PROYECTO DLP: POLÍTICAS DE SEGURIDAD Y RESTRICCIÓN DE DISPOSITIVOS USB

1. INTRODUCCIÓN AL DATA LOSS PREVENTION (DLP)

El Data Loss Prevention (DLP) o Prevención de Pérdida de Datos es un conjunto integral de políticas, procesos y tecnologías diseñadas para evitar que información confidencial y sensible salga de la organización de forma no autorizada, ya sea por error humano o por intención maliciosa.

El objetivo principal del DLP es:
• Identificar datos sensibles dentro de los sistemas corporativos
• Controlar y monitorizar cómo se utilizan esos datos
• Bloquear, alertar o registrar cuando se detecta un posible intento de filtración
• Prevenir la salida de información a través de USB, correo personal, servicios en la nube no autorizados o dispositivos extraíbles

La importancia del DLP dentro de una organización radica en:

• Cumplimiento Normativo: Facilita la adhesión a regulaciones como RGPD (Reglamento General de Protección de Datos), PCI-DSS (estándares de seguridad para datos de tarjetas de crédito), HIPAA (protección de datos sanitarios) y otras legislaciones de protección de datos.

• Protección de Propiedad Intelectual: Previene la fuga de información estratégica como diseños, fórmulas, código fuente y planes comerciales.

• Reducción de Riesgos: Mitiga el impacto de ataques internos, robo de dispositivos, suplantación de identidad y compromisos de seguridad.

• Reputación Empresarial: Protege la imagen de la empresa ante filtración de datos de clientes o información confidencial.

• Costos Operacionales: Evita gastos derivados de brechas de seguridad, como multas, litigio, notificación a afectados y pérdida de confianza.

2. CLASIFICACIÓN DE DATOS

Para implementar un DLP efectivo, es fundamental establecer un sistema claro de clasificación de datos. La organización TechCorp Inc. clasificará la información en tres categorías principales según su nivel de sensibilidad:

2.1 DATOS PÚBLICOS

Definición: Información que puede ser compartida libremente sin riesgo alguno para la organización.

Características:
• Su divulgación no causa impacto legal, económico ni reputacional
• Está diseñada para ser conocida por el público general
• No contiene información competitiva o estratégica

Ejemplos:
• Notas de prensa oficiales
• Contenido web público de la empresa
• Material de marketing general
• Informes anuales publicados
• Comunicados oficiales

2.2 DATOS INTERNOS

Definición: Información de uso interno cuya divulgación no autorizada podría causar molestias operativas menores o impacto de imagen leve.

Características:
• Está restringida a personal de la organización
• Su filtrado tendría impacto operativo pero no crítico
• No afecta directamente al cumplimiento normativo o a ingresos
• Requiere control de acceso basado en departamento o rol

Ejemplos:
• Procedimientos internos y manuales operativos
• Documentación técnica no sensible
• Correos corporativos generales
• Calendarios de proyectos internos
• Políticas de recursos humanos públicas

2.3 DATOS SENSIBLES

Definición: Información crítica cuya filtrado o acceso no autorizado tendría impacto legal, económico o reputacional grave.

Características:
• Acceso altamente restringido
• Sujeta a cumplimiento normativo (RGPD, PCI-DSS, etc.)
• Su pérdida causaría daño significativo a la organización
• Requiere encriptación, auditoría y monitoreo estricto

Ejemplos:
• Datos personales de clientes (nombres, correos, teléfonos)
• Información financiera y nesting de proyectos estratégicos
• Números de tarjetas de crédito y datos de pago
• Nóminas y datos de empleados
• Credenciales de acceso y tokens de seguridad

• Diseños de productos y código fuente propietario
• Registros de auditoría y logs de seguridad críticos
• Acuerdos contractuales confidenciales

3. ACCESO Y CONTROL - PRINCIPIO DEL MENOR PRIVILEGIO

El Principio del Menor Privilegio es un concepto fundamental de seguridad que establece que cada usuario solo debe tener acceso al mínimo conjunto de datos y permisos necesarios para realizar su trabajo.

