

SECURITY BANCARIA E VISION 2000

MASSIMO PALLOTTA

Socio benemerito A.I.PRO.S. - Socio AICQ Triveneta

PREMESSA

Questo intervento si pone l'obiettivo di fornire una sorta di *abstract* alla "Guida" riportandone sinteticamente alcuni degli elementi più significativi.

L'obiettivo prioritario del nostro lavoro non è stato quello di arrivare ad una "certificazione" della nostra attuale struttura, ma di organizzarla al meglio per poter rispondere alle richieste "strategiche" che sono arrivate/stanno arrivando in questi momenti di integrazioni o fusioni di banche.

Abbiamo "lavorato" individuando le strutture "chiave" della *security* e le abbiamo riportate, per governarle meglio, in una organizzazione/funzione "autonoma" che abbiamo chiamato "Struttura di *security* - SdS" e che abbiamo ipotizzato erogare (in outsourcing o come funzione interna) i propri servizi ad una Banca o a un gruppo di Banche in stretta collaborazione con le stesse.

Nella **Guida** sono raccolti in appositi riquadri o allegati alcuni esempi di applicazioni pratiche del Sistema Gestione Qualità della SdS. Questi esempi potranno servire quale spunto per le vostre incombenze quotidiane (per consentire una lettura "contigua" alla norma, la "Guida" adotta stessa numerazione dei capitoli e dei paragrafi della norma ISO 9001:2000).

Se la vostra struttura non ha ancora adottato un Sistema di Gestione per la Qualità, potrete trovare utili suggerimenti per una sua impostazione efficace e non burocratica.

1. INTRODUZIONE

La norma UNI 10549:95 definisce la "security aziendale" quale: "Studio, sviluppo ed attuazione delle strategie, delle politiche e dei piani operativi volti a prevenire, fronteggiare e superare eventi in prevalenza di natura dolosa e/o colposa che possono danneggiare le risorse materiali, immateriali, organizzative e umane di cui l'azienda dispone o di cui necessita per garantirsi un'adeguata capacità concorrenziale nel breve, nel medio e nel lungo termine".

I principali eventi analizzati sono: Rapina - Furto - Frode/Truffa - Attentati/Danneggiamenti - Computer crime. Sono state quindi individuate le principali attività ("servizi") della "SdS": Progettazione - Analisi - Gestione - Esercizio - Protezione da rischi specifici.

2. IMPOSTAZIONE CONCETTUALE DELLA ISO 9001:2000

Le VISION 2000 (ed i Sistemi di Gestione per la Qualità ivi trattati) non impongono alcun modello operativo generico preconstituito (o fotocopiato), ma forniscono strumenti metodologici per meglio analizzare l'efficacia e l'efficienza del proprio sistema di gestione enfatizzando i suoi punti di forza e fornendo, per i punti deboli individuati, appropriate soluzioni.

Si ricorda anche che le VISION 2000:

- consentono di adeguare il SGQ alla realtà di ogni singola azienda, offrendo una significativa (e responsabile) libertà operativa;
- concepiscono il SGQ come un investimento in grado di garantire all'azienda i dovuti ritorni - anche economici.

Per consentire una più agevole individuazione dei traguardi a cui il SGQ fa riferimento, sono stati tenuti presenti i seguenti "principi di gestione per la qualità" (che riflettono le impostazioni - di buona tecnica - dei più recenti modelli organizzativi e gestionali):

Organizzazione orientata al cliente. Una risposta più flessibile, rapida ed efficace alle esigenze/aspettative - non solo esplicite - del cliente consente di aumentare le "quote di mercato".

Coinvolgimento del personale. Per responsabilizzare il personale, stimolando innovazione, creatività e desiderio di contribuire al miglioramento dell'efficienza e dell'efficacia dell'azienda.

Approccio per processi. L'utilizzo efficace delle risorse disponibili permette di meglio individuare le priorità d'intervento, di ottenere minori costi e di raggiungere risultati migliori.

Approccio sistemico alla gestione. L'integrazione e l'allineamento dei processi favorisce l'individuazione dei processi più importanti, il raggiungimento degli obiettivi aziendali ed il consolidamento della fiducia di tutte le parti interessate sulla efficacia ed efficienza dell'azienda.

Miglioramento continuativo. Per migliorare le potenzialità organizzative e garantire una maggior flessibilità e prontezza nel rispondere alle esigenze/aspettative del cliente.

Decisioni basate su dati di fatto. L'analisi di dati ed informazioni consente decisioni razionali basate su fatti reali e bilanciate con l'esperienza, la competenza e l'intuizione.

Rapporti di reciproco beneficio con i fornitori. Per ottimizzare costi e risorse, creare valore e rispondere adeguatamente alle esigenze/aspettative del cliente.

Leadership. Per motivare il personale nel raggiungere gli obiettivi aziendali rendendo coerenti le diverse attività e riducendo le difficoltà di comunicazione fra i diversi livelli aziendali.

Il modello di Sistema Gestione Qualità, basato sui processi, evidenzia due cicli distinti, ma fra loro interconnessi:

- Ciclo "Interno": parte dal ruolo trainante del "Vertice", evidenzia l'esigenza di adeguate risorse per garantire la realizzazione dei prodotti aziendali e ritorna poi al "Vertice" con i risultati delle misurazioni, delle analisi e di quanto è stato attivato per consentire il miglioramento del SGQ;
- Ciclo "Esterno": il cliente stabilisce i requisiti del prodotto/servizio, riceve quindi questo prodotto/servizio rispondente a quanto richiesto e fornisce poi all'organizzazione indicazioni utili per renderlo sempre più rispondente alle proprie esigenze/aspettative.

3. IMPOSTAZIONE PER PROCESSI

Nella norma ISO 9001:2000, al punto 0.2, si ha: "L'applicazione di un sistema di processi nell'ambito di una organizzazione, unitamente all'identificazione e alle interazioni di questi processi nonché alla loro gestione, viene denominata "approccio per processi".

