DLP Security Policies

Part 1: Define and Establish DLP Security Policies

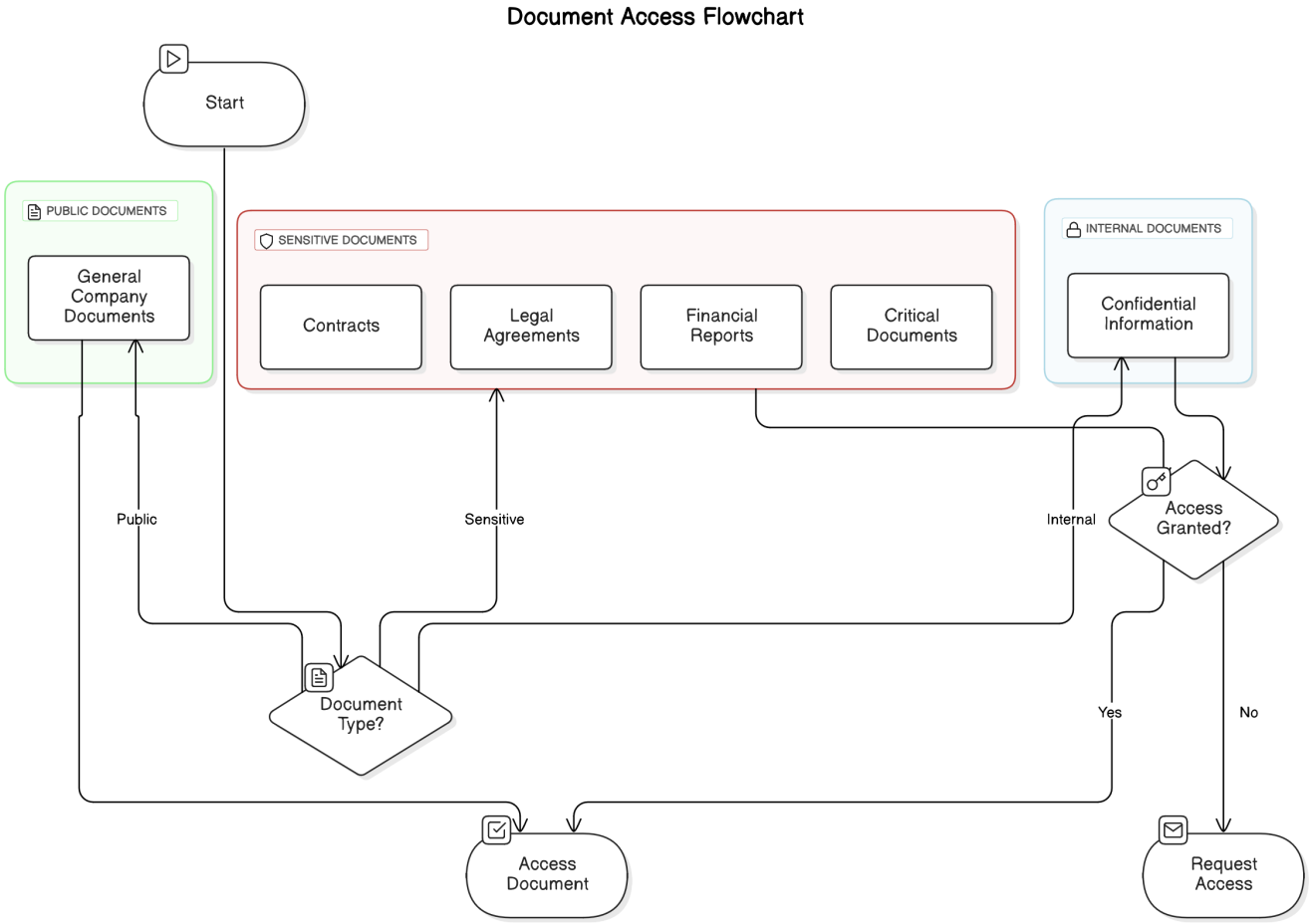
Introduction to Data Loss Prevention

Data Loss Prevention (DLP) is an essential security measure designed to protect sensitive or confidential data within an organization. It involves implementing policies, procedures, and technologies that aim to prevent the unauthorized disclosure of such information through various means like accidental leaks, cyber attacks, or insider threats.

DLP solutions help organizations monitor and control how they use data in real-time by analyzing metadata and content, identifying patterns of data misuse, and taking corrective actions. This ensures compliance with regulations and policies while protecting sensitive corporate assets from loss or misuse. Organizations that implement DLP policies can significantly reduce the risk of data breaches, thereby maintaining their reputation, complying with legal requirements, and safeguarding critical information.

Data Classification

To effectively manage access to Google Drive documents, TechCorp Solutions will classify its data into three categories based on sensitivity:



1. **Public Documents**: These are general company documents that are accessible by all employees within the organization.
2. **Internal Documents**: This category includes confidential information that is restricted to specific personnel and departments within TechCorp Solutions who have a legitimate business need for access.
3. **Sensitive Documents**: Highly sensitive data such as contracts, legal agreements, financial reports, and other critical documents will be protected with special measures and are only accessible to the most authorized personnel necessary.

Access and Control

Applying the Principle of Least Privilege is crucial when managing access to Google Drive files and folders. According to this principle, employees should have access only to data directly relevant to their job functions or projects.

