

Care Colleghe, Cari Colleghi,

prosegue la nuova serie di Newsletter legata agli Schemi di Certificazione di AICQ SICEV. Questa volta la "pillola formativa" si riferisce ai timori ed ai dubbi che possono sorgere durante l'esecuzione di "audit in incognito", che mi ha messo a disposizione il collega e amico Ugo de'Sperati, che in ambito AICQ SICEV, opera come Referente per lo Schema Mystery Auditing. Troverete i Suoi riferimenti, in calce all'articolo, che Vi consentiranno di contattarlo qualora necessitate di chiarimenti e ulteriori informazioni.

Buona lettura e buon lavoro.

Roberto De Pari
Direttore AICQ SICEV

Know how in pillole:

AUDIT IN INCOGNITO: ALCUNI TIMORI E DUBBI DA FUGARE

L'**audit in incognito**, così come da definizione della norma UNI/TS 11312, ha *lo scopo di valutare la qualità delle attività di interfaccia tra cliente ed Organizzazione* di servizi e quindi è, in sostanza, una metodologia di monitoraggio delle prestazioni. Essa viene oggi utilizzata in modo più o meno approfondito con risultati anche molto diversi, in funzione degli obiettivi e del campo di applicazione.

Il tipo di metodo di monitoraggio impiegato fornisce sicuramente importantissimi elementi per valutare realmente, nelle Organizzazioni che erogano servizi, **performances, ambienti, attività, professionalità**.

Il fatto che non sia soltanto un audit "a sorpresa", cioè senza preannuncio, che già costituirebbe maggiore garanzia di attendibilità di quanto valutato ma sia proprio "in incognito", nel senso che nessuno sa chi è e quando agisce il valutatore perché questi potrebbe essere un cliente o utente qualunque (nella definizione della UNI/TS 11312 si cita che l'auditor non deve *farsi riconoscere come tale dal personale dell'Organizzazione auditanda*), aumenta di gran lunga la **credibilità** dei dati e informazioni raccolti e del tipo di "sistema di misurazione". E' sicuramente tra i migliori metodi di controllo della qualità dei servizi in tempo reale utilizzabili oggi e si basa su un principio semplice ma fondamentale: **il cliente è il miglior indicatore della qualità erogata attraverso l'esperienza personale di fruizione (e percezione) di un servizio**. Il fulcro del metodo dunque sta proprio nel **cliente-valutatore** e l'efficacia della sua azione dipende in particolare dalle sue **caratteristiche personali**, dalla sua **professionalità**, dal suo **rigore etico**.

Nonostante sia un metodo di monitoraggio dei servizi molto efficace esso è ancora troppo poco o mal conosciuto e limitatamente applicato. Spesso la sua conoscenza si riduce a quelle applicazioni in termini di "mystery shopping" che, nella stragrande maggioranza dei casi, utilizzano tale metodo con "basse" finalità e scarse professionalità e che alimentano timori e scetticismi. Il recente schema di certificazione di parte terza della professionalità di Mystery Auditor, messo a punto da AICQ SICEV, va sicuramente a colmare alcune criticità in questo senso e garantisce maggiormente le caratteristiche professionali e deontologiche richiamate sopra.

Un ulteriore elemento di resistenza rispetto a tale metodo è costituito, a prescindere dalle applicazioni, da un atteggiamento comune di timore: diverse persone infatti temono le valutazioni, anche se indirette, afferenti al proprio lavoro, figuriamoci se queste avvengono in incognito.

Inoltre è naturale che chi conosce poco la metodologia o di essa ha esperienze limitanti si ponga dei dubbi sulla legittimità di alcuni procedimenti.

I fattori legati al timore delle valutazioni passano sicuramente attraverso considerazioni di natura culturale e/o legate all'organizzazione del lavoro.