Nella definizione possono riconoscersi due dei "principi di gestione per la qualità" precedentemente cennati:

1. L'approccio per processi. Un risultato desiderato si ottiene con maggior efficienza quando le relative risorse ed attività sono gestite come un processo.
2. Approccio sistemico alla gestione. Identificare, capire e gestire un sistema di processi interconnessi, mirati a determinati obiettivi, migliora l'efficacia e l'efficienza dell'organizzazione.

La norma sottolinea la necessità di migliorare in modo continuo anche l'efficienza dei processi e delle loro interazioni e di provvedere ad una loro identificazione.

Una corretta analisi dei processi parte dal macroprocesso che caratterizza gli obiettivi aziendali, individuando i dati d'ingresso, i vincoli, le risorse necessarie e gli elementi in uscita.

In questo capitolo della "Guida" sono riportati alcuni esempi di processi rappresentati utilizzando diverse metodologie.

4. SISTEMA DI GESTIONE PER LA QUALITÀ

Inizia da questo capitolo l'analisi della norma ISO 9001:2000 che è articolata in:

introduzione: presenta le caratteristiche generali su cui è impostata la norma, l'approccio per processi, la contiguità con la ISO 9004:2000, etc.;

- capitolo 1:** delinea le finalità della norma precisando i criteri da seguire per la sua applicazione;
- capitolo 2:** richiama altre norme i cui contenuti hanno valore anche per la norma stessa;
- capitolo 3:** rinvia, per il significato dei termini utilizzati nella norma, alla ISO 9000:2000;
- capitolo 4:** tratta dei requisiti generali per l'applicazione della norma e dei requisiti previsti per la documentazione;
- capitolo 5:** evidenzia l'importanza del vertice aziendale sia direttamente che come elemento determinante per l'impostazione e l'attuazione del SGQ;
- capitolo 6:** riguarda tutti i tipi di risorse, sia quelle umane sia quelle strumentali in senso lato (infrastrutture) e precisa i requisiti dell'ambiente di lavoro;
- capitolo 7:** tratta di come il SGQ deve essere applicato ai processi attraverso i quali l'organizzazione esercita la sua attività;
- capitolo 8:** riassume le diverse attività per assicurare il funzionamento del SGQ, la rispondenza dei processi ai requisiti e le opportunità di miglioramento;
- due appendici:** corrispondenza fra la ISO 9001:2000 e la ISO 14001:1996 - corrispondenza fra la ISO 9001:2000 e la ISO 9001:1996.
- La decisione di adottare un SGQ compete al "Vertice" della "SdS". Tale decisione (di valenza strategica) non deve essere solo formale: il "Vertice" deve dare il "buon esempio" anche vigilando sulla applicazione del SGQ e stimolando il suo progressivo miglioramento.
 - Per una corretta individuazione (e attribuzione) delle responsabilità nello svolgimento delle diverse attività fra loro interagenti, l'approccio per processi risulta necessario, soprattutto quando si è in presenza di unità operative/funzionali diverse.
 - Per migliorare il livello di controllo, anche qualitativo, dei processi "esternalizzati"/in "outsourcing" (almeno per quelli più importanti e significativi: manutenzione impianti di allarme, vigilanza, etc.). sono richieste adeguate forme di sorveglianza.
 - La documentazione comprende: la politica per la qualità ed i relativi obiettivi, il manuale della qualità, le procedure espressamente richieste ("documentate") dalla norma, i documenti necessari per pianificare/realizzare/controllare e rendere efficaci i processi della "SdS" e le registrazioni della qualità che servono a dimostrare l'efficacia del SGQ e la sua conformità alla norma.
 - Per alcune attività la norma obbliga all'emissione di procedure "documentate". Vale a dire per la gestione di: documentazione, registrazioni della qualità, verifiche ispettive (audit) del SGQ, non conformità, azioni correttive e azioni preventive.
 - Tutta la documentazione deve essere immediata, comprensibile e deve contenere solo quanto necessario per garantire il raggiungimento degli obiettivi aziendali. Durante la fase di preparazione dei documenti dovrebbe avvenire il coinvolgimento di chi dovrà poi sviluppare i processi reali.
 - Il "manuale della qualità" fornisce al personale riferimenti sintetici ed univoci sulla interazione fra i processi della "SdS" e sulle procedure del SGQ, garantendo un quadro d'insieme utile per un maggior coinvolgimento del personale. Il manuale è utile anche per le relazioni "esterne".
 - Per garantire l'efficacia e l'efficienza dell'attività della "SdS" è doverosa una gestione controllata della documentazione, non solo perché richiesta dalla norma, ma soprattutto perché è necessario poter disporre di documenti correttamente progettati, elaborati, verificati, approvati, registrati, riproducibili e rintracciabili.
 - La norma prevede che venga predisposta una apposita "procedura documentata" per tenere sotto controllo la documentazione.
 - Sono da considerarsi registrazioni tutti quei documenti che affermano l'avvenuta esecuzione delle attività riportandone i relativi risultati e che registrano situazioni accertate (ad esempio: non conformità, serie di misurazioni, etc.).

- Dalla norma è previsto l'obbligo di manutenzione e conservazione delle registrazioni in 21 casi. La "SdS" può (deve) altresì ritenere opportuno, per diverse motivazioni, raccogliere e conservare altre registrazioni di proprio interesse.
- Per garantire riservatezza, facilità nella rintracciabilità e nella analisi è opportuno che tutta la documentazione sia archiviata in modo "protetto" e funzionale alla organizzazione.

5. RESPONSABILITÀ DELLA DIREZIONE

In questo capitolo sono riportate le "evidenze" che la norma pone in capo al "Vertice" aziendale.

