Relazione di attività

Gruppo di lavoro per l’attuazione della normativa in tema di sicurezza informatica

La crescente diffusione dei sistemi e delle tecnologie informatiche ha determinato, sia in ambito internazionale che nazionale, una sempre maggiore sensibilizzazione al problema della sicurezza.

Nel contesto internazionale, tra le altre, le *“OECD Guidelines for the Security of Information Sistems and Networks”* adottate, appunto, dall’OCSE il 25 luglio 2002 e dirette, seppur in modo non vincolante, a tutti i soggetti che detengono, sviluppano, gestiscono ed usano i sistemi informatici, hanno evidenziato la necessità di effettuare una periodica attività di valutazione dei rischi, creando ed incrementando una consapevolezza dell’esigenza di sicurezza informatica, nonché la responsabilità per la sicurezza stessa, con azioni tempestive dirette a prevenire e reagire agli incidenti, dettate da una progettazione e gestione della sicurezza efficace e costantemente aggiornata.

Principi similari erano stati indicati, in ambito nazionale, anche dalla direttiva del Dipartimento per l’Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri del 16 gennaio 2002 (pubblicata nella G.U. n. 69 del 22.03.2002) diretta a fornire linee di condotta per la sicurezza dei sistemi informatici e dei dati gestiti mediante tali strumenti, con riguardo anche ai dati personali.

L’Istituto Nazionale di Fisica Nucleare, già sensibile alle tematiche relative alla sicurezza informatica, aveva costituito nel 2002, seppur informalmente, un gruppo di lavoro diretto ad approfondire tale materia e ad indicare proposte per l’individuazione di misure tecniche e modalità di condotta dirette a garantire un uso corretto dei sistemi informatici e dei dati ed informazioni attraverso tali sistemi gestiti.

Il gruppo di lavoro, composto dai sigg.ri:

Roberto Cecchini	INFN – Firenze (coordinatore)
Silvia Arezzini	INFN – Pisa
Eleonora Bovo	INFN – Amm.ne Centrale
Paolo Lo Re	INFN – Napoli
Ombretta Pinazza	INFN – Bologna
Alessandro Spanu	INFN – Roma,

avuto riguardo agli aspetti sia tecnici che giuridici connessi alle questioni della sicurezza, aveva individuato al momento della sua costituzione i seguenti obiettivi:

a) redazione di una proposta di Regolamento per l’uso delle Risorse di Calcolo diretto ad individuare norme di condotta, uniformi per gli utenti di tutte le Strutture ed idonee ad un uso corretto delle risorse di calcolo dell’INFN.

b) predisposizione di una proposta di Documento Programmatico sulla Sicurezza, di cui all’allora vigente art. 6 del DPR 28 luglio 1999 n. 318, circa il trattamento dei dati personali sensibili e giudiziari;

Regolamento per l’uso delle risorse di calcolo e reti

Obiettivo del gruppo di lavoro è stato quello di predisporre un Regolamento per l’uso delle risorse di calcolo che, traendo ispirazione da alcuni documenti già redatti in alcune Strutture (Bologna e Laboratori di Nazionali di Frascati), provvedesse ad indicare in modo uniforme per tutte le articolazioni dell’Istituto, le linee di condotta per un corretto uso delle risorse informatiche.

Nel corso dei lavori, come detto sopra, la Presidenza del Consiglio dei Ministri – Dipartimento per l’Innovazione e le Tecnologie – ha emanato la direttiva 16 gennaio 2002, in materia di “Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni”, con la quale veniva richiesto alle pubbliche amministrazioni di attivare le *“... necessarie iniziative per posizionarsi sulla [base minima di sicurezza] ... che consenta di costruire, con un approccio unitario e condiviso, le fondamenta della sicurezza della pubblica amministrazione”*.

Alla luce di tale documento si è ritenuto opportuno riesaminare il proposito iniziale ed in particolare rivedere la proposta di Regolamento per l’uso delle risorse di calcolo, adeguandolo alle indicazioni contenute nella direttiva.

Il provvedimento del 16 gennaio, articolato in due allegati, ha indicato, per le pubbliche amministrazioni, una attività preliminare di auto valutazione del livello di sicurezza, seguita da indicazioni finalizzate proprio ad organizzare e gestire la sicurezza informatica in ciascuna amministrazione.

La fase di autovalutazione era diretta ad evidenziare, con risultati destinati a rimanere comunque interni e riservati all’amministrazione, il quadro organizzativo della stessa, con riferimento:

- all’esistenza ed al grado di completezza di una politica di sicurezza informatica;
- all'individuazione di ruoli e responsabilità in materia di sicurezza;
- all'indicazione di norme e procedure specifiche;
- all'organizzazione della sicurezza con individuazione di apposite professionalità;
- alle metodologie adottate per efficaci analisi dei rischi informatici;
- all'esistenza e sviluppo di programmi di formazione diretti a sensibilizzare e rendere consapevole il personale sulle tematiche di sicurezza.

La fase operativa invece, che avrebbe dovuto essere definita progettata e realizzata nell’arco temporale orientativo di 12 mesi e per la quale era prevista per le Amministrazioni un’attività di supporto da parte dei singoli Ministeri, si articolava nell’individuazione di:

- un Presidio globale in grado di assicurare una visione unitaria e strategica delle questioni di sicurezza;

- una corretta responsabilizzazione
- un bilanciamento tra Rischio e Sicurezza
- una separazione dei compiti che distingua tra monitoraggio e verifica della sicurezza.

