

# **LE POLICY DI SICUREZZA INFORMATICA**

## **LA FORMAZIONE**

Il Sanpaolo IMI ha, da qualche tempo, dato corso ad un profondo cambiamento circa l'approccio alle problematiche di Sicurezza Informatica che, da un insieme ancorché complesso, articolato ed integrato di sistemi, strumenti e meccanismi, viene ora considerata un vero e proprio *processo* che coinvolge tutte le strutture organizzative e tutte le funzioni dell'azienda e di cui è indispensabile presidiare con la dovuta attenzione anche gli *aspetti non tecnologici e non operativi*.

Per far fronte in modo adeguato a questo nuovo approccio, nel corso del 2001 è stato attuato un intervento di tipo organizzativo nell'ambito della struttura informatica con la creazione di una nuova entità alla quale sono stati affidati due compiti ben precisi:

- ✓ presidiare tutte le attività svolte a livello di sistema bancario inerenti l'area specifica della sicurezza informatica;
- ✓ presidiare tutte le attività aziendali di natura non operativa nell'area stessa.

Grazie al secondo dei due compiti citati (che è di fatto diventato successivamente l'impegno principale del gruppo di lavoro) e, in particolare, grazie al fatto di aver, appunto, svincolato la nuova struttura da attività operative e gestionali, è stato possibile avviare e portare a termine una serie di iniziative fondamentali ad integrazione del contesto operativo della sicurezza informatica aziendale.

La prima iniziativa è stata quella di rivisitazione della Policy di Sicurezza aziendali attraverso la creazione di un corpo documentale organico strutturato su due livelli:

- ✓ Livello 1: questo livello, articolato su due documenti, comprende i concetti generali di sicurezza informatica e le relative norme di comportamento;
- ✓ Livello 2: questo livello, articolato su più documenti, comprende le norme e le regole comportamentali relative alle diverse aree della sicurezza (controllo accessi fisici e logici, virus informatici, posta elettronica, sviluppo e manutenzione del software, internet, ...).

L'attività di stesura delle Policy è consistito prevalentemente nella raccolta organica e sistematica di tutte le norme comportamentali già presenti nei diversi materiali operativi (manuali, circolari, normativa, ...) e nella distribuzione dei documenti con l'avallo dell'Alta Direzione il che ha dato una doppia valenza agli stessi: ha sottolineato il valore strategico della sicurezza ed ha formalizzato la condivisione della visione circa le policy di sicurezza a tutti i livelli aziendali.

Ad Agosto 2002 le Policy sono state diffuse a tutto il personale nella prima versione: il documento di livello 1 è stato distribuito in forma cartacea nominalmente ad ogni dipendente, mentre i documenti di livello 2 sono stati pubblicati sulla rete interna.

Inoltre le Policy di Sicurezza sono state inserite come argomento di apprendimento in un corso sulla sicurezza erogato a tutti i dipendenti.

Quale complemento, ad integrazione dell'insieme dei documenti di Policy, è stato predisposto altro materiale documentale relativo all'insieme delle leggi, norme e regolamenti in materia di sicurezza informatica.

Infatti nel corso dell'attività relativa alla stesura delle policy stesse è risultato evidente come la sicurezza sia oggi oggetto di norme e leggi specifiche o abbia comportato adeguamenti significativi a norme e leggi esistenti emanate dallo Stato, dalla Comunità Europea, dagli organismi istituzionali di sistema, bancari e non, e dalla Banca d'Italia. Questa nuova situazione ha fatto sì che le scelte aziendali, in termini di investimento per la sicurezza dei sistemi informativi, non siano più solamente guidate da valutazioni esclusivamente interne, ma condizionate anche dal rispetto degli obblighi di legge e delle normative. Fra l'altro, è necessario sottolineare come il nuovo contesto legislativo e normativo può condizionare non solamente le scelte tecniche, ma può influenzare anche le scelte organizzative, quelle operative e, in molti casi, anche quelle relative al business.

Inoltre in tale contesto risultano molto ben definite le responsabilità degli utenti e dei gestori del sistema informativo.

Al fine, quindi, di inquadrare le problematiche di sicurezza non solo in termini di responsabilità aziendale ma di obblighi di legge è stato deciso di predisporre un insieme di documenti che, con evidente scopo divulgativo, descrivessero il nuovo contesto normativo e legislativo in un linguaggio e con una forma facilmente comprensibile ai non addetti ai lavori.

Questi documenti sono stati pubblicati a fine 2002 e fanno parte integrante del corpo documentale delle Policy di Sicurezza.

L'attività sulle Policy di Sicurezza prevede un aggiornamento continuo sia in termini di stesura di nuove Policy che in termini di intervento sulle Policy già pubblicate in modo da tenerle costantemente aggiornate sulla base dell'evoluzione tecnologica, organizzativa ed operativa; proprio per tale motivo i documenti di livello 2 sono stati diffusi su rete aziendale anziché essere distribuite su supporto cartaceo.

Come già detto una delle attività portate a compimento da parte della nuova struttura è stata quella relativa alla predisposizione ed alla diffusione di un corso specialistico sulla sicurezza informatica.

Questo corso ha come obiettivo la diffusione della conoscenza e la sensibilizzazione di tutto il personale circa i concetti base della sicurezza informatica; un secondo obiettivo del corso è quello di costituire un ulteriore

strumento di diffusione delle policy e del contesto normativo/legislativo. Infatti i concetti di base vengono illustrati in modo integrato e con precisi riferimenti alle policy ed alle diverse leggi in modo da rendere gli utenti del sistema informativo consapevoli del proprio operato sia in termini di tutela del patrimonio informativo aziendale che in termini di tutela delle proprie responsabilità.

Il corso è stato predisposto con la collaborazione della struttura di Formazione aziendale ed è stato fruito inizialmente dalle risorse appartenenti alla struttura informatica; a questa prima fase, completata a fine 2002 seguirà una seconda fase, nel corso della prima metà del 2003, che vedrà coinvolti tutti i dipendenti del Sanpaolo IMI.

Il corso, articolato in 5 unità didattiche ed erogato secondo la tecnica della formazione a distanza, comprende anche un'unità finale di valutazione basata sulla risposta a 10 domande scelte casualmente fra 30 disponibili.