- **Restricted Access**: Employees will be granted read-only permissions by default for all documents except those explicitly designated as needing editing rights.
- **Permission Review Workflow**:
    - **Quarterly Reviews**: All Google Drive files and folders will undergo a quarterly review process conducted jointly by IT staff, HR personnel, and compliance officers. The purpose of these reviews is to ensure that access levels remain aligned with employees' current roles, responsibilities, and the security policies in place.
- **Temporary Access**:
    - When temporary access to sensitive documents is required (e.g., for project work), formal authorization must be obtained through a well-defined approval process. Temporary access will have clear expiration dates or conditions under which it will automatically terminate.
- **Limited Editing Permissions**: Only direct supervisors and designated project managers can edit documents with editing permissions. Other employees will typically only have read-only access, except when explicitly required for their roles.

Monitoring and Auditing

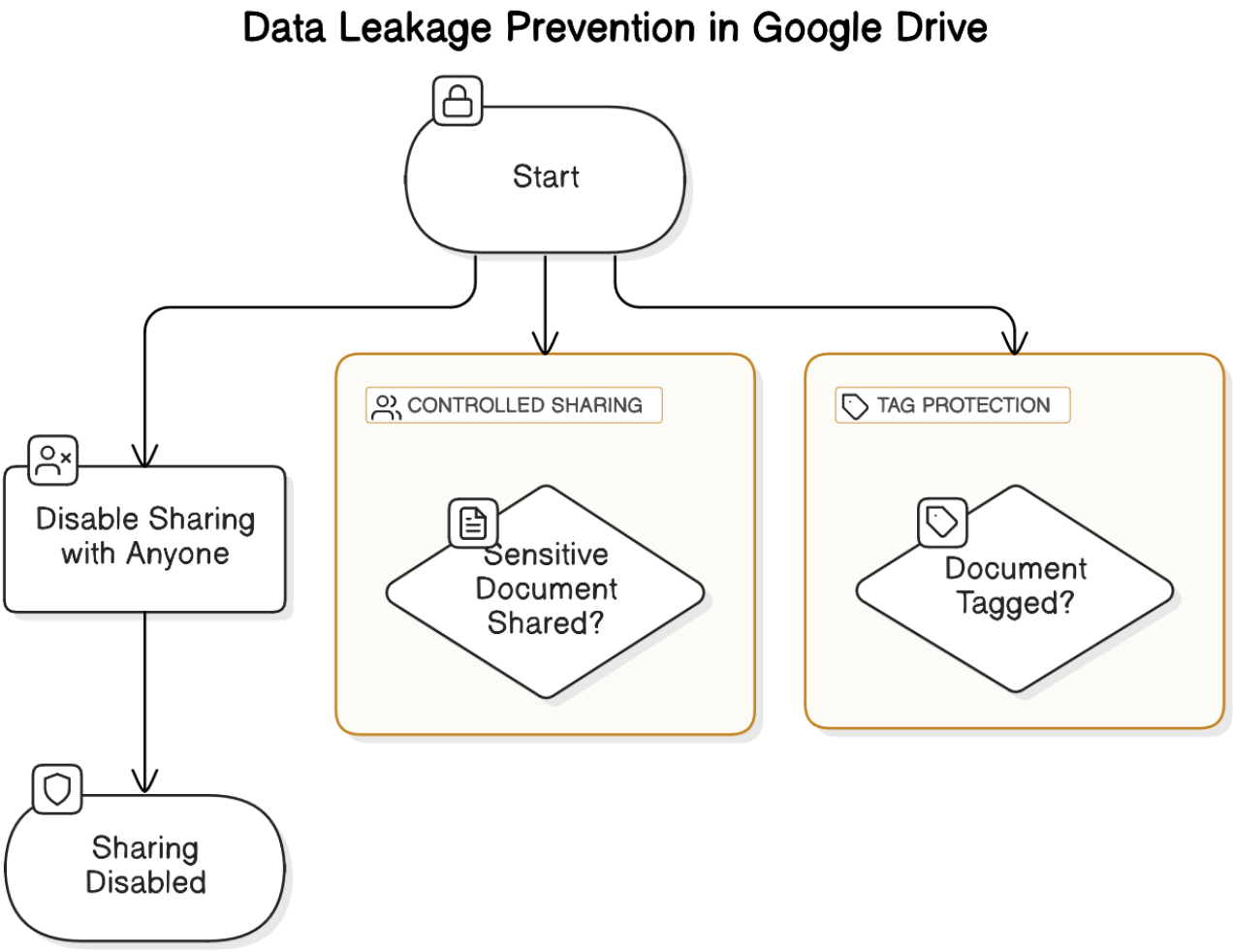
To detect unauthorized access attempts and monitor data usage patterns on Google Drive, TechCorp Solutions will implement the following:

- **Activity Logging**: Regular activity logs from Google Workspace features such as Drive, Gmail, or Cloud audit tools will be generated to track actions taken by employees within the Google ecosystem. These logs include information about file operations (e.g., access, edit, delete), emails sent and received, and other relevant activities.
- **Security Alerts**:
    - **Unauthorized Access**: Automated alerts will notify security personnel when sensitive documents are shared with unauthorized parties or external users without proper justification.
    - **Incorrect Permissions**: Alerts will also be triggered when inappropriate sharing permissions (e.g., "Anyone with the link") are set for sensitive files.

- **Regular Audits**:
    - **Quarterly Audits**: Compliance officers and IT security personnel will conduct quarterly audits of access rights to ensure that employees only have authorized access levels. During these audits, any discrepancies or potential risks will be identified and addressed promptly.

Leak Prevention

To prevent the unauthorized leakage of sensitive data from Google Drive:



- **Disable Sharing with Anyone**: By default, TechCorp Solutions will disable the option for users to share files or folders with anyone who has a link to them. This prevents accidental sharing or misuse of sensitive information.
- **Controlled Sharing**:
    - Sensitive documents can only be shared with approved personnel or partners using explicit read-only permissions.
    - Download and copy options are restricted for sensitive data unless explicitly allowed by an authorized user due to a legitimate need.
- **Tag Protection**: Documents classified as highly sensitive will carry a "Confidential" or "Internal Use Only" tag. These documents require special authorization to download, further securing them against

unauthorized access.

