	Infine, per quanto riguarda l'abuso di privilegi da parte degli utenti, questo fenomeno può essere contrastato con un approccio basato su più aspetti: - Diffondere tra gli utenti un documento di politiche di sicurezza che spieghi qual è l'uso corretto delle risorse. - Impiegare meccanismi di tracciamento delle operazioni effettuate dagli utenti in grado di registrare i tentativi di accesso non riusciti a risorse per le quali non si dispone delle necessarie autorizzazioni, nei limiti imposti dalle leggi vigenti. - Informare gli utenti attraverso "banner" di accesso (oltre alle citate politiche di sicurezza) dell'esistenza di tali meccanismi di tracciamento. - Educare gli utenti ad un uso corretto delle risorse attraverso corsi di formazione.

5.1.4 Crittografia

Protezione delle informazioni strumentali all'accesso	
Minaccia	Crittografia debole o non validata.
Contromisure	- Non sviluppare e utilizzare algoritmi di crittografia personalizzati/propri. - Utilizzare servizi, funzioni e algoritmi crittografici la cui robustezza sia comprovata da certificazioni e standard riconosciuti a livello internazionale, e che risultino esenti da vulnerabilità note. A titolo esemplificativo e non esaustivo, per la crittografia deve essere usato quanto meno l'algoritmo AES a 128 bit (o meglio a 256 bit se possibile), per le funzioni di hashing quanto meno lo SHA-256 (MD5 e SHA-1 sono deprecati), per le connessioni internet sicure almeno TLS 1.2 (SSL e TLS precedenti alla 1.2 sono vulnerabili e deprecate). - Per quanto riguarda prodotti di crittografia a titolo esemplificativo devono disporre quanto meno di certificazione Common Criteria In genere EAL 4+ (ma a seconda dei casi possono essere richiesti livelli minori o anche superiori in base a regolamenti e norme di legge). - Mantenersi informati sugli algoritmi manomessi e sulle tecniche utilizzate per la manomissione, attraverso i bollettini di sicurezza emessi sia dai vendor sia da fonti internazionali autorevoli, sia dal CERT della PA.

Protezione dei dati di autenticazione (trasmissione)	
Minaccia	Crittografia debole o non validata.
Contromisure	Meccanismi, strumenti, procedure o abilità tecniche atti a prevenire l'accesso non autorizzato al sistema e a proteggere i dati di autenticazione quando memorizzati o trasmessi.

Protezione delle informazioni	
Minaccia	Crittografia debole o non validata.
Contromisure	I controlli crittografici devono essere utilizzati in conformità a tutti gli accordi, leggi e regolamenti pertinenti. Considerare di adeguarsi alle best practices di crittografia. Di seguito vengono indicate le principali: - Trasmissione dati: usare TLS 1.2 o 1.3. A partire dalla prima metà del 2020 le versioni 1.0 e 1.1 del protocollo, verranno considerate deprecate (viceversa SSL v2 e v3 sono considerate insicure). - Cifratura dati: usare AES con una chiave a 256 bit (3DES solo per backward compatibility, DES è considerato insicuro). - Hashing: usare SHA-256 (evitare SHA-1, mentre MD5 è considerato insicuro).

	- RSA: usare chiavi a 2048 bit. - Algoritmo di scambio chiavi: Utilizzare la feature "Forward Secrecy" conosciuta anche come "Perfect Forward Secrecy", per garantire che nel caso di compromissione di una chiave privata ciò non pregiudichi anche le chiavi delle altre sessioni. Per abilitare tale feature è necessario configurare TLS 1.2 in modo tale che venga adottato come algoritmo di scambio delle chiavi l'Elliptic Curve Diffie-Hellman (con Diffie-Hellman come algoritmo di fallback), ed evitare totalmente, se possibile, lo scambio chiavi tramite RSA. L'utilizzo di TLS 1.3 invece garantisce l'impiego della forward secrecy per tutte le sessioni TLS attraverso l'uso del protocollo di scambio chiavi Ephemeral Diffie-Hellman. - Ripristino della sessione TLS: Analogamente all'utilizzo del keepalives impiegato per mantenere le connessioni TCP persistenti attive, l'abilitazione del ripristino della sessione TLS "TLS Session Resumption" consente al server Web di tenere traccia delle ultime sessioni SSL/TLS negoziate e quindi di ripristinarle, scongiurando l'overhead computazionale dovuto alla negoziazione della chiave di sessione.

Protezione delle informazioni	
Minaccia	- Violazione di leggi, di regolamenti, di obblighi contrattuali. - Compromissione delle comunicazioni. - Falsificazione di identità.
Contromisure	I controlli crittografici devono essere utilizzati in conformità a tutti gli accordi, leggi e regolamenti pertinenti. Considerare di adeguarsi alle best practices di crittografia. Di seguito vengono indicate le principali: - Trasmissione dati: usare TLS 1.2 o 1.3 (viceversa SSL v2 e v3 sono considerate insicure). - Cifratura dati: usare AES con una chiave a 256 bit (3DES solo per retro-compatibilità, DES è considerato insicuro). - Hashing: usare SHA-256 (evitare SHA-1, mentre MD5 è considerato insicuro). - RSA: usare chiavi almeno a 2048 bit. - Algoritmo di scambio chiavi: Utilizzare la feature "Forward Secrecy" conosciuta anche come "Perfect Forward Secrecy", per garantire che nel caso di compromissione di una chiave privata ciò non pregiudichi anche le chiavi delle altre sessioni. Per abilitare tale feature è necessario configurare TLS 1.2 in modo tale che venga adottato come algoritmo di scambio delle chiavi l'Elliptic Curve Diffie-Hellman (con Diffie-Hellman come algoritmo di fallback), ed evitare totalmente, se possibile, lo scambio chiavi tramite RSA. L'utilizzo di TLS 1.3 invece garantisce l'impiego della forward secrecy per tutte le sessioni TLS attraverso l'uso del protocollo di scambio chiavi Ephemeral Diffie-Hellman. - Ripristino della sessione TLS: Analogamente all'utilizzo del keepalives impiegato per mantenere le connessioni TCP persistenti attive, l'abilitazione del ripristino della sessione TLS "TLS Session Resumption" consente al server Web di tenere traccia delle ultime sessioni SSL/TLS negoziate e quindi di ripristinarle, scongiurando l'overhead computazionale dovuto alla negoziazione della chiave di sessione.

Protezione delle informazioni strumentali all'accesso	
Minaccia	Generazione e/o gestione inadeguata delle chiavi crittografiche.
Contromisure	Utilizzare routine di crittografia integrate che includono la gestione delle chiavi