4GeeksAcademy

Implementa Políticas de Seguridad DLP a dispositivos de almacenamiento externo

Introducción al Data Loss Prevention (DLP)

La Prevención de Pérdida de Datos (DLP) es un conjunto de herramientas y procesos diseñados para detectar y prevenir el uso y transmisión no autorizados de información sensible. DLP es crucial en el panorama digital actual por varias razones:

1. **Protección de Datos Sensibles**: DLP ayuda a las organizaciones a salvaguardar su activo más valioso - la información.
2. **Cumplimiento**: Muchas industrias están sujetas a regulaciones que requieren la protección de tipos específicos de datos.
3. **Gestión de la Reputación**: Las filtraciones de datos pueden dañar severamente la reputación de una organización y la confianza del cliente.
4. **Mitigación de Amenazas Internas**: DLP puede ayudar a prevenir fugas de datos tanto accidentales como intencionales por parte de los empleados.

Clasificación de datos.

La implementación de un programa de DLP es efectivo y crucial para así poder establecer un esquema de clasificación de datos basado en el nivel de sensibilidad, importancia y criticidad. La organización adoptará las siguientes tres categorías de clasificación:

1. Datos Públicos

Aquella información que cualquiera pueda acceder y ser compartida libremente con el público sin ningún tipo de riesgo que pueda afectar a la empresa.

- Ejemplos: Comunicados de prensa, contenido del sitio web, redes sociales, anuncios de marketing.

2. Datos Internos

Esta información está destinada únicamente para uso interno dentro de la empresa esta no puede ser compartida ni filtrada con otros organismos que no sean de los empresa.

Ejemplos: Políticas internas, procedimientos operativos, reportes internos no confidenciales, verificación de dos factores

3. Datos Sensibles

Toda la información a partir de aquí es crítica que, es decir en caso de ser divulgada, podría provocar daños significativos a la organización, personal y clientes.

- Ejemplos: Datos financieros, información personal identificable (PII), propiedad intelectual, datos protegidos por normativas como GDPR o HIPAA.

Acceso y Control

Principio del Menor Privilegio

Para ello aplicaremos el principio del menor privilegio, asegurando que tanto los empleados y los colaboradores tengan acceso únicamente a los datos necesarios que vayan a necesitar para desempeñar sus funciones.

Políticas de Acceso

1. **Asignación de los permisos según la clasificación de importancia**: Estos permisos de acceso serán asignados en función de roles y responsabilidades que vayan a necesitar y de manera temporal según un tiempo de momento justo.
2. **Revisión periódica del sistema**: Todos los permisos de acceso otorgados a los empleados serán revisados periódicamente según las necesidades por los administradores de sistemas y monitoreados por sus superiores de cada área correspondiente.
3. **Roles Responsables**:
    - **Administrador de Seguridad**: Configuración inicial del sistema y revisión de los permisos otorgados a cada uno de los distintos empleados.
    - **Personal de monitoreo y validación de credenciales**: Validación de accesos necesarios para su equipo.

Revisión periódica de los movimientos.

1. Solicitud de acceso por parte del personal.
2. Evaluación continua por el administrador de seguridad.
3. Aprobación de solicitudes de acceso por el personal de monitoreo y validación de credenciales.
4. Auditoría de accesos y ajustes de los permisos si es necesario ser modificados de manera temporal.

Monitoreo y Auditoría

Reglas de Monitoreo

1. Monitoreo continuo por parte del personal encargado de la actividad en torno a datos clasificados como sensibles que puedan comprometer la estructura de la empresa y su seguridad.
2. Generación de alertas de manera automática ante accesos sospechosos o no permitidos además de intentos de extracción de datos independientemente de si es un empleado para llevar un registro adecuado de esto.

Herramientas Utilizadas

- **Soluciones SIEM (Security Information and Event Management)**: Para recopilar y analizar eventos relacionados con la seguridad.
- **Herramientas DLP Específicas**: Soluciones como Symantec DLP o Microsoft Information Protection para poder así monitorear el uso, transferencia y almacenamiento de datos sensibles.