3.1 POLÍTICA DE ACCESO POR NIVEL DE CLASIFICACIÓN

Datos Públicos:
• Acceso: Disponible para todo el personal de la organización
• Jefe de Aprobación: No requiere aprobación especial
• Control: Registro de acceso básico
• Ejemplo: Un analista de marketing puede acceder a notas de prensa

Datos Internos:
• Acceso: Restringido por departamento y rol
• Jefe de Aprobación: Líder del departamento
• Control: Autenticación y registro detallado de accesos
• Ejemplo: Solo el equipo de TI puede acceder a procedimientos internos de IT

Datos Sensibles:
• Acceso: Altamente restringido a roles específicos
• Jefe de Aprobación: Director de Seguridad o CTO + Responsable del Departamento
• Control: Autenticación multifactor, cifrado, auditoría continua
• Ejemplo: Solo Finanzas puede acceder a estados financieros, RRHH a nóminas

3.2 FLUJO DE REVISIÓN Y APROBACIÓN DE PERMISOS

Paso 1: Solicitud Inicial
• El empleado o su líder directo solicita acceso a través del sistema de gestsión de permisos
• Se indica el tipo de dato, el propósito del acceso y la duración esperada
• Ejemplo: "Necesito acceso a datos de clientes para la campaña de marketing Q2"

Paso 2: Revisión por el Líder Directo
• El jefe directo valida que el acceso es necesario para el rol
• Confirma que la solicitud es legitíma y coherente
• Aprueba o rechaza con justificación

Paso 3: Revisión por Seguridad / IT
• El departamento de Seguridad de IT valida:
  - Que el nivel de acceso solicitado es apropiado para el rol
  - Que los datos solicitados son necesarios
  - Que el usuario ha completado formación de seguridad requerida

Paso 4: Aprobación Final
• El propietario de datos (Data Owner) autoriza el acceso
• Se registra la aprobación con fecha y responsable

Paso 5: Implementación Técnica
• Se configura el acceso en los sistemas (bases de datos, servicios en la nube, etc.)
• Se notifica al usuario del acceso concedido
• Se establece fecha de vencimiento (si aplica)

Paso 6: Auditoría y Revisión Periódica
• Cada 6 o 12 meses se revisan los permisos activos
• Se valida que cada usuario sigue necesitando su acceso actual
• Se revocan permisos no utilizados o innecesarios
• Se documenta cualquier cambio

Responsables:
• Líder Directo: Valida la necesidad del acceso
• Departamento de Seguridad: Aplica el menor privilegio y polticas
• Propietario de Datos: Aprueba finalmente qué se comparte
• Gerencia de TI: Implementa los cambios técnicos

4. MONITOREO Y AUDITORÍA

La vigilancia continua y la auditoría exhaustiva de actividades relacionadas con datos sensibles son pilares del DLP. Se establecerán reglas y herramientas para detectar comportamientos anormales y facilitar investigaciones.

4.1 HERRAMIENTAS DE MONITOREO

SIEM (Security Information and Event Management)
• Solución central que recopila logs de todos los sistemas corporativos
• Correlaciona eventos para detectar patrones de riesgo
• Genera alertas en tiempo real ante comportamientos sospechosos
• Herramientas recomendadas: Splunk, ELK Stack, ArcSight

DLP Endpoint
• Software instalado en ordenadores corporativos que monitoriza:
  - Intentos de copiar datos sensibles a dispositivos USB
  - Descargas de archivos hacia servicios en la nube (Dropbox, OneDrive)
  - Intentos de enviar datos sensibles por correo personal
  - Conexiones a impresoras de red sospechosas
• Herramientas recomendadas: Symantec DLP, McAfee DLP, Forcepoint

Controlador de Dominio Windows
• Registro centralizado de accesos a recursos de red
• Auditoría de cambios en permisos de ficheros y carpetas
• Logs de inicio de sesión fallidos y exitosos

Auditoría de Dispositivos USB
• Registro de conexiones de dispositivos removibles
• Logs de intentos de lectura y escritura bloqueados
• Identificación de dispositivos USB conectados

