Reporte Políticas de Prevención de Perdida de Datos (DLP)

Francisco Félix Rodriguez Pellicer

Políticas de Prevención de Pérdida de Datos (DLP)

Introducción al Data Loss Prevention (DLP)

La Prevención de Pérdida de Datos, conocida como **Data Loss Prevention (DLP)**, es un conjunto de estrategias y tecnologías diseñadas para detectar, prevenir y responder ante la posible pérdida, uso indebido o acceso no autorizado a información confidencial dentro de una organización. Su objetivo principal es proteger los datos sensibles, ya sea en tránsito, en uso o en reposo, para evitar que sean filtrados hacia el exterior o utilizados de manera inapropiada internamente.

En un entorno empresarial cada vez más digital y conectado, el DLP se vuelve esencial para el cumplimiento de normativas, la protección de la reputación institucional y la garantía de la confidencialidad, integridad y disponibilidad de la información. Las políticas de DLP permiten a las organizaciones establecer controles claros sobre el manejo de los datos, minimizando riesgos y fortaleciendo la postura de seguridad.

Clasificación de Datos

La correcta clasificación de los datos es un paso fundamental para la implementación de medidas de protección efectivas. La organización adoptará el siguiente esquema de clasificación:

- **Datos Públicos:** Información que puede ser compartida abiertamente sin repercusiones legales o de seguridad. Ejemplos: comunicados de prensa, contenido del sitio web público.
- **Datos Internos:** Información destinada únicamente para uso dentro de la organización. Aunque su exposición no cause

daños graves, puede tener impactos negativos. Ejemplos: políticas internas, procedimientos operativos.

- **Datos Sensibles:** Información crítica cuyo acceso no autorizado puede generar consecuencias legales, financieras o de reputación. Ejemplos: datos personales de empleados, información financiera, propiedad intelectual, información de clientes.

Cada categoría tendrá asignadas políticas específicas de manejo, almacenamiento y acceso.

Acceso y Control

Siguiendo el **principio del menor privilegio**, se establecerán políticas que garanticen que cada empleado acceda únicamente a los datos que necesita para cumplir con sus funciones.

- Los permisos de acceso serán asignados de acuerdo con el rol del usuario dentro de la organización.
- Se implementará un proceso de **revisión periódica de accesos**, el cual será responsabilidad conjunta del área de Seguridad de la Información y los responsables de cada departamento.
- Las solicitudes de acceso a datos sensibles requerirán una justificación formal y serán aprobadas por el supervisor directo y el equipo de seguridad.

Monitoreo y Auditoría

La organización establecerá un sistema de monitoreo continuo y auditoría de toda actividad relacionada con datos sensibles.

- Se utilizarán herramientas de monitoreo como **soluciones DLP** y **plataformas SIEM (Security Information and**

Event Management) para detectar comportamientos anómalos, accesos no autorizados o movimientos inusuales de información.

- Se mantendrán registros detallados de accesos, modificaciones y transferencias de datos sensibles.
- Las auditorías se realizarán de forma trimestral y estarán a cargo del equipo de Seguridad de la Información, reportando hallazgos a la alta dirección.

Prevención de Filtraciones

Para evitar la fuga o pérdida de información sensible, se implementarán las siguientes medidas preventivas:

- **Cifrado de datos** tanto en tránsito como en reposo, asegurando que solo usuarios autorizados puedan acceder a la información.
- Configuración de **políticas automatizadas de bloqueo o alerta** mediante herramientas de DLP, para prevenir el envío de datos sensibles por canales no autorizados (correo, USB, nube, etc.).
- Limitación del uso de dispositivos externos o redes no seguras para manipulación de datos críticos.

