# Implementación de Políticas de Seguridad DLP en Dispositivos USB

Entrega: Clasificación de datos, políticas, implementación y validación

Fecha: 20/09/2025

Alumno: Daniel José Javier Ramírez

## Índice



## 1) Clasificación de Datos

Antes de proteger, hay que entender qué protegemos. La clasificación sirve para asignar esfuerzos según el impacto de una filtración. Aquí defino criterios y ejemplos para tres niveles de sensibilidad.

Criterios que uso para clasificar:

- Impacto legal y normativo (multas, incumplimientos).

- Impacto económico (pérdidas directas, fraude, sanciones).

- Impacto reputacional (pérdida de confianza de clientes/empleados).

- Impacto operacional (interrupciones del servicio o del trabajo diario).

| Categoría | Ejemplos ampliados | Por qué está aquí | Controles típicos |
|---|---|---|---|
| Públicos | Comunicados oficiales, notas de prensa, manuales de usuario publicados, guías de marketing ya publicadas. | Su exposición no causa daño significativo. | Sin restricciones especiales; control de versiones. |
| Sensibles | Nóminas, listados de clientes, tickets de soporte con PII, reportes financieros internos, contratos en negociación. | Pueden afectar reputación y generar reclamaciones si se exponen. | Acceso por rol, cifrado en tránsito, retención definida, DLP con aviso. |
| Críticos/Confidenciales | Credenciales, llaves API, secretos de I+D, código propietario, planes estratégicos, información de salud. | Su fuga puede causar fraude, sanciones o pérdidas mayores. | MFA obligatorio, cifrado en reposo, gestor de secretos, DLP con bloqueo, retención mínima. |

Nota sobre retención: cuanto más sensible el dato, más corta debe ser su retención y más controlado su borrado.

## 2) Políticas de Seguridad DLP

El objetivo de DLP es evitar que datos sensibles salgan por canales no autorizados o sin control. Aquí distingo entre políticas preventivas (bloquean) y detectivas (avisan) y explico cómo se comunican y revisan.

Tipos de políticas:

- Preventivas: bloquean movimientos prohibidos (p.ej., copiar datos críticos a USB).

- Detectivas: avisan y registran, pero no impiden la acción (p.ej., exportar datos sensibles del CRM).

Gobernanza y revisión:

- Revisión semestral de reglas, con responsables de RR.HH., Finanzas, I+D y Seguridad.

- Registro de excepciones justificadas (quién, por qué y por cuánto tiempo).

- Comunicación a usuarios mediante política interna y formación breve anual.

Ejemplos prácticos de aplicación de DLP:

- Correo: alerta o bloqueo de adjuntos con PII real (según nivel).

- Nube: impedir descargar carpetas marcadas como críticas a dispositivos no gestionados.

- Impresoras: avisar o bloquear impresión de documentos marcados como confidenciales.

- USB: denegar lectura/escritura/ejecución para usuarios estándar.

| Canal | Sensibles | Críticos/Confidenciales |
|---|---|---|
| Correo | Aviso y registro | Bloqueo o aprobación previa |
| Nube/Descargas | Aviso si no gestionado | Bloqueo si no gestionado |
| Impresión | Aviso | Bloqueo/seguimiento |
| USB | Aviso o bloqueo | Bloqueo por defecto |

Documentación de políticas: cada regla debe tener una ficha con propósito, alcance, responsables, fecha de vigencia, excepciones posibles y cómo se mide su cumplimiento.

## 3) Implementación Técnica (Restricción de Dispositivos USB)

Se eligió el control por Políticas de Grupo de Windows dentro de una máquina virtual en VirtualBox. Añado notas para evitar errores comunes y cómo revertir cambios.

VirtualBox (notas ampliadas):

- Instalar Extension Pack compatible con la versión de VirtualBox.

- En Puertos USB, seleccionar la versión adecuada (2.0 suele ser suficiente; 3.0 si el host y el dispositivo lo soportan).

- Si el USB no aparece en la VM, comprobar que el host no lo está usando (quitarlo del explorador del host y reconectar).

Windows (Políticas de Grupo):

Ruta: Plantillas Administrativas > Sistema > Acceso de almacenamiento extraíble.

Políticas a habilitar:

- Discos extraíbles: denegar acceso de lectura (evita abrir archivos).

- Discos extraíbles: denegar acceso de escritura (evita copiar/guardar archivos).

- Discos extraíbles: denegar acceso de ejecución (evita ejecutar .exe desde USB).

Aplicación y verificación:

- Ejecutar gpupdate /force para aplicar de inmediato.

- Reiniciar si no se ven los cambios.

Reversión o excepciones:

- Para revertir, colocar las políticas en 'No configurada' y ejecutar gpupdate /force.

- Para excepciones, se puede aplicar la política en 'Usuarios estándar' y dejar fuera grupos específicos (personal de IT).

Errores comunes y solución:

- El USB se monta en el host, no en la VM: reasignarlo en el menú de dispositivos de VirtualBox.

- Se aplican políticas pero el usuario aún puede leer: verificar que es cuenta estándar y que la política está en el ámbito correcto.

- El puerto USB del equipo es 3.0 pero la VM está en 2.0: cambiar el controlador a 3.0 si es compatible.

## 4) Validación y Pruebas

La validación demuestra que las políticas hacen lo que esperamos. Defino escenarios y cómo documentarlos.

Escenarios de prueba sugeridos:

- Lectura: abrir un PDF o imagen desde el USB (debería fallar).
- Escritura: intentar copiar un archivo de escritorio al USB (debería fallar).
- Ejecución: intentar ejecutar un instalador .exe desde el USB (debería fallar).
- Usuario estándar: confirmar que no tiene acceso; Usuario administrador: confirmar que puede cambiar políticas.

Cómo documentar las pruebas:

- Capturar pantalla del mensaje de error y anotar fecha/hora.
- Registrar el usuario con el que se probó y qué política bloqueó la acción.
- Guardar un pequeño informe con los resultados (aprobado/no aprobado).

Limitaciones y rutas alternativas:

- Aunque el USB esté bloqueado, un usuario puede intentar usar la nube o correo. Por eso DLP debe cubrir varios canales.
- Si se necesita operar con USB, usar dispositivos corporativos cifrados y autorizados.

## 5) Consejos

- No depender solo de una medida. Combinar bloqueo de USB con DLP en correo/nube e inventario de datos.
- Usar USB corporativos cifrados cuando sea imprescindible mover información.
- Formar a los usuarios con ejemplos reales de incidentes para que entiendan el porqué de las políticas.
- Realizar auditorías periódicas y ajustar políticas según resultados y nuevas necesidades.
- Mantener un registro de excepciones y revisarlas con fecha de caducidad.

## 6) Conclusión

Con este ejercicio comprobé que clasificar datos ayuda a priorizar controles y que el bloqueo de USB es una medida efectiva para reducir fugas comunes. Aun así, la protección real se logra cuando se combinan controles técnicos con hábitos de usuario y una revisión constante de las políticas. El resultado es un entorno más seguro sin detener el trabajo diario.