Contromisure	Eseguire l'hardening del sistema operativo che ospita il Web Server [rif. 5.2.2].

5.5.3 Utenze

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.1].

5.5.4 Autenticazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.2].

5.5.5 Autorizzazione

A i principi generali già introdotti nel paragrafo [rif. 5.1.3], si aggiungono le seguenti indicazioni per il contesto specifico:

Autorizzazione	
Minaccia	- Accesso non autorizzato ai sistemi (macchina, configurazione, ecc.). - Accesso non autorizzato alle informazioni.
Contromisure	Utilizzare e configurare opportunamente i meccanismi di controllo di accesso alle risorse esposte dal web server (a titolo di esempio l'autorizzazione di accesso a livello di specifiche URL fornita dal Framework .NET).

5.5.6 Crittografia

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.4].

5.5.7 Documentazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.5].

5.5.8 Logging

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.6].

5.5.9 Sessioni

Contrasto delle riproduzioni di sessione	
Minaccia	- Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni. - Falsificazione di identità. - Uso non autorizzato di privilegi.
Contromisure	Verificare che siano adottate le seguenti best practices: - Utilizzare token di sessione (ad es. cookie o sessionID) difficilmente predicibili (ossia random) - Configurare l'applicativo web in modo che venga verificata la validità e l'integrità di ciascun token di sessione (ad es. cookie o sessionID) associato ad una richiesta di accesso.