Modulo 6 – Protezione dei dati, sicurezza e audit (1 ora)

Obiettivi formativi

Al termine della lezione il partecipante sarà in grado di trattare i dati personali in modo lecito e proporzionato; proteggere credenziali, documenti e comunicazioni; riconoscere e segnalare un possibile incidente; assicurare reperibilità, integrità e ricostruibilità delle operazioni in sede di controllo; collegare un rilievo a un'azione correttiva verificabile.

Metodo didattico. Spiegazione guidata, domande al gruppo e analisi di tre situazioni operative. Gli esempi sono ipotetici e non descrivono eventi realmente avvenuti nel CAA.

Scaletta dell'ora

- 0–5 minuti: apertura e obiettivi.
- 5–17 minuti: finalità, liceità e uso proporzionato dei dati.
- 17–30 minuti: credenziali, postazione, documenti e comunicazioni.
- 30–40 minuti: riconoscimento e segnalazione degli incidenti.
- 40–50 minuti: pista di controllo, audit e non conformità.
- 50–60 minuti: verifica rapida, discussione delle risposte e riepilogo.

Lezione

1. Trattare soltanto i dati necessari

Apertura suggerita. «Proteggere i dati non significa soltanto evitare un attacco informatico. Significa sapere perché consultiamo un fascicolo, quali informazioni ci servono, a chi possiamo trasmetterle e come possiamo dimostrare il lavoro svolto».

Il trattamento deve rispettare liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza. Il titolare deve anche poter dimostrare il rispetto di questi principi: è la responsabilizzazione, o accountability. Riferimento: principi fondamentali del trattamento, Garante.

Liceità e autorizzazione non sono la stessa cosa. La base giuridica giustifica il trattamento; l'autorizzazione operativa delimita ciò che il singolo operatore può fare. Il consenso è una delle possibili basi giuridiche, non una soluzione universale. L'operatore segue le istruzioni ricevute e non decide autonomamente nuove finalità o nuove basi giuridiche. Riferimento sulle basi giuridiche.

Traduzione operativa del testo originario. Prima di aprire, copiare o inviare un documento, l'operatore si pone quattro domande:

1. Quale attività di servizio sto svolgendo?
2. Sono autorizzato a consultare o utilizzare queste informazioni?
3. Mi serve il documento completo oppure bastano dati specifici?
4. Sto usando l'archivio e il canale previsti dall'organizzazione?

Esempio ipotetico. Per verificare un'informazione di una pratica, non è opportuno scaricare tutti i fascicoli disponibili «per averli a portata di mano». Si consulta quanto necessario nell'ambiente autorizzato e si evitano copie prive di utilità operativa.

Conservazione e aggiornamento. Non conservare ogni copia indefinitamente e non cancellare documenti di propria iniziativa. Applicare i tempi e le modalità stabiliti dalle regole competenti, tenendo conto degli obblighi di conservazione. Quando un dato è errato, utilizzare il percorso autorizzato di rettifica, evitando di mantenere copie operative discordanti. Il principio generale richiede dati esatti e conservazione non superiore al necessario. Riferimento: esattezza e conservazione.

Domanda al gruppo. «La possibilità tecnica di aprire un fascicolo basta a giustificarne la consultazione?» Risposta attesa: no; devono esserci una ragione di servizio e un'autorizzazione coerente.

2. Proteggere credenziali, postazione e documenti

Credenziali personali. Ogni operatore usa il proprio account e non comunica password o codici di accesso a colleghi o terzi. L'urgenza non giustifica il prestito delle credenziali: se manca un'abilitazione, occorre attivare il percorso previsto per ottenerla. Se si sospetta che una password sia stata divulgata, segnalare il fatto e seguirne il ripristino attraverso i canali autorizzati.

Postazione di lavoro. Bloccare lo schermo quando ci si allontana, anche per poco tempo. Non lasciare pratiche aperte visibili a persone non autorizzate. Prima di abbandonare la postazione, verificare anche documenti sulla scrivania e stampe rimaste nel dispositivo condiviso.

Documenti cartacei. Riporre i fascicoli nei luoghi previsti, limitarne l'esposizione e gestire il passaggio tra operatori secondo le regole organizzative. Evitare che bozze o copie siano lasciate in spazi accessibili al pubblico; usare le modalità autorizzate di distruzione quando i documenti possono essere eliminati.

