

GESTIONE AUTOMATIZZATA DELLA MANUTENZIONE DEGLI IMPIANTI DI SICUREZZA

ENRICO CUOZZO

Servizio Sicurezza - Banca di Roma

La realizzazione di un'opera, e quindi anche l'installazione di un qualsiasi tipo di impianto, richiede una serie di altre attività successive connesse al suo utilizzo ed alla conservazione della sua efficienza nel tempo.

Tali attività, comprese comunemente sotto il termine di "manutenzione", risultano tanto più complesse ed onerose quanto più rilevante è il valore dell'opera e l'importanza che alla stessa si attribuisce.

La manutenzione assume una rilevanza fondamentale per tutti quegli impianti specificatamente progettati e realizzati per garantire la sicurezza di persone e di beni sotto l'aspetto della "security" perché, oltre ai provvedimenti necessari per ovviare al normale degrado tecnico degli apparati, occorre intervenire per prevenire il possibile compimento di atti dolosi o colposi che possano inficiare l'efficienza stessa degli impianti.

Dal punto di vista meramente tecnico ci si trova quindi in condizioni di soddisfare, in via prioritaria, le seguenti esigenze:

- controllare il funzionamento dell'impianto in modo continuo così da poterne rilevare tempestivamente ogni anomalia;
- poter intervenire in caso di guasto nei tempi e nei modi ritenuti *preventivamente* accettabili per riconferire all'impianto la funzionalità iniziale;
- poter disporre di un archivio degli eventi verificatisi sull'impianto e dei conseguenti provvedimenti adottati.

La gestione di queste attività elementari è ovviamente condizionata dalle dimensioni dell'installazione e dalla complessità degli impianti attivati.

Si è ritenuto opportuno richiamare questi concetti fondamentali, che saranno certa-

mente scontati per la maggior parte dei convenuti, per poter meglio illustrare come sono stati applicati in una realtà complessa qual'è quella della Banca di Roma.

La Banca di Roma, che conta attualmente una rete di circa 1.300 sportelli oltre a numerosi altri edifici ad uso funzionale (Strutture della Direzione Centrale, Centro Elaborazione Dati, Sedi delle Filiali Capo Gruppo, Archivi e Magazzini regionali, etc.) è nata, come noto, dalla fusione, avvenuta in due tempi (1/3/1991 e 1/8/1992) di tre banche preesistenti: Banco di Santo Spirito, Cassa di Risparmio di Roma e Banco di Roma.

Ognuna delle tre banche originarie aveva una propria struttura per la gestione della sicurezza (intesa essenzialmente come security) che risentiva della dimensione stessa della banca e della sua organizzazione centrale e periferica.

Ovviamente le modalità di gestione degli impianti e quindi anche della loro manutenzione non erano identiche, come non erano identiche o simili le stesse banche per modelli organizzativi, diffusione territoriale e standard tecnici adottati.

Nelle stesse banche originarie esistevano inoltre tipologie di impianti diversi in quanto realizzati in epoche differenti, secondo standard diversi e da Imprese diverse.

Il primo impegno è stato quello di costituire, prima della concentrazione delle tre banche, specifici gruppi di lavoro che hanno esaminato le realtà esistenti e progettato il modello organizzativo da attuare una volta avviato il processo di concentrazione.

Ciò ha comportato l'istituzione, presso la Direzione Centrale, del Servizio Sicurezza nel quale sono confluiti gli elementi che già operavano nelle analoghe Strutture esistenti presso le banche di provenienza.

Queste persone hanno quindi immediatamente contribuito alla gestione di tutte le attività connesse alla security nella difficile e delicata fase del processo di concentrazione fra le banche, senza che nei vari settori si manifestassero apprezzabili soluzioni di continuità e, successivamente, anche alla ricostruzione di una banca-dati unitaria dove sono stati introdotti tutti i dati degli archivi cartacei ed informatici già a disposizione dei singoli servizi od uffici preesistenti.

