolo ICMP que el Firewall de Windows permite. |
| Windows Firewall:Allow ICMP exceptions (Standard) | El valor recomendado es: **Disabled** | Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall \Standard Profile\Windows Firewall: Allow ICMP exceptions (Standard) | Este control define los tipos de mensaje del protocolo ICMP que el Firewall de Windows permite. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Windows Firewall:Apply Local connection rules (Domain) | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **No** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Notconfigured** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile Tab\Windows Firewall: Apply local connection security rules (Domain) | Este control define si es permitido que un administrador local pueda crear las reglas de seguridad de una conexión local que aplican junto con las reglas de conexión de seguridad configuradas por la política de grupo. |
| Windows Firewall:Apply Local connection rules (Private) | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **No** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Notconfigured** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile Tab\Windows Firewall: Apply local connection security rules (Private) | Este control define si es permitido que un administrador local pueda crear las reglas de seguridad de una conexión local que aplican junto con las reglas de conexión de seguridad configuradas por la política de grupo. |
| Windows Firewall:Apply Local connection rules (Public) | Valor recomendadoes: **No** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile Tab\Windows Firewall: Apply local connection security rules (Public) | Este control define si es permitido que un administrador local para crear las reglas de seguridad de una conexión local que aplican junto con las reglas de conexión de seguridad configuradas por la política de grupo. |
| Windows Firewall:Apply local | Para el perfil SSLF ya sea Controlador de dominio o | Computer Configuration\Windows Settings\Security | Este control define si es permitido que un administrador |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
Leon, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| firewall rules(Domain) | Servidor miembro el valor recomendado es: **No** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Notconfigured** | Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile Tab\Windows Firewall: Apply local firewall rules (Domain) | local pueda crear las reglas de firewall locales que aplican junto con las reglas firewall configuradas por la política de grupo. |
| Windows Firewall:Apply local firewall rules (Private) | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **No** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Notconfigured** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile Tab\Windows Firewall: Apply local firewall rules (Private) | Este control define si es permitido que un administrador local pueda crear las reglas de firewall locales que aplican junto con las reglas firewall configuradas por la política de grupo. |
| Windows Firewall:Apply local firewall rules (Public) | El valor recomendado es: **No** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile Tab\Windows Firewall: Apply local firewall rules (Public) | Este control define si es permitido que un administrador local pueda crear las reglas de firewall locales que aplican junto con las reglas firewall configuradas por la política de grupo. |
| Windows Firewall:Display a notification(Domain ) | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Yes** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced | Este control define si el Firewall de Windows despliega notificaciones cuando un programa es bloqueado por |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Seccion, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
Leon, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Notdefined** | Security\Windows Firewall Properties\Domain Profile Tab\Windows Firewall: Display a notification (Domain) | recibir conexiones entrantes. |
| Windows Firewall:Display a notification(Private) | Para el perfil SSLF ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Yes** Para el perfil corporativo ya sea Controlador de dominio o Servidor miembro el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile Tab\Windows Firewall: Display a notification (Private) | Este control define si el Firewall de Windows despliega notificaciones cuando un programa es bloqueado por recibir conexiones entrantes. |
| Windows Firewall:Display a notification(Public) | El valor recomendado es: **No** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile Tab\Windows Firewall: Display a notification (Public) | Este control define si el Firewall de Windows despliega notificaciones cuando un programa es bloqueado por recibir conexiones entrantes. |
| Windows Firewall:Firewall state (Domain) | El valor recomendado es: **On** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile Tab\Windows Firewall: Firewall state (Domain) | Este control define si el Firewall de Windows usará las configuraciones para este perfil para filtrar el tráfico de la red. Si es configurado en Off, el firewall de Windows no usará ninguna de las |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
Leon, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | | reglas del firewall o las conexiones de seguridad para este perfil. |
| Windows Firewall:Firewall state (Private) | El valor recomendado es: **On** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile Tab\Windows Firewall: Firewall state (Private) | Este control define si el Firewall de Windows usará las configuraciones para este perfil para filtrar el tráfico de la red. Si es configurado en Off, el firewall de Windows no usará ninguna de las reglas del firewall o las conexiones de seguridad para este perfil. |
| Windows Firewall:Firewallsta te (Public) | El valor recomendado es: **On** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile Tab\Windows Firewall: Firewall state (Public) | Este control define si el Firewall de Windows usará las configuraciones para este perfil para filtrar el tráfico de la red. Si es configurado en Off, el firewall de Windows no usará ninguna de las reglas del firewall o las conexiones de seguridad para este perfil. |
| Windows Firewall:Inbound connections (Domain) | El valor recomendado es: **Block** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile Tab\Windows Firewall: | Este control define si las conexiones entrantes con permitidas o bloqueadas para conectarse al sistema para este perfil. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | Inbound connections (Domain) | |
| Windows Firewall:Inbound connections (Domain) | El valor recomendado es: **Block** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile Tab\Windows Firewall: Inbound connections (Private) | Este control define si las conexiones entrantes con permitidas o bloqueadas para conectarse al sistema para este perfil. |
| Windows Firewall:Inbound connections (Domain) | El valor recomendado es: **Block** | Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile Tab\Windows Firewall: Inbound connections (Public) | Este control define si las conexiones entrantes con permitidas o bloqueadas para conectarse al sistema para este perfil. |
| Windows Firewall:Prohibit notifications (Domain) | El valor recomendado es: **Disabled** | Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\Windows Firewall: Prohibit notifications (Domain) | Este control defina si el Firewall pueda desplegar notificaciones a los usuarios cuando un programa solicita que una excepción se agregue al Firewall de Windows. |
| Windows Firewall:Prohibit notifications (Standard) | El valor recomendado es: **Disabled** | Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall \Standard Profile\Windows Firewall: | Este control define si el Firewall pueda desplegar notificaciones a los usuarios cuando un programa solicita que una excepción se |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | Prohibit notifications (Standard) | agregue al Firewall de Windows. |
| Windows Firewall:Protect all network connections (Domain) | El valor recomendado es: **Enabled** | Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\Windows Firewall: Protect all network connections (Domain) | Este control define si el Firewall de Windows se encuentra activado. |
| Windows Firewall:Protect all network connections (Standard) | El valor recomendado es: **Enabled** | Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall \Standard Profile\Windows Firewall: Protect all network connections (Standard) | Este control define si el Firewall de Windows se encuentra activado. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 9 Actualizaciones de Windows

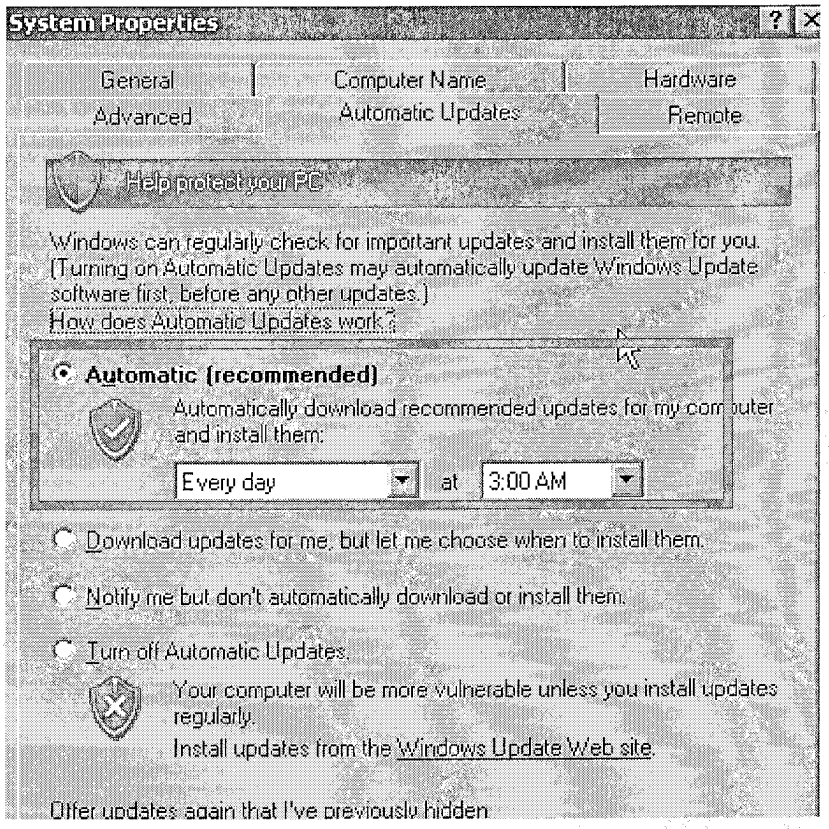



**Figura 9 Se tiene la habilitada Windows Update.**

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| Configure automatic updates | El valor recomendado es: Enabled: 3 –Auto download and notifiy for install | **Computer Configuration\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates** | Este control define si windows recibirá las actualizaciones de seguridad de Windows update o de WSUS. |
| Do not display 'Install Updates and Shut Down' option in Shut Down | El valor recomendado es: **Disabled.** | Computer Configuration\Administrative Templates\Windows Components\Windows Update\Do not display | Este control define si la opción de la instalación de actualizaciones y apagado se despliegue en el cuadro de dialogo |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Windows dialog box | | 'Install Updates and Shut Down' option in Shut Down Windows dialog box | de apagado de Windows. |
| Reprogramar Instalaciones de actualizaciones automáticas programadas | El valor recomendado es: **Enabled.** | Computer Configuration\Administrative Templates\Windows Components\Windows Update\Reschedule Automatic Updates scheduled installations | Este control define si retrasar las actualizaciones automáticas que de otra manera ocurren normalmente cuando la computadora es encendida. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 10 Control de cuentas de usuario

