Patricia Fraile

Informe sobre Políticas de Prevención de Pérdida de Datos (DLP)

1. INTRODUCCIÓN

La Prevención de Pérdida de Datos (DLP) es un conjunto de políticas y controles de seguridad cuyo objetivo es evitar que la información confidencial de una organización sea perdida, robada o filtrada sin autorización. Estas soluciones permiten identificar y proteger datos sensibles, reduciendo riesgos causados por errores humanos, ataques internos o uso indebido de la información.

2. CLASIFICACIÓN

Para aplicar correctamente las políticas de DLP, la organización clasificó su información según su nivel de sensibilidad:

- Datos Públicos: Información accesible sin restricciones, como contenido del sitio web.
- Datos Internos: Información de uso interno, como correos y documentación.
- Datos Sensibles: Información crítica, como datos personales, financieros o credenciales.

Esta clasificación permite definir qué controles de seguridad se deben aplicar a cada tipo de dato.

3. CONTROL DE ACCESO Y PRINCIPIO DEL MENOR PRIVILEGIO

La organización aplica el principio del menor privilegio, otorgando a los usuarios solo los accesos necesarios para realizar sus tareas. Los permisos se asignan según el rol del usuario y no de forma individual.

Los accesos son revisados periódicamente.

4. MONITOREO Y AUDITORÍA

Se implementan mecanismos de monitoreo para registrar accesos y actividades relacionadas con datos sensibles. Estos registros permiten detectar comportamientos sospechosos y facilitan auditorías de seguridad.

Para ello, se utilizan registros del sistema y herramientas de monitoreo como soluciones DLP y sistemas SIEM.

5. PREVENCIÓN DE FILTRACIONES

Para evitar la fuga de información sensible, se aplican las siguientes medidas:

- Cifrado de datos importantes.
- Restricción del uso de dispositivos USB.
- Bloqueo de copias no autorizadas de información.

Estas medidas reducen el riesgo de pérdida o robo de datos.

6. SENSIBILIZACIÓN DEL USUARIO

La organización capacita a los usuarios sobre el uso seguro de la información, los riesgos de seguridad y la importancia de cumplir las políticas establecidas.

7. RESTRICCIÓN DE DISPOSITIVOS USB

Como parte de la implementación práctica de DLP, se configuraron políticas de grupo en una máquina virtual con Windows para bloquear el acceso de lectura y escritura a dispositivos USB.

Las pruebas realizadas con usuarios estándar confirmaron que el acceso a dispositivos USB está correctamente restringido.

8. EXCEPCIONES Y VALIDACIÓN

Se habilitaron excepciones para usuarios autorizados con privilegios administrativos. Las pruebas demostraron que los usuarios con excepción pueden usar dispositivos USB, mientras que los usuarios normales permanecen bloqueados.

9. CONCLUSIÓN

La aplicación de políticas de DLP junto con el principio del menor privilegio y la restricción de dispositivos USB permite mejorar la protección de la información y reducir riesgos de seguridad dentro de una organización.