Contestualmente venivano istituiti presso tutte le Filiali Capo Gruppo (circa 45) dei Nuclei preposti all'assistenza tecnica delle dipendenze di aggregazione. A questi Nuclei furono assegnate anche le attività relative agli interventi da effettuarsi nell'ambito della sicurezza.

Successivamente, anche in relazione al notevole e preoccupante incremento delle rapine perpetrate ai danni del Sistema Bancario, che nei primi anni '90 interessò in misura assai rilevante anche la Banca di Roma, il Servizio Sicurezza, d'intesa con il Servizio Organizzazione, stabiliva di istituire presso ogni dipendenza la figura del Responsabile Locale della Sicurezza (generalmente coincidente con quella del Vice Capo Agenzia) e presso le Filiali Capogruppo quella dell'Addetto alla Sicurezza, con funzioni di controllo e raccordo dei Responsabili Locali della Sicurezza delle dipendenze di aggregazione, così da creare una struttura decentrata che risultasse la naturale ed immediata interlocutrice del Servizio Sicurezza della Direzione Centrale.

Successivamente, una volta accertate tutte le tipologie degli impianti di sicurezza attivi e quindi la loro entità, si provvide a stipulare specifici contratti di manutenzione del tipo "full cover service" con le Imprese installatrici e manutentrici. Tali contratti hanno interessato tutti gli impianti di allarme antifurto/antirapina e tutti gli impianti di controllo accessi.

Le caratteristiche fondamentali comuni a tutti i cennati contratti possono essere così riassunte:

- esecuzione di controlli preventivi ad intervalli prestabiliti (solo per impianti di allarme antifurto-antirapina);

- interventi su chiamata da parte della Banca in numero illimitato e comprensivi di ogni onere di mano d'opera e materiali da effettuarsi entro un tempo prestabilito e per gli impianti di allarme anche in orari non lavorativi bancari (reperibilità);
- esclusione di quegli oneri dovuti a danneggiamenti causati da cause accidentali e comunque estranee al normale uso degli impianti stessi.

La stipula di contratti del tipo "full cover service" ha contribuito a ridurre notevolmente le attività amministrative connesse alla gestione dei contratti stessi ma nel contempo ha creato l'esigenza di monitorare l'operato delle Imprese manutentrici.

Era infatti previsto che fossero le dipendenze stesse a richiedere l'intervento della Impresa manutentrica che, operando in regime "full cover service", non era indotta a segnalare puntualmente e soprattutto tempestivamente gli interventi effettuati, come invece sarebbe stata portata a fare, qualora si fosse operato con un altro tipo di rapporto contrattuale, per la contabilizzazione, fatturazione e la successiva liquidazione dei singoli interventi.

L'intervento della Struttura Centrale e specificatamente del Servizio Sicurezza era, ed è, comunque obbligatoriamente richiesto, qualora si verificassero particolari condizioni al contorno, per la istituzione di servizi di vigilanza armata a carattere straordinario quale misura cautelativa per far fronte alla temporanea inefficienza dei sistemi di sicurezza.

Tale attività comportava quindi la necessità di effettuare un puntuale controllo dell'operato dell'Impresa manutentrica con particolare riguardo ai tempi di intervento e al ripristino della piena efficienza delle apparecchiature al fine di limitare al minimo i costi connessi all'istituzione dei suddetti servizi di vigilanza.

Non era quindi possibile monitorare e gestire *tutti* gli eventi che erano risolti senza l'impiego di servizi di vigilanza straordinari. Ciò non consentiva di accertare l'effettiva funzionalità ed efficienza degli impianti né di poter intervenire in tempo utile sull'operato delle Imprese manutentrici e soprattutto, particolare non trascurabile, di poter effettuare

un'analisi critica delle segnalazioni dei guasti, o presunti tali, che - come l'esperienza insegna - a volte possono essere i sintomi di azioni criminose in atto.

Si è deciso quindi di attivare una procedura che consentisse di monitorare in tempo reale ogni evento rilevato dagli impianti di sicurezza oppure ogni anomalia cui gli stessi fossero stati soggetti.