Education and Awareness

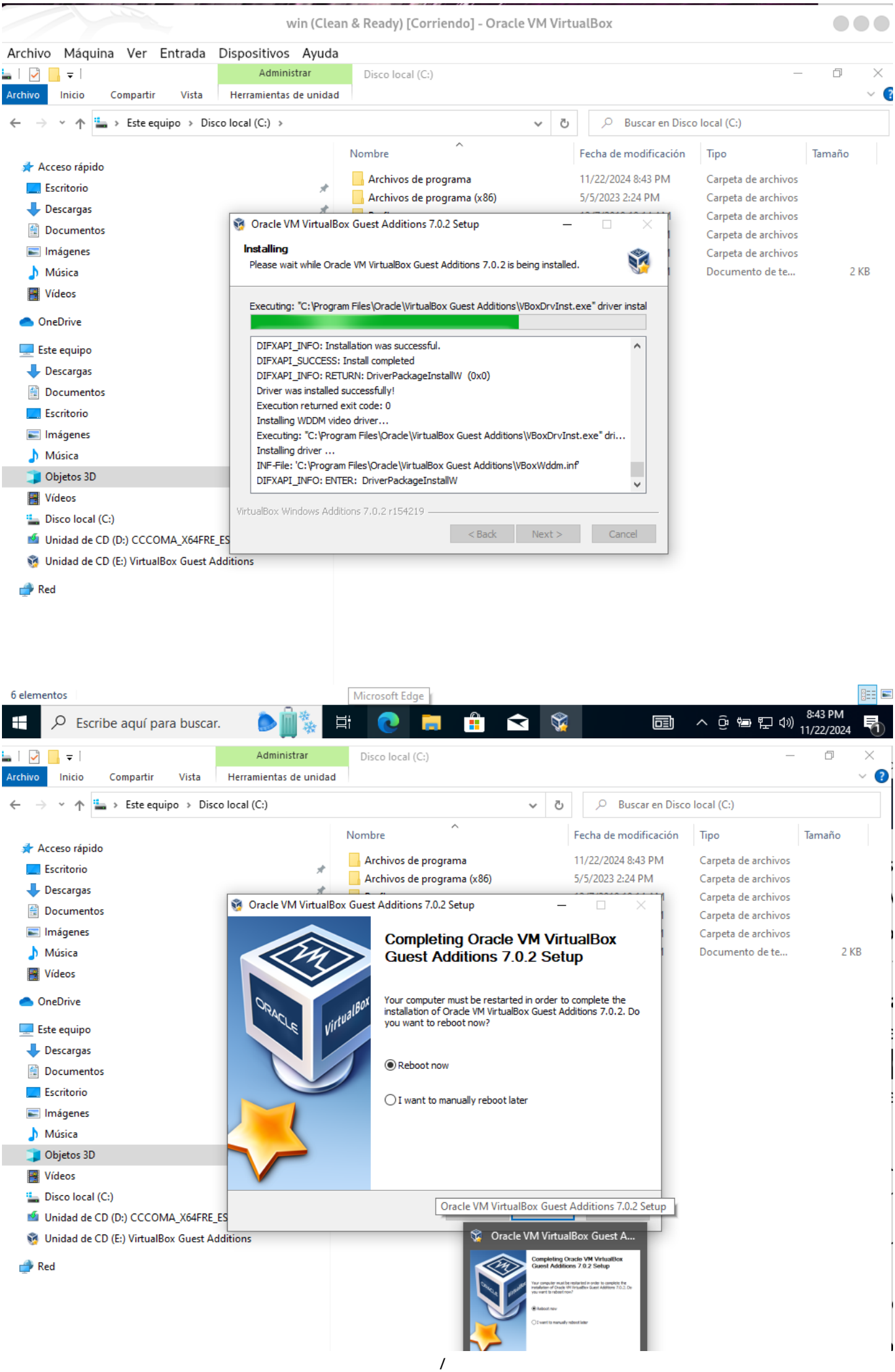
To ensure that employees understand the importance of security policies when using Google Drive:

- **Mandatory Training**:
    - Quarterly training sessions on DLP best practices will be conducted.
    - During these sessions, common incidents related to data leakage (e.g., sharing files with unintended recipients) will be presented along with practical examples and discussions.
- **Risk Awareness**: Trainees will learn about potential risks associated with poor security practices, such as accidental exposure of sensitive documents. They will also discuss how these risks can be mitigated effectively by adhering to DLP policies.