- L'adozione di un SGQ deve basarsi sull'analisi dei contenuti e potenzialità e con la convinzione della sua opportunità.
- Il "Vertice", per ottenere il coinvolgimento del personale, deve costruttivamente impegnarsi nella diffusione delle motivazioni della scelta, nella pubblicizzazione sull'andamento del SGQ, nel riconoscimento dell'impegno dimostrato dai singoli, etc.
- Il primo cliente è la Banca stessa, sia come "cliente-committente" che come "cliente-utente". È il "Vertice" che risponde delle attività svolte dalla "SdS" nei confronti dei clienti.
- La "politica per la qualità" deve quindi essere coerente e congruente con le finalità di una "SdS", soprattutto con gli obiettivi da raggiungere.
- La "politica per la qualità" deve essere periodicamente rivista per verificarne la validità e l'adeguatezza nel tempo in rapporto con la evoluzione sia delle esigenze esterne che di quelle interne.
- Un SGQ, per risultare coerente e integrato con l'operatività della SdS, deve individuare gli obiettivi per la qualità sia di tipo "tecnico" che di tipo "gestionale". Per non perdere di significato, gli obiettivi devono essere misurabili.
- Fissando gli obiettivi si stabiliscono i traguardi da raggiungere innovando il modo di orientare il lavoro del personale. Qualora alcuni obiettivi non vengano raggiunti, si dovrà analizzare le cause non per "punire", ma per trarre indicazioni per correggere e meglio orientare gli obiettivi.
- In questo punto la norma richiede al "Vertice" di assicurarsi (e vigilare) che l'attuazione e il corretto sviluppo del SGQ (e dei relativi processi) si basino su un'adeguata pianificazione.
- Una SdS, pur se con dimensioni ridotte, non può prescindere dalla definizione delle responsabilità e dalla loro attribuzione al suo interno. L'attribuzione di responsabilità è ovviamente collegata alla organizzazione ("autonoma" o "interna") della SdS.
- Pur non entrando negli aspetti organizzativi dell'organizzazione, la norma richiede che venga individuata una persona con il compito di "rappresentante della direzione" per i problemi del SGQ e della qualità.
- Il "rappresentante della direzione" deve essere dotato di adeguata autonomia ed autorevolezza e di essere in contatto con la realtà operativa dell'organizzazione. Il compito può essere svolto in contemporanea con altri incarichi anche impegnativi.
- Il "Vertice" della SdS deve assicurare la disponibilità delle risorse necessarie per l'attuazione delle strategie, per lo sviluppo delle attività e per raggiungere gli obiettivi prefissati.
- Secondo la norma il "Vertice" deve non solo adottare un SGQ e fissare gli indirizzi per la sua attuazione, ma deve anche monitorare come tale SGQ viene applicato nella realtà aziendale. La norma indica analiticamente gli elementi in ingresso da sottoporre a riesame.
- Il riesame deve essere condotto dal "Vertice", in quanto più direttamente interessato all'andamento della *security*. Il riesame deve coprire anche i contenuti tecnici dell'attività svolte e non solo gli aspetti gestionali del SGQ. La norma infatti richiede l'esame delle "prestazioni dei processi e le conformità dei prodotti".
- La pianificazione della conduzione del riesame è un compito tipico del "rappresentante della direzione" anche attraverso la predisposizione del relativo materiale di supporto.

- Per ampliare il campo del riesame anche alla “efficienza” del SGQ, la norma ISO 9004:2000 aggiunge anche altri elementi: costi/benefici della *security* - andamento dei costi della qualità e, soprattutto, della “non qualità” - etc.
- Le norme richiedono infine che vengano prese (e documentate) decisioni volte al miglioramento dell'efficacia (e anche dell'efficienza) del SGQ. Tali decisioni devono essere inquadrare nel più generale programma di miglioramento.

6. GESTIONE DELLE RISORSE

Questo capitolo della norma tratta tutti i tipi di risorse (quelle umane, quelle strumentali o “infrastrutture” e quelle relative all'ambiente di lavoro) necessarie per attuare, mantenere e migliorare il SGQ e per assicurare la soddisfazione del cliente (e delle altre parti interessate).

- I requisiti di questo punto precisano, principalmente, le finalità cui sono destinate le risorse che un'organizzazione è tenuta a mettere a disposizione.
- Le finalità richiamate sono essenzialmente due: una interna ed una esterna. La finalità interna delle risorse è relativa alla impostazione, alla gestione, all'aggiornamento ed al miglioramento continuo del SGQ (e alla sua efficacia). La finalità esterna delle risorse è relativa al cliente (e alle altre parti interessate), al modo di soddisfare i suoi requisiti, le sue esigenze e, ove possibile, le sue aspettative.
- Le attività svolte da una SdS richiedono competenze diverse del suo personale: specialistiche, tecniche, organizzative, di formazione, di relazione, etc.
- Le principali caratteristiche della preparazione del personale di una SdS sono: competenza ed esperienza. Per la competenza si rimanda alla norma UNI 10549, per l'esperienza è determinante una conoscenza approfondita delle esigenze, difficoltà e pericoli insiti nelle aree esposte al rischio *security*.
- Per fronteggiare con efficacia l'evolversi del modus operandi della malavita e per seguire le innovazioni tecniche, è opportuno attivare percorsi formativi sia per singole esigenze che per la formazione continua; soprattutto per il personale della SdS che copre ruoli che possono incidere sulla qualità dei prodotti e sulla funzionalità della SdS.
- La norma sottolinea l'importanza che il personale sia consapevole della rilevanza ed importanza del proprio ruolo per il raggiungimento degli obiettivi di qualità (da ciò discende il successo della SdS).
- La norma richiede che venga accertata l'efficacia della formazione attraverso forme documentate: giudizi dei docenti, risultati delle prove di apprendimento e soprattutto i giudizi di chi “utilizza” il personale. Nel caso di ricorso a personale esterno è opportuno prevedere forme di valutazione simili a quelle adottate per l'assunzione di personale.
- Le modalità di formazione risultano diverse se la SdS risulta “autonoma” o “interna”, comunque è opportuno che al proprio interno la SdS abbia le competenze necessarie in materia.
- La norma definisce come “infrastrutture” sia le infrastrutture propriamente dette che le risorse strumentali e i servizi di supporto necessari per svolgere le attività della SdS. Quali risorse strumentali per la SdS si possono indicare: le apparecchiature Hardware, i programmi Software, le connessioni informatiche i canali di comunicazione, etc.
- Anche se non richiesto dalla norma appare opportuno valutare anche quei fattori ambientali che possono impattare sulla motivazione e soddisfazione del personale (rif. ISO 9004:2000).