Tale procedura, parzialmente automatica per quanto concerne le segnalazioni prodotte dagli impianti di allarme antifurto-antirapina in quanto recepite direttamente dalle apparecchiature di controllo centralizzate, non lo era e non lo è per quanto riguarda gli impianti di controllo accessi né per quelle anomalie degli impianti di allarme che non abbiano originato una segnalazione di allarme.

La prima necessità emersa in questa fase fu quella di individuare una procedura che avesse i seguenti requisiti:

- certezza dell'invio e della ricezione del messaggio;
- riservatezza della segnalazione;
- univocità dei dati segnalati;
- minor coinvolgimento possibile del personale operante nelle dipendenze al fine di non intralciarne la normale attività lavorativa.

Scartati i vari sistemi connessi a comunicazioni telefoniche (segreteria telefonica, trasmissione fax, etc.) ed al fine di contenere i costi, la scelta è stata indirizzata nella ricerca di una procedura che fosse già disponibile ed utilizzata dalla Banca.

Questa è stata individuata in quella utilizzata per la gestione delle anomalie di tutte le apparecchiature *hardware* in dotazione (terminali, PC, stampanti, monitor, tastiere, etc.) denominata - "/FOR GUASTI"- è residente nei programmi disponibili dall'*host* centrale.

In realtà, è un sistema evoluto di posta elettronica, è compresa fra quelle accessibili per le normali attività bancarie ed inoltre possiede questi requisiti fondamentali:

- fa parte di quel pacchetto di procedure di normale e corrente utilizzo da parte del

personale delle dipendenze e risulta quindi *friendly* per gli stessi incaricati;

- viene gestita dal sistema centralizzato per cui rimane documentata;
- prevede già delle possibilità di *sort* dei dati raccolti;
- possiede sufficienti livelli di sicurezza e l'accesso alla stessa è condizionato dalla specifica abilitazione dell'operatore mediante *password* di sistema;
- consente di gestire completamente i guasti nonché di evidenziare quelli ancora "aperti";
- consente di individuare in modo univoco il componente guasto;
- è suscettibile di essere ulteriormente implementata con l'introduzione di processi crittografici.

È stato quindi attuato un processo di revisione di questa procedura, d'intesa con il collaterale Servizio che provvede alla gestione del sistema informativo aziendale, per adattarla anche alle esigenze degli impianti di sicurezza introducendo una serie di accorgimenti necessari ad aumentarne le sicurezze interne e ad indirizzare le segnalazioni verso un centro di ricezione ovviamente diverso da quelli in essere per la gestione dell'*hardware*. Sono stati inoltre inseriti dei controlli sui tempi di "apertura" e "chiusura" dei guasti in modo da poter avere con cadenza giornaliera la situazione dell'intero sistema.

Parallelamente all'attività suddetta è stato realizzato il *censimento* di tutti gli apparati di sicurezza esistenti (impianti di allarme antifurto-antirapina, identificati con la sigla *ALL*, ed impianti di controllo accessi, identificati con la sigla *SCA*), inserendo l'indicazione dell'Impresa costruttrice/installatrice, il modello dell'apparecchiatura e contrassegnando infine ogni *record* con un codice alfanumerico identificativo.

Questi codici sono stati quindi associati in modo irreversibile al codice proprio della dipendenza presso la quale sono installati gli apparati. In questo modo non sono possibili errori di identificazione e/o di segnalazione.

Tutte le variazioni per installazione di nuovi componenti, sostituzioni, apertura nuove di-

pendenze, trasferimenti e cessazione di attività di sportelli sono gestiti dal Servizio Sicurezza con analogo procedura che prevede comunque più livelli gerarchici (semplice accesso e supervisione).

E' prevista nell'immediato futuro l'estensione della procedura anche agli impianti televisivi a circuito chiuso che saranno identificati con la sigla *TVC*.

