Parte 1: Creación de Políticas de Seguridad DLP

1. Introducción al Data Loss Prevention (DLP)

La Prevención de Pérdida de Datos (DLP) es una estrategia de ciberseguridad que utiliza un conjunto de herramientas y procesos para asegurar que la información sensible no se filtre, se pierda o sea mal utilizada por entidades no autorizadas. Su objetivo es monitorear, detectar y bloquear el movimiento de datos confidenciales a través de la red de la organización, ya sea de forma accidental o intencionada.

La implementación de políticas DLP es fundamental para la salud y la reputación de cualquier organización. No solo ayuda a proteger la propiedad intelectual y los secretos comerciales, sino que también garantiza el cumplimiento de regulaciones como GDPR o HIPAA. Un programa DLP robusto fortalece la confianza de los clientes y minimiza el impacto financiero y reputacional que podría derivarse de una filtración de datos.

2. Clasificación de Datos

Para aplicar las políticas de DLP de manera efectiva, la organización clasificará la información en tres categorías según su sensibilidad:

- **Datos Públicos:** Información que no conlleva riesgo si se divulga al público. Esta categoría incluye comunicados de prensa, material de marketing, artículos de blog o información de contacto general de la empresa.
- **Datos Internos:** Información destinada únicamente al personal de la organización. Su divulgación podría causar una molestia o un daño menor, pero no una pérdida crítica. Ejemplos incluyen manuales de procedimientos internos, políticas de RRHH, memos de reuniones y organigramas.
- **Datos Sensibles:** Información altamente confidencial cuya pérdida o divulgación causaría un daño grave a la organización, a sus clientes o a sus socios. Esta categoría requiere la máxima protección. Incluye información de identificación personal (PII) de clientes y empleados, secretos comerciales, datos financieros de la empresa, códigos fuente y planes de proyectos estratégicos.

3. Acceso y Control (Principio del Menor Privilegio)

El **principio del menor privilegio** es la base de nuestro control de acceso. Este principio establece que a cada empleado solo se le debe otorgar el acceso mínimo indispensable para realizar sus tareas laborales. Para ello, se implementará el siguiente flujo de revisión de permisos:

1. **Solicitud:** Un empleado que necesite acceso a datos sensibles debe enviar una solicitud formal a su supervisor directo, justificando la necesidad para su rol.
2. **Aprobación:** El supervisor y el "propietario" de los datos (la persona responsable de esa información) revisarán y aprobarán la solicitud si se considera legítima.
3. **Implementación:** El equipo de TI/Seguridad de la Información otorgará el acceso, documentando la aprobación para futuras auditorías.
4. **Revisión Periódica:** Los permisos de acceso se revisarán semestralmente o cuando el rol de un empleado cambie.

4. Monitoreo y Auditoría

Para asegurar el cumplimiento de las políticas DLP, la organización implementará medidas de monitoreo continuo y auditoría. Se monitorearán actividades relacionadas con el acceso, la modificación y la transferencia de datos sensibles.

- **Herramientas:** Se utilizarán herramientas **SIEM (Security Information and Event Management)** para recolectar y analizar registros de eventos de toda la red, identificando comportamientos inusuales. Las soluciones **DLP específicas** se encargarán de inspeccionar el contenido de los datos y de aplicar las políticas de protección en tiempo real, alertando o bloqueando acciones prohibidas.

5. Prevención de Filtraciones

Se utilizarán tecnologías de DLP para prevenir la pérdida de datos de forma proactiva:

- **Cifrado de Datos:** Se cifrará la información tanto en tránsito (cuando se mueve por la red) como en reposo (cuando está almacenada en discos duros, bases de datos y dispositivos portátiles). Esto asegura que los datos permanezcan ilegibles para personas no autorizadas.
- **Tecnologías DLP:** Las herramientas de DLP se configurarán para:
    - Bloquear el envío de correos electrónicos con archivos adjuntos que contengan datos sensibles a destinatarios externos no autorizados.
    - Impedir que se copien archivos clasificados como sensibles a dispositivos de almacenamiento removibles, como unidades USB.
    - Restringir la carga de datos confidenciales a servicios en la nube no aprobados por la organización.

6. Educación y Concienciación

El elemento humano es la línea de defensa más importante. Todos los empleados de la organización recibirán una capacitación obligatoria sobre las políticas de seguridad y los riesgos asociados.

- **Contenido de la Capacitación:** Se enseñará a los empleados a identificar datos sensibles, manejar la información de forma segura, reconocer ataques de ingeniería social y cómo reportar un incidente de seguridad de inmediato.
- **Periodicidad:** Esta capacitación será obligatoria para todos los nuevos empleados y se repetirá de forma anual para todo el personal.