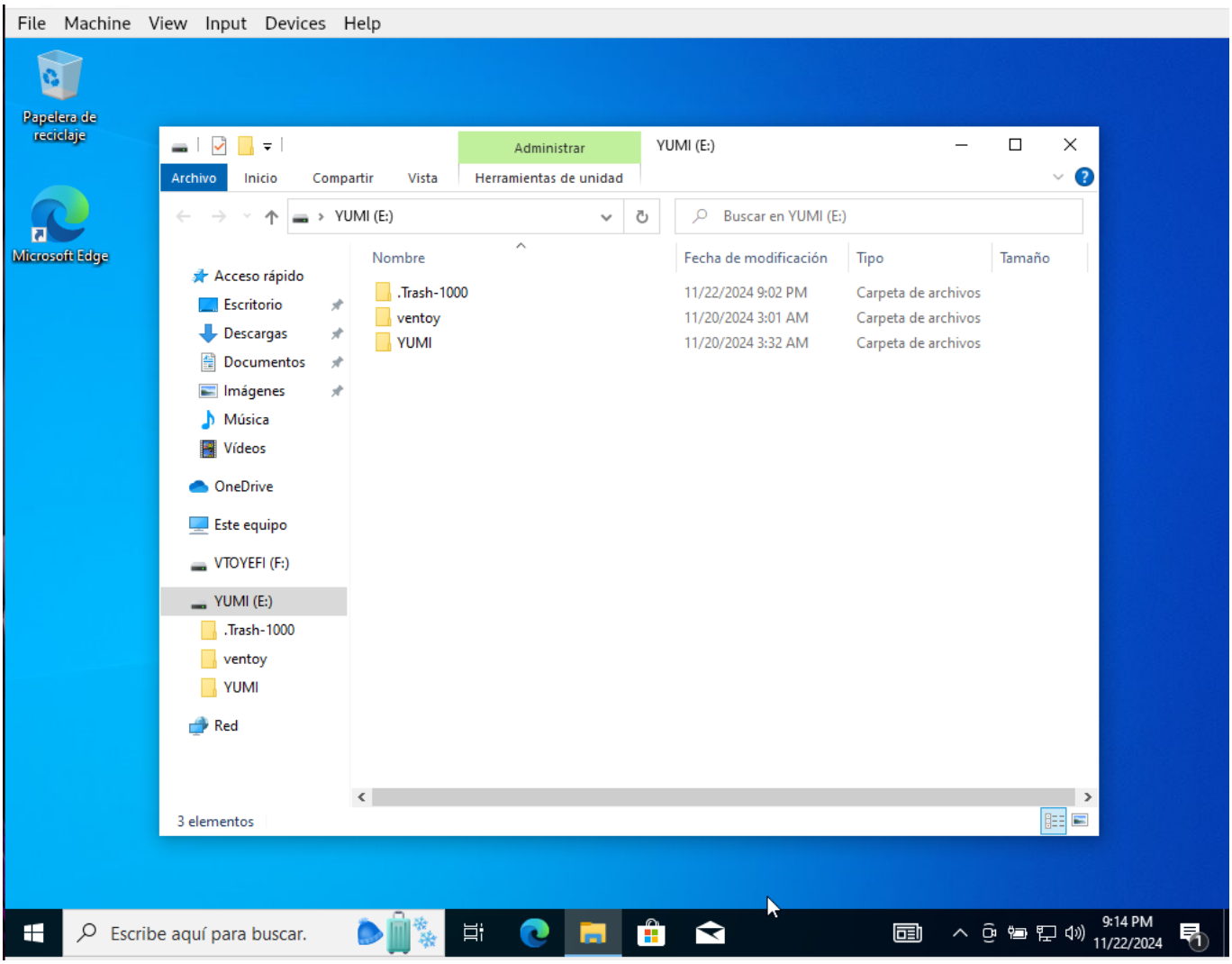
By following these guidelines, TechCorp Solutions aims to maintain a robust DLP framework that protects its most critical data while respecting the Principle of Least Privilege in its management and usage.