Auditorías Periódicas

1. Auditorías periódicas para verificar el cumplimiento de las políticas y el pleno funcionamiento de estas manera correcta.

2. Informes detallados de cada uno de los registros y movimientos realizados serán enviados a los altos cargos de dirección y equipos responsables de estos.

Prevención de Filtraciones

Tecnologías Implementadas

1. **Cifrado**:
    - Todos los datos sensibles que se comparta y el rastro o movimientos que dejen serán cifrados utilizando algoritmos robustos como AES-256.
2. **Control de Dispositivos**:
    - Restricción del intento de conexión de dispositivos externos no autorizados o de aquellos nuevos que no posean las credenciales necesarias para acceder a sectores específicos de información.
3. **Herramientas DLP**:
    - Bloqueo automático de intentos no autorizados de acceso o de transferir datos sensibles a plataformas externas, ajenos o que estas no estén en la lista de de acceso permitido por parte de la empresa.

Educación y Concientización

Capacitación del Personal

1. **Programas Iniciales**:
    - Todos los empleados recibirán una formación inicial sobre las diferentes políticas de DLP al momento de su incorporación, además en caso necesario de aparecer nuevas políticas serán necesarias para todo el equipo.
2. **Entrenamientos Periódicos**:

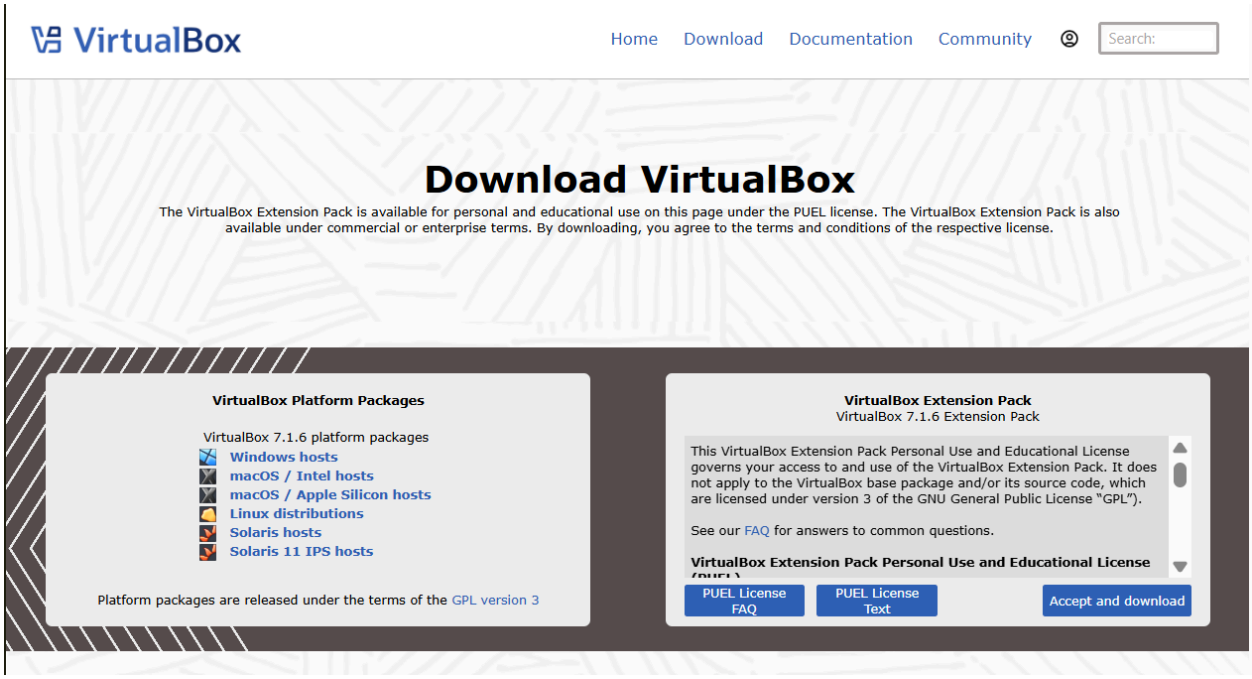
- Se realizarán sesiones periódicas de nuevas actualizaciones sobre nuevas medidas de seguridad de la información y de manejo de nuevas funciones de las distintas herramientas usadas.

