IMPLEMENTACION DE POLITICAS DE SEGURIDAD DLP

TECH CORP INC.

Introducción al Data Loss Prevention (DLP)

El Data Loss Prevention (DLP) es un conjunto de estrategias, herramientas y procesos diseñados para prevenir la pérdida, el uso no autorizado o la divulgación indebida de datos confidenciales dentro de una organización. Su importancia radica en la necesidad de proteger información crítica, como datos personales, financieros y propiedad intelectual, evitando riesgos que puedan comprometer la seguridad y cumplimiento normativo de la empresa.

Las soluciones DLP permiten monitorear, detectar y controlar el flujo de datos en redes, dispositivos y aplicaciones, asegurando que la información crítica permanezca dentro de la organización y solo sea accesible por usuarios autorizados.

Clasificación de Datos

Para garantizar una protección adecuada de la información, los datos serán clasificados en las siguientes categorías:

1. **Datos Públicos**: Información que puede ser divulgada sin restricciones, como material promocional, comunicados de prensa y contenido publicado en la página web corporativa.
2. **Datos Internos**: Datos cuyo acceso está restringido a empleados y colaboradores autorizados. Incluye documentos de trabajo, procedimientos internos y reportes operativos.
3. **Datos Sensibles**: Información crítica que requiere protección adicional, como datos personales de clientes y empleados, información financiera, propiedad intelectual y estrategias comerciales confidenciales.

Acceso y Control

Siguiendo el principio del menor privilegio, se establecerán políticas de acceso que permitan a los usuarios acceder solo a los datos estrictamente necesarios para el desempeño de sus funciones.

- **Asignación de permisos**: Se definirán roles y responsabilidades dentro de la organización para la asignación y revisión de permisos.
- **Revisión periódica**: Se llevará a cabo una auditoría trimestral para evaluar los accesos y eliminar permisos innecesarios.
- **Roles responsables**: El equipo de seguridad de la información y los administradores de sistemas serán responsables de gestionar y auditar los permisos de acceso.

Monitoreo y Auditoría

Se implementarán herramientas especializadas para el monitoreo continuo del uso de datos sensibles. Entre ellas:

- **Sistemas SIEM (Security Information and Event Management)**: Para la recolección y análisis de eventos de seguridad en tiempo real.
- **Soluciones DLP**: Para la detección y prevención de fugas de información mediante el monitoreo de correos electrónicos, almacenamiento en la nube y dispositivos extraíbles.
- **Registros de auditoría**: Se mantendrán logs detallados de accesos y modificaciones a datos sensibles para su revisión periódica.

Prevención de Filtraciones

Para evitar la pérdida o fuga de datos, se aplicarán las siguientes medidas:

- **Cifrado de datos**: Los datos sensibles serán cifrados tanto en reposo como en tránsito.
- **Restricciones en almacenamiento y transferencia**: Se prohibirá el uso de dispositivos USB y se establecerán restricciones para compartir información a través de servicios en la nube no autorizados.
- **Políticas de seguridad en dispositivos**: Se implementará el uso de autenticación multifactor (MFA) y acceso controlado en dispositivos corporativos.

