Implementación de Políticas de seguridad DLP a dispositivos de almacenamiento externo.

Introducción.

El Data Loss Prevention (DLP) es un conjunto de estrategias y herramientas que protegen datos confidenciales de pérdidas o accesos no autorizados. Su importancia radica en garantizar la seguridad de información sensible, como datos personales y financieros, así como en cumplir con regulaciones y salvaguardar la reputación de la organización. En un contexto de crecientes amenazas cibernéticas, el DLP se convierte en un elemento clave de la estrategia de seguridad, ayudando a prevenir violaciones de datos y a mantener la confianza de clientes y socios.

Clasificación de datos.

Para garantizar una gestión adecuada y una protección efectiva de la información, la organización clasificará los datos en función de su sensibilidad en las siguientes tres categorías:

1. **Datos Públicos**

Definición: Información que puede ser compartida sin restricciones y que no representa un riesgo para la organización si es divulgada.

Ejemplo: Material de marketing, comunicados de prensa, información sobre productos y servicios disponibles al público.

2. **Datos Internos**

Definición: Información que es esencial para las operaciones diarias de la organización y que no debe ser divulgada fuera de la misma. Su divulgación podría causar inconvenientes, pero no necesariamente daños graves.

Ejemplo: Políticas internas, informes de rendimiento, comunicaciones entre departamentos, manuales de empleados.

3. **Datos Sensibles**

Definición: Información crítica cuya divulgación o acceso no autorizado podría resultar en daños significativos a la organización o a individuos, incluyendo consecuencias legales.

Ejemplo: Datos personales identificables (PII) como números de seguro social, información financiera, registros de salud de empleados y secretos comerciales.

Acceso y Control

Principio del Menor Privilegio:

La organización aplicará el principio del menor privilegio, otorgando a los empleados solo los permisos necesarios para realizar sus funciones. Esto se implementará a través de las siguientes políticas:

- **Clasificación de Roles:**
  - **Administradores de Sistemas:** Acceso total a datos internos y sensibles, necesarios para la gestión del sistema.
  - **Personal de Recursos Humanos:** Acceso a datos sensibles de empleados, pero sin acceso a datos financieros.
  - **Personal de Marketing:** Acceso a datos públicos y algunos datos internos, pero no a datos sensibles.

Flujo de Revisión de Permisos:

- **Responsables:**
  - **Gerentes de Departamento:** Realizarán revisiones trimestrales de los permisos de sus equipos.
  - **Equipo de Seguridad de la Información:** Revisará los resultados de las auditorías de permisos y propondrá ajustes.

Monitoreo y Auditoría

Reglas para el Monitoreo:

- **Datos Sensibles:** Se implementará monitoreo en tiempo real sobre el acceso y uso de datos sensibles, especialmente PII y registros financieros.

Herramientas Utilizadas:

- **Soluciones SIEM (Security Information and Event Management):** Para la recopilación y análisis de logs de eventos, detectando actividades sospechosas.
- **Herramientas DLP:** Para prevenir la transferencia no autorizada de datos sensibles, como el uso de USBs o envíos de correos electrónicos no seguros.

Prevención de Filtraciones.

Tecnologías Implementadas:

- **Cifrado:**
    - Todos los datos sensibles almacenados estarán cifrados, tanto en reposo como en tránsito, para proteger la información ante accesos no autorizados.
- **Herramientas de DLP:**
    - Implementación de software DLP que detecta y bloquea intentos de envío no autorizado de datos sensibles a través de correo electrónico o almacenamiento en la nube.

