	L'organizzazione dovrebbe definire un processo affinché l'utente "proprietario" o altri utenti possano segnalare immediatamente - H24 - eventi/incidenti di sicurezza inerenti l'informazione segreta di autenticazione, quali: la divulgazione non autorizzata o la perdita di segretezza.

5.1.3 Autorizzazione

Definizione della politica di controllo accesso logico	
Minaccia	Accesso non autorizzato alle informazioni (ad es. causato dal personale utente per carenza di una politica per il controllo degli accessi che accoglie i requisiti di sicurezza).
Contromisure	Definire e documentare la politica che regola le autorizzazioni per ciascun utente e gruppo di utenti con una granularità che consenta un rigoroso rispetto del principio del ''need to know''. Deve essere soddisfatta la regola del ''tutto proibito tranne ciò che è espressamente concesso''. La politica deve tenere conto di: - requisiti di sicurezza delle applicazioni e dei rischi che le informazioni gestite da tali applicazioni possono incontrare; - leggi e obblighi contrattuali che riguardano la protezione degli accessi a dati e servizi; - gestione dei diritti di accesso in un ambiente distribuito e di rete che riconosce ogni tipo di connessione disponibile; - separazione dei ruoli riguardanti il controllo degli accessi (richiesta di accesso, autorizzazione degli accessi, amministrazione degli accessi); - rimozione dei diritti di accesso per le credenziali non utilizzate da almeno sei mesi.

Separazioni dei compiti e delle responsabilità	
Minaccia	Abuso di risorse.
Contromisure	I compiti e le aree di responsabilità in conflitto tra loro devono essere separati al fine di ridurre le possibilità di accedere, modificare o utilizzare asset dell'organizzazione impropriamente, senza autorizzazione o misure di controllo.

Definizione di regole di trattamento ed etichettatura	
Minaccia	Compromissione della sicurezza dell'informazione per carenza di regole di classificazione e trattamento delle informazioni
Contromisure	Definire criteri e procedure per la corretta etichettatura delle informazioni (non solo in forma elettronica, ma anche cartacea). Considerare le seguenti etichette: - Confidenziale (Informazione la cui impropria diffusione può provocare danni molto gravi, ad esempio: perdite economiche, conseguenze legali, conseguenze sul patrimonio, danno di immagine) - Riservata (Informazione la cui impropria diffusione può provocare danni gravi, ad esempio: perdita di vantaggio competitivo) - Interna (Informazione la cui diffusione può provocare danno lieve) - Pubblica (Informazione la cui diffusione non può provocare danno) Definire procedure che regolino come debba avvenire il trattamento delle informazioni ai vari livelli di classifica con riferimento alle attività di elaborazione, diffusione, utilizzo, custodia, riclassificazione, distruzione. Rendere disponibili le procedure a tutto il personale.

Definizione e assegnazione di ruoli e responsabilità	
Contromisura	Compromissione della sicurezza dell'informazione per carenza dell'organizzazione

	interna
Contromisure	Dare la responsabilità delle informazioni (insieme di dati) e delle risorse associate per la loro elaborazione (processo di business, gruppo specifico di attività, applicazioni) ad una determinata parte dell'organizzazione per assicurare l'appropriata classificazione e l'applicazione delle politiche di controllo degli accessi a tali risorse. In particolare: - identificare e definire chiaramente i vari beni (quali i server, le postazioni di lavoro client, gli apparati di rete e di sicurezza, i sistemi di storage, i dispositivi di stampa, i sistemi di continuità elettrica, ecc.) e i processi di sicurezza (es. gestione degli incidenti, gestione delle configurazioni di sistema, gestione degli aggiornamenti, gestione dei sistemi antivirus, gestione dei sistemi firewall, gestione delle verifiche tecniche di vulnerability assessment, gestione delle non conformità e monitoraggio dei rientri, ecc.); - nominare un responsabile della sicurezza di ciascun bene e un responsabile per ciascun processo di gestione della sicurezza e documentare in modo; dettagliato i processi, definendo in modo chiaro i ruoli e le responsabilità - definire chiaramente i livelli di autorizzazione per l'accesso o l'utilizzo di ciascun bene.

Protezione dell'accesso ai dati	
Minaccia	- Abuso di privilegi da parte dell'utente. Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Accesso non autorizzato alle informazioni. - Furto di credenziali di autenticazione.
Contromisure	Per quanto riguarda il furto di credenziali di autenticazione e quel che ne consegue (accesso non autorizzato a sistemi e informazioni, furto d'identità, ecc.), è necessario stabilire meccanismi di autenticazione la cui robustezza sia adeguata alla criticità dell'applicazione e ancor più alla sensibilità dei dati che l'applicazione tratta. Ad es. per applicazioni critiche o dati particolarmente sensibili è necessario adottare meccanismi di autenticazione a due fattori, basati ad es. su SMS inviati su un numero di cellulare precedentemente "certificato", o codici inviati tramite una app per smartphone o altri metodi equivalenti. Tuttavia qualsiasi misura di sicurezza in tale ambito può risultare inefficace se non accompagnata da una appropriata campagna di diffusione della consapevolezza delle problematiche di sicurezza ("security awareness") verso gli utenti che devono essere informati e responsabilizzati verso un uso corretto delle credenziali di autenticazione con documenti (politiche di sicurezza) ed eventualmente corsi di formazione. Per impedire l'accesso non autorizzato ai dati, a riposo e/o in transito, da parte di utenti reali (ma non abilitati per i dati in oggetto) e per limitare le possibilità di accesso di eventuali utenti che abbiano ottenuto illecitamente delle credenziali valide non di propria pertinenza, i dati memorizzati all'interno dei sistemi (file e cartelle) devono essere adeguatamente protetti attraverso l'assegnazione di diritti di accesso il più possibile granulari e specifici (dal punto di vista delle risorse). Qualora i dati siano conservati in archivi elettronici (es. database) accertarsi che l'accesso ai dati avvenga mediante un'adeguata profilatura degli utenti e che le applicazioni che accedono ai database non utilizzino una singola utenza di "super-amministratore" per tutte le operazioni, dato che tale configurazione può essere sfruttata da un malintenzionato per prendere pieno possesso dell'archivio. L'organizzazione dovrebbe adottare controlli di accesso fisico e/o logico per l'isolamento di applicazioni, dati o sistemi critici o sensibili. Per l'accesso ai dati critici o sensibili definire requisiti di sicurezza più stringenti applicando tecniche di cifratura o altri meccanismi di sicurezza per rafforzare la protezione dell'accesso.