4.2 EVENTOS MONITOREADOS

Acceso a Datos Sensibles:
• Cuándo y quién accede a información clasificada como sensible
• Qué datos fueron consultados
• Desde qué dispositivo o ubicación geográfica

Operaciones Masivas:
• Descargas de más de N ficheros en poco tiempo
• Cópia de archivos grandes de datos sensibles
• Cambios masivos de permisos

Salida de Datos:
• Intentos de copiar a USB (bloqueados)
• Carga a servicios en la nube no autorizados
• Envío de datos sensibles por correo personal

Comportamiento Anormal:
• Accesos fuera de horario laboral
• Acceso desde dispositivos no corporativos
• Acceso desde países o ciudades inusuales
• Intento de acceso por usuarios que no utilizan normalmente ciertos datos

Eventos de Seguridad:
• Fallos de autenticación múltiples
• Intentos de escalada de privilegios
• Modificación o eliminación de logs de auditoría

4.3 AUDITORÍA Y REPORTES PERIÓDICOS

Auditoría Trimestral
• Revisión de todos los accesos a datos sensibles
• Análisis de intentos bloqueados de copia a USB
• Evaluación de cambios en permisos
• Identificación de usuarios inactivos con acceso a datos

Auditoría Anual
• Revisión integral de las políticas DLP
• Evaluación de efectividad de controles
• Cumplimiento normativo y recomendaciones de mejora

Reportes de Incidentes
• Cada alerta genera un registro que debe ser investigado

• Se documenta la causa raiz del evento
• Se aplican correcciones o sanciones si procede

5. PREVENCIÓN DE FILTRACIONES

La prevención de filtraciones requiere una combinación de tecnologías y políticas que impidan que datos sensibles abandonen los sistemas corporativos no autorizados.

5.1 CIFRADO DE DATOS

Cifrado en Repós (At Rest)
• Todos los discos duros de ordenadores corporativos deben estar cifrados con BitLocker (Windows) o FileVault (macOS)
• Bases de datos con datos sensibles deben usar cifrado AES-256
• Bloquea el acceso físico a discos si el dispositivo es robado
• El usuario solo puede acceder después de proporcionar credenciales correctas

Cifrado en Tránsito (In Transit)
• Todas las comunicaciones de red deben usar TLS 1.2 o superior
• Obligar HTTPS en el acceso a aplicaciones web con datos sensibles
• VPN para conexiones remotas a recursos internos
• Evita la interceptación de datos en la red

Cifrado de Archivos Compartidos
• Archivos sensibles compartidos por correo o servicios en la nube deben estar cifrados
• Usar herramientas como VeraCrypt o Cryptomator para crear contenedores cifrados
• El receptor debe tener la contraseña para acceder

5.2 RESTRICCIÓN DE DISPOSITIVOS USB

Bloq Completo
• Por defecto, bloquear el acceso de lectura y escritura a todos los dispositivos USB en usuarios estándar
• Esto previene:
  - Copia de datos a USB personales
  - Instalación de malware desde USB no autorizados
  - Robo de información mediante dispositivos removibles

Excepciones Autorizadas
• Crear una lista blanca de dispositivos USB corporativos permitidos
• Solo administradores pueden habilitar excepciones
• Las excepciones se auditan y se registran

Implementación Técnica (en sección 7)
• Usar Group Policy en Windows para deshabilitar acceso a discos extraífbles
• Políticas: "Discos extraífbles: denegar lectura" y "Discos extraífbles: denegar escritura"

5.3 CONTROL DE SALIDA DE DATOS

Restricción de Servicios en la Nube
• Bloquear carga de archivos a servicios no autorizados (Dropbox, Google Drive personal, OneDrive)
• Permitir solo servicios corporativos como Microsoft Teams, SharePoint, Slack corporativo
• Auditar cualquier intento de carga