7. REALIZZAZIONE DEL PRODOTTO

L'applicazione dei requisiti di questo capitolo deve far riferimento alle attività effettivamente svolte da una SdS. Qualora altre attività vengano svolte all'esterno, la norma richiede che una SdS definisca le modalità, mantenga il controllo sui processi “esternalizzati” e si accerti che i risultati del processo rispondano ai requisiti prestabiliti.

- Le forme di pianificazione devono essere adeguate al modo di operare di una SdS e al grado di preparazione degli utilizzatori. Nel caso di attività “a commessa” è opportuna l’adozione di appositi “piani di qualità” supportati da adeguati strumenti (per la pianificazione e per il controllo).
- Nel caso di servizi continuativi la pianificazione richiede, fra l’altro, una programmazione temporale delle attività, la turnazione del personale e la sua formazione.
- Spetta alla SdS individuare i requisiti relativi al prodotto sulla base di un elenco riportato nella norma e altri/diversi documenti dai quali trarre (e rispettare) i requisiti applicabili.
- Per assicurarsi che i requisiti siano chiari, completi e rispondenti alle specifiche applicazioni e che la struttura abbia risorse, capacità o potenzialità per onorare gli impegni derivanti; deve far seguito, alla raccolta dei requisiti, un riesame prima della loro utilizzazione.
- Per stabilire con i clienti (e, se del caso, con le altre parti interessate) rapporti interattivi, devono essere individuati adeguati canali di informazione tali da garantire lo scambio bidirezionale in materia di *security*.
- Le attività di progettazione inquadrabili sotto questo punto della norma sono diverse e riguardano, ad esempio: l’impostazione generale della *security* - le analisi dei dati relativi a siti/processi - la determinazione delle priorità d’intervento - la progettazione funzionale dei sistemi di *security* - l’impostazione delle attività di formazione presso i clienti - la definizione/programmazione delle verifiche, della manutenzione e della vigilanza/sorveglianza sui sistemi anticrimine.
- I requisiti di questo punto trovano applicazione anche quando le attività vengono svolte da parte di strutture diverse dalla SdS. L’importanza che riveste la progettazione per la *security* è tale che la SdS ne rimane comunque responsabile anche se l’attività di progettazione viene “esternalizzata”. Questa responsabilità richiede che siano definiti gli ambiti e i relativi requisiti tecnici e siano attivate adeguate forme di controllo su quanto appaltato.
- Una SdS deve individuare e pianificare: le diverse fasi della progettazione e le relative responsabilità - le risorse e le collaborazioni necessarie - gli elaborati e le registrazioni da predisporre - i programmi temporali comprensivi delle fasi di controllo - quant’altro necessario a predefinire lo sviluppo dell’attività. La norma richiede inoltre che la pianificazione venga aggiornata.
- Tenuto conto che per l’attività di una SdS la progettazione è particolarmente significativa, deve essere predisposta (anche se non esplicitamente richiesta dalla norma) una apposita procedura con le modalità gestionali della progettazione.
- Gli elementi d’ingresso della “impostazione generale” della *security* sono costituiti da: obblighi di tipo legislativo, regolamentare e sindacale, dati storico-statistici del settore bancario, tecniche adottate per la valutazione dei rischi, etc.
- La norma richiede che i dati d’ingresso vengano documentati. I piani di progettazione costituiscono la sede più adatta per tale documentazione.
- Già nella fase di pianificazione della progettazione, devono essere individuati gli elaborati che costituiscono gli “elementi in uscita della progettazione”.
- Per valutare l’accettabilità delle soluzioni tecniche e i costi/risultati relativi, gli elaborati di carattere propedeutico allo sviluppo delle attività SdS devono contenere chiare indicazioni per il loro utilizzo. Un esempio di elaborato propedeutico viene riportato nella “Guida” in appendice C: “Esempio di metodo di calcolo del grado di sicurezza”.
- Il RIESAME deve: valutare la compatibilità delle scelte aziendali per lo specifico contesto - evidenziare eventuali altri aspetti da prendere in considerazione nella fase di progettazione - concordare le soluzioni agli eventuali problemi emersi, etc. Nel caso della “impostazione generale” della *security*, il riesame è un’occasione anche per la valutazione periodica delle strategie adottate e delle relative scelte.
- La VERIFICA è opportuno sia affidata ad un soggetto diverso ed indipendente da chi ha predisposto gli elaborati in quanto deve accertare che i risultati della progettazione siano coerenti con i requisiti e gli elementi in ingresso.
- La VALIDAZIONE intende riscontrare se quanto progettato e realizzato soddisfa le esigenze (anche implicite o inizialmente inesprese) dei futuri utenti della *security*. La norma suggerisce che la

validazione sia effettuata contestualmente al primo periodo di fruizione del prodotto/servizio, peraltro è opportuno che venga tenuta separata concettualmente dalla fase contrattuale di collaudo e di primo funzionamento.

