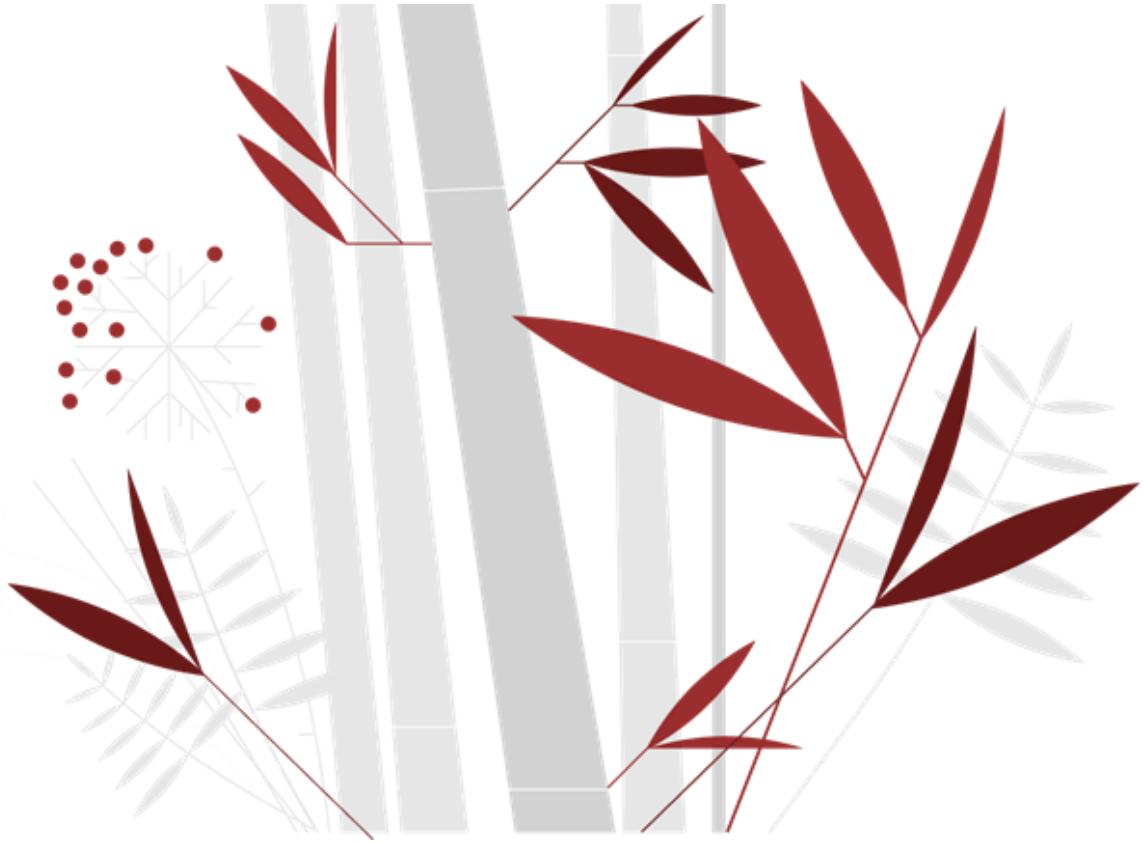
# CYBER SECURITY & ETICHAL HACHING

## Windows Server

**Sara Maimone**

**S10.L5**

06/12/2024



# INDICE

# PROGETTO

Esercizio di oggi: Creazione di Gruppi in Windows Server 2022

Obiettivo:

Lo scopo di questo esercizio è di familiarizzare con la gestione dei gruppi di utenti in Windows Server 2022.

Imparerai a creare gruppi, assegnare loro permessi specifici e comprendere l'importanza della gestione dei gruppi per la sicurezza e l'amministrazione del sistema.

Istruzioni

1. Preparazione
2. Creazione dei Gruppi
3. Assegnazione dei Permessi
4. Verifica permessi
5. Documentazione

# Windows Server

**Windows Server** è un sistema operativo avanzato sviluppato per ambienti aziendali, progettato per gestire in modo efficace reti, utenti e risorse.

Serve per:

- **Gestire utenti, gruppi e risorse condivise**
- **Fornire servizi di rete (**es. condivisione file)
- **Rafforzare la sicurezza e il controllo sui dati aziendali**.