La procedura opera, quindi, in modo tale che per l'attivazione di una segnalazione di guasto (generalmente denominata *apertura guasto*) è necessario:

- ⇒ accedere alla procedura con la *password* di sistema (tale *password* è associata sia alla persona abilitata sia alla dipendenza presso la quale opera: si inibisce così agli operatori la possibilità di aprire guasti di altre dipendenze);
- ⇒ effettuare la scelta del tipo di impianto interessato dall'anomalia (*ALL* per gli impianti di allarme, *SCA* per i sistemi di controllo accessi);
- ⇒ digitare il codice identificativo del componente guasto. Tale codice in realtà è fornito per *default* dal sistema unitamente alla descrizione codificata dell'elemento e l'operazione esatta che deve fare l'operatore è quella di confermare il codice dell'elemento o degli elementi che risultano in guasto;
- ⇒ inserire un breve messaggio, facoltativo, per fornire ulteriori dettagli circa l'anomalia riscontrata;
- ⇒ indicare se l'impianto è operativo o meno;
- ⇒ procedere all'invio della segnalazione ed eventualmente ricavare una copia a stampa della stessa per le proprie esigenze.

La segnalazione di guasto, una volta ricevuta da un apposito settore del Nucleo Operativo Sicurezza (comunemente denominato "*help desk*"), viene verificata dall'operatore, inserita su un PC di gestione e quindi trasmessa all'impresa manutentrice via facsimile. Tale Nucleo dispone inoltre l'istituzione di servizi di vigilanza straordinari o di altre misure cautelative secondo le varie e più diverse necessità.

Infatti, poiché l'*help desk*, come detto, opera all'interno dello stesso Nucleo Opera-

tivo Sicurezza si rende possibile l'immediata acquisizione, da parte del Responsabile della struttura, delle notizie di anomalie degli impianti in tempo quasi reale. E' pertanto possibile mettere in relazione detti eventi con le altre informazioni riservate, inerenti la sicurezza delle dipendenze, e disporre in tempi brevissimi i necessari provvedimenti.

Si ritiene inoltre utile sottolineare come nel sistema di gestione computerizzato siano inserite anche le anomalie esterne agli impianti, ma che ne influenzano comunque l'efficienza, quali possono essere ad esempio i guasti dei sistemi di ricetrasmisione dei segnali (guasti delle linee **TELECOM**).

Tali eventi, essendo "esterni" alla dipendenza, non vengono notificati con la procedura "*FOR GUASTI*" e possono essere segnalati direttamente dagli impianti di allarme antifurto (in caso di caduta del collegamento) oppure dal personale responsabile delle dipendenze a mezzo filo. Una volta ricevuti vengono quindi inseriti nel sistema a cura del personale che presiede il suddetto *help desk*, che ne cura anche i successivi sviluppi fino alla totale eliminazione dell'anomalia.

Analogo procedura viene seguita per la memorizzazione degli interventi di manutenzione programmata che sono identificati mediante un codice diverso così come tutti gli altri interventi effettuati sull'impianto stesso per modifiche, implementazioni, etc.

In definitiva il programma consente la gestione di una *scheda elettronica* per ogni tipologia di impianto di sicurezza e rende così possibile l'estrazione delle più diverse associazioni di dati secondo le varie necessità.

Si prevede di automatizzare ulteriormente l'attività mediante l'inserimento sui PC delle imprese manutentrici di specifici programmi di gestione (in fase di realizzazione da parte di specifiche strutture della Banca) e quindi effettuare la trasmissione via modem della segnalazione nel momento stesso del suo inserimento sul PC di gestione dell'*help desk*.

Ovviamente sono possibili anche ulteriori contatti telefonici per richiesta di migliori informazioni sia nei confronti della dipendenza che ha aperto il guasto sia verso l'Impresa

manutentrice. Questi contatti sono sviluppati anche direttamente dalle Imprese manutentrici per accertare più esattamente possibile la reale natura del guasto verificatosi.

