	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.

Adozione di misure idonee a garantire inalterabilità e integrità dei log registrati	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Abuso di privilegi da parte dell'utente - Abuso di risorse. - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste; tale verifica avviene in conformità alla normativa in materia di protezione dei dati personali (Privacy) e dei principi di sicurezza. Proteggere i file di log utilizzando ACL restrittivi. Attraverso un processo automatico schedulato a intervalli regolari (ad es. ogni notte), spostare i file di log fin lì prodotti in una posizione diversa da quella predefinita e comprimerli. Predisporre un processo automatico per la raccolta dei log compressi e il loro trasferimento su un server centralizzato.

Registrazione e Analisi periodica dei log degli errori	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	Le segnalazioni di errori (es. di malfunzionamenti, di eventi anomali di sicurezza che possono essere segnali di un probabile attacco o palesi tentativi di intrusione) devono essere registrate cronologicamente nei file di log del sistema, archiviate centralmente su un sistema dedicato e analizzate periodicamente per rilevare prontamente eventuali segnali che possono indicare l'insorgenza di un malfunzionamento (che può portare a un disservizio) o per rilevare tentativi di attacco. I file di log raccolti sul sistema centralizzato devono essere mantenuti per un congruo periodi di tempo (in genere sei mesi), allo scopo di consentire analisi anche in tempi successivi e per analisi di tipo statistico. Si noti che i file di log relativi a transazioni bancarie, dati di traffico telematico e telefonico, dati personali, sensibili e giudiziari, sono soggetti a specifiche norme di legge che prescrivono tra l'altro tempi massimi consentiti di mantenimento, oltre i quali devono essere obbligatoriamente cancellati.

Conservazione dei log registrati degli amministratori di sistema	
Minaccia	- Cancellazione dei log di accountability e/o ripudio di operazioni effettuate. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali. - Abuso di privilegi da parte degli utenti. - Abuso di risorse.
Contromisure	- Tracciare eventi chiave come gli eventi di login e logout, i tentativi di login falliti, l'uso di privilegi elevati, le transazioni applicative critiche dal punto di vista della sicurezza, l'accesso e il tentativo fallito di accesso a oggetti e risorse critiche per la sicurezza. - Non utilizzare account condivisi o di ruolo poiché non è possibile determinare la vera identità dei soggetti. Gli accessi degli amministratori devono essere sempre nominativi e i relativi identificativi in caso siano revocati non devono più essere riassegnati ad altri utenti neppure in tempi diversi. - Salvare i log di accesso amministrativo ai sistemi e quelli di audit (operazioni che richiedono l'uso di privilegi) su sistemi di raccolta centralizzati.