Estrategias de Concientización

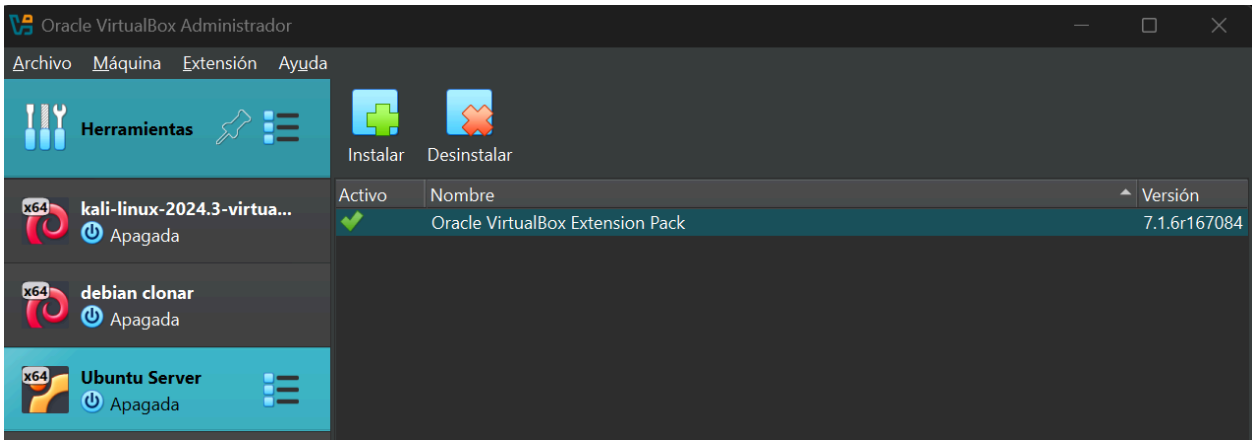
1. **Campañas Internas**:
   - Charlas concienciativas y pósters con recomendaciones de buenas prácticas.
2. **Simulaciones de Incidentes**:
   - Realizar ejercicios prácticos similares a casos reales para poder así identificar y responder a posibles amenazas relacionadas con fugas de datos.