Molti lavoratori temono infatti possibili ripercussioni sul proprio lavoro o sulla propria persona. Ciò è ancora più vero in Organizzazioni dove l'ambiente di lavoro, a partire dal management, è fortemente competitivo e dove vi è scarsa fiducia e stima nelle persone, Organizzazioni cioè ancora impostate secondo una vecchia logica gerarchica post-Tayloristica e poco collaborativa. Un salto culturale in questo senso permetterebbe di innalzare la qualità del lavoro e delle relazioni e potrebbe innescare meccanismi virtuosi che fanno vivere il giudizio altrui e il confronto sereno con gli altri come sprono per migliorarsi e per rendere migliori le proprie prestazioni. In ogni caso l'esempio di manager pronti a farsi valutare per primi costituirebbe un tassello fondamentale nel ciclo virtuoso del miglioramento e nei meccanismi di fiducia da parte dei lavoratori all'interno dell'ambiente di lavoro. Se in un'Organizzazione si cerca di vivere questo spirito sarà molto semplice condividere una metodologia come quella dell'audit in incognito che, nella maggior parte delle applicazioni, serve a migliorare, sicuramente non a punire.

Possono inoltre esserci situazioni in cui, dai giudizi espressi nei risultati desunti dalla metodologia del "mystery auditing", è possibile risalire alle persone esecutrici delle prestazioni oggetto dell'audit. Va in questo caso ricordato che normalmente i report degli audit in incognito sono redatti nella forma più anonima possibile. Come riportato nel par 8.3 della linea guida UNI/TS 11312 le modalità di redazione dei report di visita e addirittura l'eventuale citazione, nelle relazioni di visita, dei nominativi del personale, devono essere definiti preventivamente in sede progettuale/contrattuale e/o nell'ambito della sottoscrizione delle regole comuni.

In ogni caso, il principio basilare è che chi lavora con professionalità e con coscienza non ha nulla da temere da un audit che, anzi, costituisce un'occasione per riflettere, confrontarsi e crescere; se anche si sbaglia, come accade a chiunque lavora, è fondamentale che non ci si senta colpevolizzati, ma che gli errori diventino, sempre, occasioni di miglioramento.

Una situazione limite potrebbe presentarsi invece in professioni e situazioni dove l'errore o l'omissione può diventare un potenziale rischio di reato per i responsabili. Si pensi ad esempio a situazioni rilevate in audit in incognito che evidenziano un alimento scaduto o, peggio, una prestazione medica inadeguata o un dispositivo antincendio fuori uso o, ancora, una procedura di sicurezza non effettuata. E' chiaro che, in questi casi, occorre, per prima cosa tenere conto di quale sia la finalità dell'audit in incognito e di chi lo abbia commissionato. Paradossalmente la metodologia dell'audit in incognito potrebbe essere anche commissionata da una Autorità Pubblica di controllo (es. una Procura o un Tribunale o i NAS). I dati e i rilievi servono a capire situazioni e problemi per migliorarli e correggerli, ad elaborare soluzioni e azioni sistematiche per prevenire potenziali criticità e non necessariamente per "punire", sanzionare, denunciare; la metodologia rappresenta uno strumento in più per prevenire situazioni e derive più gravi.

E' ovvio che, a fronte di mancanze del tipo sopra descritto, deve sempre seguire un'azione e un successivo controllo, documentato, con responsabilità definite.

Questi aspetti critici fanno capire, ancor più, come i dati, le registrazioni e i risultati dell'audit in incognito debbano essere salvaguardati e utilizzati con attenzione.

Per contro, esistono diversi casi di applicazione dove le stesse Organizzazioni hanno concordato con i lavoratori che i premi e gli incentivi retributivi siano, anche, legati agli esiti di valutazioni in incognito effettuate nell'ambito di programmi aziendali.

Vale la pena ricordare che il punto 4.2 della linea guida UNI/TS 11312 sugli aspetti etici indica, nei casi di applicazioni differenti da benchmarking e ricerche di mercato, che *il personale dell'Organizzazione auditanda dovrebbe essere consapevole ed informato che il proprio lavoro può essere oggetto, in ogni momento, all'audit condotto in incognito e che altri soggetti eventualmente coinvolti (Sindacati, Associazioni di*

categoria, Associazioni dei consumatori, ecc.) dovrebbero condividere finalità e metodologia. Eventualmente possono esserne sottoscritte le regole (per esempio attraverso disciplinari, regolamenti, contratti, ecc.).