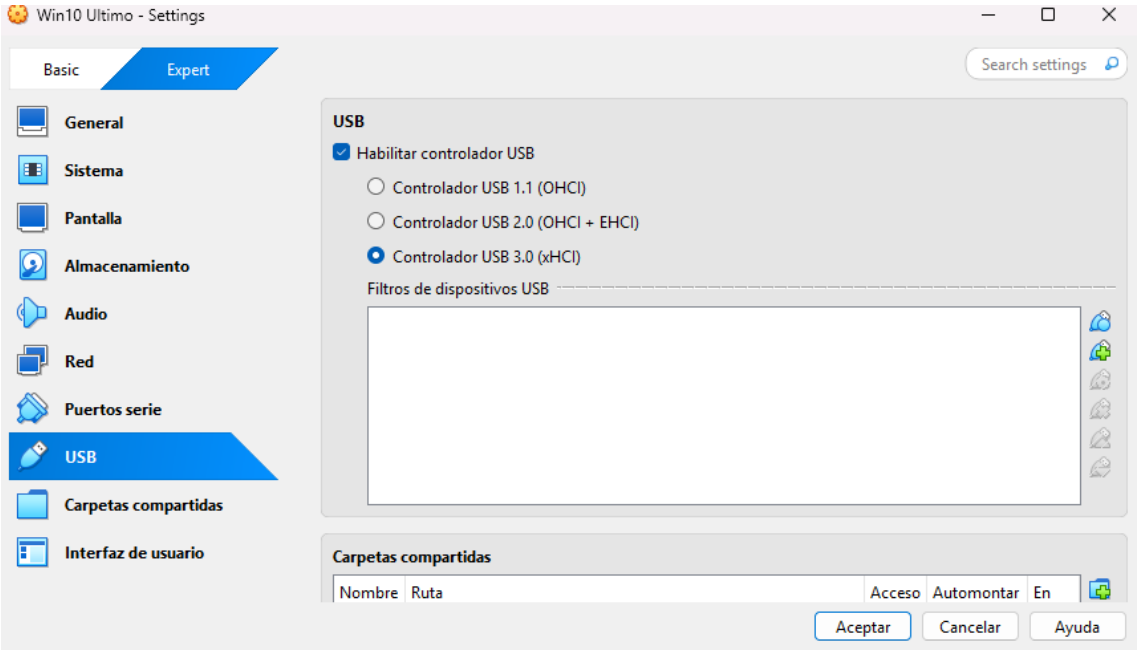
Educación y Concientización

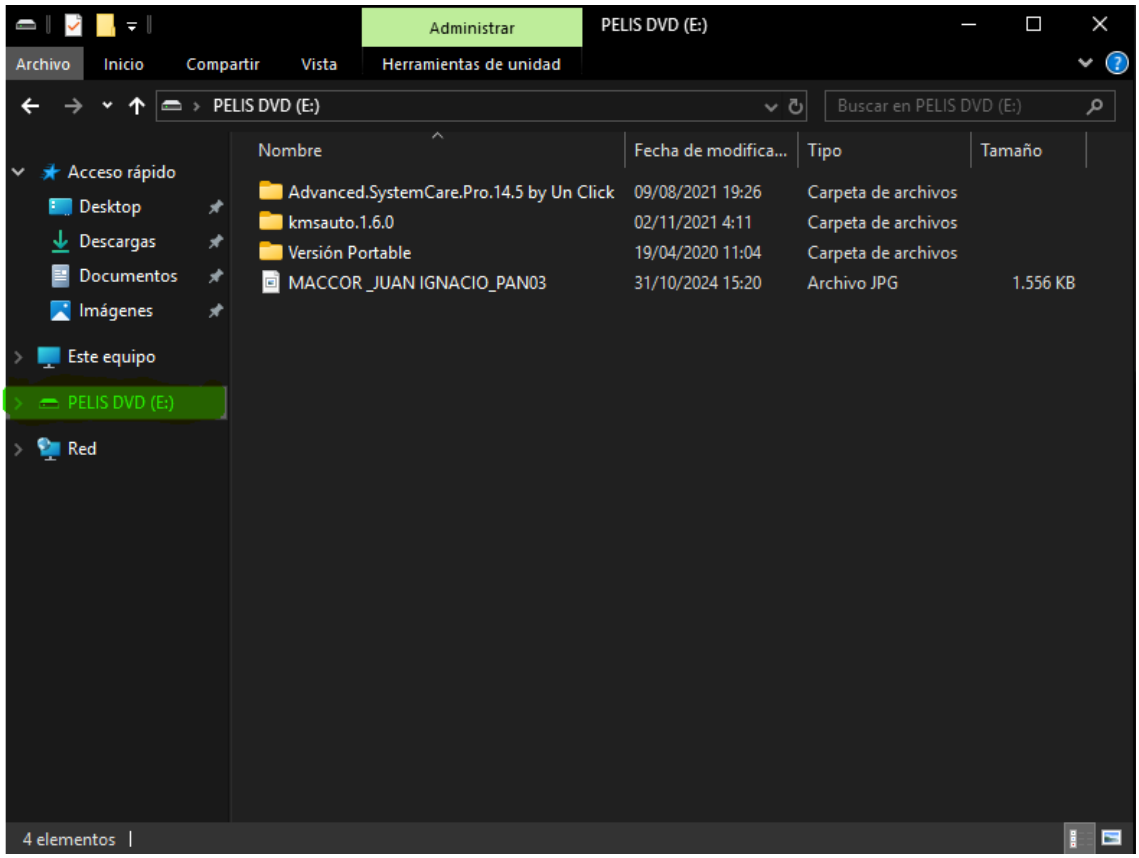
La capacitación del personal es fundamental para garantizar el cumplimiento de las políticas de seguridad. Para ello, se desarrollarán:

