

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 525 di mercoledì 27 marzo 2002

Pubblicata sulla GU la direttiva per la sicurezza informatica nella pubblica amministrazione

Nel documento le indicazioni per valutare il livello di rischio ed individuare le iniziative per raggiungere la "base minima di sicurezza".

"Le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese. Questo patrimonio deve essere efficacemente protetto e tutelato..."

Da questi presupposti nasce la direttiva del 16 gennaio 2002 "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali", emanata dal ministero dell'Innovazione e pubblicata sulla Gazzetta Ufficiale n.69 del 22 marzo 2002.

La direttiva e' solo un primo passo e punta al raggiungimento di una "base minima di sicurezza" per tutte le pubbliche amministrazioni, in attesa che il ministero predisponga un vero e proprio sistema nazionale di sicurezza Informatica e delle Telecomunicazioni (ICT) della pubblica amministrazione.

Le Amministrazioni dovranno progettare e realizzare, entro un anno, le misure indicate nella "base minima di sicurezza".

Autodiagnosi

Per tutelare il patrimonio "informazioni" delle amministrazioni pubbliche e' innanzitutto fondamentale valutare il rischio connesso con la gestione delle informazione e dei sistemi.

La direttiva invita, quindi, le amministrazioni a realizzare una rapida "autodiagnosi" del proprio livello di sicurezza, rispetto alla base minima raccomandata.

Il ministero ha predisposto un questionario (allegato 1) che ha lo scopo di guidare l'Amministrazione in questo processo di auto-valutazione.

Nel questionario sono state definite sei schede, una per ciascuna delle aree chiave della sicurezza: Policy, Ruoli e Responsabilità, Norme e Procedure, Amministrazione della Sicurezza, Analisi del Rischio, Formazione e Sensibilizzazione.

Base minima di sicurezza

La direttiva invita le amministrazioni ad attivare le necessarie iniziative per posizionarsi sulla "base minima di sicurezza", descritta dell'allegato 2, precisando che il suo raggiungimento non costituisce una risposta completa ed esaustiva, ma pone solo le "fondamenta".

L'allegato 2 vuole fornire "alcune indicazioni per assistere i Ministeri nell'individuazione delle misure di protezione che debbono essere realizzate e gestite con assoluta priorità, al fine di supportare le Amministrazioni sia nell'applicazione degli adempimenti normativi di riferimento (es 675-318) sia nel contrastare eventuali potenziali minacce."

Si tratta di una "una serie di indicazioni tecnico-operative".

Le amministrazioni dovranno definire, progettare e realizzare, nell'arco temporale orientativo di 12 mesi, le misure indicate nell'allegato 2.

Tra queste misure e' indicato anche il controllo logico/fisico degli accessi per garantire che tutti gli accessi agli oggetti del sistema ICT avvengano esclusivamente secondo modalità prestabilite.

Il "controllo fisico" degli accessi deve restringe i diritti di accesso del personale alle zone che ospitano risorse aziendali informatiche e non (magazzini tecnici, aree con dati e/o apparati ad alto rischio, uffici riservati, ecc.).

In particolare l'accesso ai Centri di produzione (Data Center, Call Center, ecc.) deve essere controllato tramite l'uso di badge magnetici/smart card strettamente personali rilasciati esclusivamente al personale conosciuto.

Il documento si conclude indicando le linee sulle quali si articolerà il programma per la sicurezza informatica nella PA, tra le quali la creazione di un Comitato nazionale della sicurezza ICT, formulazione il Piano nazionale della sicurezza ICT della pubblica amministrazione, realizzazione della certificazione di sicurezza ICT nella pubblica amministrazione.

La Direttiva 16 gennaio 2002.

www.puntosicuro.it