

# **Seguridad de los Sistemas Informáticos**

## **PARTE 1 – Seguridad en Windows.**

### **Práctica 3: Directorio Activo. Políticas de Grupo.**

## Objetivo General del tema

**Comprender** los distintos sistemas relacionados con la Seguridad que integran los sistemas operativos Windows, y **ser capaces** de configurarlos y usarlos dentro de la política de seguridad que la Empresa haya establecido.

# Objetivos específicos del tema

1. **Conocer y ser capaz de configurar y utilizar** de manera adecuada el sistema de ficheros NTFS para garantizar la **seguridad de la información** almacenada en el sistema.
2. **Conocer y ser capaz de configurar y utilizar** de manera adecuada el **Sistema de Ficheros Encriptado (EFS)**, para asegurar la confidencialidad de la información.
3. **Conocer y ser capaz de configurar y utilizar** de manera adecuada el **Directorio Activo** para gestionar de la mejor manera posible los activos del sistema.
4. **Conocer y ser capaz de configurar y utilizar** de manera adecuada las **políticas de grupo** para gestionar de la mejor manera posible la seguridad de los activos del sistema

# Políticas de grupo

- Las políticas de grupo son un **conjunto de configuraciones** de diversos aspectos del sistema y que se pueden aplicar a usuarios o a equipos.
- Permiten establecer multitud de opciones de configuración relacionadas con muy diversos conceptos (de **seguridad**, entre otros). Estas configuraciones podrán establecerse de manera muy flexible a distintos niveles
  - **Local a cada máquina** (Directiva de grupo local – Local Group Policy).
  - **De todos los objetos de un dominio AD** (Directiva del Dominio – Domain Policy).

## Plantillas de seguridad

- Otro concepto relacionado es el de las plantillas de seguridad. Permiten definir **conjuntos de ajustes** a valores de las propiedades de objetos del dominio.
- Las plantillas de seguridad **facilitan** la aplicación de las políticas de grupo, dado que contienen los valores a aplicar a distintas propiedades en **función de la utilidad** de la plantilla.

## Políticas de grupo

- Están **integradas** dentro de Directorio Activo, y permiten definir configuraciones para aplicar a múltiples usuarios y ordenadores.
- Las políticas de grupo se **despliegan automáticamente** por toda la empresa.
- Se guardan en **GPOs** (Group Policy Objects).
- Se pueden crear todas las que sean necesarias, y vincularlas a Usuarios, Sites, UO o dominios.

# Políticas de Grupo

- Las políticas de grupo se aplican cuando arranca un ordenador vinculado a uno de los elementos (dominio, UO, ...) a los que estén asociadas. Se aplicarán todas las GPOs asociadas, en este orden:
  1. **Políticas locales.**
  2. **Vinculadas al Site (parámetros de equipos, no de usuarios).**
  3. **Políticas del dominio.**
  4. **Políticas de la UO del ordenador/usuario.**
- Cada configuración sobrescribe, en general, a la anterior.
- Las políticas se aplicarán a usuarios o máquinas del ámbito donde estén definidas.
- Los cambios en las políticas no se aplican de inmediato (90'-120'), aunque puede reiniciarse la máquina o forzarse su aplicación (gpupdate [/force]).

# Políticas de Grupo

- Dado que la política de grupo que se va a aplicar a un determinado objeto es la “suma” de todas las que le afectan, es recomendable crear **varios GPOs con configuraciones relacionadas** (directivas de passwords, directivas de acceso a carpetas, programas no permitidos, etc).



# Políticas de Grupo: capacidades

- Las políticas de grupo permiten:
  - Controlar la seguridad IP.
  - Administrar el uso de encriptación de ficheros.
  - Restringir la ejecución de software.
  - Gestionar certificados.
  - Definir Derechos de usuarios.
  - Definir Auditorías.
  - Asignar Políticas de passwords
  - Controlar cambios en el registro.
  - Controlar la pertenencia a grupos locales.