## Principali Funzionalità

### Active Directory (AD)

Un servizio fondamentale in Windows Server che organizza utenti, gruppi e dispositivi all'interno della rete.

- **Domini**: Insiemi di utenti e risorse gestiti centralmente.
- **Controller di Dominio**: Il server che ospita l'Active Directory e gestisce l'autenticazione e l'accesso alle risorse.

### Gruppi e Permessi

- **Gruppi**: Consentono di assegnare permessi simultaneamente a più utenti, semplificandone la gestione.
- **Permessi**: Definiscono le operazioni che un utente può eseguire su risorse come file, cartelle o applicazioni.

### Cartelle Condivise

Le cartelle condivise sul server permettono agli utenti della rete di accedere ai file in base ai permessi assegnati, migliorando l’efficienza e la sicurezza.

# Gestione dei Permessi

## Tipologie di Permessi

1. **Permessi NTFS (File e Cartelle)**

Controllano quali utenti possono leggere, scrivere, modificare o eseguire file e cartelle.

   a. Lettura
   b. Scrittura
   c. Modifica
   d. Controllo Completo

2. **Esecuzione di Programmi Specifici**

Permettono agli utenti di avviare applicazioni in base ai loro ruoli o necessità operative.

3. **Modifiche alle Impostazioni di Sistema**

Riservate agli amministratori, includono configurazioni di rete, installazione software e gestione della sicurezza.

4. **Accesso Remoto**

Consente agli utenti di connettersi al server tramite il Remote Desktop Protocol (RDP) da un altro dispositivo.

## Gruppi e Sicurezza

Organizzare gli utenti in gruppi:

- Riduce errori nella gestione dei permessi.
- Migliora la sicurezza garantendo che le autorizzazioni siano coerenti e gestibili.

Assegnare i permessi ai gruppi anziché ai singoli utenti facilita la scalabilità e semplifica le operazioni amministrative.

## Esecuzione

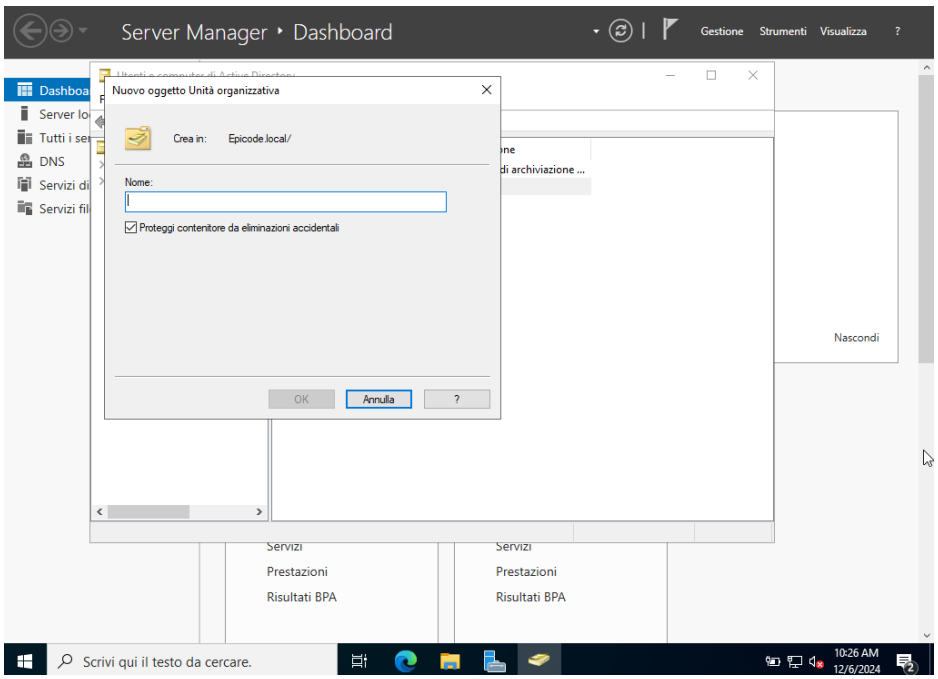
La prima fase dell'esercizio consiste nell'impostare il server affinché possa operare come controller di dominio.  Per farlo, abbiamo utilizzato Windows Server 2022 e configurato Active Directory Domain Services (AD DS).

