Creación de políticas de seguridad DLP

Propietario	 Ayala Arroyo Raúl
Etiquetas	

Políticas de Seguridad DLP para el Sistema de Almacenamiento en la Nube: OneDrive for Business

Introducción al Data Loss Prevention (DLP)

El Data Loss Prevention (DLP) es un enfoque estratégico de seguridad diseñado para proteger los datos confidenciales de una organización contra la exposición no autorizada, el uso indebido o la pérdida accidental. En un entorno donde las organizaciones dependen cada vez más de sistemas de almacenamiento en la nube, el DLP se vuelve esencial para garantizar que la información crítica permanezca segura, cumpliendo con regulaciones y estándares de seguridad.

OneDrive for Business, como solución de almacenamiento en la nube, permite almacenar, sincronizar y compartir datos corporativos. Sin embargo, el acceso sin control adecuado puede ser un riesgo significativo de pérdida de datos. Las políticas DLP detalladas a continuación tienen como objetivo mitigar estos riesgos y proteger la información confidencial de la organización.

Clasificación de Datos

La correcta gestión de datos requiere clasificarlos en categorías según su nivel de sensibilidad. Para OneDrive for Business, la organización implementará las siguientes clasificaciones:

1. **Datos Públicos:**

- Información no confidencial, disponible para el público o compartida internamente sin riesgo, como material promocional, comunicados de prensa.

2. **Datos Internos:**
   - Información restringida al personal de la organización, cuya divulgación podría generar impactos operativos como manuales internos, reportes de desempeño.
3. **Datos Sensibles:**
   - Datos altamente confidenciales que requieren controles estrictos. La exposición podría causar daño financiero, legal o reputacional como información financiera, contratos legales, datos personales protegidos por normativas (como RGPD o HIPAA).

Acceso y Control

Basado en el **Principio del Menor Privilegio**, se implementarán políticas estrictas para limitar el acceso a los datos almacenados en OneDrive for Business:

- **Restricción de Acceso:**

  Los usuarios tendrán acceso únicamente a los archivos y carpetas necesarios para sus funciones laborales.
  - Directores: Acceso a datos sensibles dentro de sus áreas.
  - Empleados: Acceso limitado a datos internos relevantes para su departamento.
- **Revisión de Permisos:**
  - **Frecuencia:** Revisión trimestral de los permisos asignados, asegurando que usuarios inactivos o desvinculados no mantengan accesos.
  - **Responsables:** Los administradores de TI y supervisores de equipo serán responsables de realizar auditorías regulares.
- **Acceso Temporal:**

  Para proyectos específicos, se otorgará acceso temporal a los datos necesarios. Este acceso será revocado automáticamente al finalizar el

proyecto o tarea.

- **Jerarquías de Edición:**

  Solo roles superiores (supervisores y administradores) tendrán permisos de edición. El resto de los usuarios tendrá permisos de solo lectura.

Monitoreo y Auditoría

La organización utilizará herramientas de monitoreo y auditoría específicas para OneDrive for Business, con el fin de detectar actividades sospechosas o inusuales:

- **Registro de Actividades:**
  - OneDrive for Business ofrece un historial detallado de accesos, ediciones y descargas.
  - La información registrada incluirá quién accedió al archivo, desde dónde y qué acciones realizó.
- **Alertas de Seguridad:**

  Se configurarán alertas automáticas para notificar al equipo de seguridad ante acciones no autorizadas, como compartir archivos sensibles con usuarios externos.
- **Auditorías Programadas:**
  - Cada trimestre se revisará el acceso y las actividades realizadas en los datos clasificados como sensibles.
  - Estas auditorías estarán a cargo del equipo de seguridad de TI y serán documentadas para futuras referencias.

Prevención de Filtraciones

Para evitar fugas de datos, se implementarán las siguientes medidas tecnológicas y políticas:

1. **Cifrado de Datos:**

   Todo el contenido en OneDrive for Business estará cifrado tanto en tránsito como en reposo, utilizando estándares como TLS 1.2 para transferencias

seguras.