Control de Correo Electrónico
• Implementar herramientas DLP de correo que detecten:
  - Envío a cuentas de correo personales
  - Archivos sensibles adjuntos a correos externos
  - Patrones de contenido (números de tarjeta, SSN, etc.)
• Bloquear o alertar al usuario y su gestor

Control de Impresoras
• Permitir impresión solo en impresoras corporativas autenticadas
• Monitorizar qué se imprime
• Requerir PIN o tarjeta para liberar documentos

Control de Puertos
• Deshabilitar puertos no necesarios (Bluetooth, infrarrojo) en dispositivos corporativos
• Esto previene transferencias de datos a otros dispositivos personales

5.4 PROTECCIÓN DE DISPOSITIVOS

MDM (Mobile Device Management)
• Para dispositivos móviles corporativos:
  - Encriptación obligatoria
  - Bloqueo de pantalla después de inactividad
  - Capacidad de borrado remoto si el dispositivo se pierde
  - Restricción de instalación de apps

EDR (Endpoint Detection and Response)
• Software de detección de amenazas en tiempo real
• Identifica comportamiento de malware o movimiento lateral de atacantes
• Herramientas: CrowdStrike, Microsoft Defender, Sentinelone

6. EDUCACIÓN Y CONCIENTIZACIÓN

La educación del personal es uno de los factores más importantes para el éxito del DLP. Los errores humanos son responsables de la mayoría de las filtraciones de datos.

6.1 PROGRAMA DE FORMACIÓN

Formación Inicial (Onboarding)
• Todo nuevo empleado debe recibir formación obligatoria sobre:
  - Qué es DLP y por qué es importante
  - Clasificación de datos de la empresa

  - Sus responsabilidades respecto a la protección de datos
  - Las consecuencias de incumplimiento
• Duración: 1-2 horas
• Evaluación: Prueba corta (mínimo 80% para pasar)
• Certifié registrado en el expediente del empleado

Formación Especíalizada
• Para roles con acceso a datos sensibles:
  - Finanzas: protección de información financiera
  - RRHH: confidencialidad de datos de empleados
  - Desarrollo: seguridad de código y propiedad intelectual
  - Soporte Técnico: manejo seguro de datos de clientes
• Duración: 2-4 horas según el rol

Formación Anual Obligatoria
• Refrescamiento de conocimientos para todo el personal
• Actualización sobre nuevas políticas o amenazas
• Casos prácticos y escenarios reales
• Todos deben completarla dentro del año fiscal

Formación Reactiva
• Si un empleado comete una violación de seguridad:
  - Recibe formación correctiva inmediata
  - Se documenta el incidente
  - Se evalúa el desempeño en prueba siguiente

6.2 CAMPAÑA DE CONCIENTIZACIÓN

Correos Periódicos
• Mensajes cortos (1x al mes) sobre:
  - Riesgos de seguridad actuales
  - Buenas prácticas de higiene digital
  - Casos de éxito de protección de datos

Persías de Información
• Carteles en zonas comunes recordando:
  - "No dejes documentos sensibles en el escritorio"
  - "Bloquea tu ordenador antes de salir"
  - "Desconecta el USB cuando termines"
  - "Reporta comportamiento sospechoso"

Sesiones de Q&A
• Reuniones mensuales (30 min) donde:
  - El equipo de Seguridad responde preguntas
  - Se discuten dudas sobre DLP
  - Se comparten casos reales (anonimizados)

Simulaciones de Phishing

• Envíos de correos falsos para probar si los empleados:
  - Reconocen intentos de phishing
  - Reportan mensajes sospechosos
• Quien cae en el phishing recibe formación adicional
• Se registran métricas de mejora

6.3 REPORTES Y RESPONSABILIDAD

Canal de Reportes
• Los empleados pueden reportar:
  - Intentos de phishing
  - Comportamientos sospechosos de compañeros
  - Vulnerabilidades de seguridad
  - Violaciones potenciales de DLP
• Email seguro: security@company.com
• Línea de denuncia anónima (si aplica)