Una volta avviato il server, il primo passo è stato accedere al Server Manager, e dopo aver avviato l'installazione del ruolo AD DS, è stato necessario promuovere il server a controller di dominio. Questo processo ha incluso la creazione di una nuova foresta, che rappresenta la struttura iniziale per gestire utenti, computer e risorse. Abbiamo scelto di chiamare la foresta epicode.local.

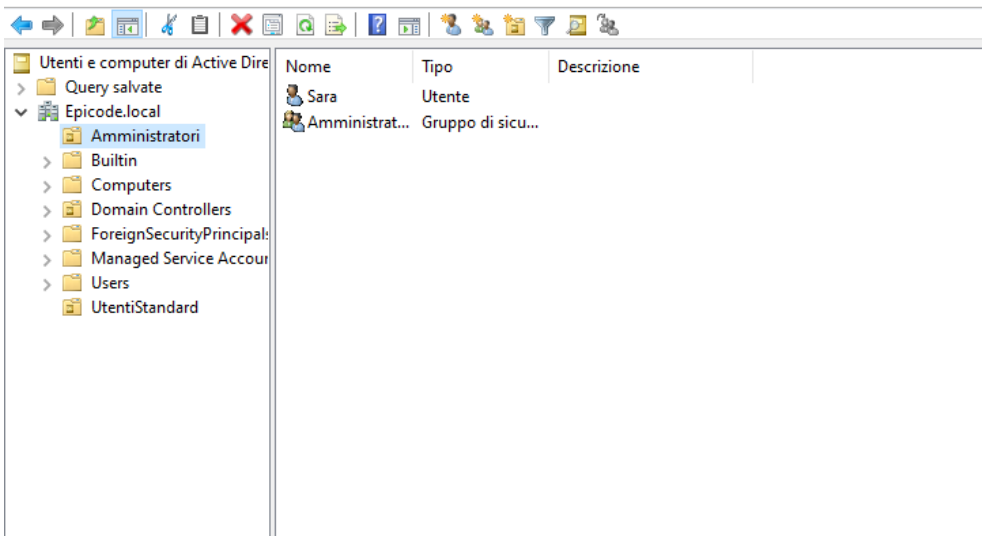
Durante la configurazione, sono state impostate le opzioni predefinite per il livello funzionale della foresta. Una volta completata la configurazione e riavviato il server, il sistema è operativo.

## Creazione e Gestione di Gruppi

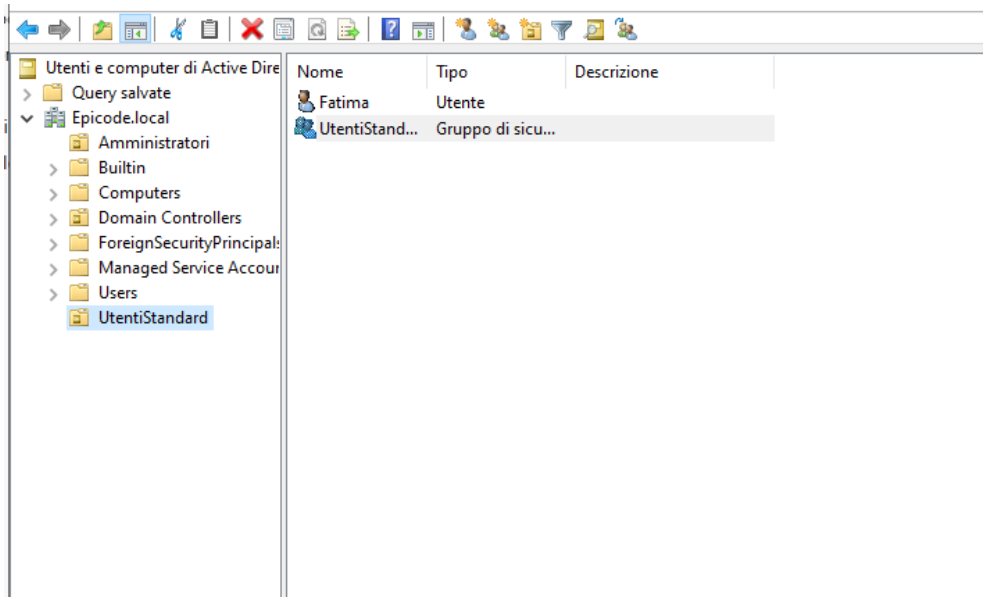
Una volta configurato il dominio, siamo passati alla creazione e gestione di gruppi e utenti. Abbiamo utilizzato la console Utenti e computer di Active Directory, accessibile direttamente dal Server Manager, per creare due gruppi principali:



- **Amministratori**, responsabili della gestione del sistema e della configurazione del server. In questo gruppo abbiamo aggiunto un utente di nome Sara.