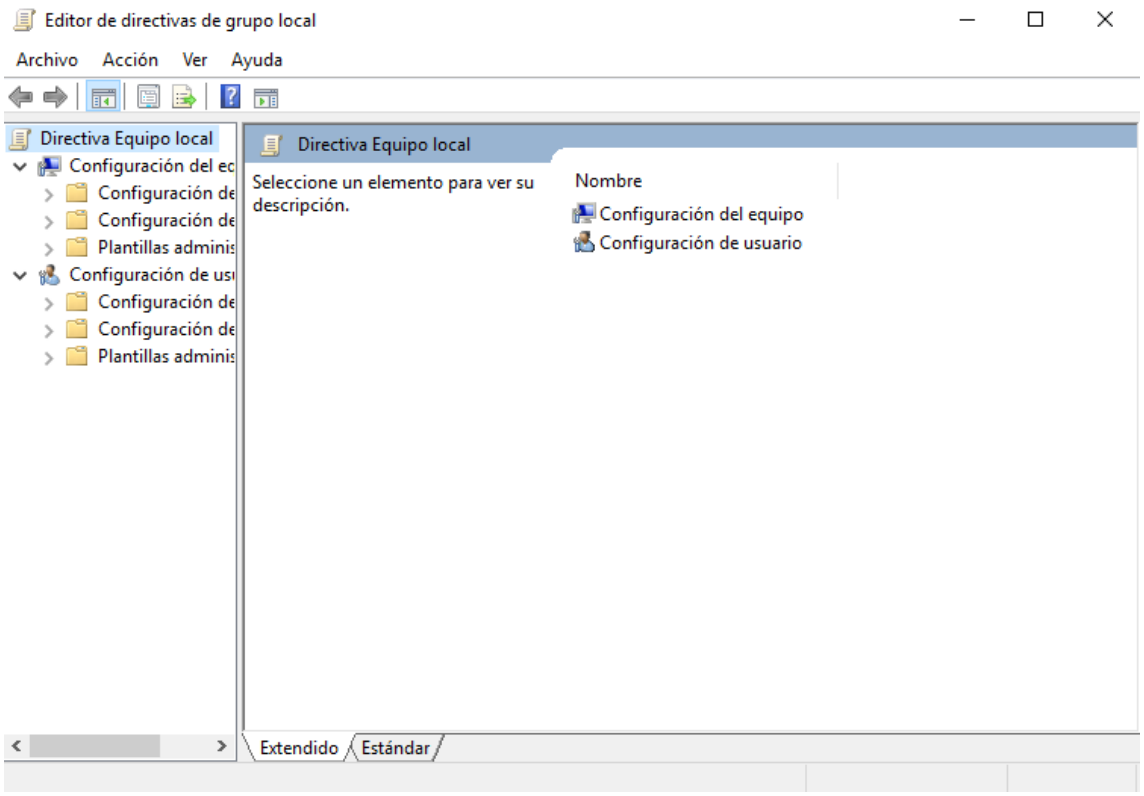
- **Talleres y cursos**: Se impartirán capacitaciones periódicas sobre seguridad de la información y concientización en riesgos de ciberseguridad.
- **Simulaciones de phishing**: Para evaluar y mejorar la capacidad de los empleados en la identificación de amenazas.
- **Políticas de seguridad accesibles**: Se proporcionará documentación clara sobre el manejo de datos y procedimientos de seguridad.