Part 2: Restrict the use of USB devices

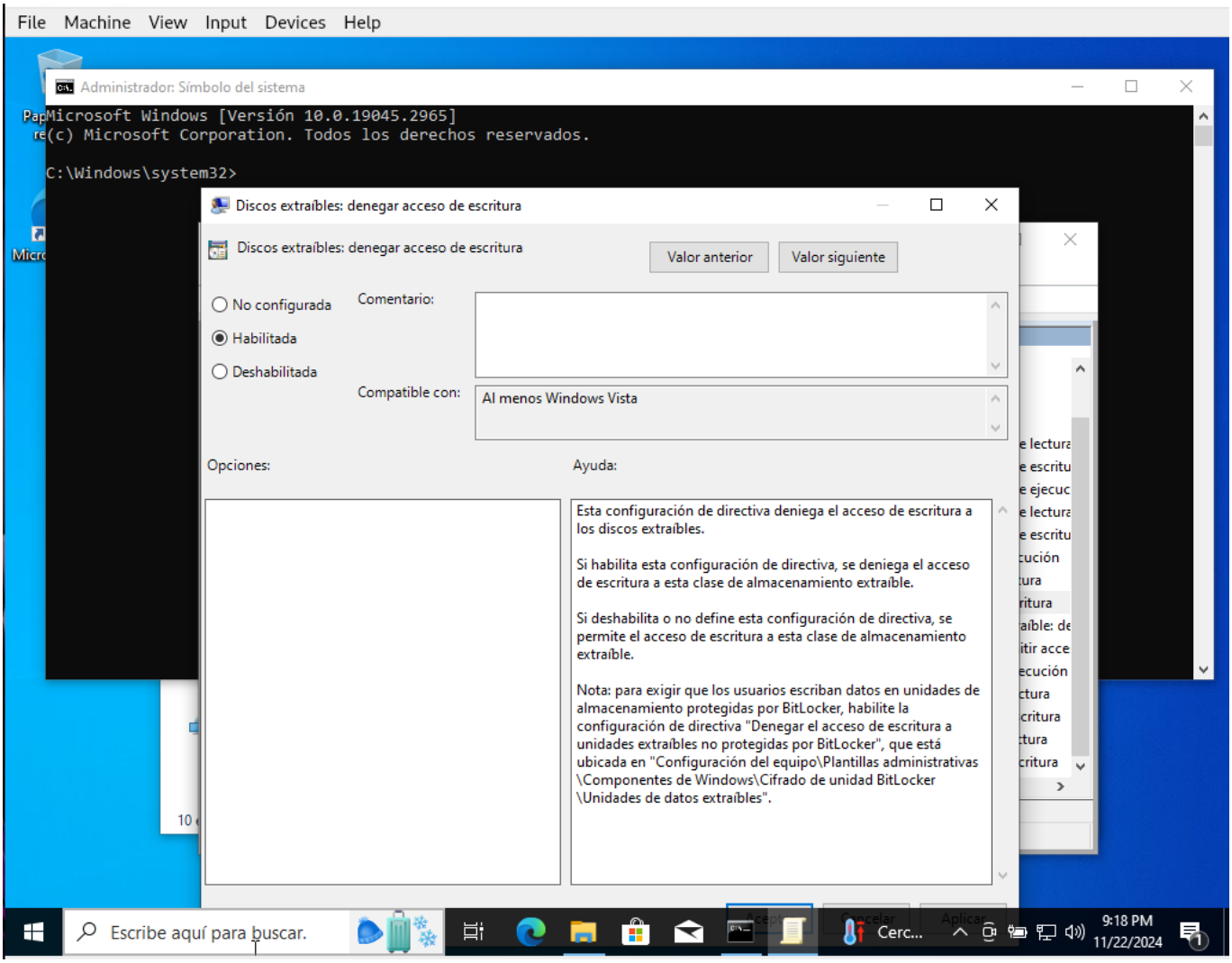
Guest Addition Install

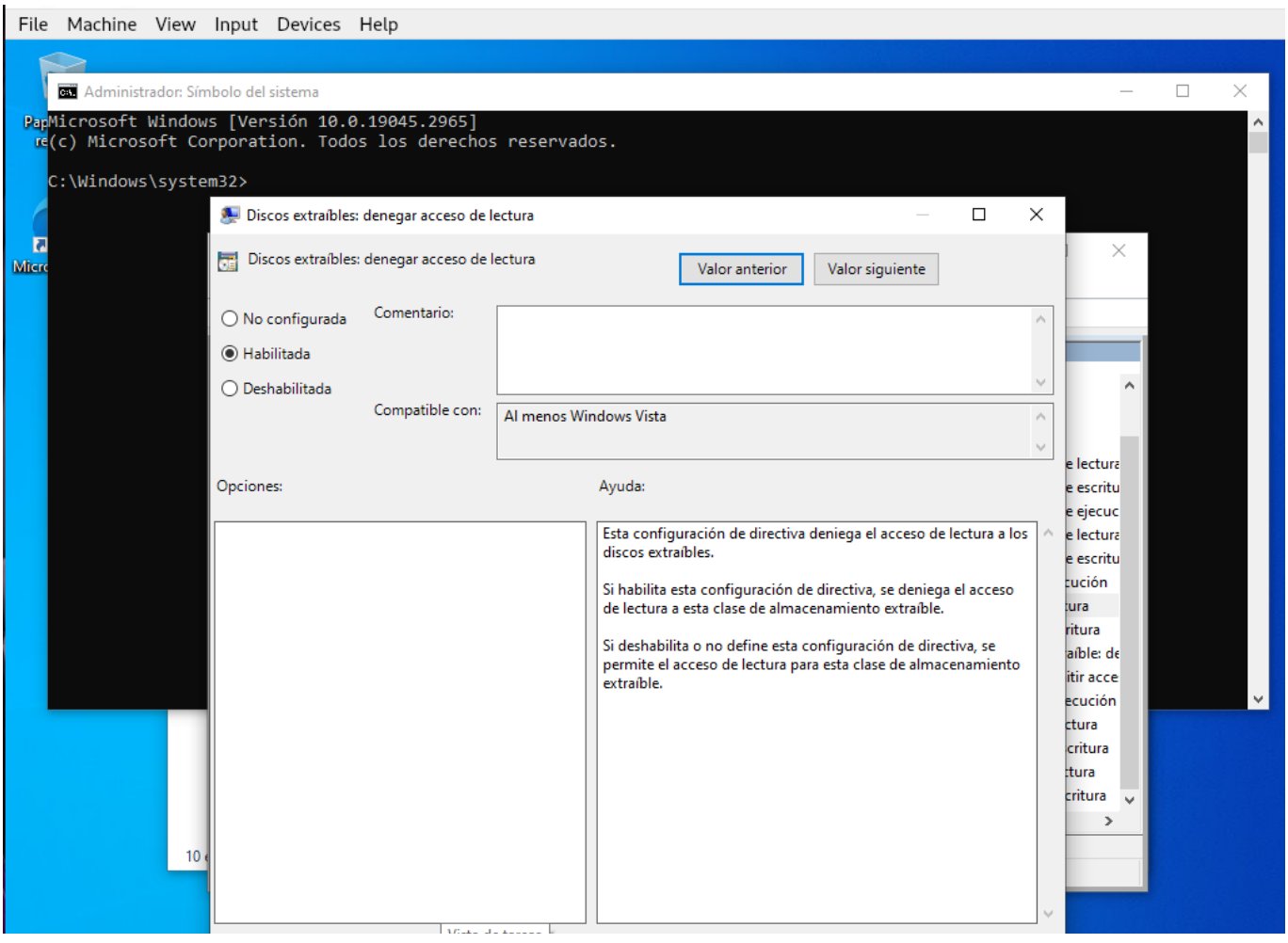

win (Clean & Ready) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrar
Disco local (C:)
Archivo Inicio Compartir Vista Herramientas de unidad
Este equipo › Disco local (C:) ›
Buscar en Disco local (C:)
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
OneDrive
Este equipo
Descargas
Documentos
Escritorio
Imágenes
Música
Objetos 3D
Vídeos
Disco local (C:)
Unidad de CD (D:) CCCOMA_X64FRE_ES
Unidad de CD (E:) VirtualBox Guest Additions
Red
Nombre
Fecha de modificación
Tipo
Tamaño
Archivos de programa
11/22/2024 8:43 PM
Carpeta de archivos
Archivos de programa (x86)
5/5/2023 2:24 PM
Carpeta de archivos
Documento de te...
2 KB
Oracle VM VirtualBox Guest Additions 7.0.2 Setup
Installing
Please wait while Oracle VM VirtualBox Guest Additions 7.0.2 is being installed.
Executing: "C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxDrvInst.exe" driver instal
DIFXAPI_INFO: Installation was successful.
DIFXAPI_SUCCESS: Install completed
DIFXAPI_INFO: RETURN: DriverPackageInstallW (0x0)
Driver was installed successfully!
Execution returned exit code: 0
Installing WDDM video driver...
Executing: "C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxDrvInst.exe" dri...
Installing driver ...
INF-File: 'C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxWddm.inf'
DIFXAPI_INFO: ENTER: DriverPackageInstallW
VirtualBox Windows Additions 7.0.2 r154219
< Back
Next >
Cancel
6 elementos
Microsoft Edge
Escribe aquí para buscar.
8:43 PM
11/22/2024
Oracle VM VirtualBox Guest Additions 7.0.2 Setup
Completing Oracle VM VirtualBox Guest Additions 7.0.2 Setup
Your computer must be restarted in order to complete the installation of Oracle VM VirtualBox Guest Additions 7.0.2. Do you want to reboot now?
Reboot now
I want to manually reboot later
Oracle VM VirtualBox Guest Additions 7.0.2 Setup
Oracle VM VirtualBox Guest A...

