

Tutta la sicurezza in una sola norma

Un documento redatto da Iso e Iec, le due massime autorità in materia, riunisce in una sola norma gli standard e le best practice da seguire in materia di sicurezza informatica. Dedicata alle organizzazioni che davvero vogliono agire in sicurezza, non prevede nessuna certificazione esterna.

Iso (International Organization for Standardization) e Iec (International Electrotechnical Commission) hanno stabilito congiuntamente la norma Iso/Iec 17799:2000 a riguardo della sicurezza informatica. La norma ha il grande merito di coprire in un solo documento l'insieme delle esigenze in materia di sicurezza informatica, permettendo a qualsiasi impresa e individuo di misurarsi a dei criteri identici in questo dominio. Si iscrive nella famiglia delle norme di qualità ma, al contrario d'Iso 9001, non dà luogo ad una certificazione.

La norma inizia con una parte 'educativa', che precisa la nozione di sicurezza delle informazioni e definisce nel seguente modo le esigenze che tratta:

Confidenzialità: assicurare che l'informazione non sia accessibile a estranei.

Integrità: assicurare la precisione e l'esattezza delle informazioni e dei mezzi di trattamento.

Disponibilità: assicurare la disponibilità delle informazioni agli autorizzati.

Il pericolo è attribuire un'importanza esagerata agli aspetti tecnici, a discapito di quelli legati alle persone e all'organizzazione. Per questa ragione la norma insiste sui fattori critici seguenti, indispensabili per una riuscita dell'implementazione della sicurezza:

- Esistenza di una politica di sicurezza adeguata con le attività e le prestazioni attese dal sistema informatico.
- Esistenza di una sollecitazione per la sicurezza credibile e realizzabile. Dovrà entrare nella cultura dell'organismo e far parte della strategia.

- Sostegno visibile e dichiarato della direzione in materia di realizzazione di misure di sicurezza.

- Buona comprensione delle esigenze di sicurezza, dell'analisi e della padronanza dei rischi per le persone incaricate dell'implementazione della sicurezza.

- Diffusione delle nozioni di sicurezza a tutti i livelli dell'organizzazione.

- Creazione e diffusione delle direttive di sicurezza per il personale interno e per gli esterni, diffusione delle direttive ai posti di lavoro.

In modo generale la norma Iso 17799 indica la via da seguire per l'implementazione della sicurezza. Insiste sul fatto che i principi che essa contiene siano oggetto di una messa in opera propria di ciascun organismo, sottoforma di specifiche direttive connesse al luogo di lavoro.

Una parte importante della norma tratta la sicurezza sul posto di lavoro e l'implicazione per ogni utente. Insiste sull'integrazione delle direttive di sicurezza nella descrizione del posto di lavoro e sull'obbligo degli utenti al loro rispetto.

Ben inteso, essa rileva l'importanza della formazione necessaria ad una buona comprensione della sicurezza e la necessità di rilevare gli incidenti, le debolezze, le disfunzioni dei dispositivi, e propone la messa in opera di un sistema d'allerta e di gestione delle non-conformità.

Su un piano più dinamico, la norma insiste sugli aspetti di trattamento dell'informazione e della telecomunicazione, tiene conto delle implicazioni dell'evoluzione dei mezzi di comunicazione, e-mail, commercio elettronico, telelavoro, ecc.: questo

capitolo è particolarmente documentato e copre la preoccupazione legata alla generalizzazione dell'uso di internet. La strategia in materia dei controlli di accesso è trattata in maniera dettagliata e conferma le disposizioni attualmente in vigore.

Lo sviluppo e la manutenzione delle applicazioni fanno oltremodo parte del discorso di sicurezza. La norma fornisce tutte le indicazioni necessarie per la sicurezza dei processi di sviluppo, manutenzione e gestione delle versioni. Rileva ugualmente l'importanza dei mezzi moderni di crittografia e firma elettronica.

Generalmente le società consentono ad effettuare lo sforzo per mettere in opera un sistema di sicurezza adeguato; una volta stabile, le direttive che lo comprendono o invecchiano o cadono nell'oblio.

Delle verifiche puntuali e periodiche permetterebbero di farle vivere e continuare ad adeguarle alla situazione corrente.

Questa la ragione per cui è, come per Iso 9001, imperativo formare all'interno delle aziende uno o più ispettori della sicurezza, con l'incarico di verificare in permanenza il rispetto delle direttive stabilite. Allo stesso modo, bisognerebbe periodicamente sensibilizzare l'insieme degli utenti a questo problema e ricordar loro i pericoli e le regole da rispettare.

*Avv. Matteo Scacchi
Studio legale Broggin, Lugano*

Ated
e-mail: info@ated.ch
Casella postale 572
6512 Giubiasco