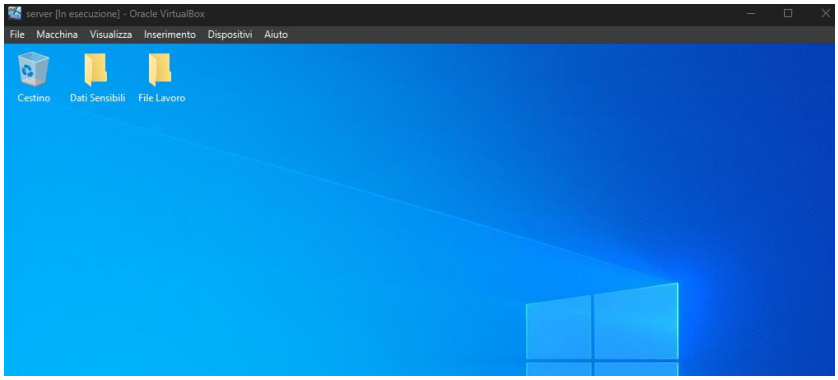



- **Utenti Standard**, destinato a utenti con permessi limitati, per esempio per accedere a risorse comuni senza compromettere la sicurezza del sistema. Questo gruppo include l'utente Fatima.

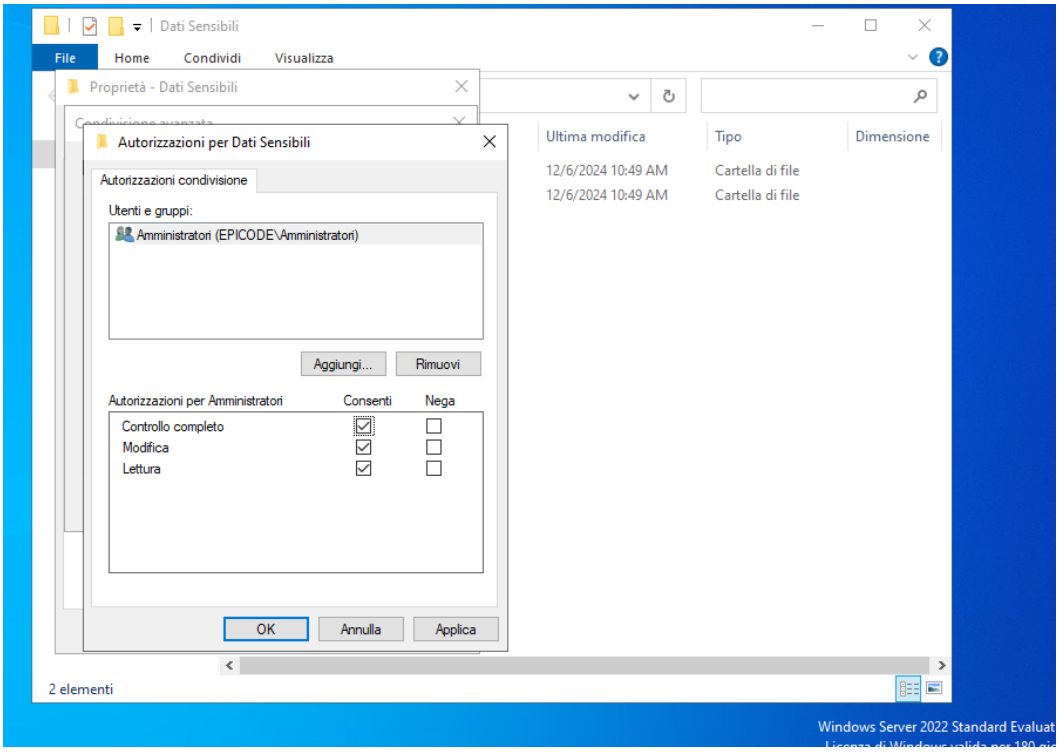


# Gestione dei Permessi

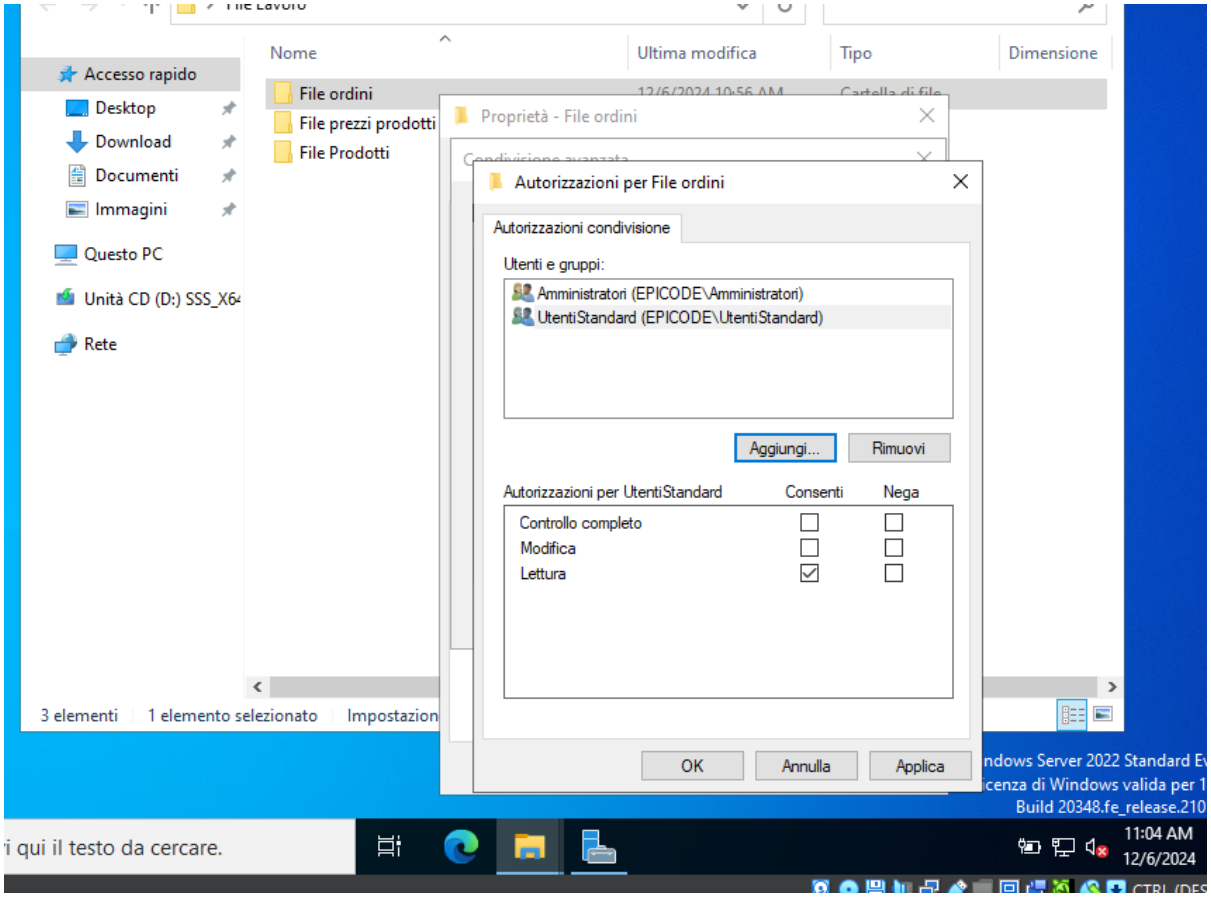
Per ogni gruppo, abbiamo assegnato permessi specifici alle cartelle create sul server. In particolare, abbiamo configurato due directory principali:




1. **Dati Sensibili**: Questa cartella contiene informazioni riservate, come indirizzi personali e IBAN. Per garantire la massima sicurezza, solo il gruppo degli **Amministratori** ha il permesso di accedere, modificare e gestire i contenuti di questa directory. Gli utenti standard non hanno accesso a questa cartella.



2. **File Lavoro**: Una directory destinata a tutti gli utenti per collaborare su documenti aziendali. Al suo interno sono state create sottocartelle come Prezzi Prodotti, Produzione e Ordini Spedizione. Il gruppo Utenti Standard ha il permesso di leggere i file contenuti, mentre il gruppo Amministratori mantiene il controllo completo.