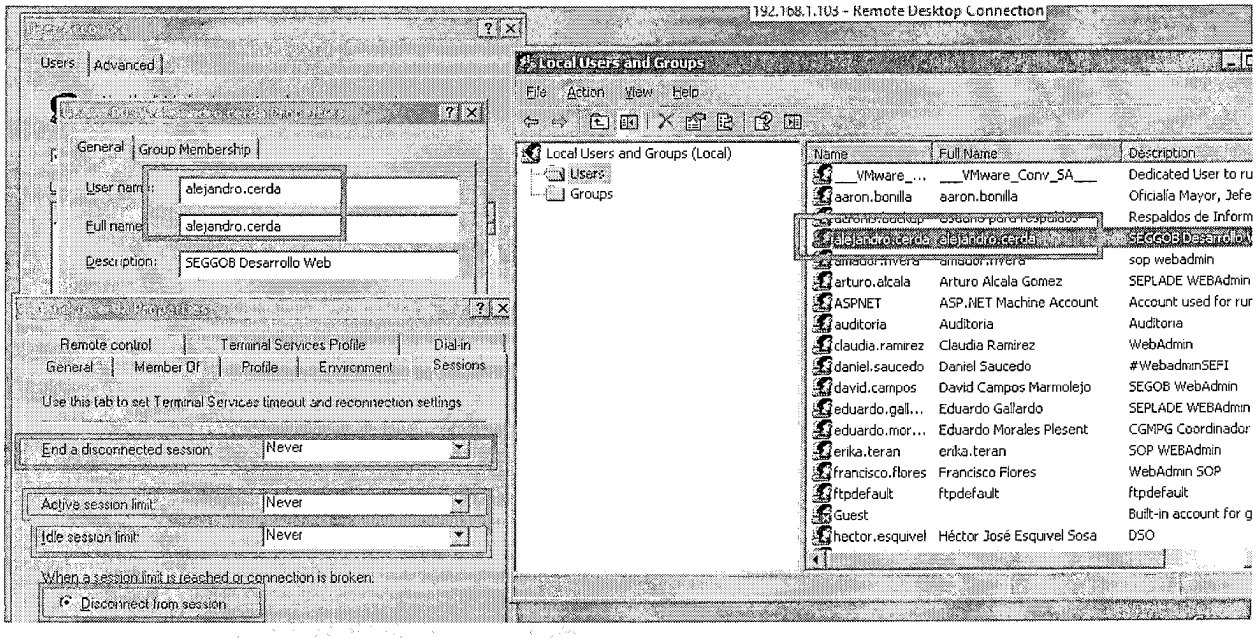



**Figura 10 La mayoría de los usuarios tienen habilitada la opción "Never".**

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| User Account Control:Admin Approval Mode for the Built-in Administrator Account | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account | Este control define si la cuenta de Built-in Administrator en modo AdminApproval. |
| User Account Control:Behavior of the elevation prompt for administrators in Admin Approval Mode | El valor recomendado es: **Promptforcredencials** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for | Este control define el comportamiento de Windows cuando un administrador intenta completar una tarea requiriendo elevar privilegios. |



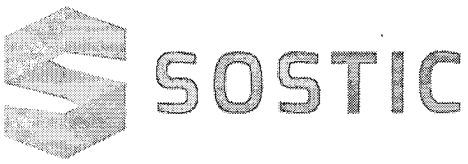
Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | administrators in Admin Approval Mode | |
| User Account Control:Behavior of the elevation prompt for standard users | El valor recomendado es: **Automaticallydenyelevationrequests** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users | Este control define el comportamiento de Windows cuando un usuario intenta completar una tarea requiriendo elevar privilegios. |
| User Account Control:Detect application installations and prompt for elevation | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Detect application installations and prompt for elevation | Este control define como Windows responde a las solicitudes de instalación de aplicaciones. |
| User Account Control: Only elevate UIAccess applications that are installed in secure locations. | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applications that are installed in secure locations | Este control ayuda a proteger Windows solamente permitiendo aplicaciones instaladas en un lugar seguro, como lo es: %Program Files% y %SystemRoot%\System32, para correr con privilegios elevados. |
| User Account Control:Run all administrators in Admin Approval Mode | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Run all administrators in Admin Approval Mode | Este control es el interruptor del Control de cuentas de usuario UAC y define si los usuarios y administradores se les solicite cuando ellos intento realizar operaciones administrativas. |
| User Account Control:Switch to secure desktop when | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security | Este control define si la elevación de UAC se despliega en escritorio seguro. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06



| | | | |
|---|---|---|---|
| prompting for elevation | | Options\User Account Control: Switch to the secure desktop when prompting for elevation | |
| User Account Control: Virtualize file and registry write failures to per-user locations | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry write failures to per-user locations | Este control define si Windows pueda virtualizar las escrituras de archivos y registros a locaciones de usuarios cuando una aplicación no compatible con la UAC intente escribir en áreas protegidas como lo es: %SYSTEMROOT%. |
| User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop | El valor recomendado es: **Disabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop | Este control define si una aplicación es permitida para que pueda elevar privilegios sin usar el escritorio seguro. |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 11 Control de cuentas de usuario

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| User Account Control:Admin Approval Mode for the Built-in Administrator Account | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account | Este control define si la cuenta de Built-in Administrator en modo AdminApproval. |
| User Account Control:Behavior of the elevation prompt for administrators in Admin Approval Mode | El valor recomendado es: **Promptforcredencials** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode | Este control define el comportamiento de Windows cuando un administrador intenta completar una tarea requiriendo elevar privilegios. |
| User Account Control:Behavior of the elevation prompt for standard users | El valor recomendado es: **Automatically denyelevationrequests** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users | Este control define el comportamiento de Windows cuando un usuario intenta completar una tarea requiriendo elevar privilegios. |
| User Account Control:Detect application installations and prompt for elevation | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Detect application installations and prompt for elevation | Este control define como Windows responde a las solicitudes de instalación de aplicaciones. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| User Account Control: Only elevate UIAccess applications that are installed in secure locations. | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applications that are installed in secure locations | Este control ayuda a proteger Windows solamente permitiendo aplicaciones instaladas en un lugar seguro, como lo es: %Program Files% y %SystemRoot%\System32, para correr con privilegios elevados. |
| User Account Control:Run all administrators in Admin Approval Mode | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Run all administrators in Admin Approval Mode | Este control es el interruptor del Control de cuentas de usuario UAC y define si los usuarios y administradores se les solicite cuando ellos intento realizar operaciones administrativas. |
| User Account Control:Switch to secure desktop when prompting for elevation | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Switch to the secure desktop when prompting for elevation | Este control define si la elevación de UAC se despliega en escritorio seguro. |
| User Account Control: Virtualize file and registry write failures to per-user locations | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry write failures to per-user locations | Este control define si Windows pueda virtualizar las escrituras de archivos y registros a locaciones de usuarios cuando una aplicación no compatible con la UAC intente escribir en áreas protegidas como lo es: %SYSTEMROOT%. |
| User Account Control: Allow UIAccess applications to prompt for elevation without using | El valor recomendado es: **Disabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Allow UIAccess | Este control define si una aplicación es permitida para que pueda elevar privilegios sin usar el escritorio seguro. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| the secure desktop | | applications to prompt for elevation without using the secure desktop | |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