Como instalar

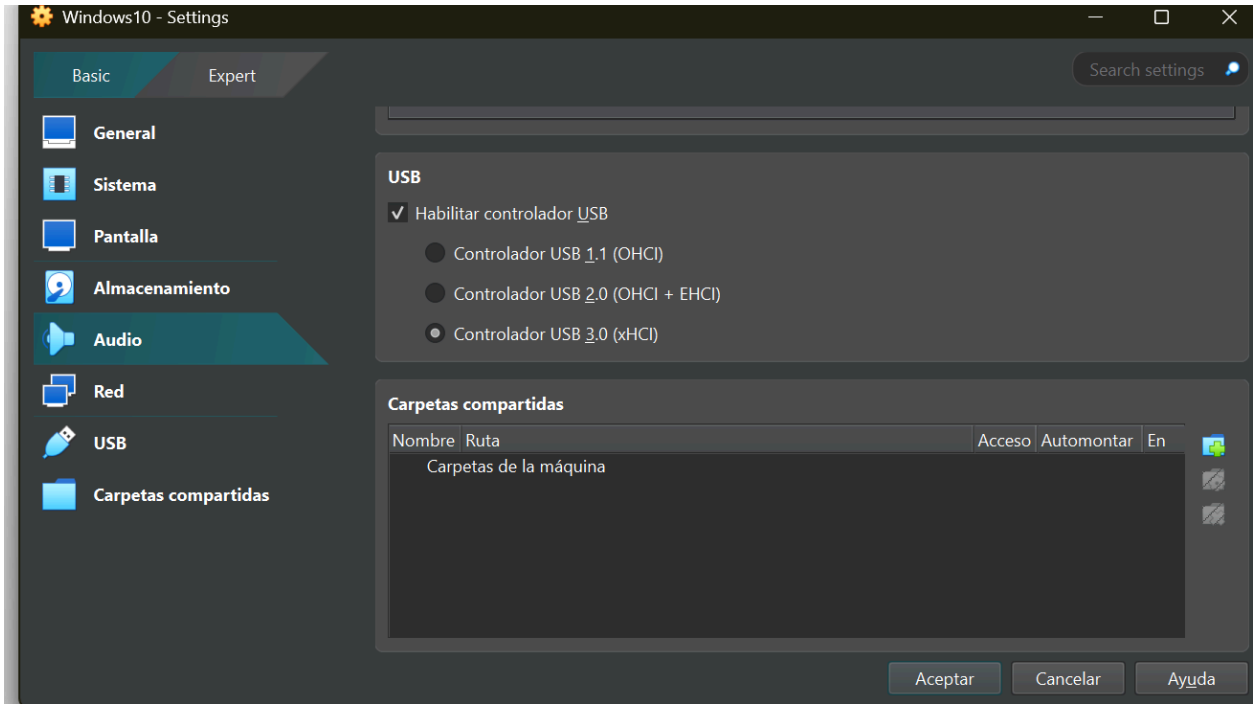
Primero vamos a la página web y descargamos la extensión