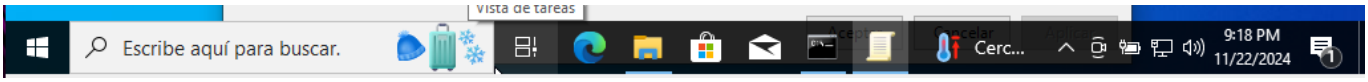
USB reconized



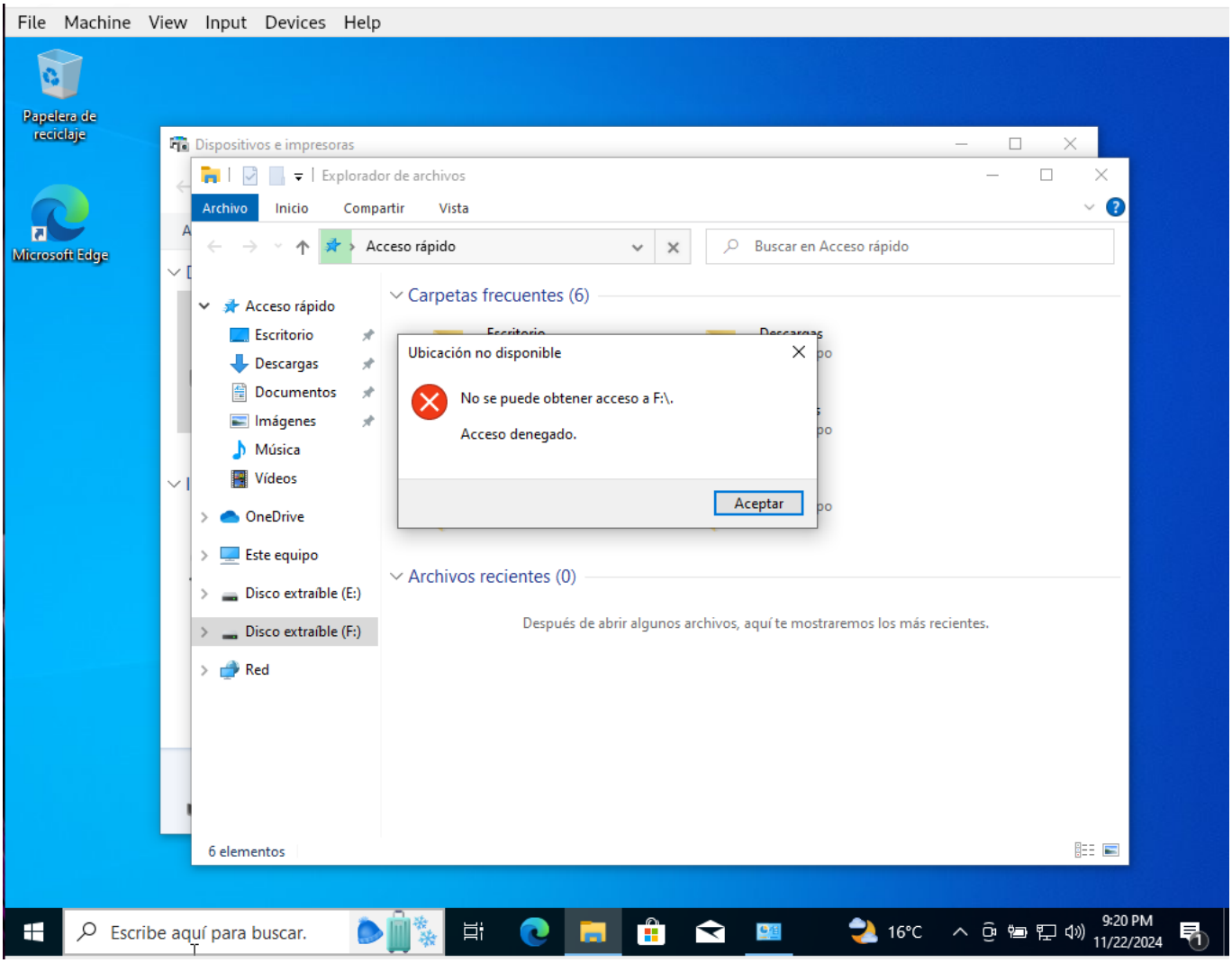
Restriction Config

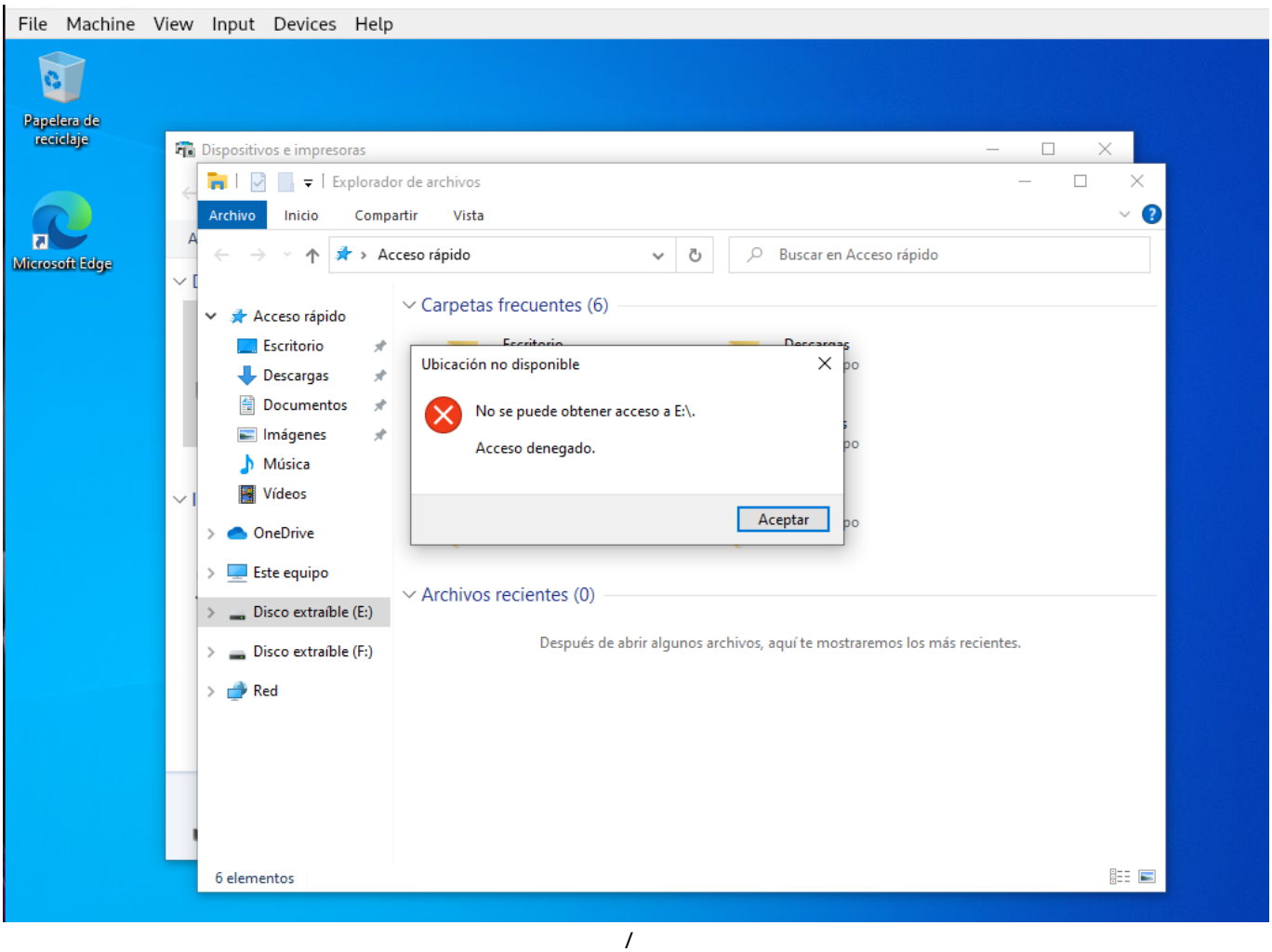

File Machine View Input Devices Help
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Windows\system32>
Discos extraíbles: denegar acceso de escritura
Discos extraíbles: denegar acceso de escritura
Valor anterior
Valor siguiente
No configurada
Habilitada
Deshabilitada
Comentario:
Compatible con:
Al menos Windows Vista
Opciones:
Ayuda:
Esta configuración de directiva deniega el acceso de escritura a los discos extraíbles.
Si habilita esta configuración de directiva, se deniega el acceso de escritura a esta clase de almacenamiento extraíble.
Si deshabilita o no define esta configuración de directiva, se permite el acceso de escritura a esta clase de almacenamiento extraíble.
Nota: para exigir que los usuarios escriban datos en unidades de almacenamiento protegidas por BitLocker, habilite la configuración de directiva "Denegar el acceso de escritura a unidades extraíbles no protegidas por BitLocker", que está ubicada en "Configuración del equipo\Plantillas administrativas\Componentes de Windows\Cifrado de unidad BitLocker\Unidades de datos extraíbles".
Escribe aquí para buscar.
9:18 PM
11/22/2024

