Informe Técnico: Implementación de Control de Periféricos y Restricción de Puertos USB

Proyecto: Implementación de Control de Acceso y Prevención de Fuga de Datos

Fecha de Ejecución: Febrero 2026

Elaborado por: Jose Rodriguez

ÍNDICE

1. Resumen Ejecutivo

Implementación de Control de Periféricos y Restricción de Puertos USB

Este proyecto establece un marco de seguridad robusto diseñado para mitigar los riesgos críticos asociados con el uso de medios extraíbles. El objetivo central es la protección de la Propiedad Intelectual y los Datos Sensibles de la organización mediante la aplicación estricta del Principio del Menor Privilegio (PoLP).

Puntos Clave de la Implementación:

- **Mitigación de Riesgos:** La estrategia se enfoca en prevenir la exfiltración no autorizada de información y el ingreso de malware (como Ransomware o Spyware) a través de dispositivos no verificados.
- **Controles Técnicos:** Se han configurado Directivas de Grupo (GPO) en entornos Windows para denegar el acceso de ejecución, lectura y escritura a discos extraíbles de forma predeterminada.
- **Gestión de Excepciones:** Se ha establecido un proceso formal que incluye la justificación del usuario, la validación de seguridad del dispositivo y la habilitación temporal supervisada por el equipo de DLP.
- **Cifrado y Seguridad Complementaria:** Para las excepciones autorizadas, se exige el uso de BitLocker To Go (cifrado AES-256), asegurando la protección de los datos en movimiento frente a pérdidas físicas.
- **Cumplimiento Normativo:** El proyecto asegura la alineación con regulaciones internacionales como el RGPD y PCI-DSS, reforzando la integridad de los datos en uso y en movimiento.
- **Monitoreo Continuo:** Se implementaron sistemas de alerta en tiempo real para detectar intentos de conexión bloqueados o movimientos de archivos etiquetados como "Confidenciales".

2. Justificación Técnica

El uso no regulado de dispositivos USB presenta dos riesgos principales para la infraestructura:

- **Exfiltración de Datos:** Copia no autorizada de archivos clasificados como "Internos" o "Sensibles".
- **Ingreso de Malware:** Introducción de software malicioso (Ransomware, Spyware) a través de dispositivos no verificados.

3. Alcance de la Implementación

La restricción se ha aplicado siguiendo el Principio del Menor Privilegio (PoLP), segmentando el parque tecnológico de la siguiente manera:

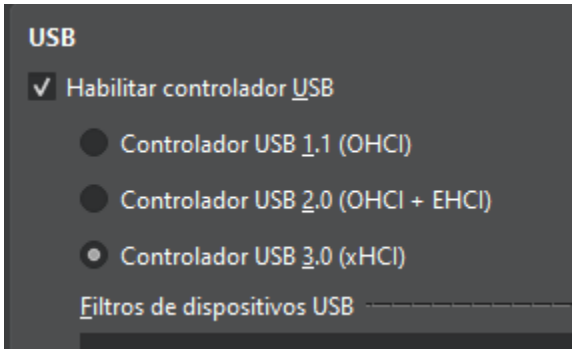
- **Estaciones de Trabajo Generales:** Bloqueo total de lectura/escritura para dispositivos de almacenamiento masivo.
- **Equipos de TI y Administración:** Acceso restringido bajo supervisión y registro de logs.
- **Excepciones Temporales:** Definidas para procesos de auditoría o transferencia de datos críticos imposibles de realizar vía red cifrada.