Inoltre aspetto fondamentale indicato a chiare lettere: *le risultanze dell'audit non devono essere utilizzate contro il personale interno ed esterno che collabora con l'Organizzazione.*

Nel caso di utilizzo della metodologia per programmi di incentivazione della forza lavoro dovrebbe essere preventivamente richiesto il consenso personale.

In relazione ai dubbi di legittimità di alcune procedure impiegate normalmente nell'audit in incognito spesso viene posta la seguente domanda: **quali dati e informazioni si possono raccogliere, registrare e trattare durante un audit in incognito ?**.

La risposta a questo quesito, come peraltro a molte altre domande su questo tipo di metodo, dipende certamente da quello che è lo scopo dell'audit in incognito, dal settore e campo di applicazione, dal committente.

E' evidente la necessità dei dovuti approfondimenti della legislazione applicabile in materia, una volta individuato l'obiettivo del monitoraggio.

Lo stesso punto 6 della UNI/TS 11312 riguardo al **criterio di riservatezza** richiama al rispetto delle leggi cogenti in materia, già in fase progettuale.

Si applicano quindi i dettami applicabili relativi alla **legge 20 maggio 1970, n. 300**. In nessun caso infatti potrà essere effettuato un controllo a distanza dei lavoratori di un'Organizzazione o qualunque pratica in disaccordo con lo Statuto dei Lavoratori.

Sicuramente risulta quasi sempre applicabile il **D. Lgs. 196/03** relativo alla "privacy". Vale quindi in generale il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone, in particolare il diritto alla riservatezza e all'identità personale.

Inoltre nel caso di fotografie e video si applica anche la **legge n. 633**, del 1941 ma ancora attuale, sulla "protezione del diritto d'autore e di altri diritti connessi al suo esercizio".

Effettuando un audit in incognito, infatti, a seconda del settore di applicazione, dei requisiti da verificare e degli strumenti di indagine utilizzati, si potrebbe venire a conoscenza di informazioni "delicate", cui si applicano le cogenze di cui sopra, quali:

- 1) dati personali, ad esempio dati identificativi e anagrafici relativi al personale con cui si è interagito, dati di altri clienti, fotografie o video raffiguranti personale con cui si è interagito, fotografie o video raffiguranti altri clienti
- 2) dati sensibili, ad esempio di natura medica inerenti la salute di altri clienti, legati all'appartenenza del personale o di altri clienti ad associazioni politiche e sindacali, relativi alle preferenze politiche o religiose del personale o di altri clienti
a cui si aggiungono:
- 3) informazioni sui comportamenti, che possono riguardare attuazioni od omissioni da parte del personale di determinate procedure, comportamenti lesivi (verbali o fisici) nei confronti dei clienti, comportamenti omertosi o fraudolenti nei confronti dei clienti o della proprietà.

Le situazioni sono molto diverse tra loro e possono far nascere azioni ed eventuali livelli di autorizzazione differenziati tra loro in relazione alla finalità dell'audit, sia in fase di sola raccolta delle evidenze (le registrazioni) sia in fase di comunicazione e trasmissione a terzi (per esempio al committente).

Nel caso 1) va certamente ricordato che ogni Organizzazione ha il compito di accordare con i propri dipendenti, consulenti o collaboratori il trattamento dei loro dati personali che spesso è una sorta di "liberatoria" sull'uso di essi per finalità connesse all'attività lavorativa. Pertanto sui **dati personali** di natura anagrafica non vi sono particolari problemi anche perché, in generale, si tratta spesso di un'osservazione di un dato pubblico, cioè osservabile da chiunque, per esempio un nominativo di una persona operante nell'Organizzazione auditata visibile su un badge o ascoltato in una conversazione con un addetto e quindi non dovrebbe costituire un problema poiché verrebbe utilizzato o citato nell'ambito nelle normali mansioni di lavoro.

