Il controllo di accesso è garantito tramite l’utilizzo di username e password per gli utenti che hanno accesso a contenuti sensibili, per prevenire eventuali creazioni o modifiche a oggetti che modellano entità del dominio, in modo da prevenire accessi non autorizzati a dati sensibili. Inoltre, almeno nella prima versione non saranno implementati metodi di recupero o modifica password.

Per scelte progettuali, il salvataggio delle password sarà in chiaro sul database: non ci sarà nessun tipo di cifratura, almeno nella versione iniziale del sistema.

Le operazioni che gli utenti della piattaforma desktop possono effettuare sugli oggetti sono riportati nella tabella che segue:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Oggetti  Attore | Utenza | Prodotto | Scontrino | Ticket | Richiesta  fornitura |
| Cassiere | Autenticazione  Logout | Scanner prodotto | Stampa scontrino |  |  |
| Magazziniere | Autenticazione  Logout | Richiesta nuovo prodotto |  |  | Richiesta  fornitura |
| Addetto Assistenza | Autenticazione  Logout |  |  | Crea nuovo ticket per prodotti in garanzia |  |
| Cliente |  | Scelta prodotto | Ritira scontrino | Ritira il ticket |  |

Dalla tabella si evince come l’utente non abbia interazione dirette con il controllo di accesso al database, cui accedono i singoli sottosistemi di business: per questo motivo si è deciso di non riportare nella matrice d’accesso.