Sanciones por Incumplimiento
• Primera violación: Advertencia formal + formación correctiva
• Segunda violación: Suspensión de acceso temporal + investigación
• Violación grave (intencional): Despido + acción legal
• Las sanciones se aplican de manera consistente

6.4 CULTURA DE SEGURIDAD

Responsabilidad Compartida
• Todos los empleados son responsables de la seguridad
• Los líderes deben dar ejemplo cumpliendo normas
• Los "campeones de seguridad" por departamento ayudan a difundir buenas prácticas

Recursos Disponibles
• Página intranet de seguridad con guías y FAQ
• Contacto del oficial de privacidad (Data Protection Officer)
• Herramientas de protección personal (VPN, gestor de contraseñas corporativo)

7. IMPLEMENTACIÓN TÉCNICA: RESTRICCIÓN DE DISPOSITIVOS USB EN WINDOWS VM

7.1 PREPARACIÓN DEL ENTORNO

Instalar VirtualBox Extension Pack

1. Descargar el Extension Pack desde https://www.virtualbox.org/wiki/Downloads que coincida con tu versión de VirtualBox (ej: VirtualBox 7.0.10 Extension Pack para VirtualBox 7.0.10)

2. Abrir VirtualBox

3. Ir a Archivo > Herramientas > Extensiones

4. Hacer clic en el icono de agregar y seleccionar el archivo descargado

5. Aceptar la licencia y confirmar la instalación

Habilitar Soporte de USB en la VM

1. Con la máquina virtual apagada, hacer clic derecho en la VM en VirtualBox

2. Seleccionar "Configuración"

3. Ir a la pestaña "Puertos" > "USB"

4. Marcar la casilla "Habilitar controlador USB"

5. Seleccionar "USB 2.0 (EHCI)" o "USB 3.0 (xHCI)" según tus necesidades

6. Hacer clic en "Aceptar"

Conectar dispositivo USB a la VM

1. Conectar el dispositivo USB a tu máquina física

2. Iniciar la máquina virtual

3. En el menú de la VM, seleccionar "Dispositivos" > "USB"

4. Marcar el dispositivo USB que deseas compartir

5. El dispositivo ahora será accesible dentro de la VM

7.2 CONFIGURACIÓN DE POLÍTICAS DE GRUPO

Abrir el Editor de Políticas de Grupo

1. Iniciar sesión con una cuenta administrativa en la VM

2. Presionar Win + R para abrir "Ejecutar"

3. Escribir gpedit.msc y presionar Enter

4. Se abrirá el "Editor de Políticas de Grupo Local"

Navegar a Configuración de Dispositivos Removibles

1. En el árbol de la izquierda, expandir:

Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento removible

2. En el panel central aparecerán todas las políticas disponibles

Activar Políticas de Restricción

1. Hacer doble clic en "Discos extraífbles: denegar acceso de lectura"

2. Seleccionar "Habilitado"

3. Hacer clic en "Aplicar" y "Aceptar"

4. Hacer doble clic en "Discos extraífbles: denegar acceso de escritura"

5. Seleccionar "Habilitado"

6. Hacer clic en "Aplicar" y "Aceptar"

Reiniciar la Máquina Virtual

1. Presionar Win + R, escribir shutdown /r /t 0 y presionar Enter

2. Alternativamente, reiniciar manualmente a través del menú de inicio

3. Los cambios se aplicarán después del reinicio

7.3 VALIDACIÓN DE LA RESTRICCIÓN

Crear un Usuario Regular de Prueba

1. Iniciar sesión como administrador

2. Ir a Inicio > Configuración (Win + I)

3. Ir a Cuentas > Familia y otros usuarios

4. Hacer clic en "Agregar a otra persona a este equipo"

5. Seleccionar "No tengo la información de inicio de sesión"

6. Hacer clic en "Agregar un usuario sin cuenta de Microsoft"

7. Escribir nombre de usuario (ej: "testuser") y contraseña

8. Hacer clic en "Siguiente" y "Finalizar"

9. El usuario se creará como usuario estándar (sin privilegios de administrador)

Prueba de Restricción

1. Cerrar sesión del usuario administrador

2. Iniciar sesión con el usuario de prueba (testuser)

3. Conectar un dispositivo USB a la VM

4. Intentar acceder al dispositivo USB en "Mi PC" o Explorador de Archivos

5. El sistema debe mostrar un mensaje "Acceso denegado" o similar

6. El usuario NO debe poder:
   - Ver el contenido del USB
   - Copiar archivos hacia el USB
   - Transferir archivos desde el USB