Quindi se un auditor in incognito, nell'ambito della sua verifica, osserva un nominativo su qualche supporto visivo, ascolta una telefonata in cui l'interlocutore si presenta o riporta per iscritto il cognome di un addetto che si è qualificato, può farlo; non è peraltro detto che gli sia richiesta tale attività. Non può mai invece, ancorché utile, riportare nominativi e dati di altri clienti.

Se poi l'attività di auditing in incognito è rivolta a percorsi di miglioramento o a erogazione di bonus o premi ai dipendenti può diventare addirittura necessario, oltre che raccogliere evidenze sui nominativi del personale e informazioni sul rispetto delle procedure, indicare tali dati precisamente sulle risultanze dell'audit (es. sulle relazioni di visita consegnate alla committenza). Sarà uno specifico disciplinare concordato tra il committente e i lavoratori (e/o loro rappresentanti) a disciplinare tali regole che devono includere le modalità e finalità di trattamento dei dati.

Sicuramente anche tra il committente e chi gestisce ed effettua le verifiche in incognito deve esistere un documento, di solito facente parte di un codice di condotta, che disciplina la raccolta dati nell'ambito del programma di audit.

Per quanto riguarda le **fotografie**, come anche indicato al cap. 7 della UNI/TS 11312, è consigliabile, generalmente, anche per evitare particolari richieste di autorizzazione, che i "Mystery Auditor", nell'eseguirle, non scelgano soggetti umani ma immortalino elementi strutturali: tali foto solitamente supportano alcune evidenze riscontrate che è necessario far presente in modo circoscritto (es. un segno di cattiva manutenzione o imperizia, un elemento di pulizia circoscritto, un cartello segnaletico particolare, un posizionamento errato di un prodotto, ecc.).

Videoregistrazioni e fotografie che riprendono volti umani e dialoghi vanno invece effettuate solamente se sono state preventivamente autorizzate dagli interessati (liberatoria per il diritto all'immagine, informativa e consenso sulla privacy), rispetto all'obiettivo dell'audit. Va da sé che gli altri clienti non devono mai essere né ripresi né fotografati nel corso di un audit in incognito o se fortuitamente lo sono il relativo materiale non può costituire evidenza documentale e va distrutto.

Nel caso in cui l'audit fosse invece condotto per verificare e/o denunciare pubblicamente situazioni anomale o illecite (es.: da un'Associazione Consumatori o in una trasmissione televisiva autorizzata) è necessario raccogliere evidenze sui comportamenti ma non, a meno di "liberatorie" particolari richieste, rendere pubblici i nominativi (e i volti) del personale "incriminato". In tali casi vi è comunque il diritto di cronaca, aspetto che non sarà mai applicabile al caso del "mystery auditing" finalizzato alla verifica della qualità e del miglioramento.

La raccolta e la comunicazione a terzi di dati personali fuori dall'ambito segnalato precedentemente e di **dati sensibili**, come nel caso 2), deve essere invece sempre effettuata attraverso un'informativa al trattamento e autorizzata dai diretti interessati (per quelli sensibili anche dal Garante della privacy). Qualora ciò non si possa effettuare e/o non abbia ragione di essere effettuato, già in sede progettuale occorre tenere in conto che le evidenze di tali dati non devono essere neppure raccolte dagli auditor in incognito. Tra l'altro questi tipi di dati difficilmente hanno utilità per le varie finalità dell'audit.

Un caso comune è rappresentato da un audit presso una struttura sanitaria in cui, tra i requisiti di verifica, si richiede proprio di verificare se e in che modo i dati sensibili dei pazienti sono salvaguardati da riservatezza. Se il Mystery Auditor osservasse che documenti riservati dei pazienti fossero tranquillamente leggibili da terzi, allora dovrebbe certamente segnalare gli estremi di tale problematica riscontrata (luogo/reparto, tipo di documento, ...), ma non i nominativi e le informazioni di natura medica ivi contenuti.

Discorso analogo nel caso di dati sensibili di altra natura, diversa da quella medica.

Il codice di condotta sottoscritto dal valutatore in incognito con il proprio Organismo e il disciplinare delle regole sottoscritto dall'Organizzazione che effettua gli audit con il committente deve sicuramente, se applicabile, escludere la raccolta di tali dati.