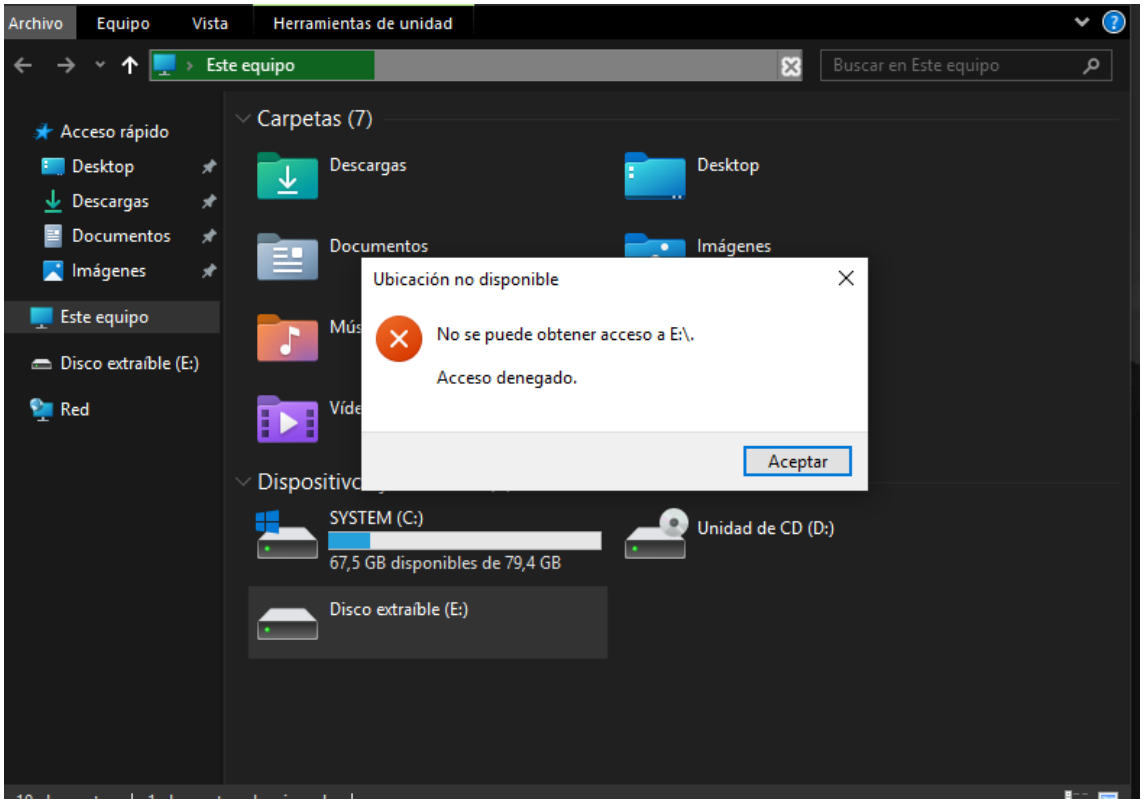
Con estas medidas, la organización asegurará la protección de su información crítica, minimizando riesgos de filtraciones y garantizando el cumplimiento de normativas de seguridad.