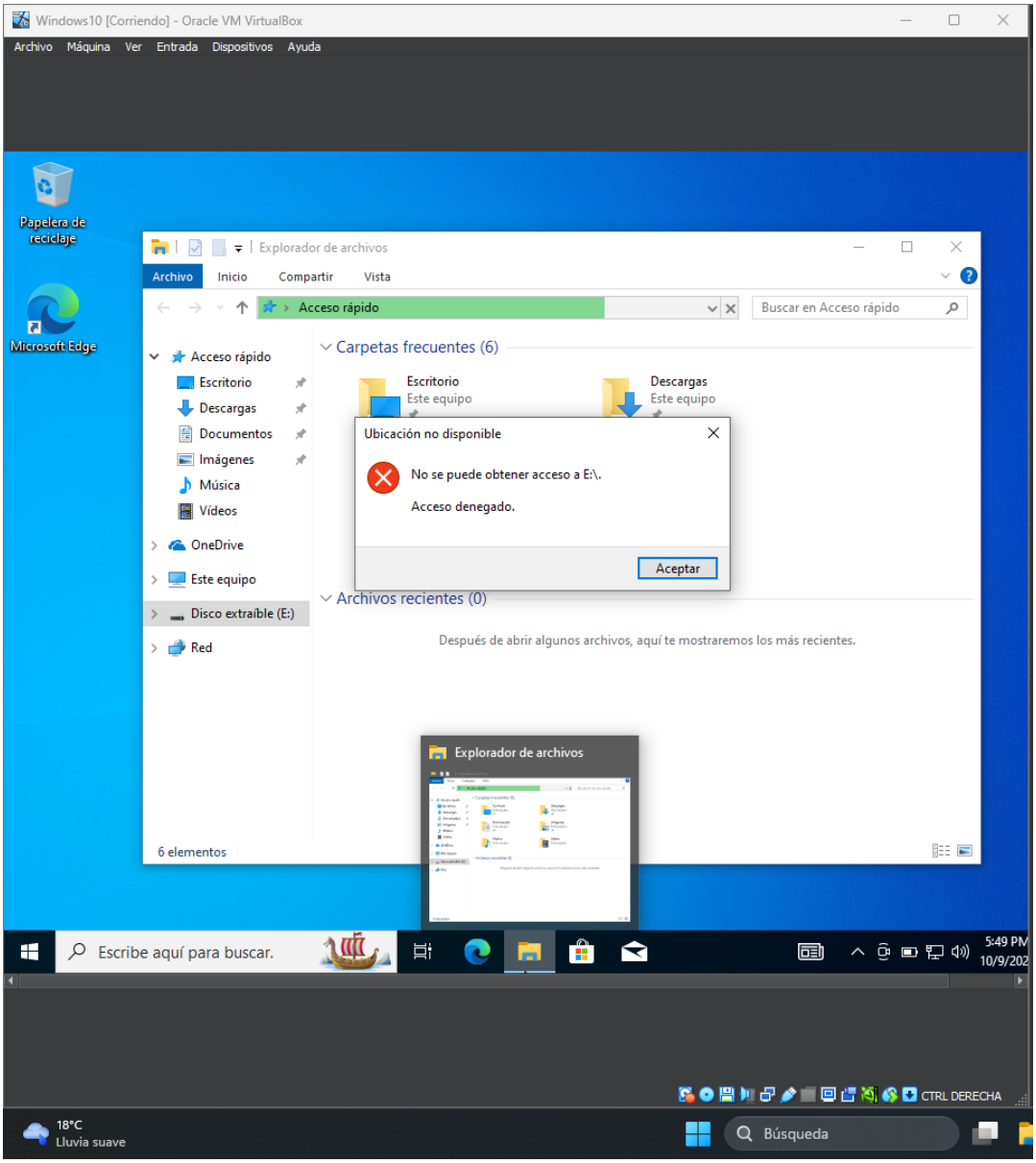
Educación y Concientización.

Capacitación del Personal:

- **Programa de Capacitación: Todos** los empleados recibirán una capacitación inicial sobre las políticas de seguridad y el manejo de datos sensibles al momento de su incorporación. Se realizarán sesiones de actualización anuales para revisar cambios en políticas y nuevas amenazas.
- **Concientización Continua:** Envío regular de boletines informativos sobre mejores prácticas de seguridad y casos recientes de violaciones de datos para mantener al personal informado y alerta.

Implementación de Políticas de restricción de Dispositivos USB.

Aquí adjuntamos captura del resultado esperado que era iniciar sesión con el nuevo usuario regular que en este caso es el usuario Rider28 y conecta el dispositivo USB para verificar que no tenga acceso debido a las restricciones aplicadas.


Windows10 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Papelera de reciclaje
Microsoft Edge
Explorador de archivos
Archivo Inicio Compartir Vista
Acceso rápido
Buscar en Acceso rápido
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
OneDrive
Este equipo
Disco extraíble (E:)
Red
Carpetas frecuentes (6)
Escritorio
Este equipo
Descargas
Este equipo
Ubicación no disponible
No se puede obtener acceso a E:\.
Acceso denegado.
Aceptar
Archivos recientes (0)
Después de abrir algunos archivos, aquí te mostraremos los más recientes.
6 elementos
Explorador de archivos
Escribe aquí para buscar.
5:49 PM
10/9/202
CTRL DERECHA
18°C
Lluvia suave
Búsqueda