In generale vanno:

- determinate le azioni sui dati e le relative regole di trattamento e autorizzazione eventuale, in relazione alle finalità dell'audit e alla legislazione cogente
- elaborati dei documenti, da condividere con le parti interessate, contenenti tali regole (almeno: scopo di utilizzo dei dati; quando devono essere utilizzati e a chi devono/possono essere mostrati; dove e per quanto tempo devono essere archiviati).

Nel caso 3) vi è poi la possibilità di incorrere, durante l'audit in incognito, in osservazioni di reati. Eventuali illeciti, cui eventualmente il Mystery Auditor è stato soggetto attivo (commessi verso di lui) o passivo (osservatore di una situazione), soppesandone comunque la gravità e usando il buon senso e la propria coscienza, vanno evidentemente trattati come in qualunque altro caso in cui si viene a conoscenza di essi, fino quindi, se del caso, alla denuncia presso la Procura. Tale aspetto è peraltro analogo al caso di altri audit, per esempio di sistema.

In altri casi ancora si addita la metodologia del "mystery auditing" come metodo per effettuare dello spionaggio industriale. Niente di più sbagliato. Va sgomberato dal campo ogni equivoco. Tutto quello che l'auditor in incognito osserva è alla luce del giorno: è esattamente quello che osservano tutti gli altri clienti. Anche nel caso di analisi della concorrenza, non vi è divieto né di osservare le pratiche altrui né eventualmente di copiarne le "best practices".

In quest'ultimo caso, come anche per le ricerche di mercato, ancorché abbia utilità raccogliere evidenze circa dati personali delle risorse umane (e di altri clienti) in attività di benchmarking, ne è comunque vietata la registrazione di ogni tipologia, anche perché un accordo tra le parti difficilmente può sussistere. Anche la UNI/TS 11312, nel paragrafo 8.3, indica che *eventuali documenti o copie di essi (fax, mail, ecc.) relativi a verifiche presso concorrenti che sono utilizzati nelle relazioni finali devono essere resi anonimi nelle parti relative ai dati del personale (nomi, indirizzi e-mail, ecc.)*.

Le risultanze dell'audit non devono essere in ogni caso utilizzate per atti di concorrenza sleale.

Un ultimo caso di resistenza all'uso massiccio di tale metodo potrebbe essere costituito dal timore dell'"arma a doppio taglio". E' infatti un metodo che "dice la verità", e la verità per diversi motivi può essere temuta perché scomoda (oltre che mal interpretata o, peggio, mal utilizzata).

Si pensi, ad esempio, alla pubblicità (negativa o positiva) che potrebbe derivare dai risultati di un ciclo di audit in incognito presso delle strutture sanitarie per i soggetti politici coinvolti, nel caso del settore pubblico o per gli imprenditori, nel caso del privato. Peraltro se i risultati fossero positivi ci sarebbe evidentemente un aumento della reputazione e un accordo maggiore di fiducia da parte di utenti e cittadini, come dovrebbe avvenire, d'altra parte, (e in taluni luoghi e paesi avviene) quando si impiega una tipologia di controllo realmente seria.

Un buon progetto, delle regole ben codificate, il personale auditando coinvolto e messo a conoscenza adeguatamente, un field di valutatori professionale sono i presupposti per scongiurare qualsiasi tipo di timore o dubbio in merito all'uso della metodologia.

Con queste condizioni, l'auditing in incognito, a maggior ragione fornendo informazioni "non filtrate" o "inquinata", perché condotto in tempo reale e senza sapere *chi e quando* è anche un metodo molto amato. Chi crede realmente nella Qualità e nel miglioramento non può infatti che augurarsi che tale metodo assuma un rilievo e un'incidenza sempre maggiore nel mondo della Qualità nei servizi, in particolare nella Pubblica Amministrazione, certamente con le dovute garanzie e con la necessaria professionalità.

Ugo de'Sperati
Auditor Team Leader certificato AICQ SICEV per gli Schemi Qualità e Audit in Incognito.
Referente AICQ SICEV per lo Schema "Mystery Auditing".
u.desperati@fastwebnet.it