Una volta effettuato l'intervento tecnico, ed eliminate le anomalie precedentemente segnalate, si procede alla immediata **chiusura del guasto**, che può essere effettuata soltanto dall'incaricato abilitato, nel seguente modo:

- il sistema fornisce la situazione dei guasti che risultano ancora **aperti** per la dipendenza interessata;
- l'incaricato della dipendenza identifica quello relativo all'intervento di manutenzione appena effettuato e digita il comando di chiusura guasto;
- il sistema acquisisce i dati e li evidenzia all'operatore del Nucleo Operativo Sicurezza. Quest'ultimo a sua volta archivia i dati nel PC di gestione e provvede alla dismissione di eventuali servizi di vigilanza straordinaria nel frattempo eventualmente istituiti.

Una procedura simile viene osservata per la chiusura dei guasti inseriti direttamente dall'*help desk*.

La registrazione dei dati raccolti dalla procedura centralizzata *"/FOR GUASTI"* risulta necessaria, allo stato attuale, per poter disporre di più informazioni circa l'anomalia segnalata e il dettaglio delle operazioni di manutenzione eseguite fino a poter memorizzare il singolo componente dell'impianto, il nominativo del tecnico dell'Impresa manutentrica che ha eseguito l'intervento e la effettive operazioni eseguite.

Tali dati sono ricavabili dalle bolle di lavoro che devono obbligatoriamente essere compilate e rilasciate in occasione di ogni intervento su impianti di sicurezza - *anche in caso di accertata assenza di anomalie* - e che, una volta sottoscritte dal personale responsabile della dipendenza (Responsabile Locale della Sicurezza), vengono trasmesse con il corriere interno al Servizio Sicurezza.

L'impiego di una procedura informatizzata di controllo ha consentito di:

- potere immediatamente accertare i tempi di intervento dell'Impresa manutentrica

con applicazione contestuale delle penali, contrattualmente previste, nei casi di inadempienza accertata e non giustificata;

- conseguire la razionalizzazione dei servizi di vigilanza straordinari istituiti in seguito ai guasti degli impianti di sicurezza con evidenti notevoli risparmi in quanto gli stessi servizi vengono immediatamente fatti cessare non appena eliminata l'anomalia e riconferita all'impianto la funzionalità necessaria;
- stabilire l'*MTBF* di ogni impianto e quindi valutare sia l'efficienza funzionale dello stesso sia le caratteristiche di capacità operativa dell'impresa fornitrice/manutentrica;
- poter accertare l'entità globale degli interventi di manutenzione su chiamata;
- valutare la validità degli standard in essere ed adottare eventuali provvedimenti migliorativi;
- avere a disposizione un archivio storico di tutti gli eventi che hanno interessato l'impianto di sicurezza.

Quest'ultima possibilità riveste, a nostro avviso, un'importanza fondamentale per la gestione di impianti di sicurezza in quanto rappresenta un ottimo deterrente nei confronti di eventuali e sempre possibili, anche se estremamente difficili, tentativi di sabotaggio degli apparati.

La procedura sopradescritta non deve comunque intendersi come punto terminale dello sviluppo della materia. E' infatti allo studio un'ulteriore approfondimento della stessa in relazione al previsto aggiornamento del sistema di comunicazione aziendale che potrà avvalersi, in un futuro non remoto, di una rete interna tipo Internet. Ciò faciliterà indubbiamente l'accesso al sistema da parte dei Responsabili locali della Sicurezza per l'introduzione dei dati afferenti i guasti degli apparati di sicurezza e le successive attività connesse alla loro gestione.

Sono altresì ipotizzabili ulteriori integrazioni fra il centro di gestione ed i sistemi di sicurezza quando questi avranno raggiunto un livello di omogeneizzazione tale da consentire l'interfacciamento diretto degli apparati con l'unità centrale di controllo. In tale ipotesi le anomalie verrebbero recepite auto-

maticamente dalla procedura e trasmesse alle imprese manutentrici senza richiedere l'intervento umano che sarebbe dedicato u-

nicamente al controllo ed all'interpretazione degli eventi.

ORGANIZZAZIONE DELLA SECURITY IN BANCA DI ROMA