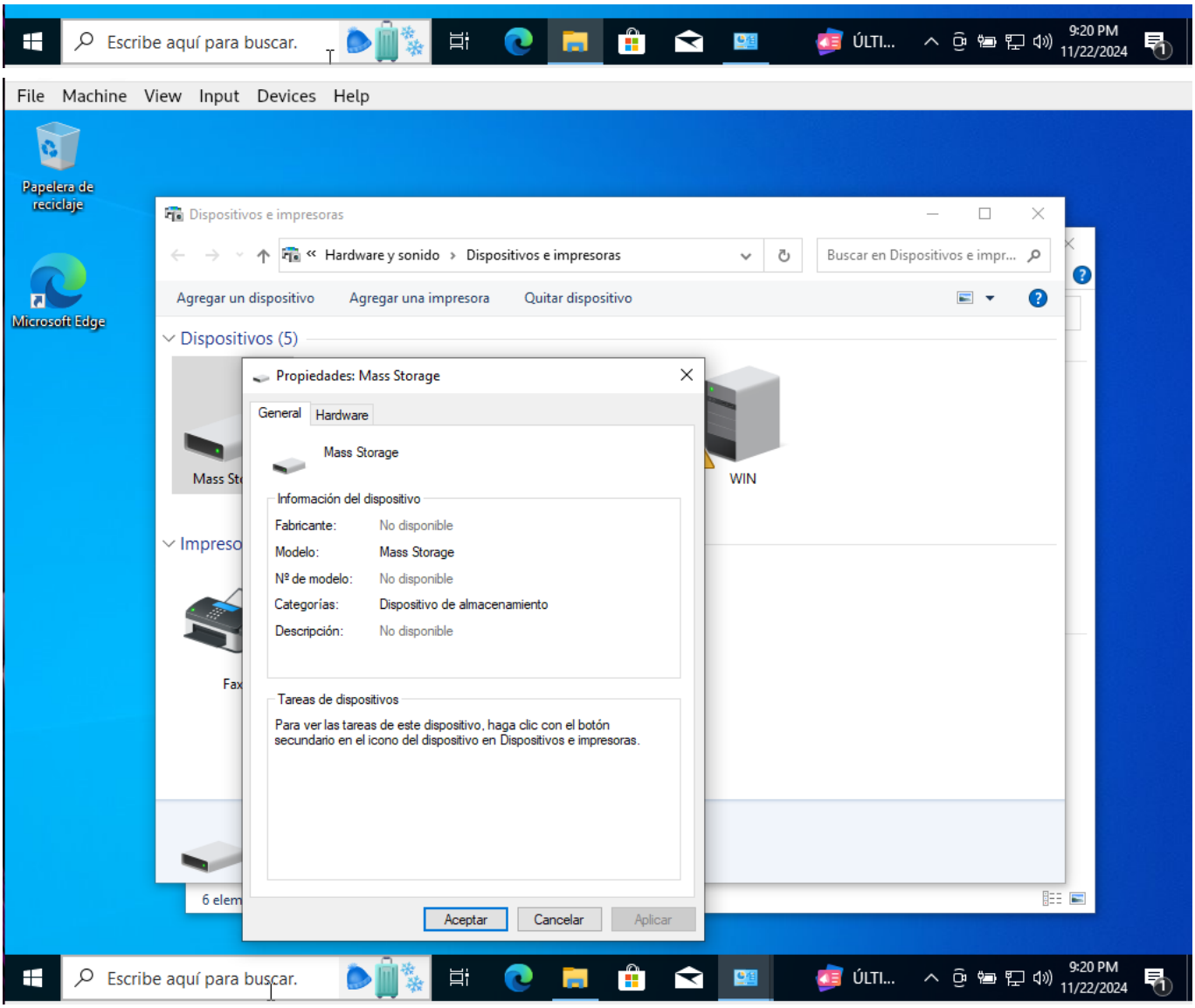

File Machine View Input Devices Help
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Windows\system32>
Discos extraíbles: denegar acceso de lectura
Discos extraíbles: denegar acceso de lectura
Valor anterior
Valor siguiente
No configurada
Habilitada
Deshabilitada
Comentario:
Compatible con:
Al menos Windows Vista
Opciones:
Ayuda:
Esta configuración de directiva deniega el acceso de lectura a los discos extraíbles.
Si habilita esta configuración de directiva, se deniega el acceso de lectura a esta clase de almacenamiento extraíble.
Si deshabilita o no define esta configuración de directiva, se permite el acceso de lectura para esta clase de almacenamiento extraíble.



Restriction Check


File Machine View Input Devices Help
Papelera de reciclaje
Microsoft Edge
Dispositivos e impresoras
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:)
Disco extraíble (F:)
Red
Carpetas frecuentes (6)
Ubicación no disponible
No se puede obtener acceso a F:\.
Acceso denegado.
Aceptar
Archivos recientes (0)
Después de abrir algunos archivos, aquí te mostraremos los más recientes.
6 elementos
Escribe aquí para buscar.
16°C
9:20 PM
11/22/2024


File Machine View Input Devices Help
Papelera de reciclaje
Microsoft Edge
Dispositivos e impresoras
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:)
Disco extraíble (F:)
Red
Carpetas frecuentes (6)
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


Escribe aquí para buscar.
9:20 PM
11/22/2024
File Machine View Input Devices Help
Papelera de reciclaje
Microsoft Edge
Dispositivos e impresoras
Hardware y sonido › Dispositivos e impresoras
Buscar en Dispositivos e impr...
Agregar un dispositivo
Agregar una impresora
Quitar dispositivo
Dispositivos (5)
WIN
Propiedades: Mass Storage
General
Hardware
Mass Storage
Información del dispositivo
Fabricante: No disponible
Modelo: Mass Storage
Nº de modelo: No disponible
Categorías: Dispositivo de almacenamiento
Descripción: No disponible
Tareas de dispositivos
Para ver las tareas de este dispositivo, haga clic con el botón secundario en el icono del dispositivo en Dispositivos e impresoras.
Aceptar
Cancelar
Aplicar
6 elem
Escribe aquí para buscar.
9:20 PM
11/22/2024