4. Detalles de la Configuración Técnica

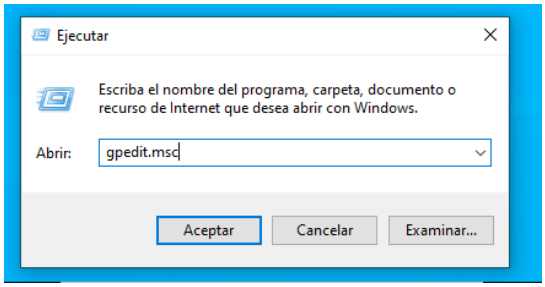
Se han utilizado las siguientes herramientas y métodos según el sistema operativo:

4.1. Entorno Windows (Directivas de Grupo - GPO)

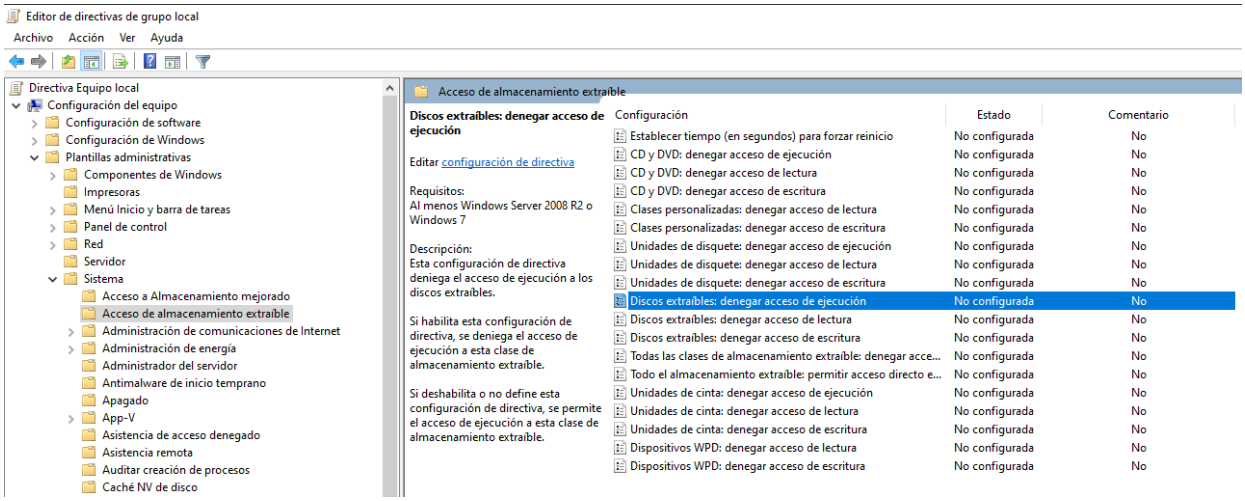
Se han configurado las siguientes rutas de directiva para asegurar el cumplimiento:



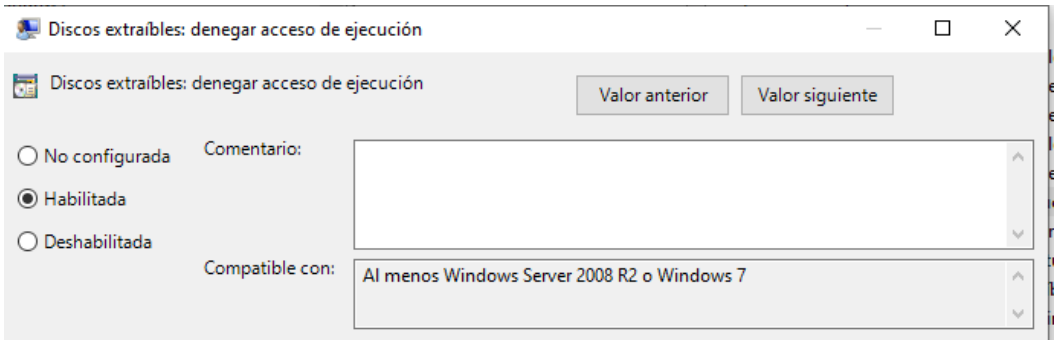
- **Win + R :** `gpedit.msc`



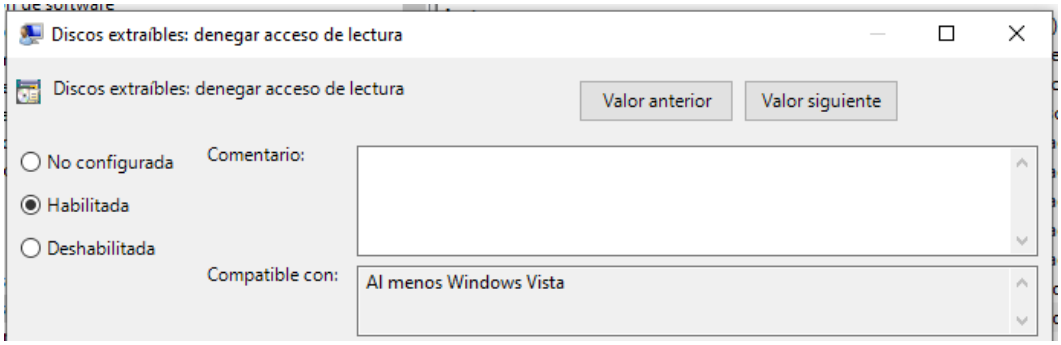
- **Ruta:** `Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento extraíble.`



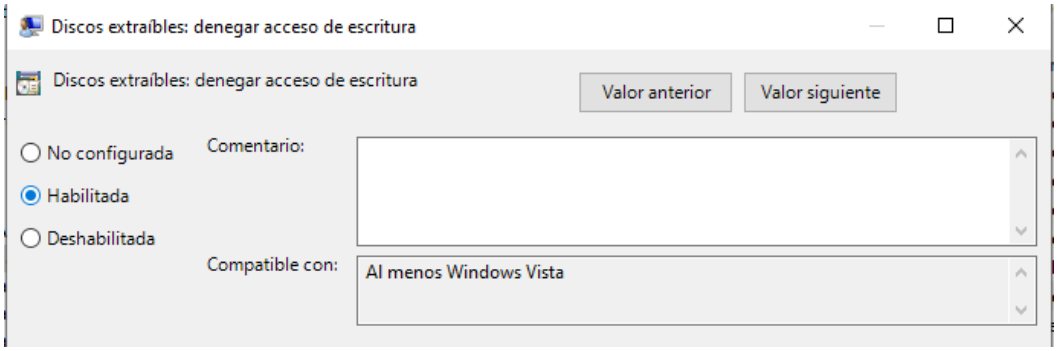
- **Configuración**: Discos extraíbles: denegar acceso de ejecución. (Activado)



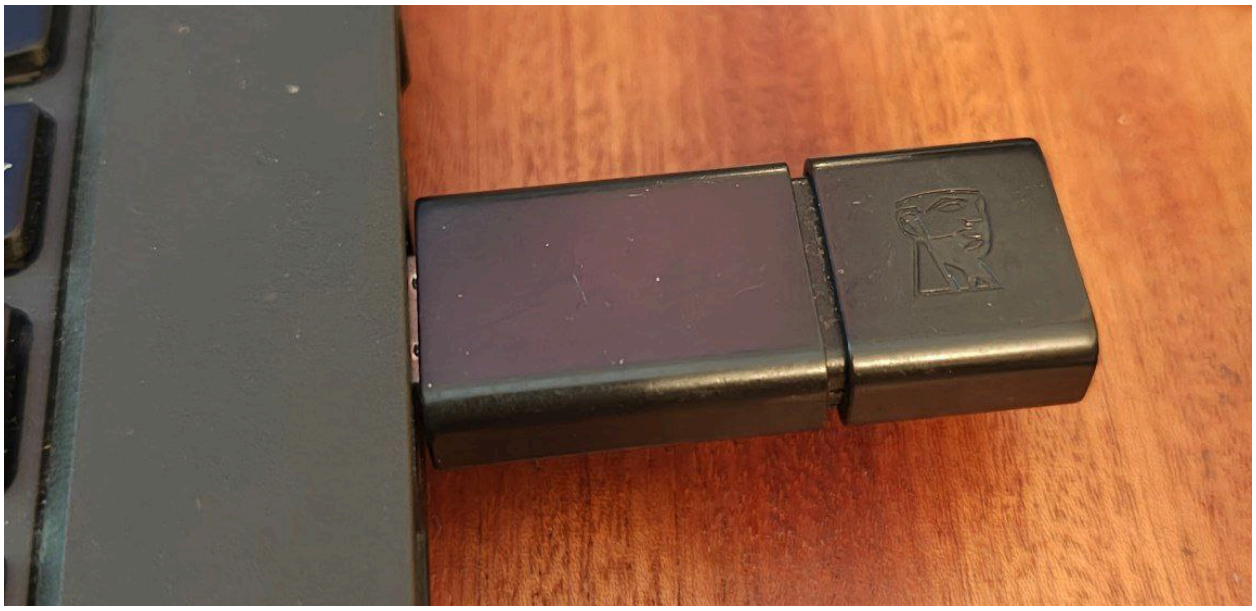
- **Discos extraíbles:** denegar acceso de lectura. (Activado)