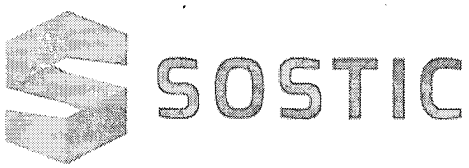
SOSTIC

## 12 Derechos de usuario

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| Access this computer from the network | Para servidores miembros del perfil Corporativo y SSLF el valor recomendado es: **Administrators, AuthenticatedUsers** Para el perfil de Controlador de dominio Corporativo y SSLF el valor recomendado es:**Administrators, Authenticatedusers, ENTERPRISE DOMAIN CONTROLERS** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access this computer from the network | Este control define si otros usuarios en la red son permitidos para conectarse a una computadora. |
| Act as part of the operating system | El valor recomendado es: **No one** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system | Este control define si un proceso es permitido para asumir la identidad de un usuario. |
| Adjust memory quotas for a process | Para el perfil SSLF para servidores miembros y controlador de dominio es valor recomendado es: **Administrators, LOCAL SERVICE, NETWORK SERVICE.** Para el perfil Corporativo para servidores miembros y controlador de dominio el valor | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Adjust memory quotas for a process | Este control permite que un usuario pueda modificar la cantidad máxima de memoria disponible a un proceso. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06



| | | | |
|---|---|---|---|
| | recomendado es: **Notdefined.** | | |
| Back up files and directories | Para el perfil SSLF para servidores miembros y controlador de dominio el valor recomendado es: **Administrators.** Para el perfil Corporativo para servidores miembros y controlador de dominio el valor recomendado es: **Notdefined.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories | Este control define si un usuario es permitido para realizar respaldos a archivos y directorios en un sistema. |
| Bypass traversechecking | Para el perfil Corporativo de servidor miembro es valor recomendado es: **Administrators, AuthenticatedUsers, BackupOperators, Local Service, Network Service** Para el perfil Corporativo de controlador de dominio, el valor recomendado es: **Notdefined.** Para el perfil SSLF de controlador de dominio el valor recomendado es: **AuthenticatedUsers, Local Service, Network Service.** Para el perfil SSLF de servidor miembro el valor recomendado es: **Administrators, AuthenticatedUsers, BackupOperators,** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Bypass traverse checking | Este control define si un usuario que no tenga el permiso de acceso de recorrer carpetas es permitido a travesar a través de carpetas mientras navegan NTFS o el registro. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | **Local Service, Network Service** | | |
| Changethesystem time | El valor recomendado es: **LOCAL SERVICE, Administrators.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time | Este control define que usuarios y grupos son permitidos para cambiar la hora y la fecha del sistema. |
| Create a pagefile | Para los perfiles Servidor miembro corporativo, servidor miembro y controlador de dominio SSLF el valor recomendado es: **Administrators** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a pagefile | Este control define si un usuario es permitido para modificar el tamaño del archivo de paginación. |
| Create a token object | El valor recomendado es: **No one** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a token object | Este permiso provee la habilidad de alterar el acceso al token del objeto para cualquier proceso o un usuario autenticado. |
| Create global objects | Para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Notdefined** Para el perfil SSLF de servidor miembro y controlador de dominio el valor recomendado es: **Administrators, SEVICE, Local Service, Network Service.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create global objects | Este control define si un usuario es permitido para crear objetos globales que se encuentran disponibles para todas las sesiones. |
| Create permanent shared objects | El valor recomendado es: **No one** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights | Este control define si un usuario es permitido para crea nuevos objetos compartidos. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | Assignment\Create permanent shared objects | |
| Deny Access to this computer from the network | El valor recomendado es: **guests.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny access to this computer from the network | Este control define que cuentas no son permitidas para conectarse a computadoras locales de la red. |
| Force shutdown from a remote system | Para el perfil SSLF de servidor miembro y controlador de dominio el valor recomendado es: **Administrators** Para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system | Este control define si una cuenta de usuario es permitida para apagar una computadora remotamente. |
| Impersonate a client after authentication | El valor recomendado es: **Administrators, SERVICE, Local Service, Network Service** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Impersonate a client after authentication | Este control define si un servicio o aplicación que se ejecuta bajo una cuenta dada es permitida para despersonalizar la cuenta de un cliente que se conecta después de que el cliente se ha autenticado. |
| Increasescheduling priority | Para el perfil SSLF de servidor miembro y controlador de dominio el valor recomendado es: **Administrators** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority | Este control define si un usuario es permitido para cambiar la clase de prioridad base de un proceso. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | Para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Notdefined** | | |
| Load and unload device drivers | El valor recomendado es: **Administrators.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Load and unload device drivers | Este control define si una cuenta de usuario es permitida para que dinámicamente pueda cargar un driver de un nuevo dispositivo en el sistema. |
| Profile single process | El valor recomendado es: **Administrators** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile single process | Este control define si un usuario es permitido para usar herramientas para monitorear el desempeño de los procesos que no son de sistema. |
| Profilesystem performance | El valor recomendado es: **Administrators** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile system performance | Este control define si un usuario es permitido para usar herramientas para ver el desempeño de los procesos del sistema. |
| Remove computer from docking station | El valor recomendado es: **Administrators** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Remove computer from docking station | Este control define si un usuario es permitido para darle click a la poción expulsar la PC en el menú de inicio para desbloquear la computadora |
| Replace a process level token | El valor recomendado es: **LOCAL SERVICE, NETWORK SERVICE.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights | Este control define si un proceso es permitido para iniciar otro servicio o proceso con un token |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | Assignment\Replace a process level token | de acceso de seguridad diferente. |
| Shutdown de system | El valor recomendado es: **Administrators** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system | Este control define si un usuario es permitido para apagar el sistema operativo cuando se autentican en una computadora localmente. |
| Addworkstationsto domain | Para el perfil SSLF de servidor miembro y controlador de dominio el valor recomendado es: **Administrators** Para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Add workstations to domain | Este control define si un usuario es permitido para agregar estaciones de trabajo a un dominio. |
| Allow log onlocally | El valor recomendado es: **Administrators** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on locally | Este control define si un usuario es permitido para que el inicio de sesión a una computadora sea interactivo. |
| Allow log on through Terminal Services | El valor recomendado es: **Administrators** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Terminal Services | Este control define si un usuario es permitido para autenticarse como cliente de Terminal Services. |
| Change de time zone | El valor recomendado es: **LOCAL SERVICE, Administrators** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights | Este control define si un usuario es permitido para cambiar el "time zone" de una computadora. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | Assignment\Change the time zone | |
| Createsymbolic links | Para el perfil SSLF de servidor miembro y controlador de dominio el valor recomendado es: **Administrators** Para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create symbolic links | Este control define si un usuario es permitido para crear ligas simbólicas en un sistema. |
| Deny log onlocally | El valor recomendado es: **Administrators** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally | Este control define que cuentas impiden logearse localmente en una computadora |
| Deny log on though terminal services | El valor recomendado es: **Guests** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Terminal Services | Este control define si un usuario es permitido para autenticarse a un cliente de terminal services. |
| Generate security audits | Para el perfil SSLF de servidor miembro y controlador de dominio el valor recomendado es: **LOCAL SERVICE, NETWORK SERVICE** Para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits | Este control define si un usuario es permitido para producir registros de auditoría en la bitácora de seguridad. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Increase a process working set | Para el perfil SSLF de servidor miembro y controlador de dominio el valor recomendado es: **LOCAL SERVICE, Administrators** Para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase a process working set | Este control define si un usuario es permitido para incrementar o disminuir el tamaño del set de procesos trabajando que es un set de páginas de memoria visible en el proceso de la memoria física RAM. |
| Log on as a batch job | Para el perfil SSLF de servidor miembro y controlador de dominio el valor recomendado es: **No one** Para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Log on as a batch job | Este control define si una cuenta es permitida para logearse para usar el servicio de programación de tareas. |
| Restore files and directories | Para el perfil SSLF de servidor miembro y controlador de dominio el valor recomendado es:**Administrators** Para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Adminsitrators, Back up Operators** | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories | Este control define si un usuario es permitido para evitar un archivo, directorio, registro y otro permisos a objetos cuando la información de respaldo se esté restaurando. |
| Take ownership of files or other objects | El valor recomendado es: **Administrators** | Computer Configuration\Windows Settings\Security | Este control define si un usuario es permitido para tomar |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | Settings\Local Policies\User Rights Assignment\Take ownership of files or other objects | propiedad de archivos, carpetas, llaves de registro, procesos e hilos. |
| Access credential manager as a trusted caller | El valor recomendado es: **No one** | Computer Configuration\Windows Settings\Local Policies\User Rights Assignment\Access credential Manager as a trusted caller | Este control define si un usuario es permitido para acceder las credenciales de usuario a través del administrador de credenciales. |
| Synchronizedirectory data | El valor recomendado es: **No one** | Computer Configuration\Windows Settings\Local Policies\User Rights Assignment\Synchronize directory service data | Este control define si un proceso puede leer todos los objetos y propiedades en directorio, sin tener en cuenta la protección en los objetos y las propiedades. |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