# Plantillas de seguridad: capacidades

- Además de poder establecer manualmente cada uno de los elementos de seguridad de un sistema, pueden utilizarse *plantillas de seguridad*, que son **ficheros (de texto plano) que almacenan un conjunto de opciones de seguridad.**
- Las plantillas de seguridad, además de lo configurable a través de la interfaz de las políticas de grupo, permiten:
  - **Configurar permisos sobre ficheros.**
  - **Configuración del escritorio.**
  - **Acceso del usuario a distintas partes de Windows.**

# Plantillas de seguridad: funcionamiento

- Una plantilla de seguridad es un fichero **.INF** que contiene una configuración de seguridad. Pueden encontrarse las plantillas por defecto en C:\WINDOWS\security\templates (XP) C:\Windows\inf\defltbase.inf (W7, 2003, 2008...).
- Al ser simples ficheros de texto, es **sencillo distribuirlas** entre distintos ordenadores y compararlas con su configuración actual.
- Si se aplican varias, al igual que en las GPOs **la última sobrescribe a la primera**.
- En general, las **plantillas de seguridad** se utilizan para contener definiciones de seguridad **complejas**, mientras que las **GPO** se usan para definir cuestiones **sencillas**.

# Plantillas y políticas de seguridad

- Windows dispone de varias **plantillas predefinidas**, con la configuración de seguridad que se supone debe tener un tipo de entorno determinado (securews para estaciones de trabajo seguras, hisecws para estaciones de trabajo de alta seguridad, ...).
- Estas plantillas funcionarán sobre sistemas Windows XP o posteriores; hay que **evitar tener sistemas antiguos** en la empresa. (XP dejó de tener soporte en 2014/04)
- Hay que tener mucho cuidado al aplicar políticas y plantillas. Un mal uso puede dar lugar a:
  - **Dejar agujeros de seguridad.**
  - **Impedir el trabajo de usuarios o servicios legítimos.**

# Plantillas y políticas de seguridad

- Si creamos nuestras propias plantillas, es recomendable seguir el mismo criterio que las GPOs: **utilizar plantillas pequeñas dedicadas a aspectos concretos de seguridad:**
  - Es sencillo crear políticas de seguridad complejas aplicando un conjunto de plantillas simples.
  - Podemos reusar las plantillas, aplicando un subconjunto de ellas distinto en cada parte del sistema en función de las necesidades de cada uno.

# Plantillas y políticas de seguridad

- Microsoft proporciona de forma gratuita una herramienta que nos permite **configurar** fácilmente los equipos de nuestra empresa mediante el uso de GPO y el System Center Configuration Manager (SCCM). Es el **Microsoft Security Compliance Manager** (<https://technet.microsoft.com/es-es/library/cc677002.aspx>).
- Esta herramienta incluye políticas y DCM (para usar con el SCCM) por defecto basadas en las recomendaciones de Microsoft y en *best practices*. Estas plantillas se pueden utilizar tal y como vienen o ser adaptadas a nuestras necesidades para luego ser aplicadas a nuestro entorno.

# Plantillas y políticas de seguridad

Microsoft Security Compliance Manager

File View Help

Custom Baselines

- Microsoft Baselines
  - Exchange Server 2007 SP3
  - Exchange Server 2010 SP2
  - Internet Explorer 10
    - Attachments \ Guides
      - IE10 Computer Security Compliance 1.0**
      - IE10 User Security Compliance 1.0
    - Internet Explorer 8
    - Internet Explorer 9
    - Microsoft Office 2007 SP2
    - Microsoft Office 2010 SP1
  - Windows 7 SP1
    - Attachments \ Guides
      - Win7SP1 Extended DCM Checks 1.0
      - Win7SP1 Bitlocker Security 1.0
      - Win7SP1 Computer Security Compliance 1.0
      - Win7SP1 Domain Security Compliance 1.0
      - Win7SP1 User Security Compliance 1.0
    - Windows 8
    - Windows Server 2003 SP2
    - Windows Server 2008 R2 SP1
      - Attachments \ Guides
        - WS2008R2SP1 AD Certificate Services Server Security Compliance 1.0
        - WS2008R2SP1 DHCP Server Security Compliance 1.0
        - WS2008R2SP1 DNS Server Security Compliance 1.0
        - WS2008R2SP1 Domain Controller Security Compliance 1.1
        - WS2008R2SP1 Domain Security Compliance 1.0
        - WS2008R2SP1 File Server FCI 1.0
        - WS2008R2SP1 File Server Security Compliance 1.0
        - WS2008R2SP1 Hyper-V Security Compliance 1.0
        - WS2008R2SP1 Member Server Security Compliance 1.1
        - WS2008R2SP1 Network Access Services Server Security Compliance 1.0
        - WS2008R2SP1 Print Server Security Compliance 1.0
        - WS2008R2SP1 Remote Desktop Services Security Compliance 1.0
        - WS2008R2SP1 Web Server Security Compliance 1.0
      - Windows Server 2008 SP2
      - Windows Server 2012
      - Windows Vista SP2
      - Windows XP SP3
  - Other Baselines

