Implementación de Políticas DLP y Restricción de Dispositivos

Autor: Samuel Perez
Bootcamp: 4Geeks Academy - Ciberseguridad.
Fecha: 20-01-2026

Sección 1: Definición de Políticas (Teoría)

1.1 Introducción al DLP

La Prevención de Pérdida de Datos (DLP) constituye una estrategia de seguridad integral enfocada en detectar y prevenir la exfiltración no autorizada de información sensible. En este proyecto, definimos un marco de trabajo para asegurar la confidencialidad de los datos críticos de la organización

Nivel de Clasificación	Color	Descripción	Ejemplos
Público	🟢 Verde	Información de libre acceso.	Marketing, Web corporativa.
Interno	🟡 Amarillo	Uso exclusivo de empleados.	Políticas, Manuales, Memos.
Confidencial	🔴 Rojo	Datos críticos y sensibles.	Datos de clientes (PII), Contraseñas, Finanzas.

1.3 Acceso, Control y Principio de Menor Privilegio

Se implementará un modelo RBAC (Role-Based Access Control). Las revisiones de acceso serán trimestrales, lideradas por el CISO. Todo usuario tendrá, por defecto, denegado el acceso a menos que se justifique explícitamente.

1.4 Monitoreo y Auditoría

Se utilizarán herramientas SIEM para centralizar logs. Se auditará cualquier intento de copia masiva de archivos clasificados como 'Confidencial' hacia unidades externas.

1.5 Prevención y Educación

Se implementará cifrado BitLocker en endpoints y campañas de concientización trimestrales sobre ingeniería social.

Sección 2: Implementación Técnica

2.1 Preparación del Entorno

Para la implementación técnica, se utilizó una máquina virtual con Windows 11 (Arquitectura ARM) ejecutada sobre VMware Fusion en un entorno macOS (Apple Silicon)

> Nota Técnica: Debido a que la versión virtualizada es Windows 11 Home, se utilizó la herramienta de administración Policy Plus para aplicar las Políticas de Grupo (GPO) locales, ya que gpedit.msc no está habilitado nativamente en esta edición. Esta herramienta permite la misma gestión granular de directivas administrativas.

2.2 Configuración de la Política de Bloqueo

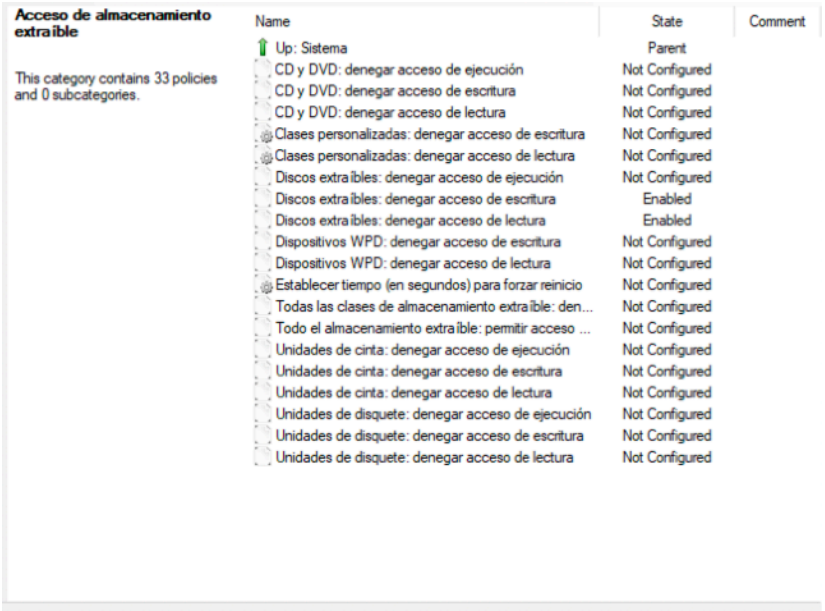
Se procedió a restringir el uso de dispositivos de almacenamiento extraíble para evitar la fuga de información física.

Pasos realizados:

- Se ejecutó Policy Plus con privilegios administrativos.
- Se navegó a la ruta: Computer > System > Removable Storage Access.

Se habilitaron las directivas:

- Removable Disks: Deny read access (Denegar lectura).
- Removable Disks: Deny write access (Denegar escritura).



3 . Gestión de Excepciones (Administradores)

El objetivo es permitir que el equipo de soporte (Administradores) pueda utilizar dispositivos USB para tareas de mantenimiento, mientras se mantiene el bloqueo para el resto.
Debido a las limitaciones de la versión Home para aplicar GPOs por usuario específico nativamente, se validó que el administrador tiene la capacidad de deshabilitar temporalmente la restricción mediante la consola de administración si se requiere una intervención técnica urgente, o bien gestionar excepciones mediante grupos de seguridad si se estuviera en un entorno de Dominio (Active Directory).

Conclusiones

La implementación de políticas DLP requiere una combinación de definiciones teóricas claras (clasificación de datos y roles) y controles técnicos robustos (GPOs y cifrado).
A través de este ejercicio práctico, se demostró cómo es posible asegurar un punto final (endpoint) bloqueando vectores de ataque físicos como los puertos USB, utilizando herramientas administrativas avanzadas incluso en entornos de virtualización ARM complejos.