	- Generare un nuovo identificativo di sessione dopo il login (per evitare il session fixation ossia che il session ID sia forzato dall'esterno). - Limitare il periodo di scadenza del token di sessione in modo da limitare il tempo disponibile per sferrare un attacco. - Utilizzare un protocollo di comunicazione cifrato (TLS 1.2 o successivo) per la creazione di un canale di comunicazione protetto, e configurare il protocollo in modo che i cookie di autenticazione transitino solo mediante connessione HTTPS; - Configurare il client web (browser) in modo da consentire di non archiviare i dati di sessione sulla postazione di lavoro; - Prevedere un meccanismo che imponga di terminare una sessione qualora ne venga avviata una nuova con le medesime credenziali di autenticazione della precedente. - Attivare un meccanismo per la disconnessione automatica delle sessioni di lavoro dopo un periodo di inattività inferiore ai 5 minuti.

Gestione delle informazioni segrete di autenticazione degli utenti	
Minaccia	- Accesso non autorizzato alle informazioni. - Crittografia debole o non validata. - Falsificazione di identità. - Uso non autorizzato di privilegi.
Contromisure	Mentre l'SSL/TLS protegge i cookie in rete, non impedisce loro di essere modificati nel computer del client. Per contrastare la minaccia di manipolazione dei cookie, crittografare i cookie utilizzando un HMAC.

5.5.10 Procedure

A i principi generali già introdotti nel paragrafo [rif. 5.1.7], si aggiungono le seguenti indicazioni per il contesto specifico:

Controlli sulla regolamentazione dell'uso del codice mobile per Web Server	
Minaccia	- Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	Controllare che nel caso in cui si sia concesso l'utilizzo del mobile code (codice, come Java Applet, che è trasmesso via rete e eseguito su una macchina remota, "a fianco" di altro mobile code, potenzialmente malevolo) non siano effettuate operazioni non autorizzate rispetto alla politica definita per l'utilizzo del codice mobile. In particolare, controllare il rispetto delle politiche riguardanti: - esecuzione del mobile code in un ambiente isolato logicamente; - blocco di ogni utilizzo di mobile code; - blocco della ricezione di mobile code dall'esterno; - attivazione di controlli crittografici per autenticare univocamente il mobile code. - rispetto delle security guidelines di programmazione sicura per il per mobile code.

Inventario piattaforma web	
Minaccia	- Attacchi all'integrità dei sistemi (software e configurazioni). - Errori di amministrazione dei sistemi. - Negazione dei servizi.
Contromisure	Mantenere un inventario aggiornato che evidenzi: - Le date di pubblicazione dei dati forniti dal servizio web; - La release software del servizio web con l'indicazione, nelle Release Notes, di tutte

	le modifiche introdotte (come nuove funzionalità, plug-in, etc.); - I sistemi su cui è implementato il servizio web; - L'owner o funzione responsabile dei servizi web e dei relativi sistemi.

Collaudo del servizio web	
Minaccia	- Accesso non autorizzato alle informazioni. - Uso non autorizzato di privilegi. - Negazione dei servizi.
Contromisure	Effettuare un collaudo del servizio web prima di renderlo operativo, a tal proposito: - Svolgere il test in un ambiente diverso da quello dello sviluppo; - Considerare, nelle specifiche di collaudo, le tipologie di browser maggiormente diffuse e le versioni più recenti; - Assicurarsi che durante la fase di testing siano predisposte verifiche mirate non solo alla componente funzionale ma si attui anche una mirata attività dedicata alle eventuali falle di sicurezza. A questo riguardo: • Utilizzare specifici software per il controllo della qualità del codice (analisi statica) che tenga conto dei princìpi di sicurezza della programmazione (SAST). • Utilizzare specifici software per l'analisi dinamica del codice (DAST).

Procedura di monitoraggio sull'uso del web server	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Negazione dei servizi.
Contromisure	Definire procedure che specifichino le modalità con cui monitorare il web server per garantirne la funzionalità e l'uso corretto. La procedura deve specificare cosa monitorare (ambito del monitoraggio) e quando eseguire l'audit rimanendo conformi ai requisiti di legge e alle policy in vigore nell'organizzazione. Gli aspetti da considerare sono: - accessi autorizzati, includendo dettagli quali: • user ID; • indirizzo IP del client; • data e ora degli eventi chiave; • i tipi di eventi; • indirizzo delle risorse accedute; - tutte le operazioni privilegiate, come: • l'uso di account privilegiati (supervisor, root, administrator); • avvio e arresto del sistema; • collegamento e scollegamento di dispositivi di input/output; - tentativi di accesso non autorizzato, come: • azioni degli utenti falliti o rifiutati; • azioni fallite o rifiutate che coinvolgono dati o altre risorse; • violazioni della policy di accesso e notifiche generate da gateway e firewall; • alert da sistemi di intrusion detection; - alert o avaria dei sistemi come: • alert o messaggi inviati alle console di amministrazione; • eccezioni dei log dei sistemi; • allarmi provenienti da sistemi di gestione della rete;