Proyecto de Políticas de Prevención de Pérdida de Datos (DLP) y Restricción de Dispositivos USB

Parte 1: Creación de Políticas de Seguridad DLP

1. Introducción a la Prevención de Pérdida de Datos (DLP)
La Prevención de Pérdida de Datos (DLP) es un conjunto de políticas, tecnologías y procesos diseñados para garantizar que la información sensible dentro de una organización no se filtre, pierda o acceda de manera no autorizada. La implementación de DLP es crucial para proteger los datos confidenciales, prevenir el robo de información y cumplir con regulaciones legales. En un entorno corporativo, DLP ayuda a mitigar riesgos de filtraciones de datos y asegura que los empleados solo tengan acceso a la información necesaria para realizar su trabajo.

---

2. Clasificación de Datos
Para garantizar una correcta protección de los datos, se establecen las siguientes categorías de clasificación de datos según su sensibilidad:

- **Datos Públicos:** Información accesible por el público en general, como materiales de marketing y contenido de la página web.
- **Datos Internos:** Información relevante solo para empleados de la empresa, como políticas internas y procesos operativos.
- **Datos Sensibles:** Información altamente confidencial, que incluye datos personales de empleados y clientes, información financiera y secretos comerciales.

---

3. Acceso y Control
Se aplicará el principio de menor privilegio, permitiendo que solo los usuarios autorizados accedan a los datos sensibles, limitando el acceso a lo estrictamente necesario. El flujo de revisión de permisos será realizado trimestralmente por el equipo de TI, que llevará a cabo una auditoría para garantizar que solo los usuarios adecuados mantengan acceso a los datos clasificados como sensibles. El proceso de revisión involucrará el análisis de las funciones laborales y los permisos actuales de acceso.

---

4. Monitoreo y Auditoría
Para mantener la seguridad de los datos sensibles, se implementarán herramientas de

monitoreo y auditoría como SIEM (Security Information and Event Management) y software DLP especializado. Estas herramientas permitirán detectar y registrar cualquier actividad inusual o no autorizada relacionada con el acceso a datos sensibles. Las actividades de monitoreo incluirán registros de acceso, transferencias de datos y actividades de modificación de información.

---

5. Prevención de Filtraciones
Para evitar la fuga de datos, se implementarán tecnologías de cifrado y herramientas DLP avanzadas. Los datos sensibles serán cifrados tanto en reposo como en tránsito. Además, se utilizarán herramientas DLP que impidan la transferencia no autorizada de datos a dispositivos externos o a la nube, y que alerten cuando se intente compartir información de manera inapropiada.

---

6. Educación y Concienciación
El personal será capacitado periódicamente sobre las políticas de seguridad de datos, los riesgos asociados con la pérdida de datos y las mejores prácticas para el manejo de información sensible. Los empleados deberán asistir a sesiones de formación para comprender cómo proteger los datos y cómo evitar infracciones a las políticas de seguridad.

Parte 2: Implementación de Políticas de Restricción de Dispositivos USB

1. Configuración de la Máquina Virtual para Acceso a Dispositivos USB
La máquina virtual (VM) fue configurada para reconocer y acceder a dispositivos USB conectados al host físico mediante la instalación del *VirtualBox Extension Pack* y la habilitación de soporte USB en la VM. Se aseguraron los permisos de acceso a USB 2.0 o 3.0 según el dispositivo utilizado, y se verificó que la VM podía reconocer dispositivos USB de manera correcta.

---

2. Restricción de Acceso a Dispositivos USB en Windows
Se implementaron políticas de restricción de dispositivos USB utilizando el Editor de Políticas de Grupo (gpedit.msc). Las siguientes políticas fueron activadas:

- **Discos removibles: Denegar acceso de lectura.**
- **Discos removibles: Denegar acceso de escritura.**

Estas configuraciones aseguran que los usuarios estándar no puedan acceder a los dispositivos USB conectados, evitando la transferencia no autorizada de datos sensibles a dispositivos externos.

---

3. Validación y Pruebas de Restricción de USB
Se creó un usuario estándar y se verificó que, al conectar un dispositivo USB, este fuera inaccesible para el usuario sin privilegios de administrador. Se recibió un mensaje indicando la denegación de acceso, confirmando que las políticas se implementaron correctamente.

---

4. Creación y Pruebas de un Usuario Regular
Se configuró un nuevo usuario estándar en Windows y se probó la restricción de acceso a dispositivos USB. El usuario estándar no pudo acceder a los dispositivos USB, lo que demuestra que las políticas de restricción fueron exitosas.

---

5. Habilitación de Excepciones para Usuarios Específicos
Se investigó cómo habilitar excepciones para usuarios o grupos específicos en el Editor de Políticas de Grupo, permitiendo que ciertos administradores u otros roles de confianza pudieran acceder a dispositivos USB. La política fue aplicada con éxito y se verificó que solo los usuarios con privilegios de administrador pudieran acceder a dispositivos USB.

Conclusión

Este proyecto proporciona un marco sólido para la protección de datos sensibles en TechCorp Inc. Mediante la implementación de políticas DLP y restricciones sobre el uso de dispositivos USB, se logra reducir significativamente el riesgo de fuga de información y mantener la seguridad de los datos dentro de la organización. La formación continua del personal y el monitoreo constante de la actividad relacionada con los datos sensibles son esenciales para garantizar el éxito a largo plazo de estas medidas.