SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

SAT
Servicio de Administración Tributaria

APÉNDICE 6

Políticas de seguridad para la imagen de software

(APS-3)

Este apéndice es de carácter informativo, por lo que deberá considerarse como referencias aproximadas y no definitivas.

Este folio es consecutivo en orden alfabético por empresa: 54784

Índice

Este folio es consecutivo en orden alfabético por empresa: 54785

1. Políticas de seguridad para la imagen de software

El procedimiento para la verificación de la seguridad Básica de los equipos con Microsoft Windows 7 y posteriores es el siguiente:

SEGURIDAD LÓGICA DEL SISTEMA
Sistema de archivos
El equipo debe contar con por lo menos dos particiones, una de las particiones deberá de contener al menos 40 GB de espacio, para el respaldo de la información del usuario.
Las particiones del equipo deben ser NTFS.
Cuenta de Administrador
El usuario Administrador debe estar renombrado y debe contar con un password complejo de 12 caracteres
Perfiles de usuario
El usuario Guest (invitado) debe estar desactivado o removido
Las conexiones tipo Anonymous deben estar deshabilitadas para accesos remotos al registry y al archivo LSA (ver Registry)
Sólo el grupo de Administrators debe tener permisos para Administrar la Auditoria y los logs de seguridad
Solo el grupo de Administrators debe tener permisos para manipular los archivos u otros objetos del S.O.
El equipo debe contar con perfiles específicos para dar soporte, transmitir información, instalar paquetes, monitorear y auditar el equipo en producción
Auditoría
La auditoría debe estar habilitada para Logon y Logoff no exitosos
La auditoría debe estar habilitada para cambios en las políticas de seguridad exitosas y no exitosas
Los archivos "regedt32.exe" y "regedit.exe" deben ser accesados solo por el grupo Administrators
Directiva de contraseñas
Forzar el historial de contraseñas a 4 días
Vigencia máxima de la contraseña es 42 días
Vigencia mínima de la contraseña es 2 días
Longitud mínima de la contraseña es 8 caracteres
Las contraseñas deben cumplir los requisitos de complejidad con dígitos alfanuméricos
Bloqueo de cuentas
Duración del bloqueo de cuenta es 30 min.
Umbral de bloqueo de cuenta es de 3 intentos
Restablecer el bloqueo de cuenta está después de 30 min.
Antivirus

Este folio es consecutivo en orden alfabético por empresa: 54786

El equipo debe mantener actualizada la versión de antivirus institucional o la proporcionada por el proveedor de servicios APS
Service packs y hotfixes
El equipo debe contar con el service pack más reciente del sistema operativo, los parches específicos de sistemas operativos y aplicativos, y los hot fixes liberados hasta ese momento previa validación de funcionalidad en el Centro de Certificación. Esto es válido para todo momento durante la vigencia del contrato de servicios de APS.
Registry
Hive: HKEY_LOCAL_MACHINE \SYSTEM; Key: CurrentControlSet\Control\LSA; Value: Name RestrictAnonymous; Type: REG_DWORD; Value: 2
Hive: HKEY_LOCAL_MACHINE \SYSTEM; Key: \CurrentControlSet\Control\SecurePipeServers; Value Name: \winreg; Asignar Full control solo al grupo de Administradores
Servicios
No se deberá cargar inicialmente software de servicios web, ambientes de desarrollo, servidores de correo ni ftp salvo para los perfiles de desarrollador.

1.1 Objetivo

Poner en claro los pasos que se deben seguir para la verificación de la configuración de seguridad en equipos de escritorio.

1.2 Alcance

Equipos de escritorio y móviles del proyecto APS-2.

1.3 Imagen del sistema operativo, aspectos elementales.

a) El Sistema de Archivos deberá ser NTFS.
b) Servicios

El siguiente es el cuadro de servicios de sistema operativo y el estatus que deberán tener en la configuración inicial.