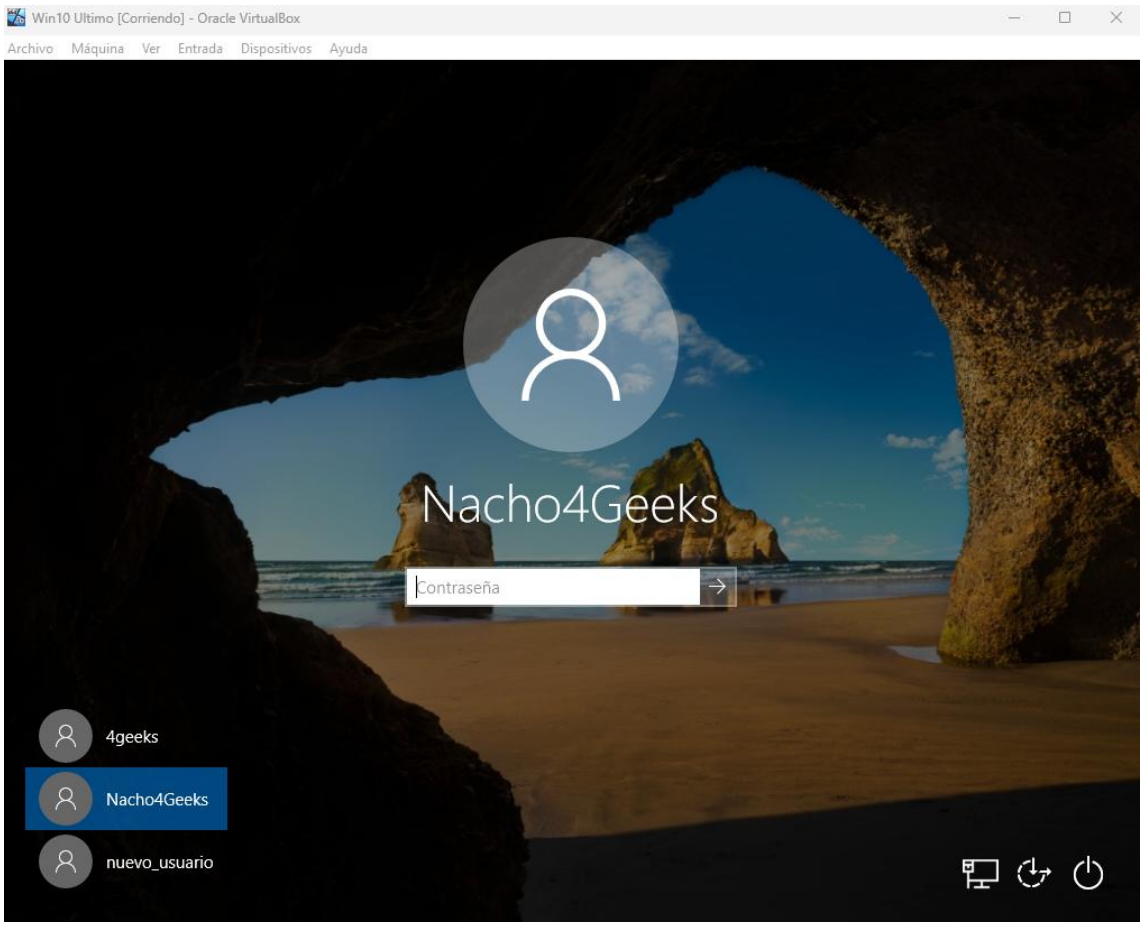
Configuracion de una Maquina para el acceso al usb