2. **Políticas de Compartición Controlada:**
    - Desactivar la opción de compartir con "cualquier persona con el enlace" para archivos clasificados como sensibles.
    - Limitar la compartición a usuarios internos o socios externos previamente aprobados.
3. **Restricciones de Descarga:**
    - Archivos etiquetados como "Confidenciales" no podrán descargarse sin una autorización explícita.
    - Implementar marcas de agua en documentos críticos para rastrear posibles filtraciones.

Educación y Concientización

El éxito de cualquier política de seguridad radica en la comprensión y adopción por parte de los empleados. La organización llevará a cabo las siguientes actividades:

1. **Capacitación Obligatoria:**
    - Realizar entrenamientos trimestrales sobre las políticas DLP y el uso seguro de OneDrive for Business.
    - Incluir módulos sobre el reconocimiento de intentos de phishing y otras amenazas.
2. **Simulaciones Prácticas:**
    - Ejercicios que simulen posibles escenarios de fuga de información, enseñando a los empleados a reaccionar adecuadamente.
3. **Campañas de Concientización:**
    - Carteles, boletines y recordatorios que refuercen las políticas de uso y los riesgos asociados.

Conclusión

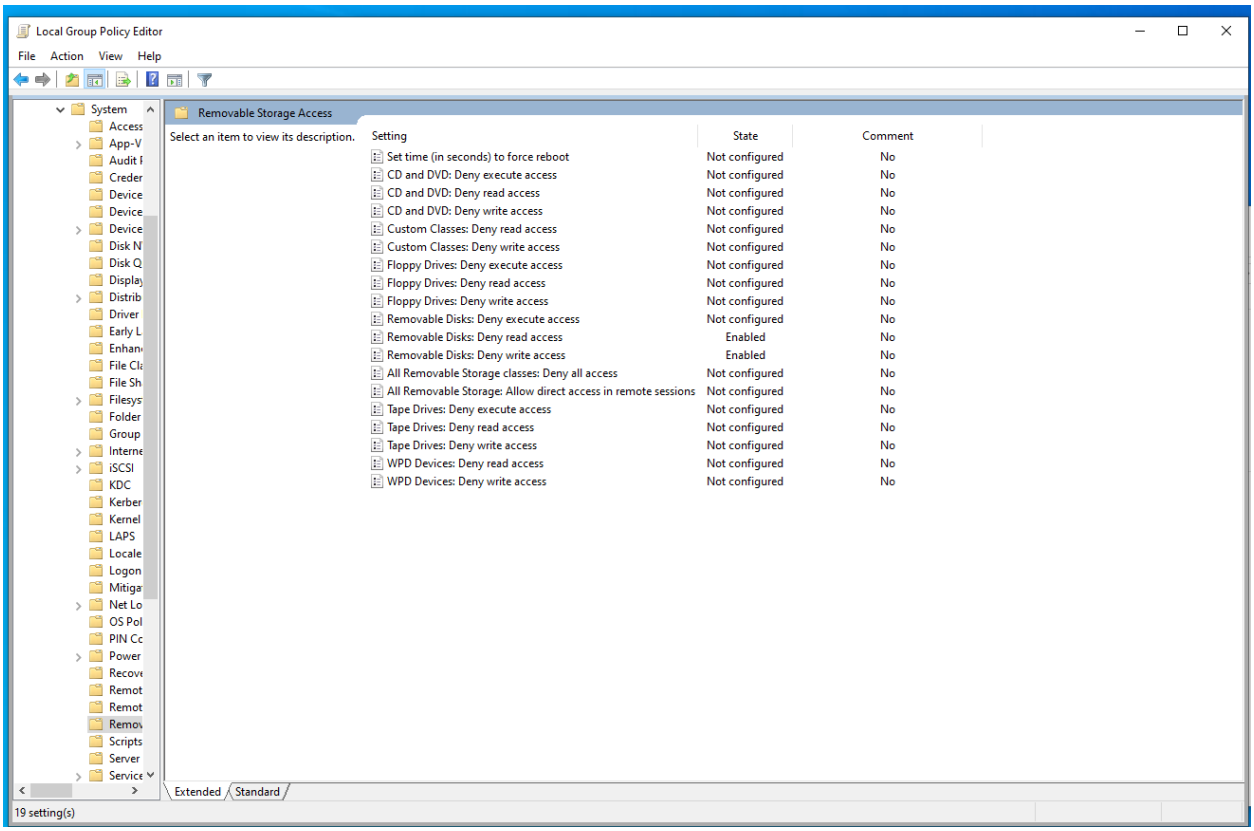
La implementación de políticas DLP específicas para OneDrive for Business, combinada con educación y controles tecnológicos, garantizará la protección de la información crítica de la organización. Estas medidas, alineadas con el **Principio del Menor Privilegio**, no solo minimizarán los riesgos de fugas de datos, sino que también fomentarán una cultura de seguridad dentro de la empresa.