SERVICE	FULL NAME	STATUS
AppMgmt	Application Management	DISABLED
Cisvc	Indexing Service	DISABLED

Este folio es consecutivo en orden alfabético por empresa: 54787

SERVICE	FULL NAME	STATUS
ClipSrv	ClipBook	DISABLED
Dmadmin	Logical Disk Manager Administrative Service	DISABLED
Fax	Fax Service	DISABLED
IsmServ	Intersite Messaging	DISABLED
Kdc	Kerberos Key Distribution Center	DISABLED
Mnmsrvc	NetMeeting Remote Desktop Sharing	DISABLED
MSIServer	Windows Installer	DISABLED
NetDDEdsdm	Network DDE DSDM	DISABLED
Netman	Network Connections	DISABLED
NtLmSsp	NTLM Security Support Provider	DISABLED
RasAuto	Remote Access Auto Connection Manager	DISABLED
RasMan	Remote Access Connection Manager	DISABLED
RemoteAccess	Routing and Remote Access	DISABLED
Rpclocator	Remote Procedure Call (RPC) Locator	DISABLED
RSVP	QoS Admission Control (RSVP)	DISABLED
ScardDrv	Smart Card Helper	DISABLED
ScardSvr	Smart Card	DISABLED
SharedAccess	Internet Connection Sharing	DISABLED
SysmonLog	Performance Logs and Alerts	DISABLED
TapiSrv	Telephony	DISABLED
TermService	Terminal Services	DISABLED
TlntSvr	Telnet	DISABLED
TrkSrv	Distributed Link Tracking Server	DISABLED
UPS	Uninterruptible Power Supply	DISABLED
UtilMan	Utility Manager	DISABLED
Print SP	Windows Print Spooler	DISABLED

c) Puertos

La configuración de los puertos de red deberá adecuarse a la siguiente tabla:

PORT	TCP	UDP
1025	x	
1032	x	

Este folio es consecutivo en orden alfabético por empresa: 54788

PORT	TCP	UDP
1033	x	
1065	x	
1066	x	
1067	x	
1433	x	
2835	x	
2836	x	
138		x
500		x
1434		x

d) Directivas de contraseñas

Directiva	Configuración mínima recomendada
Forzar el historial de contraseñas	4 contraseñas recordadas
Vigencia máxima de la contraseña	42 días
Vigencia mínima de la contraseña	2 días
Longitud mínima de la contraseña	8 caracteres
Las contraseñas deben cumplir los requisitos de complejidad	Habilitado
Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio	Deshabilitado

e) Bloqueo de cuentas

Directiva	Configuración mínima recomendada
Duración del bloqueo de cuenta	30 minutos
Umbral de bloqueo de cuenta	3 intentos incorrectos de inicio de sesión
Restablecer el bloqueo de cuenta después de	30 minutos

Directiva	Configuración del equipo
Auditar sucesos de inicio de sesión de cuenta	error
Auditar la administración de cuentas	error

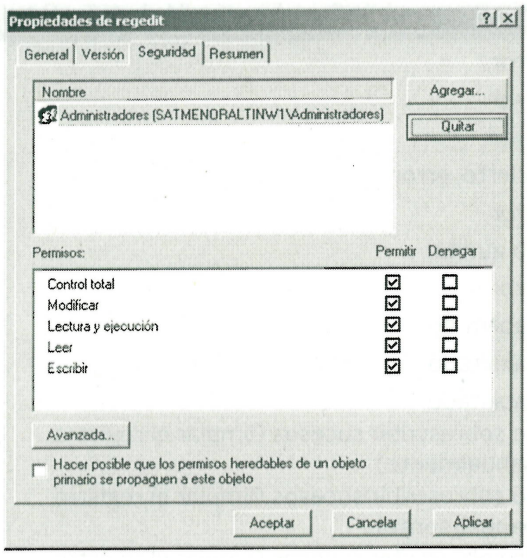
Este folio es consecutivo en orden alfabético por empresa: 54789