Global setting search

**IE10 Computer Security Compliance 1.0** 147 unique setting(s)

Advanced View

Name	Default	Microsoft	Customized	Severity	Path
<b>Authentication Types</b> 3 Setting(s)					
Logon options	Prompt for user name and password	Enabled	Enabled	Important	Computer Configuration\Administrat
Turn on Basic feed authentication ov		Not Configured	Not Configured	Optional	Computer Configuration\Administrat
Logon options	Automatic logon only in Intranet zone	Enabled	Enabled	Important	Computer Configuration\Administrat
<b>Certificate Management</b> 3 Setting(s)					
Check for server certificate revocatio	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Prevent ignoring certificate errors	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Turn on certificate address mismatch		Enabled	Enabled	Critical	Computer Configuration\Administrat
<b>Key Management</b> 1 Setting(s)					
Turn off Encryption Support	Disabled	Not Configured	Not Configured	Critical	Computer Configuration\Administrat
<b>Least Functionality</b> 124 Setting(s)					
Allow drag and drop or copy and pa	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Download signed ActiveX controls	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Make proxy settings per-machine (ra		Not Configured	Not Configured	Optional	Computer Configuration\Administrat
Allow script-initiated windows witho	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Allow only approved domains to use		Enabled	Enabled	Important	Computer Configuration\Administrat
Allow META REFRESH	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Script ActiveX controls marked safe f	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Logon options	Prompt for user name and password	Enabled	Enabled	Important	Computer Configuration\Administrat
Allow cut, copy or paste operations f	Enabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Prevent changing the URL for checki		Not Configured	Not Configured	Optional	Computer Configuration\Administrat
Allow active scripting	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Java permissions		Enabled	Enabled	Critical	Computer Configuration\Administrat
Java permissions	High Safety	Enabled	Enabled	Critical	Computer Configuration\Administrat
Turn on Protected Mode		Enabled	Enabled	Important	Computer Configuration\Administrat
Access data sources across domains	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Initialize and script ActiveX controls r	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Turn on SmartScreen Filter scan		Enabled	Enabled	Critical	Computer Configuration\Administrat
Turn on SmartScreen Filter scan		Enabled	Enabled	Critical	Computer Configuration\Administrat
Allow updates to status bar via script		Enabled	Enabled	Important	Computer Configuration\Administrat
Run .NET Framework-reliant compon	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Allow cut, copy or paste operations f	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat
Java permissions		Enabled	Enabled	Critical	Computer Configuration\Administrat
Turn on Protected Mode		Enabled	Enabled	Important	Computer Configuration\Administrat
Do not allow ActiveX controls to run		Enabled	Enabled	Optional	Computer Configuration\Administrat
Prevent specifying the update check		Enabled	Enabled	Important	Computer Configuration\Administrat
Userdata persistence		Enabled	Enabled	Important	Computer Configuration\Administrat
Intranet Sites: Include all network pat	Not configured.	Disabled	Disabled	Important	Computer Configuration\Administrat

**Import**

- GPO Backup (folder)
- SCM (.cab)

**Export**

- Excel (.xlsm)
- GPO Backup (folder)
- SCAP v1.0 (.cab)
- SCCM DCM 2007 (.cab)
- SCM (.cab)