Con un monitoreo constante, revisiones regulares y una participación activa de los empleados, se podrá mantener un entorno seguro y en cumplimiento con las normativas globales.

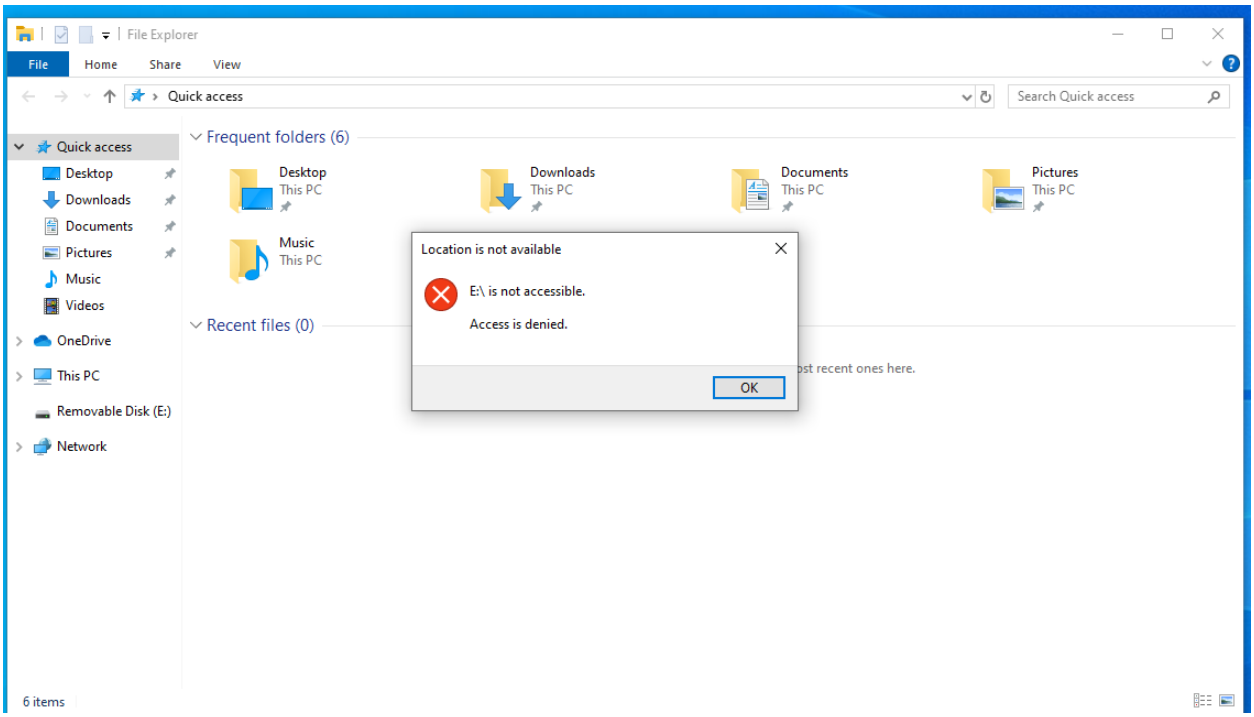
Práctica

Aplicación de políticas siguiendo:

1. **Abrir el Editor de Políticas de Grupo (Group Policy Editor)**. Presiona `Win + R`, escribe `gpedit.msc` y presiona `Enter` para abrir el Editor de Políticas de Grupo.
2. **Navegar a las Políticas de Dispositivos Removibles**. Ve a `Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento removible`.
3. **Configurar la Política de Prohibición de Acceso a Dispositivos USB**. Activa las siguientes políticas:
   - **Discos extraíbles: denegar acceso de lectura**.
   - **Discos extraíbles: denegar acceso de escritura**.

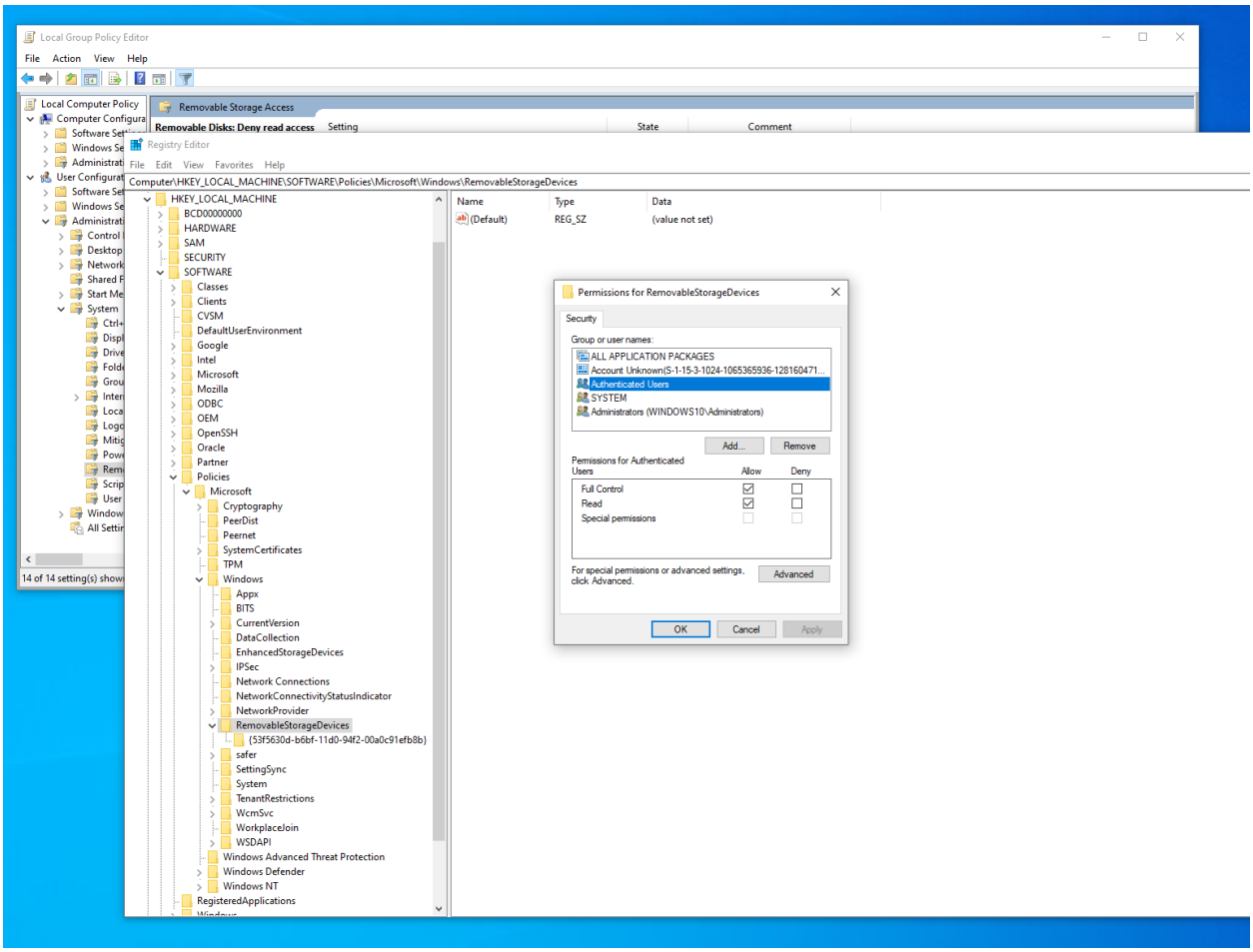


Usuario estándar:



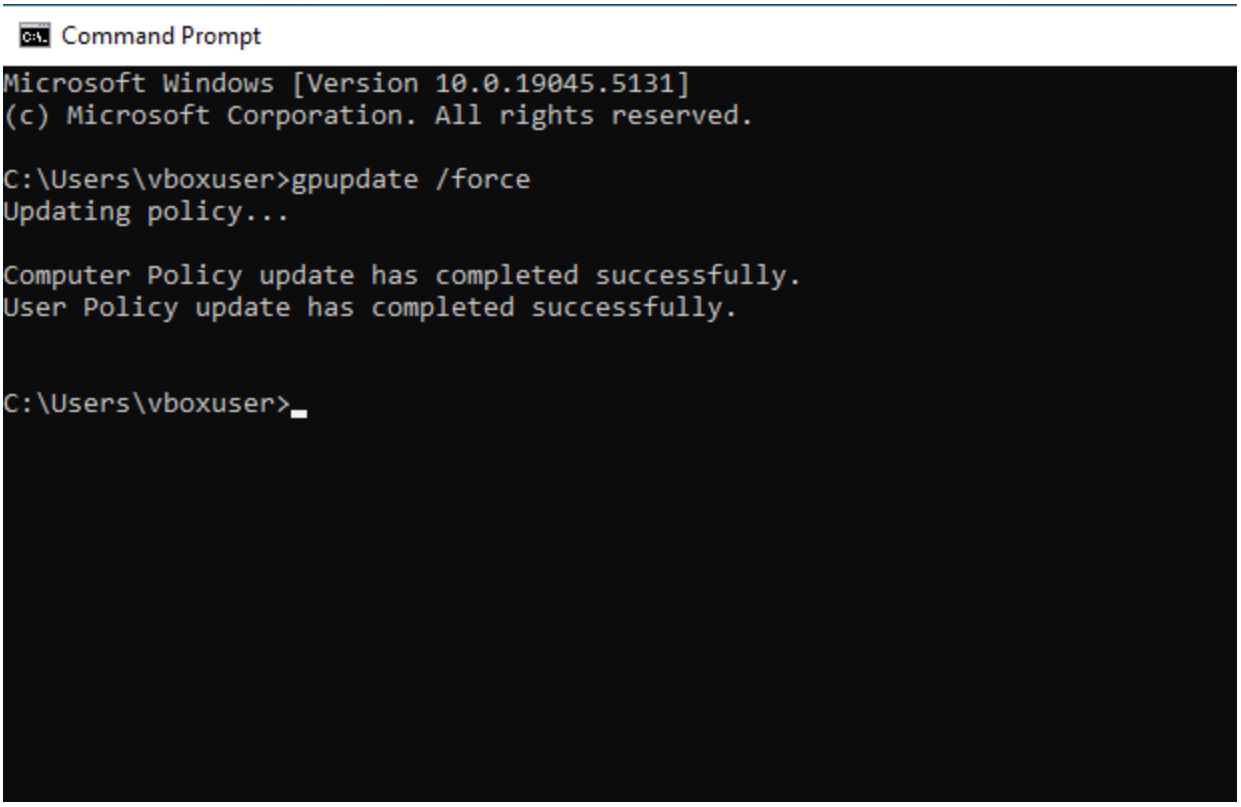
Para dar permisos a usuarios específicos

`Win + R`, y escribimos `regedit`



Después en la terminal poner:

```
gpupdate /force
```



Reiniciar y verificar cambios.