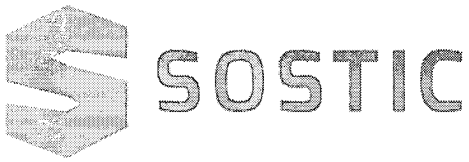
SOSTIC

## 13 Opciones de seguridad

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| Network security: Minimum session security for NTLM SSP based (including secure RPC) servers | El valor recomendado es: **Require NTLMv2 session security,Require 128-bit encryption.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers | Este control define los requerimientos mínimos de seguridad para establecer sesiones en servidores NTLM SSP. |
| Network access: Remotely accessible registry paths and sub-paths | Para el perfil SSLF de servidor miembro y controlador de dominio el valor recomendado es: **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** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths and sub-paths | Este control define si las rutas al registro y al subregistro deben ser accesibles cuando una aplicación o proceso hace referencia con la llave WinReg para determinar los permisos de acceso. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06



| | | | |
|---|---|---|---|
| | **System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog** Para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Notdefined** | | |
| Accounts: Rename administrator account | El valor recomendado es: **any value that does not contain the term "admin".** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account | Este control recomienda escoger un nombre para la cuenta built-in administrator local que es diferente a la de default. Deshabilitar la cuenta de administrador no es práctico. Sim embargo, simplemente saber el nombre de una cuenta en una computadora es muy valioso para los hackers. En un intento de esconder la cuenta, las mejores prácticas recomiendan renombrar la cuenta a un nombre único. |
| Accounts:Renameguestaccount | El valor recomendado es: **any value that does not contain the term "guest".** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account | Este control recomienda escoger un nombre para la cuenta Guest que es diferente a la default. |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Accounts:Guestaccount status | El valor recomendado es: **Disabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status | Este control puede proveer alguna regulación a los usuarios no autenticados. Deshabilitando esta cuenta prevendrá que usuarios no autenticados sean autenticados como visitantes. |
| Network access: Allow anonymous SID/Name translation | El valor recomendado es: **Disabled** | Computer Configuration\Windows Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation | Este control define si un usuario anónimo es permitido para solicitar el SID de otro usuario o usar el SID para recuperar el nombre del usuario que le corresponde. |
| Accounts: Limit local account use of blank passwords to console logon only | El valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Limit local account use of blank passwords to console logon only | Con este control la computadora rechaza los intentos de autenticación remotos si el usuario intenta usar contraseñas en blanco, aun así si la contraseña en blanco es válida para una cuenta de usuario. |
| Devices: Allowed to format and eject removable media | El valor recomendado es: **Administrators** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media | Este control gobierna el tipo de usuario el cual tienen la autoridad de remover los medios con formato NTFS de la computadora. |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Devices: Prevent users from installing printer drivers | El valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers | Este control significa que los usuarios no podrán instalar drivers de impresoras y previene que las puedan configurar. |
| Devices: Restrict CD-ROM access to locally logged-on user only | Para el perfil SSLF de servidor miembro y controlador de dominio el valor recomendado es:**Enabled**<br>Para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Restrict CD-ROM access to locally logged-on user only | Este control restringirá el uso de un drive de CD-ROM compartido con el inicio de sesión local. |
| Devices: Restrict floppy access to locally logged-on user only | Para el perfil SSLF de servidor miembro y controlador de dominio el valor recomendado es:**Enabled**<br>Para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Restrict floppy access to locally logged-on user only | Este control define si una unidad floppy es accesible a usuario remoto. |
| Domain member: Require strong (Windows 2000 or later) session key | El valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later) session key | Este control define si un canal seguro de comunicación requiere una llave de sesión robusta (128-bit) |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Domain controller: Allow server operators to schedule tasks | Para el perfil SSLF y corporativo de controlador de dominio el valor recomendado es:**Disabled** Para el perfil SSLF y corporativo de servidor miembro el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Allow server operators to schedule tasks | Este control define si los miembros del grupo Server Operator están permitidos para usar el comando AT para programar Jobs. |
| Domain controller: LDAP server signing requirements | Para el perfil SSLF de controlador de dominio el valor recomendado es: **Requiere Signing** Para el perfil SSLF de servidor miembro y para el perfil corporativo de servidor miembro y controlador de dominio el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: LDAP server signing requirements | Este control define si servidor LDAP requiere clientes LDAP para negociar firma de los datos. |
| Domain controller: Refuse machine account password changes | Para el perfil SSLF y Corporativo de controlador de dominio el valor recomendado es:**Disabled** Para el perfil SSLF y Corporativo de servidor miembro el valor recomendado es: **Notdefined** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Refuse machine account password changes | Este control define si los controladores de dominio puedan rechazar solicitudes de computadoras miembro para cambiar las contraseñas de una computadora. |
| Interactive logon: Do not display last user name | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name | Este control significa que el usuario debe introducir su id de usuario en cada autenticación que realice. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto. Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Interactive logon: Do not require CTRL+ALT+DEL | El valor recomendado es: **Disabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL | Este control define si un usuario debe presionar la secuencia de teclas CTRL+ALT+DEL antes de iniciar sesión. |
| Interactive logon: Number of previous logons to cache (in case domain controller is not available) | El valor recomendado es: **0 Logons.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Number of previous logons to cache (in case domain controller is not available) | Este control define si un usuario se puede autenticar a un Dominio de Windows usando la información de una cuenta con cache. |
| Interactive logon: Prompt user to change password before expiration | El valor recomendado es: **14 días.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration | Este control define cuantos días por adelantado un usuario es notificado para realizar el cambio de su contraseña |
| Interactive logon: Require Domain Controller authentication to unlock workstation | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Require Domain Controller | Este control define si un usuario es requerido autenticación del controlador de dominio para desbloquear una computadora. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | authentication to unlock workstation | |
| Interactive logon: Smart card removal behavior | El valor recomendado es: **Lock Workstation** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior | Este control define que pasa cuando la smartcard de un usuario autenticado es removida de un lector de smartcards. |
| Interactive logon: Message text for users attempting to log on | El valor recomendadoes: **The text blessed by your organization** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message text for users attempting to log on | Este control define un mensaje de texto que muestra a los usuarios cuando inician sesión. |
| Interactive logon: Message title for users attempting to log on | El valor recomendadoes: **The text blessed by your organization** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message title for users attempting to log on | Este control define el texto que se muestra en la barra de titulo de Windows el usuario ve cuando se inicia sesión en el sistema. |
| Interactive logon: Require smart card | Para el perfil SSLF, servidor miembro y controlador de dominio el valor recomendado es:**Enabled**<br>Para el perfil Corporativo, servidor miembro y controlador de dominio el | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Require smart card | El control define si un usuario es requerido para la iniciar sesión en una computadora con una smartcard. |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto. Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | valor recomendado es: **Notdefined** | | |
| Microsoft network client: Digitally sign communications (always) | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always) | Este control define si un paquete de firma es requerido por el componente de un cliente SMB. |
| Microsoft network client: Digitally sign communications (if server agrees) | El valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (if server agrees) | Este control define si un paquete de firma es requerido por el componente de un cliente SMB. |
| Microsoft network client: Send unencrypted password to third-party SMB servers | El valor recomendado es: **Disabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Send unencrypted password to third-party SMB servers | Este control define si un servidor puede transmitir contraseñas en texto plano a través de la red hacía otras computadoras que ofrezcan servicios SMB. |
| Microsoft network server: Amount of idle time required before suspending session | El valor recomendado es: **15 minutos** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft | Este control define el monto de tiempo de ocio que debe pasarse a una sesión SMB antes de que la sesión se suspenda por inactividad. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | network server: Amount of idle time required before suspending session | |
| Microsoft network server: Digitally sign communications (always) | El valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always) | Este control determina si el servicio SMB de lado del servidor es requerido para realizar la firma de paquetes SMB. |
| Microsoft network server: Digitally sign communications (if client agrees) | El valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees) | Este control determina si el servicio SMB de lado del servidor se requiera firmar para una conexión de cliente. |
| Microsoft network server: Disconnect clients when logon hours expire | El valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logon hours expire | Este control define si desconectar una sesión cuando las horas de un usuario válido expiren. |
| Network access: Do not allow anonymous | El valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security | Este control define si un usuario anónimo es permitido para enumerar de usuario |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| enumeration of SAM accounts | | Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts | que se encuentran en la SAM. |
| Network access: Do not allow anonymous enumeration of SAM accounts and shares | El valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares | Este control define si un usuario anónimo es permitido para enumerar de usuario y shares que se encuentran en la SAM. |
| Network access: Do not allow storage of credentials or .NET Passports for network authentication | Para el perfil SSLF, servidor miembro y controlador de dominio el valor recomendado es: **Enabled.**<br>Para el perfil Corporativo, servidor miembro y controladores de dominio el valor recomendado es: **Enabled.** | **Windows 2003** Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of credentials or .NET Passports for network authentication.<br>**Windows 2003 R2** Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and | Este control define si los nombres de usuarios y contraseñas almacenadas puedan salvar sus credenciales para su uso posterior cuando la autenticación de dominio se logre. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | credentials for network authentication | |
| Shutdown: Clear virtual memory pagefile | El valor recomendado es: **Disabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Clear virtual memory pagefile | Este control define si la paginación de la memoria virtual se limpia cuando el sistema se apaga. |
| Shutdown:Allow system to be shutdown without having to logon | El valor recomendado es: **Disabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on | Este control define si una computadora puede apagarse cuando un usuario no ha iniciado sesión. |
| System objects: Require case insensitivity for non-Windows subsystems | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Require case insensitivity for non-Windows subsystems | Este control define el caso de insensibilidad se force para todos los subsistemas. |
| System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) | El valor recomendado es: **Enabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Strengthen default | Este control define la robustez de las listas de control de acceso discrecional por default que ayudan a asegurar los objetos compartidos en el sistema. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | permissions of internal system objects (e.g. Symbolic Links) | |
| System cryptography: Force strong key protection for user keys stored on the computer | Para el perfil SSLF, servidor miembro y controlador de dominio el valor recomendado es: **Usermustenter a passwordeach time they use a key.** Para el perfil Corporativo, servidor miembro y controladores de dominio el valor recomendado es: **Userispromptedwhenthe keyisfirstused.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\System cryptography: Force strong key protection for user keys stored on the computer | Este control define si una llave privada de usuario requiere contraseña para ser usada. |
| System settings: Optional subsystems | el valor recomendado es: **None** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\System settings: Optional subsystems | Este control define que sub-sistemas se usan para soportar aplicaciones en su ambiente. |
| System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies | Para el perfil SSLF, servidor miembro y controlador de dominio el valor recomendado es: **Enabled.** Para el perfil Corporativo, servidor miembro y controladores de dominio el valor recomendado es: **Notdefined.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies | Este control define si los certificados digitales se procesan cuando software que restringe políticas es habilitado y un usuario o un software que intenta correr un programa con una extensión .exe. |
| MSS: (AutoAdminLogon) Enable Automatic Logon | el valor recomendado es: **Disabled.** | Computer Configuration\Windows Settings\Security | Este control define si un usuario con acceso físico a una computadora puede |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
Leon, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| (not recommended) | | Settings\Local Policies\Security Options\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) | automáticamente iniciar sesión. |
| MSS: (DisableIPSource Routing) IP source routing protection level (protects against packet spoofing) | el valor recomendadoes: **Highest protection, source routing is completely disabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (DisableIPSource Routing) IP source routing protection level (protects against packet spoofing) | Este control determina si Windows aceptará paquetes enrutados. Ruteo de una fuente permitirá que el que envía el paquete dicte la ruta del paquete que tomará para su destino. |
| MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | el valor recomendado es: **Disabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | Este control define si el protocol ICMP se redirige para reemplazar rutas generadas de OSPF. |
| MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds | Para el perfil SSLF, servidor miembro y controlador de dominio el valor recomendado es: **5 minutos.** Para el perfil Corporativo, servidor miembro y controladores de dominio el valor recomendado es: **Notdefined.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (KeepAliveTime) How often keep-alive packets are | Este control define cada cuantos intentos de TCP para enviar un paquete de KeepAlive para verificar conexiones osciosas se encuentran intactas. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | sent in milliseconds | |
| MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic | El valor recomendadoes: **Only ISAKMP is excempt (recommended for Windows Server 2003).** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic | Este control define si las excepciones de IPsec sean configuradas para varios tipos de tráfico tales como IKE y Kerberos. |
| MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | El valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | Este control define si una computadora no toma en cuenta las solicitudes de liberación del nombre de NETBIOS excepto para aquellos que vengan de un servidor WINS en el SCE. |
| MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended) | El valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 | Este control defines si una computadora puede generar nombres de archivos estilo 8.3. |