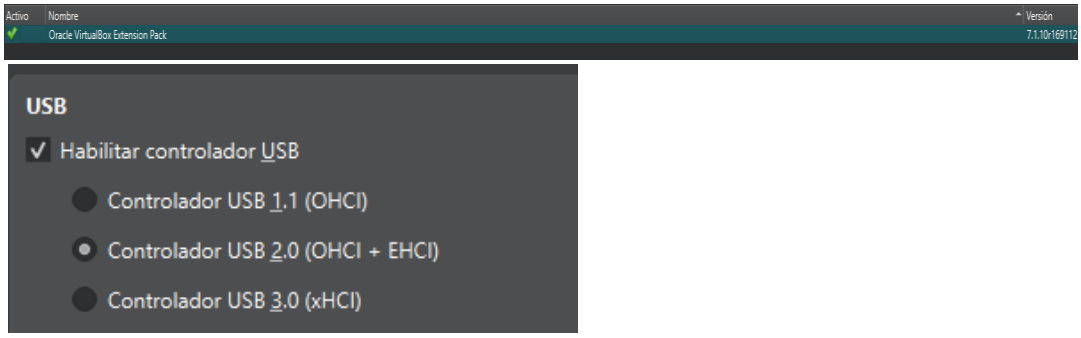
Parte 2: Implementación de Políticas de Restricción de Dispositivos USB

A continuación, se documenta el proceso de implementación de políticas de seguridad para la restricción de dispositivos USB, con el fin de prevenir la pérdida de datos.

1. Preparación de la Máquina Virtual (VM)

Se realizaron los siguientes pasos para asegurar que la máquina virtual pudiera acceder a los dispositivos USB del host.

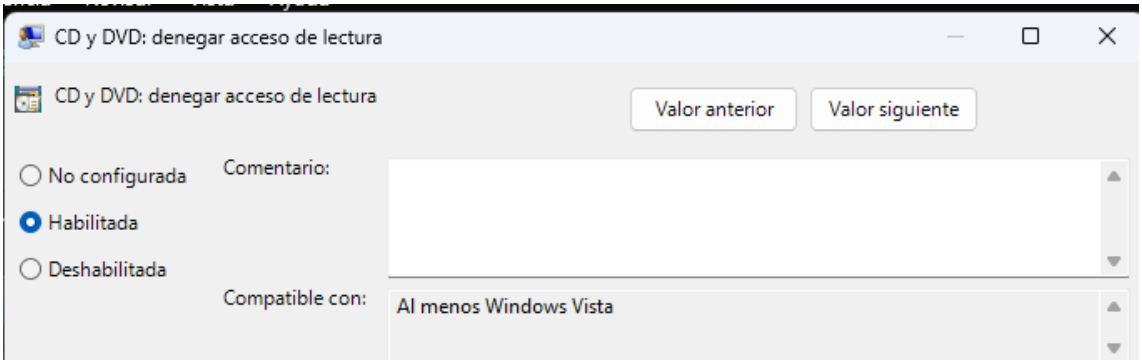
- **Instalación del VirtualBox Extension Pack**: Se descargó e instaló el **Extension Pack** para la versión de VirtualBox utilizada, habilitando el soporte para USB 2.0 y 3.0.
- **Habilitación del Soporte USB en la VM**: En la configuración de la VM, se activó el controlador USB 2.0. A continuación se adjunta una captura de pantalla que lo demuestra.

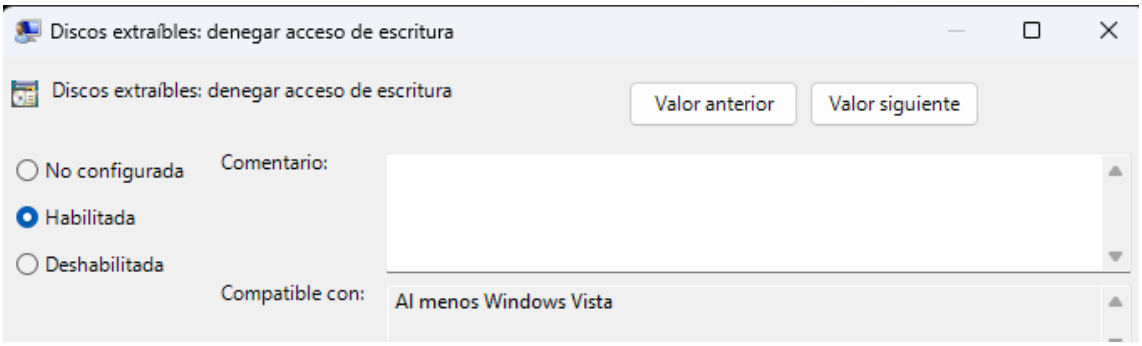


2. Aplicación de las Políticas de Restricción

Se utilizaron las Políticas de Grupo de Windows para aplicar las restricciones de acceso a dispositivos USB.

- **Acceso al Editor de Políticas de Grupo**: Se abrió el Editor de Políticas de Grupo (gpedit.msc).
- **Configuración de las Políticas**: Se navegó a **Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento removible**. Las políticas **"Discos extraíbles: denegar acceso de lectura"** y **"Discos extraíbles: denegar acceso de escritura"** se configuraron como **"Habilitado"**.





3. Validación y Pruebas

Se realizaron pruebas para verificar que las políticas de restricción de USB funcionaban correctamente.

- **Creación de un Usuario Regular**: Se creó una cuenta de usuario estándar sin privilegios de administrador.
- **Prueba de Acceso Denegado**: Se inició sesión con el usuario regular y se intentó acceder a un dispositivo USB. La acción fue bloqueada por el sistema.

4. Habilitación de Excepciones para Usuarios Específicos

Se investigó y se implementó un método para permitir que un usuario específico, con privilegios de administrador, pudiera tener acceso al USB, mientras que el resto de usuarios permanecieran con la restricción. Se utilizó el filtro de seguridad de la política de grupo para crear la excepción.

- **Verificación de la Excepción**: Al iniciar sesión con la cuenta con privilegios de administrador, se verificó que el acceso al dispositivo USB era permitido, a diferencia de los usuarios regulares.