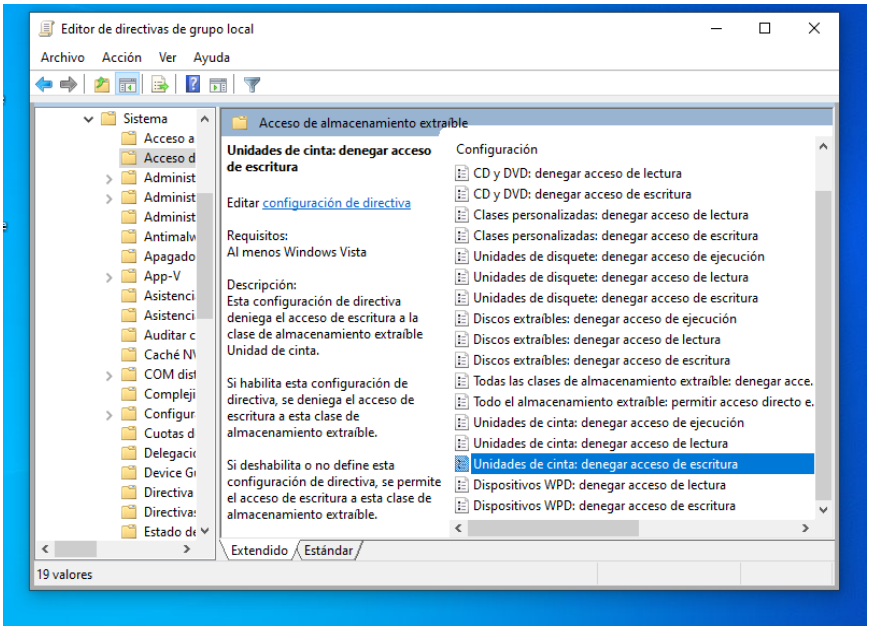
Educación y Concientización

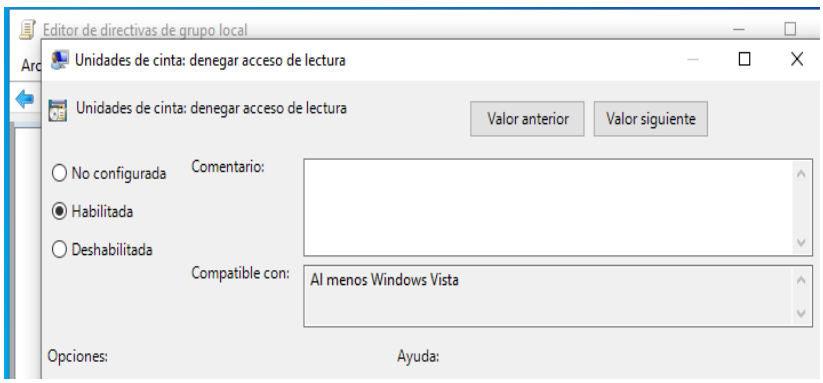
La seguridad de la información no solo depende de herramientas, sino también de las personas. Por ello, se implementará un programa de **educación y concientización en seguridad informática** que incluirá:

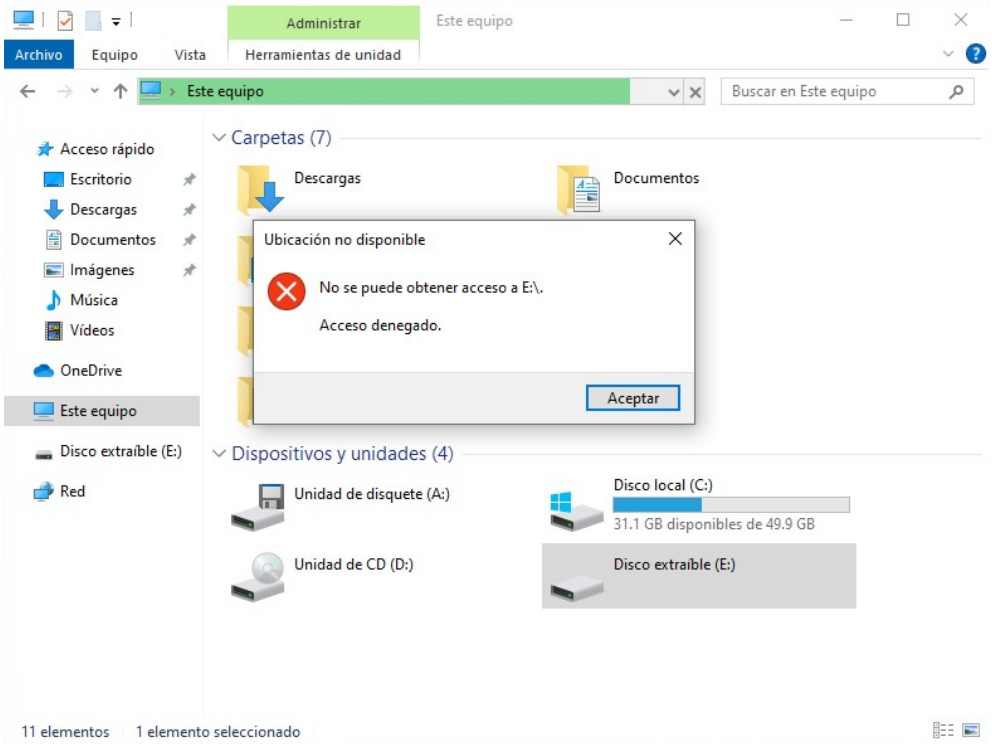
- Capacitación inicial para todo nuevo empleado sobre políticas de seguridad y clasificación de datos.

- Campañas periódicas de concientización sobre riesgos cibernéticos, phishing y buenas prácticas en el manejo de la información.
- Evaluaciones anuales para reforzar los conocimientos y detectar posibles brechas de comprensión.

Segunda Parte (Implementación de medidas especificas)






Administrar
Este equipo
Archivo
Equipo
Vista
Herramientas de unidad
Este equipo
Buscar en Este equipo
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
OneDrive
Este equipo
Disco extraíble (E:)
Red
Carpetas (7)
Descargas
Documentos
Ubicación no disponible
No se puede obtener acceso a E:\.
Acceso denegado.
Aceptar
Dispositivos y unidades (4)
Unidad de disquete (A:)
Disco local (C:)
31.1 GB disponibles de 49.9 GB
Unidad de CD (D:)
Disco extraíble (E:)
11 elementos
1 elemento seleccionado