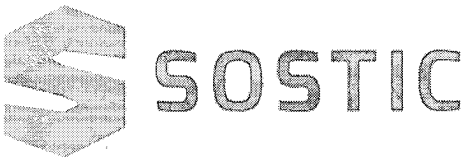
Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | style filenames (recommended) | |
| MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | El valor recomendado es: **Disabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | Este control define si el protocolo IRDP es usado automáticamente para detectar y configurar direcciones de default Gateway. |
| MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) | El valor recomendado es: **Enabled** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) | Este control define si una aplicación es forzada para empezar una búsqueda de archivos DLL en el path del sistema antes de buscar en la carpeta que actualmente se está trabajando. |
| MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) | El valor recomendado es: **0** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) | Este control define en segundos entre que el protector de pantalla se activa cuando la consola de la computadora este bloqueada. |
| (TCPMaxDataRetransmissions) How many times | El valor recomendado es: **3** | Computer Configuration\Windows | Este control define el número de veces que TCP retransmita un |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06



| | | | |
|---|---|---|---|
| unacknowledged data is retransmitted (3 recommended, 5 is default) | | Settings\Security Settings\Local Policies\Security Options\MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | segmento de información antes de que la conexión se aborte. |
| MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning | El valor recomendado es: **90% o menos** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning | Este control define si una entrada se agrega a log de eventos de seguridad cuando el log alcanza el límite definido para los usuarios. |
| MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) | El valor recomendadoes: **Highest protection, source routing is completely disabled.** | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) | Este control determina si Windows aceptará paquetes enrutados de una fuente. |
| MSS: (TCPMaxDataRetransmissions) | El valor recomendado es: **3** | Computer Configuration\Windows Settings\Security | Este control define el número de veces que TCP retransmite a un segmento de datos |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| IPv6 How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | | Settings\Local Policies\Security Options\MSS: (TCPMaxDataRetransmissions) IPv6 How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | individual antes de que se aborte la conexión. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 14 Servicios de Terminal

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| Always prompt client for password upon connection | El valor recomendado es: **Enabled** | Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt client for password upon connection | Este control define si los servicios de terminal o escritorio remoto soliciten una contraseña aun si el cliente de escritorio remoto ya la hubiera proporcionado. |
| Set client connection encryption level | El valor recomendado es: **Enabled: High Level** | Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Set client connection encryption level | Este control define si la computadora que hospeda una conexión remota obligará un nivel de cifrado para la conexión. |
| Do not allow drive redirection | Para el perfil SSLF, servidor miembro y controlador de dominio el valor recomendado es: **Notconfigured.** Para el perfil Corporativo, servidor miembro y controladores de dominio el valor recomendado es: **Enabled.** | Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow drive redirection | Este control define si un usuario es permitido para compartir sus drives locales en el cliente de servicios de terminal que ellos acceden. |
| Do not allow passwords to be saved | El valor recomendado es: **Enabled.** | Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection | Este control define si el cliente de los servicios de terminal pueda salvar contraseñas. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto. Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | Client\Do not allow passwords to be saved | |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto. Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 15 Internet