**Baseline**

- Compare / Merge
- Delete
- Duplicate
- Properties

**Setting**

**Setting Group**

**Help**

- About
- Help Topics
- Release Notes
- Send Feedback
- Privacy Statement

# Plantillas y políticas de seguridad

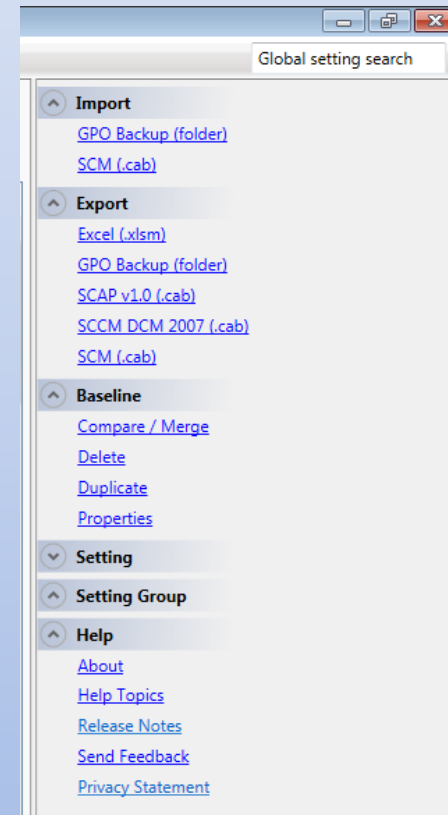
The screenshot displays the Microsoft Security Compliance Manager interface. The left pane shows a tree view of various baselines, with 'IE10 Computer Security Compliance 1.0' selected. The main pane shows the configuration for this policy, which has 147 unique settings. The 'Advanced View' is active, showing a table of settings. The 'Authentication Types' section is expanded, showing 'Logon options' set to 'Prompt for user name and password', 'Enabled', and 'Severity: Important'. The 'Setting Details' section provides a description, vulnerability, potential impact, and countermeasure for the 'Logon options' setting. The right pane shows a sidebar with links for Import, Export, Baseline, Setting, Setting Group, and Help.

Name	Default	Microsoft	Customized	Severity	Path
<b>Authentication Types 3 Setting(s)</b>					
Logon options	Prompt for user name and password	Enabled	Enabled	Important	Import: Computer Configuration\Administrat
<p><b>Setting Details</b></p> <p><b>UI Path:</b> Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone</p> <p><b>Description:</b> This policy setting allows you to manage settings for logon options. If you enable this policy setting, you can choose from the following logon options: Anonymous logon disables HTTP authentication and uses the guest account only for the Common Internet File System (CIFS) protocol. Prompt for user name and password queries users for user IDs and passwords. After a user is queried, these values can be used silently for the remainder of the session. Automatic logon only in Intranet zone queries users for user IDs and passwords in other zones. After a user is queried, these values can be used silently for the remainder of the session. Automatic logon with current user name and password attempts logon using Windows NT Challenge Response (also known as NTLM authentication). If Windows NT Challenge Response is supported by the server, the logon uses the user's network user name and password for logon. If Windows NT Challenge Response is not supported by the server, the user is queried to provide the user name and password. If you disable this policy setting, logon is set to Automatic logon only in Intranet zone. If you do not configure this policy setting, logon is set to Automatic logon only in Intranet zone.</p> <p><b>Vulnerability:</b> Users could submit credentials to servers operated by malicious people who could then attempt to connect to legitimate servers with those captured credentials.</p> <p><b>Potential Impact:</b> Anonymous logon disables HTTP authentication and uses the guest account, which means that users will be unable to connect to sites in this security zone that require authentication.</p> <p><b>Countermeasure:</b> The most secure option is to configure this setting to Enabled: Anonymous logon, this will prevent users from submitting credentials to servers in this security zone.</p> <p><b>Additional Details:</b> Logon options CCE-20947-8  Logon options No CCE-ID 5.0 is assigned. HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1A00 REG_DWORD:196608</p>					
Turn on Basic feed authentication ov	Automatic logon only in Intranet zone	Not Configured	Not Configured	Optional	Computer Configuration\Administrat
Logon options	Automatic logon only in Intranet zone	Enabled	Enabled	Important	Computer Configuration\Administrat
<b>Certificate Management 3 Setting(s)</b>					
Check for server certificate revocation	Disabled	Enabled	Enabled	Important	Computer Configuration\Administrat



# Plantillas y políticas de seguridad

- Nos permite importar políticas de grupo o plantillas SCM
- Exportar en diversos formatos: GPO que podemos importar en el AD, DCM (Desired Configuration Management) que se pueden utilizar en el SCCM
- El SCCM (System Center Configuration Manager) puede cargar un DCM y comprobar que todos los equipos del entorno cumplen la configuración de la plantilla.