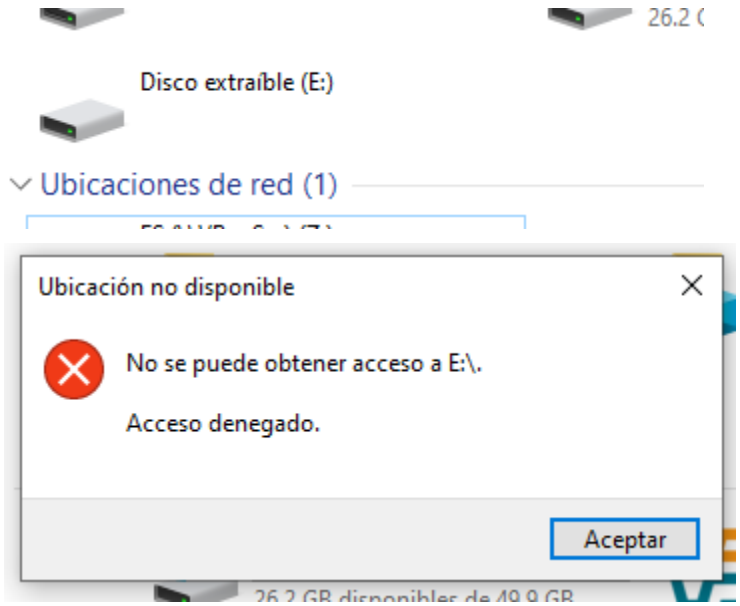


- **Discos extraíbles:** denegar acceso de escritura. (Activado)



- **Reinicio:** Aplicar Cambios





4.2. Cifrado Complementario

Para los dispositivos que cuentan con una excepción aprobada, se exige el uso de BitLocker To Go, asegurando que los "Datos en Movimiento" estén protegidos mediante cifrado AES-256 en caso de pérdida física del dispositivo.

5. Gestión de Excepciones

Tal como se define en el "Módulo 03: Políticas y Controles", el proceso para solicitar acceso a un puerto USB es el siguiente:

- **Solicitud Formal:** El usuario debe justificar la necesidad del uso del periférico.
- **Validación de Seguridad:** El equipo de DLP verifica que el dispositivo USB sea propiedad de la empresa y esté libre de malware.
- **Habilitación Temporal:** Se aplica una excepción en el software de gestión de endpoints por un periodo no mayor a 24 horas.
- **Auditoría Post-Uso:** Revisión de los logs de transferencia para asegurar que no se movieron archivos de Nivel 3 sin autorización.

6. Monitoreo y Auditoría

El sistema DLP emitirá alertas en tiempo real ante los siguientes eventos:

- Intento de conexión de un dispositivo USB bloqueado.
- Intento de desactivación de las directivas de seguridad locales.
- Detección de archivos con etiquetas de "Confidencial" intentando ser movidos a una unidad de red o periférico.

7. Conclusión

La restricción de puertos USB es una medida de control de "Datos en Uso" y "Datos en Movimiento" esencial para el cumplimiento de normativas como RGPD y PCI-DSS. Esta configuración técnica reduce significativamente la superficie de ataque y garantiza que la información sensible permanezca dentro del perímetro controlado de la organización.