- La norma richiede che le tre attività (riesame, verifica e validazione) risultino documentate e conservate e che le relative registrazioni vengano effettuate in accordo con quanto previsto al punto 4.2.4 della norma.
- Le modifiche alla progettazione che comportano la riedizione di elaborati già emessi richiedono di distinguere in modo univoco le diverse revisioni degli elaborati, di documentare le modifiche apportate e di mantenere traccia delle motivazioni che le hanno originate. Alle modifiche della progettazione vanno applicati i requisiti previsti per il riesame, per la verifica e per la validazione.
- Quando si intenda introdurre modifiche alla progettazione è opportuno valutare anche le ricadute che queste modifiche possono avere su altre fasi della progettazione. Soprattutto nel caso di modifiche alle "impostazioni generali" della *security* risulta opportuna, durante la fase di riesame/verifica, valutare anche l'impatto economico di tali modifiche.
- È necessario informare il cliente/utente della SdS, qualora le modifiche alla progettazione siano significative, riguardino elementi già concordati o vengano effettuate dopo la consegna degli impianti.
- Per circoscrivere le valutazioni ai fornitori di prodotti significativi sull'attività della SdS, si devono individuare le tipologie di prodotto/servizio per le quali è necessaria la preventiva qualificazione dei fornitori. È da tener presente che oltre all'importanza dei prodotti/servizi per la *security*, devono essere valutati anche per la loro complessità e per il loro impatto economico.
- Tenuto conto che, in genere, i prodotti/servizi approvvigionati da una SdS sono definiti e relativamente ripetitivi, si potrà adottare le esperienze pregresse come primo riferimento (purché i dati relativi siano oggettivi e documentati). Qualora venga proposto un prodotto/servizio innovativo, per la valutazione del fornitore non si potrà prescindere da pareri da parte di personale anche esterno o da esperienze di altri utilizzatori.
- Nel caso in cui l'importanza (tecnica, economica, etc.) della fornitura sia rilevante e tenuto conto che le esperienze pregresse non sempre sono sufficienti per assicurare sulla efficacia gestionale del fornitore, appare necessario richiedere l'adozione di un SGQ da parte del fornitore. La valutazione del fornitore terrà conto anche della validità sostanziale del SGQ adottato.
- La norma richiede che la valutazione dei fornitori sia documentata. Tale documentazione deve comprendere, oltre all'Albo dei fornitori, le schede di valutazione e l'eventuale altra documentazione di supporto.
- Anche se la norma non lo richiede, è opportuna la predisposizione di una procedura operativa per la gestione del processo di approvvigionamento. Tale procedura, oltre a definire lo schema di flusso del processo (con i diversi tipi di input, output, risorse, interazioni con altri processi, etc.) dovrà trattare anche i seguenti aspetti: interfacce fra le diverse funzioni dell'organizzazione - attribuzioni di responsabilità per le diverse fasi ed attività, sia interne che esterne - criteri di valutazione dei fornitori - criteri e modalità di verifica dei prodotti/servizi approvvigionati - modalità e tipi di registrazioni per garantire una corretta rispondenza delle forniture ai requisiti contrattuali.
- Nel caso di una SdS "interna", la fase di approvvigionamento coinvolge anche funzioni esterne alla SdS e pertanto dovranno essere ben definiti i rispettivi campi di azione, individuate le interfacce, concordati i documenti, etc. In particolare:
 - devono essere definite e distinte le responsabilità, mantenendo nell'ambito SdS tutti i compiti relativi ad aspetti tecnici;
 - devono essere predisposti e condivisi adeguati criteri per la scelta dei fornitori (il parametro del presunto minor costo non deve essere il solo). Ancor meglio se la scelta del vincitore di una gara viene fatta congiuntamente dalla SdS e dagli "Acquisti" della Banca.
 - si deve tener conto infatti non solo del costo d'acquisto iniziale, ma anche dei costi connessi al futuro esercizio, alla manutenzione, alla durata del prodotto, etc. (logica del "ciclo di vita").