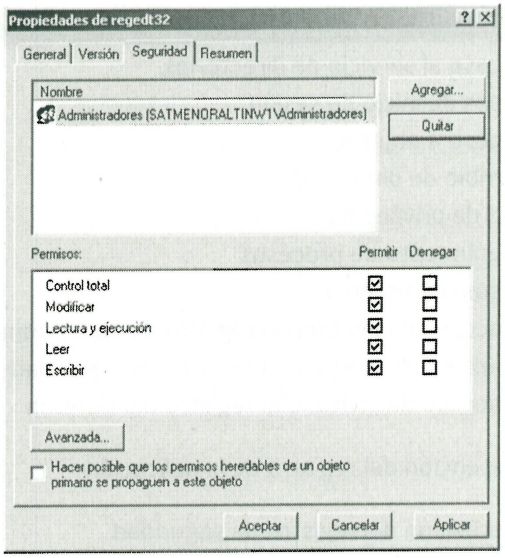
Directiva	Configuración del equipo
Auditar el acceso al servicio de directorios	Error
Auditar sucesos de inicio de sesión	error
Auditar el acceso a objetos	error
Auditar el cambio de directivas	Acierto, error
Auditar el uso de privilegios	Error
Auditar el seguimiento de procesos	No auditar
Auditar sucesos del sistema	error
Restringir el acceso de Invitado al registro de aplicaciones	Habilitado
Restringir el acceso de Invitado al registro de seguridad	Habilitado
Restringir el acceso de Invitado al registro del sistema	Habilitado
Método de retención del registro de la aplicación	No sobrescribir sucesos (limpiar el registro manualmente)
Método de retención del registro de seguridad	No sobrescribir sucesos (limpiar el registro manualmente)
Método de retención del registro del sistema	No sobrescribir sucesos (limpiar el registro manualmente)
Apagar el equipo cuando se llene el registro de auditorías de seguridad	No definido

f) Auditoria

Los archivos "regedt23.exe" (ubicado en c:\winnt\system32) y "regedit.exe" (ubicado en c:\winnt) deberán tener permiso de acceso exclusivamente para el grupo de Administrators.

Este folio es consecutivo en orden alfabético por empresa: 54790





g) Perfiles de usuario

Opción	Configuración vigente
Tomar control de archivos u otros objetos	Administradores
Administrar Auditoria y logs de Seguridad	Administradores

Opción	Configuración
Restricciones adicionales para conexiones anónimas	No obtener acceso sin permisos anónimos explícitos
Permitir a los operadores de servidor programar tareas (sólo controladores de dominio)	Por definir
Permitir apagar el sistema sin tener que iniciar sesión	Por definir
Permitir expulsar medios NTFS extraíbles	Administradores
Tiempo de inactividad requerido antes de desconectar la sesión	10 minutos
Auditar el acceso de objetos globales del sistema	Deshabilitado
Auditar el uso del privilegio de copia de seguridad y restauración	Deshabilitado
Cerrar automáticamente la sesión de los usuarios cuando termine el tiempo de sesión	De pende de la aplicación

Opción	Configuración
Cerrar automáticamente la sesión de los usuarios cuando termine el tiempo de sesión (local)	Habilitado
Borrar el archivo de páginas de la memoria virtual al apagar el sistema	Habilitado
Firmar digitalmente la comunicación con el cliente (siempre)	Habilitado
Firmar digitalmente la comunicación con el cliente (cuando sea posible)	Habilitado
Firmar digitalmente la comunicación con el servidor (siempre)	Habilitado
Firmar digitalmente la comunicación con el servidor (cuando sea posible)	Habilitado
Deshabilitar el requisito de presionar Ctrl+Alt+Supr para iniciar la sesión	Deshabilitado
No mostrar el último nombre de usuario en la pantalla de inicio de sesión	Habilitado
Nivel de autenticación de LAN Manager	Enviar sólo respuestas NTLMv2, rechazar LM y NTLM
Texto del mensaje para los usuarios que intentan conectarse	N/A
Título del mensaje para los usuarios que intentan conectarse	N/A
Núm. de inicios de sesión previos en la caché (en caso de que el controlador de dominio no esté disponible)	Por definir
Impedir el mantenimiento de la contraseña de la cuenta de equipo	Deshabilitado
Impedir que los usuarios instalen controladores de impresora	Habilitado
Pedir al usuario cambiar la contraseña antes de que caduque	14 días
Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitado
Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitado
Cambiar el nombre de la cuenta de administrador	Habilitado
Cambiar el nombre de la cuenta de invitado	Habilitado
Restringir el acceso a la unidad de CD-ROM sólo al usuario con sesión iniciada localmente	Por definir
Restringir el acceso a la unidad de disquete sólo al usuario con sesión iniciada localmente	Por definir
Canal seguro: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitado

Este folio es consecutivo en orden alfabético por empresa: 54792

Opción	Configuración
Canal seguro: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitado
Canal seguro: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitado
Canal seguro: requerir clave de sesión protegida (Windows 2000 o posterior)	Habilitado
Partición segura del sistema (sólo para plataformas RISC)	No definido
Enviar contraseña no cifrada para conectar con servidores SMB de otros fabricantes	Deshabilitado
Apagar el sistema de inmediato si no puede registrar auditorias de seguridad	Deshabilitado
Comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo
Reforzar los permisos predeterminados de los objetos globales del sistema (p.e. vínculos simbólicos)	Habilitado
Comportamiento de instalación de controlador no firmado	No permitir la instalación
Comportamiento de instalación de no controlador no firmado	Avisar pero permitir la instalación

Cerrar la ventana de Directiva de Seguridad Local (Alt+F4)

1. No deberán existir cuentas denominada Administrador (Administrator) después de la aplicación de la directiva de cambio de nombre de la misma. La cuenta invitado (Guest) deberá estar deshabilitada. Cualquier otro usuario en el sistema deberá formar parte del grupo de operación. Estos usuarios no deberán formar parte del grupo de Administradores (Administrators).
2. **Service Packs y Hotfixes**: Estos deberán mantenerse actualizados hasta el último "releáse" para sistema operativo y aplicativos específicos (office, Internet Explorer, etc.) durante el período de vigencia del contrato de servicios APS-2.
3. **Registry**: No deberán existir accesos anónimos al Registry y al archivo de seguridad local del sistema (LSA)

Solo el grupo de Administradores deberá tener acceso total en **HKEY_LOCAL_MACHINE / SYSTEM / CurrentControlSet / Control / SecurePipeServers / winreg**, en el menú de la parte superior de la ventana de **regedt32**, la opción de **Seguridad** y bajo ésta **permisos**.

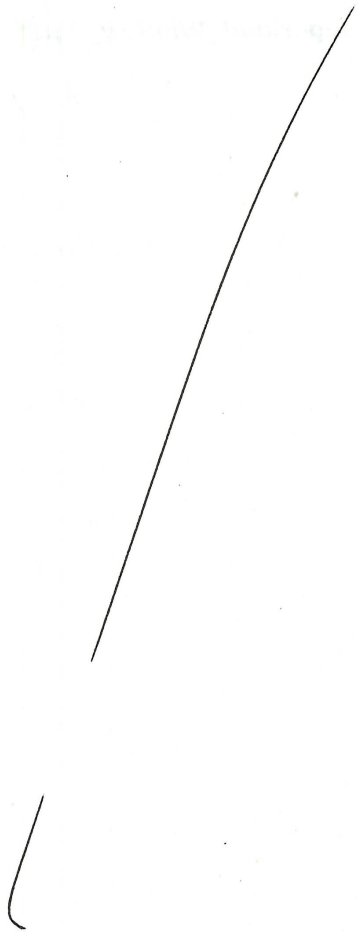
El valor de REG_DWORD deberá ser **2** en **HKEY_LOCAL_MACHINE / SYSTEM / CurrentControlSet / Control / LSA / RestrictAnonymous**.

Este folio es consecutivo en orden alfabético por empresa: 54793

Se anexan Línea base de seguridad Windows 7:

SASI-SEV-Li¦ünea_base_de_seguridad_Window_7.pdf

Este folio es consecutivo en orden alfabético por empresa: 54794



Este folio es consecutivo en orden alfabético por empresa: 54795