Prueba con Usuario Administrador

1. Cerrar sesión del usuario estándar

2. Iniciar sesión como administrador

3. Intentar acceder al USB

4. El administrador SÍ deberá poder acceder (la restricción no aplica a administradores por defecto)

Documentación de Resultados

1. Captura de pantalla del mensaje "Acceso denegado"

2. Logs de intentos bloqueados (Visor de eventos > Registros de Windows > Sistema)

3. Fecha y hora de las pruebas

4. Usuarios con los que se validó

8. HABILITACIÓN DE EXCEPCIONES PARA USUARIOS ESPECÍFICOS

A pesar de que las políticas de restricción de USB están habilitadas para todos los usuarios estándar, es necesario crear un mecanismo de excepciones para ciertos roles que genuinamente necesitan acceso a dispositivos USB por razones operativas.

8.1 PRINCIPIOS DE EXCEPCIONES

• Excepciones justificadas: Solo se autorizan si hay una razón operativa clara

• Auditoría exhaustiva: Todas las excepciones se registran y monitorean
• Revisión periódica: Las excepciones se revisan cada 6 meses
• Riesgo controlado: Las excepciones son lo más restrictivas posible

8.2 ROL PERMITIDO: SOPORTE TÉCNICO CON RESTRICCIONES

Caracterización del Rol
• Usuarios que necesitan restaurar backups desde discos externos
• Instalación de drivers desde USB cuando la red no está disponible
• Transferencia de logs de diagnóstico para análisis
• Grupo de Active Directory: "IT_Support_USB_Exception"

Implementación de Excepción en Group Policy

1. Abrir gpedit.msc como administrador

2. Crear una Unidad Organizacional (OU) para usuarios con excepciones:
  - Configuración del equipo > Directivas de grupo > Nueva directiva
  - Nombrar: "USB_Exception_IT_Support"

3. Navegar a: Configuración de usuario > Plantillas administrativas > Sistema > Acceso de almacenamiento removible

4. Modificar la polítca "Discos extraífbles: denegar acceso de lectura" para el grupo IT_Support_USB_Exception:
  - Cambiar a "Deshabilitado" (permite lectura)
  - Esto solo aplica al grupo específ ico

5. Modificar "Discos extraífbles: denegar acceso de escritura":
  - Cambiar a "Deshabilitado" (permite escritura)
  - Solo para el grupo IT_Support_USB_Exception

6. Para todos los demás usuarios, mantener ambas políticas "Habilitadas"

7. Forzar actualización: gpupdate /force

8.3 PRUEBA DE EXCEPCIÓN

Crear usuario de soporte

1. Crear usuario "tech_support1" (usuario estándar sin privilegios de admin)

2. Agregarlo al grupo "IT_Support_USB_Exception" en Active Directory

3. Forzar sincronización de políticas: gpupdate /force

Validación de Acceso

1. Cerrar sesión del administrador

2. Iniciar sesión con "tech_support1"

3. Conectar un dispositivo USB

4. RESULTADO ESPERADO: El usuario SÍ podrá:
   - Ver el contenido del USB
   - Copiar archivos desde el USB al ordenador
   - Copiar archivos del ordenador al USB