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| **Turn off downloading of print drivers over HTTP** | El valor recomendado es: **Enabled** | Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off downloading of print drivers over HTTP | Este control define si la computadora puede bajar drivers de impresora sobre HTTP. |
| **Turn off the "Publish to Web" task for files and folders** | El valor recomendado es: **Enabled** | Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Publish to Web" task for files and folders | Este control define si hacer tareas para publicación de archivos, carpetas hacia la web. |
| **Turn off Internet download for Web publishing and online ordering wizards** | El valor recomendado es: **Enabled** | Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet download for Web publishing and online ordering wizards | Este control define si Windows pueda bajar una lista de proveedores para la publicación Web. |
| **Turn off printing over HTTP** | El valor recomendado es: **Enabled** | Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off printing over HTTP | Este control define si un cliente es permitido para imprimir sobre HTTP. |
| **Turn off Search Companion content file updates** | El valor recomendado es: **Enabled** | Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off | Este control define si la búsqueda puedan automáticament e bajar actualizaciones |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | Search Companion content file updates | de contenido durante la realización de búsquedas en internet. |
| **Turn off the Windows Messenger Customer Experience Improvement Program** | El valor recomendado es: **Enabled** | Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the Windows Messenger Customer Experience Improvement Program | Este control define si el mensajero de Windows pueda recolectar y enviar información de forma anónima. |
| **Turn off Windows Update device driver searching** | Para el perfil SSLF, servidor miembro y controlador de dominio el valor recomendado es: **Enabled.** Para el perfil Corporativo, servidor miembro y controladores de dominio el valor recomendado es: **Notdefined.** | Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows Update device driver searching | Este control define si Windows buscará en el sitio Windows Update drivers de dispositivos cuando los drivers locales de un dispositivo no se encuentren. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 16 Configuraciones adicionales de seguridad

| Parámetros | Valor recomendado | Valor en la GPO | Descripción |
|---|---|---|---|
| **Registry Policy processing** | Para el perfil Corporativo y SSLF de servidor miembro el valor recomendado es: **Enabled.** Para el perfil Corporativo y SSLF,de controladores de dominio el valor recomendado es: **Notdefined.** | Computer Configuration\Administrative Templates\System\Group Policy\Registry policy processing | El control define cuando y como las políticas de registro son actualizadas. |
| **OfferRemoteAssistance** | Para el perfil SSLF, servidor miembro y controlador de dominio el valor recomendado es: **Disabled.** Para el perfil Corporativo, servidor miembro y controladores de dominio el valor recomendado es: **Notdefined.** | Computer Configuration\Administrative Templates\System\Remote Assistance\Offer Remote Assistance | Este control define si Windows permitirá ofertas no solicitadas para proveer asistencia remota a un usuario local. |
| **SolicitedRemote Assistance** | Para el perfil SSLF, servidor miembro y controlador de dominio el valor recomendado es: **Disabled.** Para el perfil Corporativo, servidor miembro y controladores de dominio el valor recomendado es: **Notdefined.** | Computer Configuration\Administrative Templates\System\Remote Assistance\Solicited Remote Assistance | Este control define si Windows permitirá que un usuario local pueda solicitar remotamente ver y controlar su sistema. |
| **Restrictions for Unauthenticated RPC clients** | Para el perfil SSLF, servidor miembro y controlador de dominio el valor recomendado es: **Enabled:Authenticated** Para el perfil Corporativo, servidor miembro y controladores de dominio el valor recomendado es: **Notdefined.** | Computer Configuration\Administrative Templates\System\Remote Procedure Call\Restrictions for Unauthenticated RPC clients | Este control define si el tiempo de ejecución de RPC en un servidor RPC para restringir clientes RPC no autenticados del servidor RPC. |
| **RPC Endpoint Mapper Client Authentication** | Para el perfil SSLF, servidor miembro y controlador de | Computer Configuration\Administrative | Este control define un cliente RPC es |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | dominio el valor recomendado es: **Enabled** Para el perfil Corporativo, servidor miembro y controladores de dominio el valor recomendado es: **Notdefined.** | Templates\System\Remote Procedure Call\RPC Endpoint Mapper Client Authentication | requerido autenticarse antes de comunicarse con el servicio EnpointMapper. |
| **Turn off Autoplay** | El valor recomendado es: **Enabled:Alldevices.** | Computer Configuration\Administrative Templates\Windows Components\AutoPlay Policies\Turn off Autoplay | Este control define si el autoplay es permitido. |
| **Enumerate administrator accounts on elevation** | Para el perfil SSLF, servidor miembro y controlador de dominio el valor recomendado es: **Disabled** Para el perfil Corporativo, servidor miembro y controladores de dominio el valor recomendado es: **Notconfigured.** | Computer Configuration\Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation | Este control define si un usuario es permitido para ver todas las cuentas de administración cuando un usuario intenta elevar de privilegios una aplicación que corre. |
| **Require trusted path for credential entry** | El valor recomendado es: **Enabled.** | Computer Configuration\Administrative Templates\Windows Components\Credential User Interface\Require trusted path for credential entry | Cuando este parámetro se habilita, en lugar de desplegar el cuadro de dialogo para solicitar credenciales, Windows primero solicitará que el usuario presione Control +ALT+Delete. |
| **Disable remote Desktop Sharing** | El valor recomendado es: **Enabled.** | Computer Configuration\Administrative | Este control define si un usuario es |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| | | Templates\Windows Components\NetMeeting\Disable remote Desktop Sharing | permitido para compartir su escritorio usando Net Meeting. |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto. Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

# CONFIGURACIÓN EN SERVIDOR WINDOWS SERVER 2003 "GEAWEB03V"



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc, Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

## 17 Servicios del sistema

Cuando se instala por primera vez Windows Server 2003 R2, se crean los servicios predeterminados del sistema y se configuran para ejecutarse cuando se inicia el sistema. Muchos de estos servicios no necesitan ejecutarse en ciertos entornos.

Existen servicios opcionales adicionales con Windows Server 2003 R2, como el servicio "Servicios de certificados de Active Directory", que no se instalan durante la instalación predeterminada de Windows Server 2003 R2. Los servicios opcionales se pueden añadir a un sistema existente habilitando roles o características manualmente, utilizando el complemento MMC Administrador del Servidor, o de manera automatizada, utilizando por ejemplo scripts o cmdlets de Powershell.

Cualquier servicio o aplicación es un punto potencial de ataque. Por lo tanto, todos los servicios o archivos ejecutables que no sean necesarios se desactivan o eliminan en el entorno objetivo.

En la siguiente tabla se detalla el estado de los servicios en la plantilla de seguridad. Se han incluido todos los servicios, incluso aquellos que no estarán instalados en una instalación por defecto:

| Nombre del Servicio | Nombre corto | Inicio | Permiso |
|---|---|---|---|
| Acceso a dispositivo de interfaz humana | hidserv | Deshabilitada | Configurado |
| Adaptador de escucha | Net.Msmq NetMsmqActivator | Deshabilitada | Configurado |
| Adaptador de escucha | Net.Pipe NetPipeActivator | Deshabilitada | Configurado |
| Adaptador de escucha | Net.Tcp NetTcpActivator | Deshabilitada | Configurado |
| Adaptador de rendimiento de WMI | wmiApSrv | Deshabilitada | Configurado |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Administración de aplicaciones | AppMgmt | Deshabilitada | Configurado |
| Administración de certificados y claves de mantenimiento | hkmsvc | Deshabilitada | Configurado |
| Administración de licencias de Escritorio remoto | TermServLicensing | Deshabilitada | Configurado |
| Administración remota de Windows (WS-Management) | WinRM | Deshabilitada | Configurado |
| Administrador de conexión automática de acceso remoto | RasAuto | Deshabilitada | Configurado |
| Administrador de conexión de acceso remoto | RasMan | Deshabilitada | Configurado |
| Administrador de credenciales | VaultSvc | Deshabilitada | Configurado |
| Administrador de cuentas de seguridad | SamSs | Automático | Configurado |
| 4 Se han incluido en la lista todos los servicios susceptibles de ser instalados en un sistema Windows Server 2003 R2 independiente mediante la activación de roles y | | | |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| características del propio Windows Server 2003 R2. Es posible que en un equipo haya otros servicios correspondientes a otras aplicaciones, como por ejemplo un antivirus. | | | |
| Administrador de identidad de redes de mismo nivel | p2pimsvc | Deshabilitada | Configurado |
| Administrador de informes de almacenamiento del servidor de archivos | SrmReports | Deshabilitada | Configurado |
| Administrador de recursos del servidor de archivos | SrmSvc | Deshabilitada | Configurado |
| Administrador de recursos del sistema de Windows | WSRM | Deshabilitada | Configurado |
| Administrador de sesión del Administrador de ventanas de escritorio | UxSms | Automático | Configurado |
| Adquisición de imágenes de Windows (WIA) | stisvc | Deshabilitada | Configurado |
| Agente de cuarentena de acceso remoto | rqs | Deshabilitada | Configurado |
| Agente de directiva | IPsec PolicyAgent | Deshabilitada | Configurado |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Agente de Protección de acceso a redes | napagent | Deshabilitada | Configurado |
| Aislamiento de claves CNG | KeyIso | Manual | Configurado |
| Almacenamiento protegido | ProtectedStorage | Manual | Configurado |
| Aplicación auxiliar de NetBIOS sobre TCP/IP | lmhosts | Deshabilitada | Configurado |
| Aplicación auxiliar IP | iphlpsvc | Deshabilitada | Configurado |
| Aplicación del sistema COM+ | COMSysApp | Deshabilitada | Configurado |
| Archivos sin conexión | CscService | Deshabilitada | Configurado |
| Asignador de detección de topologías de nivel de vínculo | lltdsvc | Deshabilitada | Configurado |
| Asignador de extremos de RPC | RpcEptMapper | Automático | Configurado |
| Audio de Windows | AudioSrv | Deshabilitada | Configurado |
| Ayuda del Panel de control de Informes de problemas y soluciones | wercplsupport | Deshabilitada | Configurado |
| Ayudante especial de la consola de administración | sacsvr | Deshabilitada | Configurado |
| BranchCache | PeerDistSvc | Deshabilitada | Configurado |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Captura SNMP | SNMPTRAP | Deshabilitada | Configurado |
| Cliente de directiva de grupo | gpsvc | Automático | Configurado |
| Cliente de seguimiento de vínculos distribuidos | TrkWks | Deshabilitada | Configurado |
| Cliente DHCP | Dhcp | Deshabilitada | Configurado |
| Cliente DNS | Dnscache | Deshabilitada | Configurado |
| Cliente para NFS | NfsClnt | Deshabilitada | Configurado |
| Cliente web | WebClient | Deshabilitada | Configurado |
| Cola de impresión | Spooler | Deshabilitada | Configurado |
| Compilador de extremo de audio de Windows | AudioEndpointBuilder | Deshabilitada | Configurado |
| Conexión compartida a Internet (ICS) | SharedAccess | Deshabilitada | Configurado |
| Conexiones de red | Netman | Manual | Configurado |
| Configuración automática de redes cableadas | dot3svc | Deshabilitada | Configurado |
| Configuración automática de WLAN | Wlansvc | Deshabilitada | Configurado |
| Configuración de Escritorio remoto | SessionEnv | Deshabilitada | Configurado |
| Conjunto resultante de proveedor de | RSoPProv | Deshabilitada | Configurado |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| directivas | | | |
| Coordinador de transacciones distribuidas | MSDTC | Deshabilitada | Configurado |
| Desencadenadores de Message Queue Server | MSMQTriggers | Deshabilitada | Configurado |
| Desfragmentador de disco | defragsvc | Deshabilitada | Configurado |
| Detección de hardware shell | ShellHWDetection | Automático | Configurado |
| Detección de servicios interactivos | UI0Detect | Deshabilitada | Configurado |
| Detección SSDP | SSDPSRV | Deshabilitada | Configurado |
| Directiva de extracción de tarjetas inteligentes | SCPolicySvc | Deshabilitada | Configurado |
| Disco virtual | vds | Manual | Configurado |
| Dispositivo host de UPnP | upnphost | Deshabilitada | Configurado |
| DLL de host del Contador de rendimiento | PerfHost | Deshabilitada | Configurado |
| Energía | Power | Automático | Configurado |
| Enrutamiento y acceso remoto | RemoteAccess | Deshabilitada | Configurado |
| Enumerador de bus IP PnP- X | IPBusEnum | Deshabilitada | Configurado |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto. Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Espacio de nombres DFS | Dfs | Deshabilitada | Configurado |
| Estación de trabajo | LanmanWorkstation | Deshabilitada | Configurado |
| Estado de servicio de ASP.NET | aspnet_state | Deshabilitada | Configurado |
| Examinador de equipos | Browser | Deshabilitada | Configurado |
| Experiencia con aplicaciones | AeLookupSvc | Deshabilitada | Configurado |
| Experiencia de calidad de audio y vídeo de Windows (qWave) | QWAVE | Deshabilitada | Configurado |
| Fax | Fax | Deshabilitada | Configurado |
| Firewall de Windows | MpsSvc | Automático | Configurado |
| Hora de Windows | W32Time | Automático | Configurado |
| Host de proveedor de detección de función | fdPHost | Deshabilitada | Configurado |
| Host de sistema de diagnóstico | WdiSystemHost | Deshabilitada | Configurado |
| Host del servicio de diagnóstico | WdiServiceHost | Deshabilitada | Configurado |
| Identidad de aplicación | AppIDSvc | Deshabilitada | Configurado |
| Información de la aplicación | Appinfo | Manual | Configurado |
| Iniciador de procesos de servidor DCOM | DcomLaunch | Automático | Configurado |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto. Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Inicio de sesión secundario | seclogon | Deshabilitada | Configurado |
| Instalador de módulos de Windows | TrustedInstaller | Manual | Configurado |
| Instantáneas de volumen | VSS | Deshabilitada | Configurado |
| Instrumental de administración de Windows | Winmgmt | Automático | Configurado |
| KTMRM para DTC (Coordinador de transacciones distribuidas) | KtmRm | Deshabilitada | Configurado |
| Llamada a procedimiento remoto (RPC) | RpcSs | Automático | Configurado |
| Message Queue Server | MSMQ | Deshabilitada | Configurado |
| Microsoft .NET Framework NGEN v2.0.50727_X64 | clr_optimization_v2.0. 50727_64 | Deshabilitada | Configurado |
| Microsoft .NET Framework NGEN v2.0.50727_X86 | clr_optimization_v2.0. 50727_32 | Deshabilitada | Configurado |
| Módulos de creación de claves de IPsec para IKE y AuthIP | IKEEXT | Automático | Configurado |
| Motor de filtrado de base | BFE | Automático | Configurado |



Aguascalientes, Ags. Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Net Logon | Netlogon | Deshabilitada | Configurado |
| Plug and Play | PlugPlay | Automático | Configurado |
| Programador de aplicaciones multimedia | MMCSS | Deshabilitada | Configurado |
| Programador de tareas | Schedule | Automático | Configurado |
| Propagación de certificados | CertPropSvc | Deshabilitada | Configurado |
| Protección de software | sppsvc | Automático | Configurado |
| Protocolo de autenticación extensible | EapHost | Deshabilitada | Configurado |
| Protocolo de resolución de nombres de mismo nivel | PNRPsvc | Deshabilitada | Configurado |
| Protocolo simple de transferencia de correo (SMTP) | SMTPSVC | Deshabilitada | Configurado |
| Proveedor de instantáneas de software de Microsoft | swprv | Deshabilitada | Configurado |
| Publicación de recurso de detección de función | FDResPub | Deshabilitada | Configurado |
| Puerta de enlace de Escritorio remoto | TSGateway | Deshabilitada | Configurado |
| Reconocimiento de ubicación de red | NlaSvc | Automático | Configurado |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Recopilador de eventos de Windows | Wecsvc | Deshabilitada | Configurado |
| Redirector de puerto en modo usuario de Servicios de Escritorio remoto | UmRdpService | Deshabilitada | Configurado |
| Registrador de configuración de Windows Connect Now | wcncsvc | Deshabilitada | Configurado |
| Registro de eventos de Windows | eventlog | Automático | Configurado |
| Registro remoto | RemoteRegistry | Deshabilitada | Configurado |
| Registros y alertas de rendimiento | pla | Deshabilitada | Configurado |
| Replicación DFS | DFSR | Deshabilitada | Configurado |
| Servicio auxiliar de host para aplicaciones | AppHostSvc | Deshabilitada | Configurado |
| Servicio biométrico de Windows | WbioSrvc | Deshabilitada | Configurado |
| Servicio Cifrado de unidad BitLocker | BDESVC | Deshabilitada | Configurado |
| Servicio de administración de web | WMSVC | Deshabilitada | Configurado |
| Servicio de administración IIS | IISADMIN | Deshabilitada | Configurado |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Servicio de caché de fuentes de Windows | FontCache | Deshabilitada | Configurado |
| Servicio de clúster | ClusSvc | Deshabilitada | Configurado |
| Servicio de detección automática de proxy web WinHTTP | WinHttpAutoProxySvc | Deshabilitada | Configurado |
| Servicio de directivas de diagnóstico | DPS | Deshabilitada | Configurado |
| Servicio de entrada de Tablet PC | TabletInputService | Deshabilitada | Configurado |
| Servicio de equilibrio de carga RPC/HTTP | RPCHTTPLBS | Deshabilitada | Configurado |
| Servicio de generación de hash de SMB | SmbHash | Deshabilitada | Configurado |
| Servicio de lista de redes | netprofm | Automático | Configurado |
| Servicio de notificación de eventos de sistema | SENS | Deshabilitada | Configurado |
| Servicio de notificación de SSP | sppuinotify | Manual | Configurado |
| Servicio de perfil de usuario | ProfSvc | Automático | Configurado |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Servicio de protocolo de túnel de sockets seguros | SstpSvc | Deshabilitada | Configurado |
| Servicio de publicación de nombres de equipo PNRP | PNRPAutoReg | Deshabilitada | Configurado |
| Servicio de publicación World Wide Web | W3SVC | Deshabilitada | Configurado |
| Servicio de puerta de enlace de nivel de aplicación | ALG | Deshabilitada | Configurado |
| Servicio de transferencia inteligente en segundo plano (BITS) | BITS | Deshabilitada | Configurado |
| Servicio de uso compartido de puertos Net.Tcp | NetTcpPortSharing | Deshabilitada | Configurado |
| Servicio del iniciador iSCSI de Microsoft | MSiSCSI | Deshabilitada | Configurado |
| Servicio del módulo de copia de seguridad a nivel de bloque | wbengine | Deshabilitada | Configurado |
| Servicio enumerador de dispositivos portátiles | WPDBusEnum | Deshabilitada | Configurado |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Servicio FTP de Microsoft | ftpsvc | Deshabilitada | Configurado |
| Servicio Informe de errores de Windows | WerSvc | Deshabilitada | Configurado |
| Servicio Interfaz de almacenamiento en red | nsi | Automático | Configurado |
| Servicio LPD | LPDSVC | Deshabilitada | Configurado |
| Servicio Registro de plataforma para canal de fibra de Microsoft | FCRegSvc | Deshabilitada | Configurado |
| Servicio Respondedor en línea | OcspSvc | Deshabilitada | Configurado |
| Servicio SNMP | SNMP | Deshabilitada | Configurado |
| Servicio WAS (Windows Process Activation Service) | WAS | Deshabilitada | Configurado |
| Servicios de base TPM | TBS | Deshabilitada | Configurado |
| Servicios de certificados de Active Directory | CertSvc | Deshabilitada | Configurado |
| Servicios de cifrado | CryptSvc | Automático | Configurado |
| Servicios de Escritorio remoto | TermService | Deshabilitada | Configurado |
| Servicios simples de TCP/IP | simptcp | Deshabilitada | Configurado |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Servidor | LanmanServer | Deshabilitada | Configurado |
| Servidor BITS compacto | BITSCompactServer | Deshabilitada | Configurado |
| Servidor de directivas de redes | IAS | Deshabilitada | Configurado |
| Servidor de orden de subprocesos | THREADORDER | Deshabilitada | Configurado |
| Servidor de Servicios de implementación de Windows | WDSServer | Deshabilitada | Configurado |
| Servidor DHCP | DHCPServer | Deshabilitada | Configurado |
| Servidor DNS | DNS | Deshabilitada | Configurado |
| Servidor iSNS de Microsoft | MSiSNS | Deshabilitada | Configurado |
| Servidor para NFS | NfsService | Deshabilitada | Configurado |
| Sistema de cifrado de archivos (EFS) | EFS | Deshabilitada | Configurado |
| Sistema de color de Windows | WcsPlugInService | Deshabilitada | Configurado |
| Sistema de eventos COM+ | EventSystem | Automático | Configurado |
| SQL Server VSS | Writer SQLWriter | Deshabilitada | Configurado |
| Tarjeta inteligente | SCardSvr | Deshabilitada | Configurado |