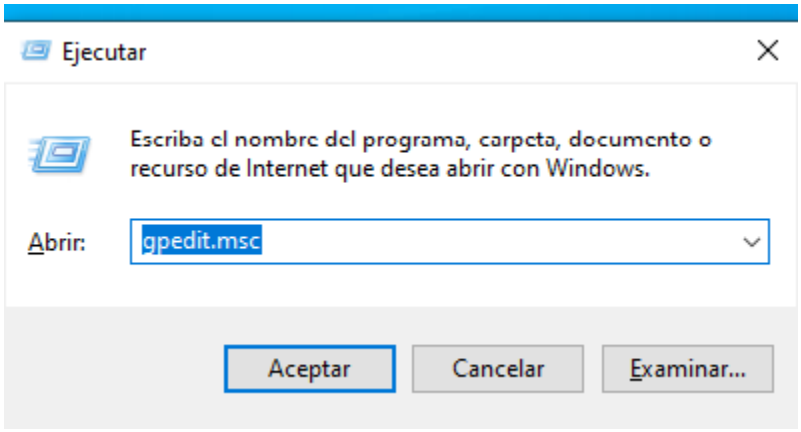
La instalamos



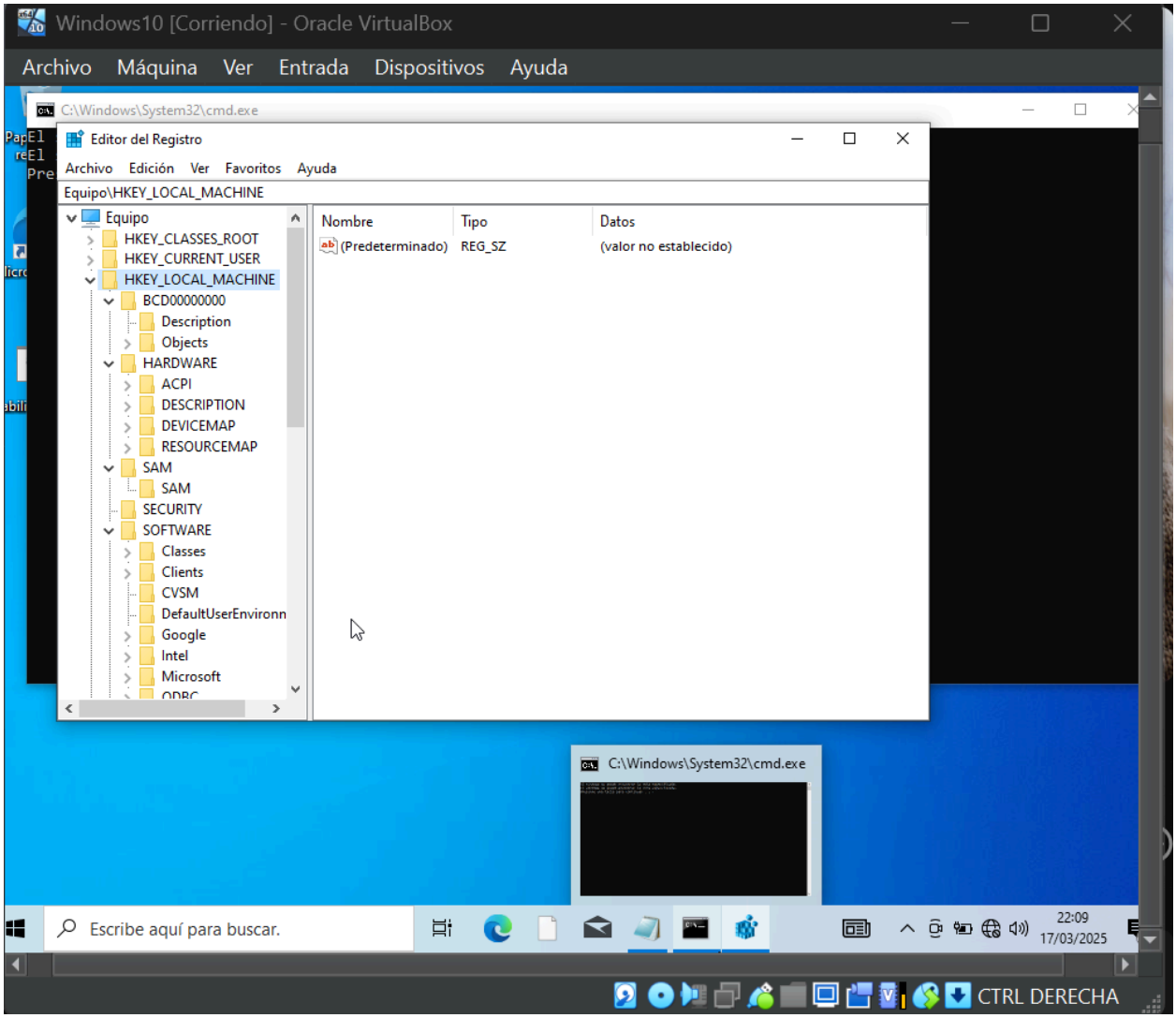
Tras esto configuramos las opciones de adaptar como nos pide la práctica