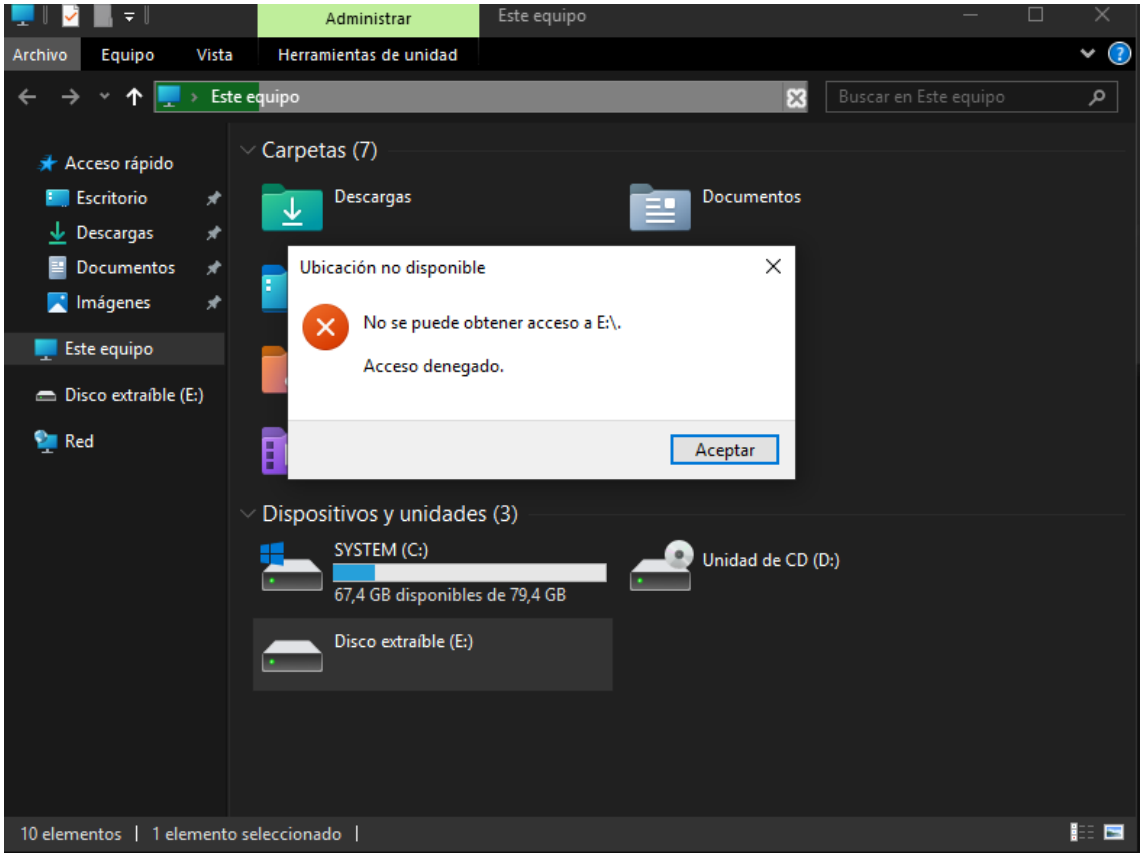





Editor de directivas de grupo local
Archivo
Acción
Ver
Ayuda
Directiva Equipo local
Configuración del ec
Configuración de
Configuración de
Plantillas adminis
Configuración de us
Configuración de
Configuración de
Plantillas adminis
Directiva Equipo local
Seleccione un elemento para ver su descripción.
Nombre
Configuración del equipo
Configuración de usuario
Extendido
Estándar


Archivo
Equipo
Vista
Herramientas de unidad
Este equipo
Buscar en Este equipo
Acceso rápido
Desktop
Descargas
Documentos
Imágenes
Este equipo
Disco extraíble (E:)
Red
Carpetas (7)
Descargas
Desktop
Documentos
Imágenes
Ubicación no disponible
No se puede obtener acceso a E:\.
Acceso denegado.
Aceptar
SYSTEM (C:)
67,5 GB disponibles de 79,4 GB
Unidad de CD (D:)
Disco extraíble (E:)


Win10 Ultimo [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Nacho4Geeks
Contraseña
4geeks
Nacho4Geeks
nuevo_usuario


Administrar
Este equipo
Archivo Equipo Vista Herramientas de unidad
Este equipo
Buscar en Este equipo
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
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 (3)
SYSTEM (C:)
67,4 GB disponibles de 79,4 GB
Unidad de CD (D:)
Disco extraíble (E:)
10 elementos | 1 elemento seleccionado |