5. Conectar con un usuario estándar (sin excepciones) para validar que sigue sin acceso

Auditoría de Excepciones

1. Registrar cada acceso USB exitoso del grupo IT_Support_USB_Exception

2. Revisar en el Visor de Eventos (Registros de Windows > Sistema) intentos de acceso

3. Generar reporte mensual de accesos a USB por rol

4. Flagging de comportamiento anormal (ej: copias masivas, horarios inusuales)

---

9. SEGUNDA EXCEPCIÓN ALTERNATIVA: SOLO LECTURA DESDE USB

Esta excepción permite a ciertos usuarios LEER datos desde un USB, pero NO permite ESCRIBIR o modificar datos. Es útil para:
• Analistas de seguridad que necesitan revisar logs o archivos de diagnóstico entregados por clientes
• Personal de cumplimiento que necesita auditar archivos externos
• Equipo forense que analiza evidencia en dispositivos USB

9.1 BENEFICIO DE ESTA EXCEPCIÓN

• Aumenta la seguridad: Los datos corporativos NO pueden salir a través del USB
• Permite operaciones: Se pueden leer archivos externos sin permitir fuga de datos
• Cumple RGPD: Se protegen datos corporativos mientras se trabaja con datos de terceros
• Trazabilidad: Se audita exactamente qué se leó de USB

9.2 IMPLEMENTACIÓN DE EXCEPCIÓN DE SOLO LECTURA

Grupo de usuarios
• Grupo de Active Directory: "Compliance_USB_Read_Only"

1. Abrir gpedit.msc como administrador

2. Crear nueva directiva: "USB_ReadOnly_Compliance"

3. Navegar a: Configuración de usuario > Plantillas administrativas > Sistema > Acceso de almacenamiento removible

4. Configurar políticas específicamente para el grupo "Compliance_USB_Read_Only":

Política 1: "Discos extraífbles: denegar acceso de lectura"
- Estado: Deshabilitado (permite lectura para este grupo)

Política 2: "Discos extraífbles: denegar acceso de escritura"
- Estado: Habilitado (bloquea escritura incluso para este grupo)

5. Aplicar la política: gpupdate /force

9.3 VALIDACIÓN DE EXCEPCIÓN DE SOLO LECTURA

Crear usuario de cumplimiento

1. Crear usuario "compliance_analyst1" (usuario estándar)

2. Agregarlo al grupo "Compliance_USB_Read_Only"

3. Forzar actualización: gpupdate /force

Pruebas de Acceso

1. Iniciar sesión con "compliance_analyst1"

2. Conectar un dispositivo USB que contenga archivo "muestra.txt"

3. Prueba 1 - Lectura (debe funcionar):
- Abrir el archivo "muestra.txt"
- Leer el contenido
- RESULTADO ESPERADO: Acceso exitoso

4. Prueba 2 - Escritura (debe ser bloqueada):
- Intentar copiar un archivo desde el ordenador al USB
- RESULTADO ESPERADO: Mensaje "Acceso denegado"
- Intentar crear un archivo nuevo en el USB
- RESULTADO ESPERADO: Mensaje "Acceso denegado"

9.4 AUDITORÍA DE SOLO LECTURA

• Registrar en logs todos los archivos LEÍDOS desde USB por este grupo
• Alertar si se intenta ESCRIBIR
• Registrar usuario, fecha, hora y nombre del archivo accedido
• Revisar mensualmente si ha habido intentos de escritura bloqueados

• Investigar si el usuario intentó leer archivos que no debería

---

10. CONCLUSIÓN Y RECOMENDACIONES

El sistema de DLP implementado crea un equilibrio entre:

• SEGURIDAD: Bloquea acceso no autorizado a datos sensibles
• OPERATIVIDAD: Permite excepciones justificadas para roles específicos
• CUMPLIMIENTO: Audita y registra todas las actividades
• TRAZABILIDAD: Mantiene un registro de quién accedió a qué

Recomendaciones para mantener la efectividad:

1. Capacitar a todos los usuarios sobre estas políticas al inicio

2. Revisar excepciones cada 6 meses y revocar las innecesarias

3. Monitorizar intentos bloqueados y investigar patrones anormales

4. Actualizar las políticas según nuevas amenazas identificés

5. Mantener registros de auditoría durante al menos 12 meses

6. Realizar pruebas periódicas para validar que las restricciones siguen en efecto

7. Comunicar cambios de política con anticipación a los usuarios afectados

Fin del documento.