## Cambios en la política de passwords

- Se gestiona a nivel de dominio. No admite cambios a otros niveles.
- Para modificarla, hay que modificar la Directiva de Seguridad del Dominio
  - Inicio – Herramientas Administrativas – Directiva de seguridad del dominio/Administración de Directivas de grupo
    - Default Domain Policy – botón derecho – Editar
    - Configuración de Equipo – Directivas – Windows – Seguridad – Cuenta -Contraseñas

## Cambios en el Control de escritorio

Se puede aplicar al Dominio, o a una UO.

- Para modificarla, podemos crear una nueva directiva en el objeto eligiéndola
  - Objetos de Directiva de Grupo – Nuevo - Configuración de usuario – Plantillas Administrativas – Menú Inicio y barra de tareas.
  - Hay muchas opciones a elegir. Para acciones relativas al escritorio, hay que habilitar el Active Desktop.
- Hacer los cambios que se desee y guardar la política.

## Configuración de auditoría

Las opciones de auditoría permiten monitorizar los eventos que ocurren en los equipos. Así, se deja constancia de todo lo que ocurre y puede utilizarse como base para investigar incidentes e incluso como evidencias en procesos legales.

- Para ello, se puede definir una política al nivel que se desee, editando las opciones de la Directiva de Auditoría (Configuración de Windows – Configuración de seguridad – Directivas locales – Directiva de Auditoría)
- En Registro de sucesos se pueden definir cuestiones relativas a éste (el tamaño máximo, por ejemplo).
- Al registro se accede con el “Visor de Sucesos”, del panel de control.

## Cambios en la configuración de Servidor de Dominio

- Dada la importancia de esta máquina en el sistema puede llevarse a cabo la definición de una política específica para esta máquina. Default Domain Controllers Policy
- Para ello, en Herramientas administrativas existe el programa Asistente para Configuración de Seguridad que nos permite crear una directiva de seguridad que podemos aplicar en una GPO
- Ahí podemos configurar esta máquina independientemente del resto.

## Utilización de plantillas de seguridad

- Para aplicar una plantilla de seguridad, sólo hay que importarla en una GPO determinada.
- En el editor de la GPO, Configuración del equipo – Configuración de Windows – Configuración de Seguridad – Click Derecho – Propiedades – Importar directiva
- Podemos elegir la que queramos de las almacenadas en el sistema (predefinida o creada por nosotros).
- Una vez importada, pueden verse los parámetros que ha establecido.

## Creación de plantillas de seguridad

- La creación de una plantilla sin una herramienta adecuada puede ser complicado.
- Afortunadamente, Windows incluye una: SCA (Security Configuration and Analysis – *Configuración y Análisis de seguridad*), que permite analizar la seguridad y configurar nuestras propias plantillas.
- Para ejecutarla, hay que agregarla como complemento al programa mmc (Microsoft Management Console), ejecutable desde la línea de órdenes.

## Creación de plantillas de seguridad (II)

- Una vez ejecutada, hay que crear una base de datos para guardar la configuración que iremos creando.
- En principio hay que importar una plantilla, aunque podemos modificar lo que queramos.



## Creación de plantillas de seguridad (III)

- Una vez importada hay que aplicarla al equipo.
- Podemos también configurar el equipo. Esto hará que se apliquen todas las políticas correspondientes al equipo.
- Así revisaremos cada entrada que nos interese, pudiendo modificar lo que consideremos oportuno. Es importante después de las modificaciones volver a analizar el equipo, para verificar que la modificación realizada tendrá efecto.
- Posteriormente podremos exportar la plantilla y llevarla al servidor para aplicarla en el entorno que nos interese.
- Todo este proceso se llevaría a cabo en un “cliente limpio”