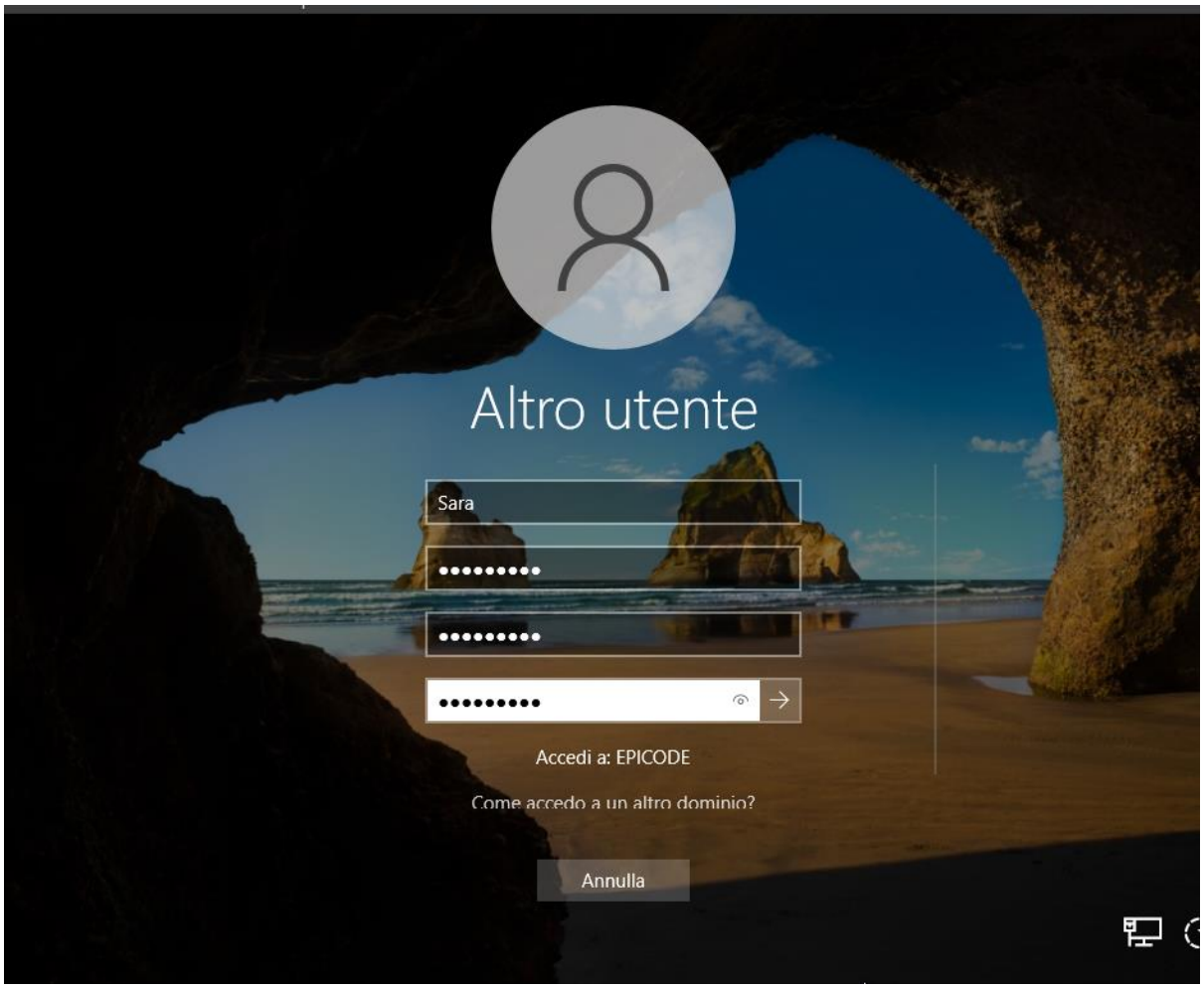



## Configurazione dei permessi

I permessi sono stati configurati accedendo alle proprietà di ciascuna cartella. Nella scheda Sicurezza, abbiamo aggiunto i gruppi corrispondenti e specificato i livelli di accesso. Per verificare i permessi, sono stati eseguiti test pratici con utenti di prova.