Documenti digitali. Utilizzare gli archivi e gli strumenti autorizzati. Non creare archivi personali su dispositivi, caselle di posta o servizi esterni non approvati. Identificare la versione utilizzabile del documento ed evitare che copie locali non aggiornate vengano scambiate per quella corrente.

Controllo prima dell'invio. Verificare destinatario effettivo, eventuali persone in copia, allegato e versione, dati strettamente necessari e canale autorizzato. Non affidarsi soltanto al nome suggerito automaticamente dalla rubrica. Se la richiesta proviene da un soggetto non verificato, sospendere l'invio e chiedere conferma attraverso un contatto già riconosciuto.

Correzioni tracciabili. Correggere un errore non significa nasconderne l'esistenza. Usare le funzioni e le registrazioni previste per rendere ricostruibili autore, data, motivo e contenuto della modifica. Questo non autorizza a conservare copie indiscriminate: le evidenze vanno mantenute nei limiti e con gli accessi previsti.

Mini-esercizio orale. «State per inviare un fascicolo: quali controlli eseguite?» Chiedere almeno tre risposte: destinatario, allegato corretto, necessità dei dati; completare con verifica del canale e delle persone in copia.

3. Riconoscere e segnalare un incidente

Una violazione dei dati personali può compromettere la **riservatezza** (accesso o divulgazione non autorizzati), l'**integrità** (alterazione) o la **disponibilità** (perdita, distruzione o impossibilità di accesso). Non riguarda quindi soltanto la pubblicazione di informazioni: anche la perdita di un fascicolo o l'alterazione di dati può richiedere una valutazione. Riferimento: violazioni dei dati personali, Garante.

Percorso operativo proposto, da raccordare alla procedura interna.

1. **Interrompere l'attività rischiosa.** Non proseguire con altri invii o consultazioni che potrebbero aggravare l'evento.
2. **Segnalare immediatamente.** Informare il referente individuato dall'organizzazione usando il canale previsto, anche quando le conseguenze non sono ancora chiare.
3. **Descrivere i fatti.** Indicare quando l'evento è stato rilevato, quale sistema o documento è coinvolto, cosa è accaduto, quali destinatari o dati sono interessati e quali prime azioni sono state compiute. Distinguere fatti accertati e aspetti da verificare.
4. **Preservare le evidenze.** Non cancellare messaggi, registrazioni o documenti per nascondere l'errore. Evitare, però, di diffonderli ulteriormente nella segnalazione.
5. **Seguire le istruzioni.** Attuare contenimento e recupero con il personale competente; non improvvisare comunicazioni esterne o interventi tecnici.

Chi valuta la notifica. Il titolare del trattamento deve notificare al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dalla conoscenza della violazione, salvo che sia improbabile un rischio per i diritti e le libertà delle persone. Il responsabile del trattamento informa tempestivamente il titolare. Il termine non è un tempo di attesa concesso all'operatore: la segnalazione interna deve essere immediata secondo il testo originario. Riferimento: obblighi e tempi di notifica.

Il titolare documenta tutte le violazioni, anche quando non è necessaria la notifica. Se la violazione presenta un rischio elevato, è prevista anche la comunicazione agli interessati, salvo le eccezioni applicabili. Non ogni errore richiede automaticamente una notifica: occorre una valutazione del caso da parte delle figure competenti. Riferimento: documentazione e comunicazione agli interessati.

Messaggio chiave. «Segnalare subito permette di intervenire; nascondere o minimizzare un errore impedisce di valutarlo correttamente».

4. Audit e pista di controllo

In sede di audit non basta che un documento sia presente: occorre poter ricostruire il percorso seguito. Il testo originario richiede di dimostrare chi ha operato, su quale base, quali controlli sono stati svolti e come sono state gestite le non conformità.

La pista di controllo. Per la pratica esaminata, ricercare le evidenze previste dalla procedura: identificazione del fascicolo, documenti utilizzati e loro versione, presupposto dell'operazione, autore e data, controlli svolti ed esito, eventuali modifiche e motivazioni, anomalie e interventi successivi. La lista è uno schema didattico, non sostituisce la modulistica ufficiale.

Reperibilità, integrità e ricostruibilità. Reperibilità significa trovare l'evidenza nell'archivio autorizzato; integrità significa proteggerla da alterazioni improprie; ricostruibilità significa collegare documenti, azioni e controlli in un percorso comprensibile. Un file presente sul computer personale non costituisce, da solo, una pista di controllo completa.