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

| | | | |
|---|---|---|---|
| Telefonía | TapiSrv | Deshabilitada | Configurado |
| Telnet | TlntSvr | Deshabilitada | Configurado |
| Temas | Themes | Deshabilitada | Configurado |
| TP AutoConnect Service | TPAutoConnSvc | Deshabilitada | Configurado |
| TP VC Gateway Service | TPVCGateway | Deshabilitada | Configurado |
| Ubicador de llamada a procedimiento remoto (RPC) | RpcLocator | Deshabilitada | Configurado |
| Windows CardSpace | idsvc | Deshabilitada | Configurado |
| Windows Defender | WinDefend | Deshabilitada | Configurado |
| Windows Driver Foundation - Usermode Driver Framework | wudfsvc | Deshabilitada | Configurado |
| Windows Installer | msiserver | Manual | Configurado |
| Windows Internal Database (MICROSOFT##SSEE) | MSSQL$MICROSOFT## #SSEE | Deshabilitada | Configurado |
| Windows Presentation Foundation Font Cache 3.0.0.0 | FontCache3.0.0.0 | Deshabilitada | Configurado |
| Windows Search | Wsearch | Deshabilitada | Configurado |
| Windows Update | wuauserv | Deshabilitada | Configurado |
| WINS | WINS | Deshabilitada | Configurado |

Normalmente, el servidor no tendrá instalados todos los servicios posibles de un servidor Windows Server 2003 R2 independiente, y por lo tanto, al revisar la plantilla aparecerá el nombre



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto. Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

corto en lugar del nombre descriptivo del servicio. En cualquier caso, la plantilla se aplicará completamente para configurar incluso los servicios que no estén instalados.

## 18 Desactivación de protocolos innecesarios

### Netbios sobre TCP/IP

Con el objetivo de reducir aún más la superficie de ataque se deshabilitarán todos aquellos protocolos de red que no sean estrictamente necesarios. Por defecto Windows Server 2003 R2 habilita diversos protocolos en todas las interfaces de red. Se recomienda deshabilitar todos los que no sean imprescindibles y en concreto deshabilita todos excepto TCP/IPv4, y dentro de la configuración de TCP/IPv4 deshabilita el uso de NetBIOS sobre TCP/IP y la búsqueda de LMHOSTS.

Esta configuración se puede realizar manualmente accediendo a las Propiedades de cada interfaz de red a través del Panel de control: Panel de control > Redes e Internet >Conexiones de red.

### IPV6

El protocolo IPv6, llamado a ser el sucesor de IPv4, se encuentra habilitado por defecto en Windows Server 2003 R2, además de IPv4, y para reducir la superficie de ataque del servidor, se recomienda deshabilitarlo mientras no sea necesario su uso.

Para deshabilitar el protocolo IPv6 en el sistema, excepto para comunicaciones internas del propio servidor, esta guía establece el valor 0xFFFFFFFF en la clave de registro DisabledComponents, bajo KLM\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters. [Ver referencia 929852].

La modificación de dicha clave de registro se realiza importando mediante el comando regedit un archivo con extensión .reg con el contenido siguiente:

*Windows Registry Editor Version 5.00*

*[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Param*

*eters]*

*"DisabledComponents"=dword:ffffffff*



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

## 19 Recomendaciones

A partir de la informacion recabada durante el proceso de revision de seguridad y el establecimietnto de la linea base de seguridad, el equipo de consultoria de TPX, recomienda:

Habilitar la opción de auditoria en cada usuario o aplicación

*Referencia: https://support.microsoft.com/es-es/kb/814595)*

Se tienen 45 cuentas que tienen habilitada la opción no expiran las credenciales de acceso, lo cual presenta un peligro, al poner el riego, la única cuenta que no debería de expirar es la de administrador único.

- Para evitar esta falla es necesario seguir con las políticas de cuentas usuarios

Se tiene más de dos administradores habilitados en la configuración.

- Solo se deben de configurar dos cuentas como máximo "SYSADMIN"

Se presentan actualizaciones desfasadas y en ocasiones ya no hay un seguimiento de actualizaciones por parte de las aplicaciones.

- Actualizar en forma manual y de acuerdo a las solicitudes de los desarrolladores.

El sistema operativo Windows 2003 server presenta alrededor de 412 modificaciones desde su lanzamiento, lo que ocasiona que sea un equipo fácil de atacar, por parte de terceras personas, como lo menciona en el siguiente link..

*Referencia: http://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-7108/Microsoft-Windows-Server-2003.html*



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06

SOSTIC

- La recomendación para evitar este tipo de anomalías, es migrar el sistema operativo por un el más reciente del mercado y el cual se adecue a las especificaciones de los desarrolladores.

*Referencia: https://technet.microsoft.com/es-es/library/dn408633(v=ws.11).aspx*

## 20 Conclusiones

El sistema operativo Windows 2003 server, que este implementado en las instalaciones de OMAGS, presenta un gran fallo de seguridad, ocasionando que las aplicaciones presenten un gran riesgo por la fuga o el borrado de información.

Se recomienda implementa de forma inmediata las medidas de recomendación contenidas en el presente documento a fin de reducir los riesgos potenciales a los que la institución se encuentra expuesta.



Aguascalientes, Ags, Montes Himalaya 703, Jardines de la Concepción 2ª Sección, C.P. 20120, E.mail. contacto@sostic.com.mx, Tel. +52 (449) 174 74 75
León, Gto, Privada de los Abedules #123 Fracc. Arboledas de Ibarrilla, CP 37200, E.mail. contacto@sostic.com.mx, Tel. +52 (477) 763 12 06