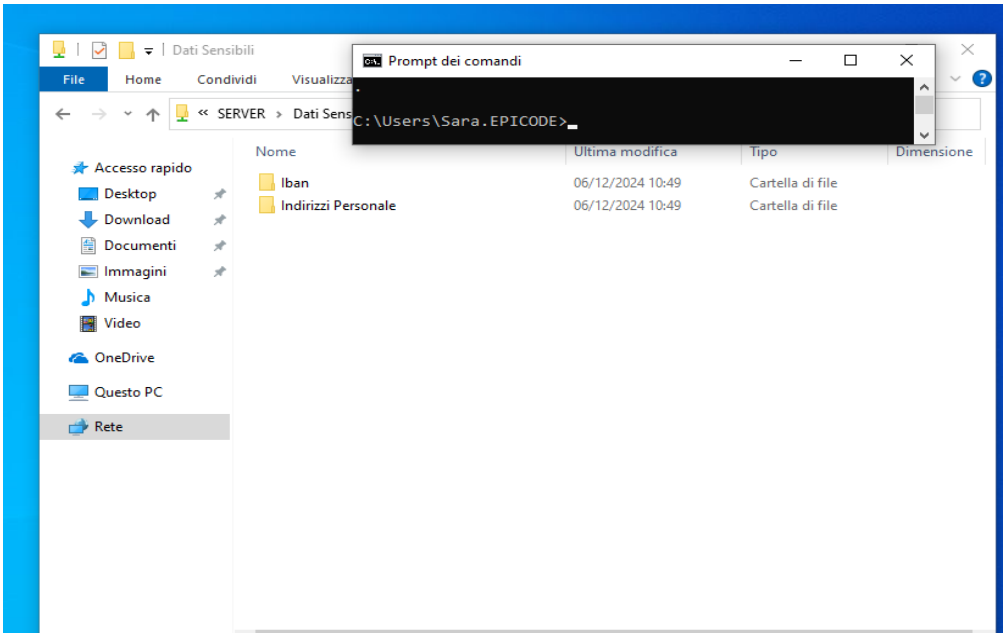
## Verifica dell’Accesso e dei Permessi tramite Windows 10

Per simulare un ambiente aziendale reale, abbiamo utilizzato un client Windows 10 per verificare l’accesso e i permessi configurati. Questo ha richiesto di connettere il client al dominio epicode.local, utilizzando le credenziali dei rispettivi utenti.



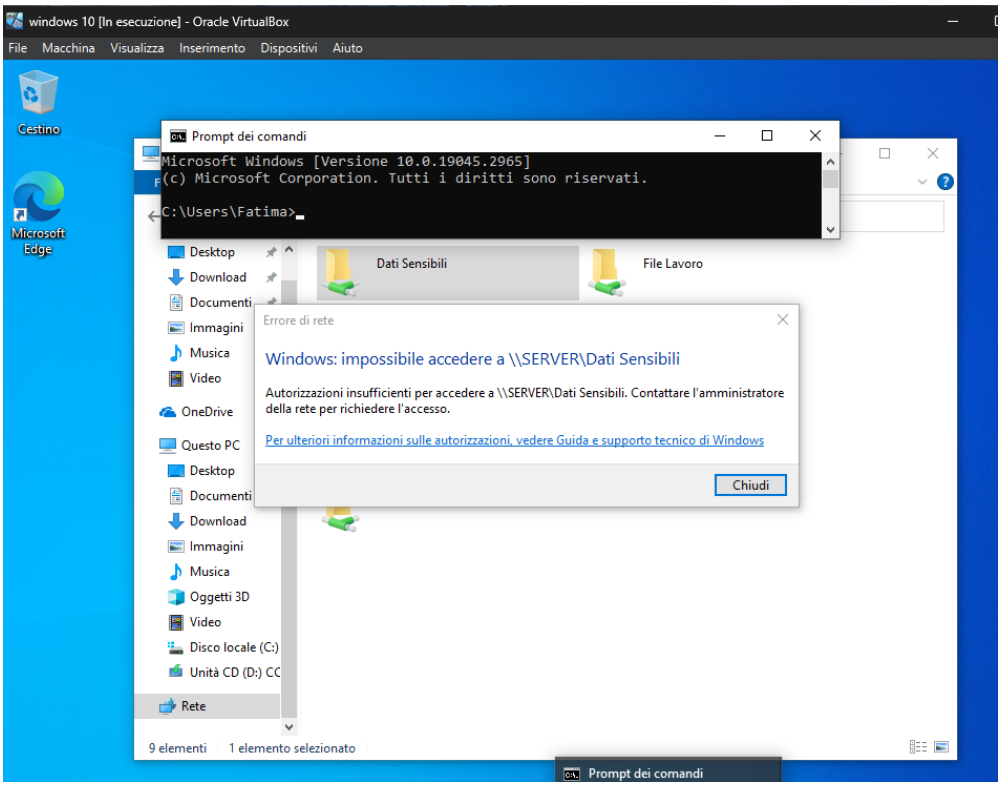
**Utente Sara (Amministratori)**:

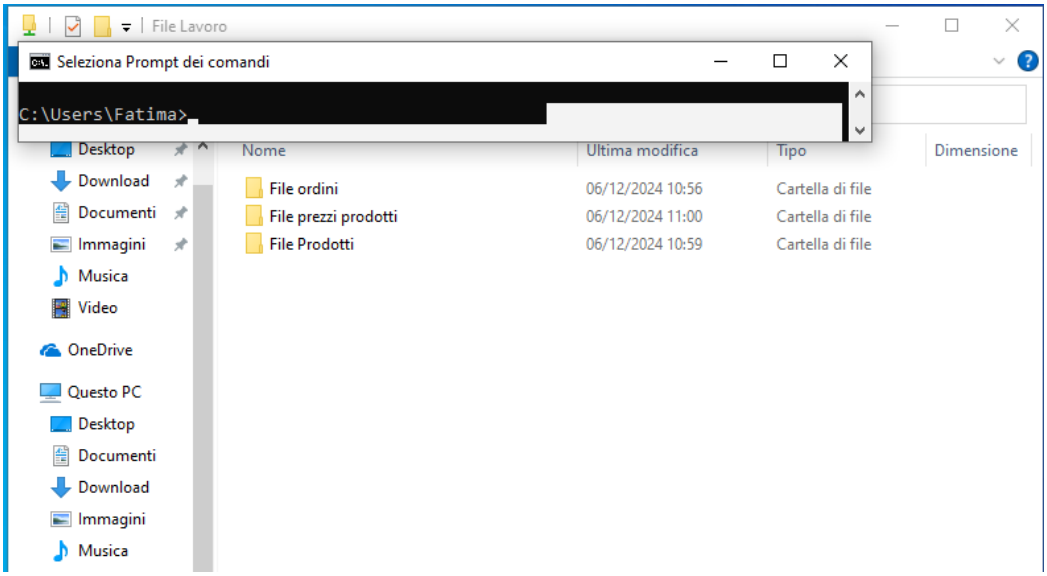
- Ha potuto accedere alla cartella Dati Sensibili, con permessi completi per leggere, modificare e gestire i file.
- Anche sulla cartella File Lavoro, Sara ha avuto il controllo totale, confermando la corretta configurazione dei permessi.



**Utente Fatima (Utenti Standard)**:

- Ha avuto accesso solo alla cartella File Lavoro, potendo leggere e modificare i file senza restrizioni.
- Come previsto, Fatima non ha potuto accedere alla cartella Dati Sensibili, ricevendo un messaggio di errore di accesso negato.




Questa verifica è stata essenziale per confermare che i permessi assegnati ai gruppi funzionano correttamente e rispettano le policy di sicurezza definite.

# Conclusioni

L'esercizio ha dimostrato come Windows Server 2022, in combinazione con Active Directory, possa essere utilizzato per creare un'infrastruttura aziendale sicura, scalabile ed efficiente. La gestione centralizzata dei gruppi e dei permessi consente di semplificare l’amministrazione del sistema e di migliorarne la sicurezza.

Grazie alla verifica eseguita da un client Windows 10, è stato possibile testare l’accesso alle risorse in un contesto pratico, confermando la corretta configurazione dei permessi. Questo approccio garantisce che solo le persone autorizzate possano accedere ai dati sensibili, mentre gli altri utenti possono operare senza compromettere l’integrità del sistema.

Windows Server 2022 si è dimostrato uno strumento potente e versatile per la gestione IT, rendendo semplice l’organizzazione e la protezione delle risorse aziendali.