Accedemos a la máquina y colocamos el comando

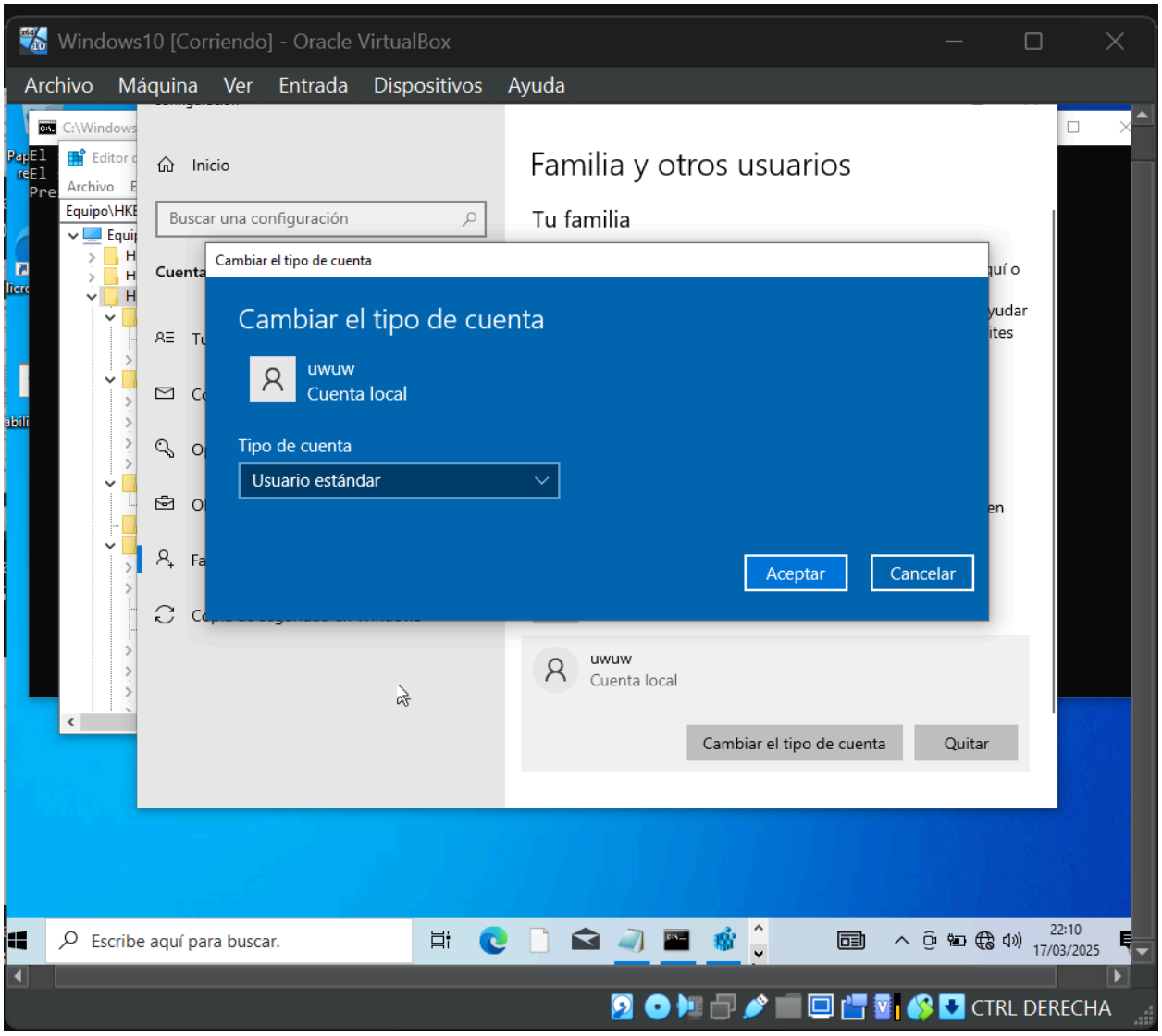


Al ser windows10 home no deja la opción pero solo sería acceder al comando anterior y realizar los permisos de ajustes.



Esta sería de otra manera pero paso lo mismo al ser windows10 home no deja realizar estas configuraciones.

El último paso sería crear la configuración de los permisos que tenga este usuario para así evitar que este pueda usar el arranque a través de usb y asignarle los permisos a este.


Windows10 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Inicio
Buscar una configuración
Familia y otros usuarios
Tu familia
Cambiar el tipo de cuenta
Cambiar el tipo de cuenta
uwuw
Cuenta local
Tipo de cuenta
Usuario estándar
Aceptar
Cancelar
uwuw
Cuenta local
Cambiar el tipo de cuenta
Quitar
Escribe aquí para buscar.
22:10
17/03/2025
CTRL DERECHA