- Con riferimento ai “Principi di Gestione per la Qualità”, si ricorda che il principio “Rapporti di reciproco beneficio con i fornitori” può comportare l’ottimizzazione dei costi e delle risorse e garantisce flessibilità e tempestività nelle risposte alle esigenze/aspettative del cliente.
- Per garantire ad entrambi (SdS e Fornitore) la completezza dei documenti contrattuali, sarebbe opportuno che i capitolati e/o le specifiche tecniche contengano: la descrizione dettagliata del prodotto/servizio - la individuazione dei requisiti applicabili (anche quelli di tipo cogente) - le norme tecniche applicabili e i relativi standard di qualità - le clausole di recesso e le eventuali penali - le garanzie sul personale della committente (anche in termini di riservatezza) - etc.
- Si ricorda che per le forniture significative per la *security* o rilevanti dal punto di vista economico, appare opportuno che i fornitori adottino un SGQ, documentando la sua attuazione e dando libero accesso alla SdS per l’effettuazione di eventuali audit.
- Si ribadisce che, nel caso di SdS “interna”, il compito e la responsabilità di gestire gli aspetti tecnico/programmatici dell’approvvigionamento è di esclusiva competenza della SdS.
- È inoltre necessario richiamare quanto previsto dall’art. 7 del D. Lgs. 626/94 in materia di obblighi a carico del committente per appalti di beni e servizi. Per garantire che l’attività di coordinamento, in capo al committente, venga effettivamente svolta, si consiglia la predisposizione di una dichiarazione congiunta (sui rischi e sulle misure di prevenzione, protezione e di emergenza relative ai luoghi di lavoro interessati dal contratto di appalto) che preveda esplicitamente l’osservanza, non solo formale, di quanto disposto dal citato Decreto Legislativo.
- La rispondenza delle forniture ai requisiti contrattuali è condizione necessaria ed essenziale affinché il quadro generale delle installazioni consenta il raggiungimento degli obiettivi di funzionalità ed operatività necessarie per assicurare la *security*. La sorveglianza va quindi adeguata al tipo di forniture, considerando principalmente le loro potenziali ricadute.
- Le attività di sorveglianza non vanno limitate solo a quelle relative ad apparecchiature ed impianti. Anche per gli appalti di servizi, quali: vigilanza delle sedi, trasporto valori, manutenzione impianti, etc., sono necessarie adeguate forme di sorveglianza .
- La conclusione di una fornitura ha quasi sempre dei riflessi di tipo amministrativo e pertanto, oltre alle verifiche di tipo tecnico il cui esito positivo è condizione determinante per l’accettazione di una fornitura, è importante anche accertare che siano stati evasi gli impegni relativi alla documentazione richiesta a corredo della fornitura.
- Nel caso di produzione ed erogazione dei servizi la SdS dovrà definire preventivamente quanto occorre per svolgere le attività anche al fine di eliminare o minimizzare disguidi, contrattempi, intoppi e situazioni anomale e monitorare lo svolgimento delle attività per assicurare che esse si svolgano secondo quanto pianificato e in modo tale da rispettare i requisiti e gli obiettivi prefissati.
- Le attività di sorveglianza sugli impianti sono normalmente continuative. Occorre pertanto pianificare turni di servizio e di reperibilità. La gestione delle situazioni di emergenza deve essere, per quanto possibile, pianificata individuando gli interventi più opportuni per le situazioni di emergenza più probabili.
- Nella maggioranza dei casi la SdS affida all’esterno le attività di: manutenzione, vigilanza, trasporto valori, etc. La SdS è comunque tenuta a svolgere alcune attività determinanti (prima e dopo l’appalto) ed in particolare:
 - la progettazione dei servizi, preparando capitolati, specifiche, requisiti, programmi, etc., che faranno parte delle prescrizioni contrattuali;
 - il controllo sui servizi erogati dall’appaltatore per verificare il rispetto delle prescrizioni contrattuali, dei requisiti cogenti e dell’efficacia dei servizi stessi (anche per poterli migliorare).
- La norma non chiarisce la differenza fra “appalto di servizi” ed “esternalizzazione di processi”. Peraltro si ritiene opportuno considerare gli appalti di particolare rilevanza (ad esempio: sorveglianza degli impianti e loro manutenzione) rientranti in quest’ultima categoria. Così facendo si dovrà mantenere all’interno della SdS il controllo sull’operato dell’appaltatore (con le modalità ritenute più adeguate dalla SdS medesima) e non solo il riscontro finale sulla ottemperanza ai requisiti contrattuali.

- Le attività di sorveglianza e manutenzione devono essere definite in apposite specifiche tecniche (nel caso di appalto) o con procedure (nel caso di gestione interna).
- Il “piano di qualità” risulta un valido supporto alla gestione della commessa in quanto, oltre alla pianificazione delle attività, consente di riunire in un unico documento: i programmi temporali - le risorse necessarie - la scelta dei fornitori - i criteri di sorveglianza - etc.
- La “validazione” dei processi risponde all’esigenza di assicurare che i processi producano i risultati attesi e riguarda, in particolare, i processi per i quali la verifica dei risultati non è possibile in corso d’opera o alla loro conclusione.
- Nel caso di monitoraggio sugli impianti l’identificazione riguarda due aspetti: il personale coinvolto e le anomalie che emergono durante il servizio. Nel primo caso l’identificazione serve anche per la pianificazione del servizio e per la conseguente turnazione del personale. Nel secondo caso (anomalie riscontrate) la loro identificazione coincide con le finalità del servizio.
- L’esigenza di identificazione delle anomalie riguarda elementi quali: il modello e/o la matricola degli impianti e/o apparecchiature interessati all’evento - l’ubicazione dello sportello/agenzia/filiale interessato - etc. L’identificazione risulta utile anche ai fini della rintracciabilità, fra l’altro, per la ricostruzione dell’evento e l’effettuazione di indagini (anche statistiche).
- L’identificazione degli impianti e/o apparecchiature risulta particolarmente utile per la manutenzione, in quanto consente di ottenere utili indicazioni sulla affidabilità degli impianti e/o apparecchiature (e dei loro fornitori). L’identificazione delle situazioni anomale ed il loro andamento nel tempo costituisce un importante dato d’ingresso per l’analisi dei rischi, per la valutazione degli impianti, per la preparazione delle norme di comportamento e per la formazione del personale.
- Per una corretta gestione delle commesse è opportuna la preparazione (ed utilizzazione) di una apposita procedura per razionalizzare e precisare: la responsabilità del capocommessa - le interfacce e i canali di comunicazione con le altre funzioni - la documentazione da scambiare - l’elenco e la struttura della documentazione da predisporre - le registrazioni e la modulistica relativa - lo schema dei programmi temporali da predisporre - le modalità di gestione del budget - la tempificazione delle verifiche e dei riesami - gli indicatori per la gestione della commessa - la struttura del rapporto di fine commessa - etc.
- Un caso di “proprietà del cliente” si ha quando il personale della banca (od un cliente della banca medesima) e il suo patrimonio risultano coinvolti in un evento di *security*. Alcune misure adottate fanno parte integrante del sistema di *security*: accessi controllati, impianti di allarme, etc.
- Un altro tipo di misure sono associate al comportamento umano per definire modalità di comportamento e per curare l’addestramento del personale della banca coinvolto in episodi criminosi.
- Nel caso di una SdS che dimanda a fornitori/appaltatori la messa in opera degli impianti di *security*, la responsabilità che i prodotti rispondano alle prescrizioni contrattuali all’atto del loro trasferimento al cliente rimane in capo alla SdS.
- Il principale campo di applicazione dei dispositivi di monitoraggio e di misurazione (“necessari a fornire evidenza della conformità dei prodotti ai requisiti determinati”) riguarda le attività di collaudo degli impianti e di monitoraggio e manutenzione.
- Nel caso che la SdS utilizzi direttamente apparecchiature/strumentazioni di misurazione, dovrà individuarli e stabilire quali di questi devono rispondere ai requisiti previsti dalla norma. Qualora tali attività vengano svolte dai fornitori, risulta necessario che la SdS ottenga che siano i fornitori medesimi a fornire garanzia del rispetto dei requisiti richiesti.

