	protette. L'interfaccia di programmazione per la protezione dei dati applicativi (DPAPI) è un esempio di un servizio di crittografia fornito su sistemi operativi Windows 2000 e successivi in cui il sistema operativo gestisce la chiave. Se si utilizza un meccanismo di crittografia che richiede di generare o gestire la chiave, utilizzare algoritmi di generazione forti delle chiavi casuali e memorizzare la chiave in una posizione protetta. Ad esempio, in una chiave del Registro di sistema protetta con un ACL restrittivo. Crittografare la chiave di crittografia utilizzando DPAPI per una maggiore sicurezza. Impostare i limiti temporali di scadenza delle chiavi ad intervalli regolari.

5.1.5 Documentazione

Protezione della documentazione di sistema da accessi non autorizzati	
Minaccia	Accesso non autorizzato alle informazioni.
Contromisure	La documentazione di sistema (ad es. relativa al software del web server/DBMS, della piattaforma ospitante il web server/DBMS, ecc.) deve essere protetta da accessi non autorizzati e conservata in modo sicuro. In particolare, la documentazione cartacea, se non utilizzata, deve essere conservata e custodita all'interno di contenitori (es. armadi, cassettiere) chiusi a chiave e accessibile esclusivamente dai soggetti autorizzati. Per la documentazione memorizzata su supporto informatico l'accesso dovrebbe essere consentito ad una lista ridotta di utenti, mediante l'utilizzo di idonei sistemi di autenticazione e autorizzazione informatica.

5.1.6 Logging

Registrazione degli eventi (audit)	
Minaccia	- Abuso di privilegi da parte dell'utente - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate. - Negazione dei servizi.
Contromisure	I log di audit che registrano le attività dell'utente, le eccezioni e gli eventi di sicurezza devono essere prodotti e conservati per essere utilizzati in indagini, come prove da esibire in caso di dispute, e monitoraggi, come elementi da considerare nell'identificazione di misure migliorative della sicurezza. Gli eventi che devono essere registrati includono: - log-on e log-off e durata dell'accesso dell'utente o applicazione software; - tentativi di accesso riusciti e falliti; - utilizzo di funzioni amministrative o di gestione; - avvio e arresto delle funzioni di audit; - errori del software. La registrazione dell'evento deve riportare almeno i seguenti dati: - identità dell'utente o l'identificativo del processo che ha scatenato l'evento; - indirizzo IP dell'utente nel caso di sessione remota; - data e ora dell'evento; - tipo dell'evento; - oggetti coinvolti dall'evento; - eventuali errori prodotti dall'evento. . Conservare i dati relativi agli eventi registrati per un periodo di tempo di almeno 5 anni.