Come rispondere a un rilievo.

1. Descrivere il fatto e il requisito non rispettato, facendo riferimento alle evidenze disponibili.
2. Valutare l'effetto sulla pratica e la necessità di intervenire subito.
3. Individuare la causa, senza limitarsi a una formula generica come «distrazione».
4. Definire, quando necessario, l'azione correttiva, il responsabile della sua attuazione e il termine.

5. Registrare l’intervento svolto e verificarne l’efficacia prima della chiusura.

Esempio ipotetico. Un fascicolo è privo della data di controllo. Non inserire una data presunta né retrodatare il documento. Verificare se esistono evidenze del controllo effettivamente svolto; se mancano, segnalare la carenza e organizzare il controllo secondo le istruzioni applicabili, registrando la data reale. Se il problema si ripete, valutare un miglioramento del processo, ad esempio un campo obbligatorio nel modello, se consentito dai sistemi e dalle regole interne.

Domanda al gruppo. «Qual è la differenza tra completare oggi un controllo mancante e dichiarare che era già stato svolto?» Risposta attesa: nel primo caso si documenta un’attività reale; nel secondo si crea un’evidenza non attendibile.

Verifica rapida

Consegna. Presentare i tre casi ipotetici senza leggere subito le soluzioni. Dedicare circa sei minuti alla discussione e quattro minuti alla restituzione e al riepilogo. Per ogni caso chiedere: quale rischio emerge, quale prima azione va compiuta, quale evidenza occorre mantenere?

Caso 1 – Password condivisa

Situazione. Un collega chiede di usare l’account di un altro operatore per chiudere una pratica urgente.

Risposta attesa. Non condividere le credenziali; richiedere l’abilitazione o l’assistenza attraverso il percorso autorizzato. Se la password è già stata condivisa, segnalare l’accaduto e seguire le istruzioni per il ripristino della sicurezza. Il rischio riguarda accessi non autorizzati e attribuzione non attendibile delle operazioni. Non inserire mai la password nella segnalazione.

Caso 2 – Allegato inviato al destinatario sbagliato

Situazione. Dopo l’invio di un messaggio, l’operatore si accorge che il destinatario non è quello previsto e che l’allegato contiene dati personali.

Risposta attesa. Segnalare subito l’evento al referente previsto e conservare le evidenze dell’invio. Seguire le istruzioni per contenere la divulgazione; l’eventuale richiesta di cancellazione o il tentativo di richiamo non dimostrano, da soli, che il destinatario non abbia avuto accesso al documento. Non inviare autonomamente notifiche al Garante: la valutazione compete alle figure preposte. La divulgazione non autorizzata rientra tra i possibili casi di violazione dei dati personali.

Caso 3 – Fascicolo privo della data di controllo

Situazione. Durante una verifica emerge una scheda compilata senza data del controllo.

Risposta attesa. Verificare le evidenze disponibili e segnalare la carenza; non aggiungere una data inventata. Se occorre ripetere o completare il controllo, registrare l’attività effettiva e il suo esito. Collegare il rilievo all’intervento necessario, con responsabile e termine. Il rischio riguarda la ricostruibilità della procedura; la sola data mancante non dimostra automaticamente una violazione di dati personali.

Criteri di verifica didattica. La risposta è completa quando identifica il rischio, propone una prima azione coerente e chiarisce quale evidenza conservare. Se un passaggio manca, chiedere al partecipante di riformularlo e discuterlo con il gruppo.

Riepilogo per il partecipante

- **Prima di accedere:** verificare esigenza di servizio e autorizzazione.
- **Durante il lavoro:** usare credenziali personali, proteggere la postazione e limitare copie e consultazioni.
- **Prima di inviare:** controllare destinatari, allegato, necessità dei dati e canale.
- **In caso di incidente:** interrompere l'attività rischiosa, segnalare immediatamente e preservare le evidenze.
- **Quando si corregge:** seguire il percorso autorizzato e mantenere ricostruibili le operazioni.
- **In sede di audit:** esibire evidenze coerenti e gestire i rilievi con azioni, responsabilità e termini.

Chiusura suggerita. «Ogni pratica deve essere necessaria, protetta e ricostruibile. Prima di agire, verificate; quando emerge un problema, segnalate; dopo l'intervento, documentate».