8. MISURAZIONI, ANALISI E MIGLIORAMENTO

Questo capitolo della norma riassume le diverse attività perché una organizzazione si assicuri che il funzionamento del SGQ (e dei suoi processi) risponda ai requisiti e le modalità per individuare le opportunità di miglioramento delle proprie attività (e del SGQ).

- I requisiti di questo punto sono di carattere generale e si applicano ai processi (che richiedono un’adeguata pianificazione) trattati qui di seguito.

- La pianificazione dei processi di monitoraggio e misurazione implica la predisposizione di strumenti e tecniche adeguatamente documentate.
- Anche se nella norma non vi sono accenni diretti, appare opportuno che la pianificazione individui (oltre alle modalità con cui svolgere le attività) anche una serie di indicatori, diretti o indiretti, e le relative periodicità o scadenze dei rilievi.
- Il monitoraggio della soddisfazione va esteso a tutte le parti interessate (non solo al committente-banca) quando si possano ricavare spunti significativi ed utili al miglioramento del SGQ.
- Tenuto conto che il monitoraggio della soddisfazione del cliente in materia di *security* è reso difficile dalla sua natura stessa, appare opportuno utilizzare non solo indagini dirette, ma anche parametri indiretti purché significativi (ad esempio indagini di fonte ABI, Ministero dell'Interno, Istituti di Ricerca, etc.). La valutazione della soddisfazione può avvenire sulla base dell'andamento temporale di alcuni parametri. Potrà sembrare che questo approccio sia troppo razionale o pragmatico (tenuto conto che si parla soprattutto di soddisfazione delle persone), ma si ritiene opportuno evidenziare il rapporto costi/benefici degli investimenti per stimolare l'interesse del committente-banca.
- Il monitoraggio della soddisfazione del cliente è un processo che richiede: progettazione delle modalità (e degli strumenti) di raccolta - pianificazione operativa e temporale - individuazione delle risorse necessarie - analisi e valutazione dei dati raccolti - loro integrazione con i dati provenienti dal monitoraggio degli indicatori interni.
- Gli audit interni hanno la funzione di riscontrare che l'impostazione del SGQ risponda ai requisiti della norma, che la attuazione del SGQ sia conforme a quanto impostato e che il sistema stesso sia efficace. È importante che gli audit non vengano "subiti", dal personale coinvolto, come attività di tipo inquisitorio.
- Qualora la SdS sia interna e alcune attività vengano svolte da altre funzioni della banca (esterne al SGQ), appare opportuno individuare forme di verifica alternative per assicurare almeno l'adeguatezza delle prestazioni alle esigenze della SdS. Ad esempio si potranno considerare tali funzioni esterne come "fornitori", mantenendo però un controllo (anche indiretto) sui processi sviluppati all'esterno.
- La norma richiede espressamente una "procedura documentata" per la gestione degli audit. Tale procedura deve individuare: l'attribuzione delle responsabilità (e le competenze) nella conduzione degli audit - le modalità di programmazione - l'individuazione delle finalità di ogni singolo audit - le modalità di pianificazione - la documentazione da produrre - etc.
- Per facilitare l'attività degli auditors è opportuna la predisposizione di adeguate liste di controllo per verificare la conformità del SGQ e per raggiungere gli obiettivi specifici dell'attività di audit.
- I risultati degli audit vanno documentati e trasmessi ai responsabili dei processi/funzioni aziendali oggetto dell'audit. Tali soggetti sono tenuti a definire ed adottare le necessarie azioni correttive e/o preventive e a riscontrare, in tempi prestabiliti, che le azioni correttive adottate abbiano risolto le non conformità rilevate ed abbiano rimosso/minimizzato le relative cause.
- Nel caso di prodotti/servizi tangibili, i controlli e la verifica di conformità ai requisiti sono in genere condotti a conclusione dei processi realizzativi. Nel caso di una SdS, ciò non sempre è facile. Ad esempio: per i servizi di tipo continuativo (vigilanza 24 ore su 24) il monitoraggio e le eventuali misurazioni su prodotto/servizio coincidono con quelli del processo di sorveglianza.
- Nella impostazione dei monitoraggi è opportuno dare priorità ai processi primari (i cui risultati sono percettibili anche dai clienti interni od esterni. È però da tener presente che il monitoraggio deve estendersi ai processi di supporto e a quelli direzionali, quando significativi (i processi gestionali del SGQ sono monitorati tramite audit).
- È da tener presente anche la differenza concettuale fra questi due punti:
 - monitoraggio di un processo per mantenere un controllo sull'andamento e sulla corretta conduzione del processo medesimo;
 - monitoraggio del prodotto/servizio per verificare la loro rispondenza e conformità ai requisiti prefissati.

Le esigenze base dei requisiti di questi due punti sono: garanzia che i prodotti/servizi rispondano ai requisiti applicabili - accertamenti nelle fasi più significative - univocità nelle relative responsabilità - predisposizione di documentazione adeguata - attivazione di provvedimenti correttivi (quando necessario).

- La norma definisce la “*non conformità*” (NC): “*mancato soddisfacimento di un requisito*”. È opportuno trattare come NC anche quelle situazioni in cui il requisito non rispettato è “*implicito*”.
- Nel caso di una SdS possono essere rilevate NC nella progettazione, nella installazione di sistemi/impianti di *security*, nella loro gestione operativa, nell'erogazione di servizi, etc.
- La individuazione e risoluzione delle NC relative alle fasi di costruzione ed installazione degli impianti vanno, in genere, riscontrate da chi esegue i lavori. Peraltro è opportuno inserire, nei documenti contrattuali, l'obbligo del fornitore/installatore di gestire e documentare le NC riscontrate e di segnalare alla SdS quelle NC che possono causare ricadute sulla futura operatività degli impianti.
- Anche se vengono affidate all'esterno molte attività (vigilanza, trasporto valori, manutenzione, etc.) attinenti la *security*, la SdS deve mantenere la responsabilità di assicurarsi che le NC vengano riscontrate e adeguatamente risolte.
- Sono pertanto riconducibili e gestibili come NC anche situazioni quali anomalie di funzionamento (essendo “*implicito*” il requisito che l'impianto debba funzionare) ed i reclami dei clienti (in quanto esprimono una aspettativa mancata).
- Spesso le NC relative agli impianti vengono risolte con interventi di manutenzione. La documentazione di tali interventi (e il loro esito positivo) possono costituire/sostituire le registrazioni richieste dalla norma per le NC.
- Le modalità operative per la gestione e la risoluzione delle NC deve costituire materia di addestramento sia per il personale interno che per il personale esterno che potrebbe essere coinvolto (personale in servizio presso filiali, agenzie, etc.).
- La norma richiede una procedura documentata per le NC. I contenuti di massima sono contenuti nella norma. Appare peraltro opportuno prendere in esame anche: individuazione dei prodotti/servizi della SdS (e relativi ambiti) per i quali è applicabile la procedura - modalità di interfaccia con i fornitori/appaltatori e attribuzione delle responsabilità per la gestione di tali rapporti - indicazione di una scala di importanza delle NC (ad esempio: critiche, importanti, secondarie) - predisposizione di indicazioni utili per la loro rapida risoluzione (per le NC di tipo ripetitivo) - la periodica elaborazione delle NC (suddivise per tipologia e per provenienza) - predisposizione di apposita modulistica (tale da consentire la caratterizzazione delle NC e l'individuazione dei servizi/prodotti coinvolti, delle decisioni prese e da chi) - etc.
- L'analisi dei dati si basa su uno degli otto principi di gestione per la qualità: “le decisioni, per essere efficaci, devono basarsi sull'analisi di dati ed informazioni”. La specificità dell'attività svolta dalla SdS richiede una lettura dei requisiti di questo punto della norma non solo per il loro formale rispetto, ma soprattutto per rispettare le finalità che essi si prefiggono.
- Le attività di misura e monitoraggio ed i dati ricavati dagli indicatori sono importanti per valutare l'efficacia e l'andamento dei processi interni ed esterni, la conformità dei prodotti/servizi, il comportamento dei fornitori/appaltatori, etc. Importanza ancor maggiore riveste l'analisi dei dati relativi alla valutazione del rischio, per la quale vengono adottate le misure di *security* e delle informazioni di ritorno dalla gestione operativa dei sistemi di *security*.
- Deve pertanto essere attivato un processo che consenta di individuare, acquisire ed analizzare i dati di interesse. Così facendo si ricaveranno indicazioni utili sia per il miglioramento del SGQ che per la riduzione del rischio (“*prodotto*” della *security*).
- Questo punto della norma (miglioramento continuo) rappresenta una introduzione/riepilogo dei principali punti aventi attinenza con il miglioramento, contiene l'esplicito requisito che il miglioramento va perseguito con continuità e mette in luce le interconnessioni logiche e operative fra i diversi punti della norma. Il miglioramento della efficacia del SGQ va inteso sia come miglioramento dei processi gestionali della SdS che come miglioramento delle sue prestazioni nei confronti dei clienti.

- Migliorare il SGQ sta infatti a significare anche individuare ed tecniche sempre più avanzate di analisi dei parametri di rischio per un adeguamento/miglioramento del grado di sicurezza - esaminare le innovazioni della tecnica per individuare la possibilità di una sempre maggior efficacia ed efficienza - verificare il mercato e le scelte degli "altri" per adottare quelle azioni che hanno evitato o minimizzato i problemi - potenziare, anche strumentalmente, i servizi di monitoraggio e di sorveglianza -ottimizzare i servizi di formazione erogati al personale esterno, utilizzando le informazioni di ritorno e curare la crescita del personale interno.
- Le azioni correttive e le azioni preventive tendono ad eliminare o minimizzare le cause di una NC. Le azioni correttive (AC) mirano ad eliminare le cause di NC già rilevate (su informazioni di ritorno dal campo). Le azioni preventive (AP) puntano ad evitare l'insorgere di NC potenziali, preventivamente ipotizzate.
- Le AC e le AP riguardano qualunque tipo di NC, anche quelle riscontrate sui processi e sulle attività in genere, segnalate da reclami dei clienti, emerse nel corso di audit, etc. È opportuna una preventiva analisi dei costi/benefici ed una scelta di priorità qualora l'adozione di AC e AP abbia significativi risvolti economici.
- Per garantire il miglioramento, la norma richiede la predisposizione di apposite procedure. Tenuto conto della somiglianza dei contenuti è accettabile predisporre un'unica procedura con evidenziate all'interno le differenze di trattamento fra AC e AP. I contenuti di questa procedura sono delineati dalla norma stessa. Risulta inoltre necessario individuare a chi spetta prendere le decisioni.

APPENDICI (della Guida)

- Appendice A** Raccoglie le principali norme (e guide) in materia di Sistemi Gestione Qualità e di *security*.
- Appendice B** Riporta un glossario con le principali voci in materia di Sistemi Gestione Qualità e di *security*.
- Appendice C** Presenta un esempio di "metodo di calcolo del grado di sicurezza" quale strumento per la valutazione del rischio e non solo.
- Appendice D** Raccoglie, sottoforma di domande, una serie di requisiti utilizzabili per la verifica dello stato di attuazione del SGQ privilegiando gli aspetti sostanziali della norma per favorire i riscontri di adeguatezza ed efficacia del SGQ. È utilizzabile dagli audit interni, dai clienti, ai fini certificativi e dal "Vertice" della struttura.