Il Dipartimento per l’Innovazione e le Tecnologie, al fine di ottenere un efficace funzionamento della sicurezza organizzativa ha indicato la necessità di *“calare sulla struttura dell’Amministrazione un sistema di gestione della sicurezza”* composto da:

- **Carta della sicurezza** diretta a definire obiettivi e finalità delle politiche di sicurezza, le strategie di sicurezza, il modello organizzativo ed i processi per attuarle;
- **Politiche generali di sicurezza**, che indicassero, coerentemente con la carta della sicurezza, le direttive per lo sviluppo, gestione, controllo e verifica delle misure da adottare;
- **Politiche specifiche di sicurezza (Norme)** costituite da regole afferenti argomenti rilevanti per l’organizzazione, il personale ed i sistemi e da aggiornare frequentemente sulla base di cambiamenti organizzativi e tecnologici;
- **Specifiche procedure**, a supporto della gestione operativa riguardanti:
  - la gestione della System Security e della Network Security;
  - la gestione operativa;
  - la gestione degli incidenti;
  - il controllo e monitoraggio del sistema di sicurezza;
  - la sicurezza del personale.

Individuati tali ambiti, la direttiva ha indicato quindi, in modo più analitico, le linee di condotta per effettuare un efficace analisi del rischio, evidenziando, poi, le attività e le misure necessarie a costituire una base minima di sicurezza nel controllo fisico e logico degli accessi alle risorse informatiche, nella protezione dai virus informatici e nella gestione degli incidenti.

In tale nuovo contesto, si è ritenuto opportuno individuare l’insieme dei documenti necessari a comporre il sistema complessivo di gestione della sicurezza, piuttosto che predisporre soltanto il regolamento di cui al disegno originario.

Data la natura tipica della direttiva che, nel dettare linee di condotta, salvaguarda, comunque, l’autonomia dei destinatari, i quali possono darvi attuazione adeguandone i principi alle proprie peculiarità organizzativo-gestionali, è sembrato più consono per l’INFN proporre in un unico documento, indicato come “**Carta della Sicurezza**”**,** sia gli obiettivi, le finalità e le strategie di sicurezza con annessi modelli organizzativi, che le politiche di sicurezza, intese, appunto, come direttive per lo sviluppo, gestione, controllo e verifica delle misure stesse.

Le **Politiche Specifiche di Sicurezza** sono state individuate in un ulteriore documento, il “**Regolamento per l'uso delle risorse informatiche dell’INFN**”, nel quale, in parte, è stato trasfuso il contenuto dell’originario Regolamento per l’uso delle risorse di calcolo.

In proposito è apparso rilevante, sempre in conformità a quanto previsto nella direttiva, dettare norme per tutti gli utenti delle risorse di calcolo INFN e dirette ad individuare in modo immediato ed auspicabilmente chiaro, sia le finalità per le quali l’Istituto consente l’uso delle proprie risorse di calcolo, che le prescrizioni fondamentali di condotta che ogni utente è tenuto ad osservare al fine di salvaguardare la sicurezza del sistema informatico oltre che dei dati e delle informazioni trattate.

Proprio perché diretto ad un numero ampio di destinatari le cui conoscenze informatiche possono essere in alcuni casi molto approfondite ed in altri ridotte ed essenziali, si è ritenuto di dover utilizzare un linguaggio quanto più possibile semplificato, inserendo le definizioni delle espressioni chiave ed esprimendo i concetti di base per un corretto uso delle risorse. Il documento riporta, inoltre, l’articolazione dei soggetti attraverso i quali si propone di comporre il sistema gestionale delle risorse, in modo da consentire agli utenti, nel modo più agevole possibile, l’individuazione di ciascuno di tali soggetti per funzioni ed attività.

Una serie di documenti, di contenuto prettamente tecnico, è stata poi predisposta al fine di individuare le **Specifiche Procedure** a supporto della gestione operativa delle contromisure tecnologiche adottate per le finalità di sicurezza.

In questi documenti sono state indicate le misure adottate dall’Ente per garantire la *Host* e la *Network security*, con indicazione delle specifiche condotte che gli utenti, i referenti dei gruppi e gli amministratori di sistema sono tenuti a seguire per far in modo che tecnicamente i sistemi informatici siano costantemente aggiornati ed adeguati a salvaguardare la sicurezza.

E’ stato individuato, inoltre, un modello di gestione operativa della sicurezza e di gestione degli incidenti, con indicazione del comportamento da seguire nel caso in cui si rilevi un incidente od un attacco ad una o più risorse di calcolo, nonché le misure da adottare dal gruppo di intervento, a seguito di una denuncia di incidente, al fine di ristabilire condizioni di sicurezza per la risorsa o le risorse presso le quali l’incidente o l’attacco si è verificato.

La documentazione prodotta, sottoposta all’attenzione della Commissione Nazionale Calcolo e Reti INFN nell’ottobre 2003, si ritiene conservi ancora interesse, dal momento che le stesse tematiche hanno costituito oggetto di un apposito studio da parte del Comitato tecnico nazionale sulla sicurezza informatica e delle comunicazioni nelle pubbliche amministrazioni la quale ha formulato, nel marzo 2004, un documento dal titolo *“Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione”* e sono ritenute tutt’ora di rilievo dal CNIPA.

Documento Programmatico sulla Sicurezza.

Con decreto del Presidente della Repubblica 29 luglio 1999 n. 318, in attuazione dell’allora vigente legge n. 675 del 31 dicembre 1996 in tema di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, il Legislatore aveva emanato un regolamento contenente norme per l’individuazione delle misure minime di sicurezza per il trattamento dei dati personali, indicando misure da adottare nel trattamento dei dati effettuato sia mediante strumenti elettronici, che con mezzi diversi.

Tale provvedimento poneva particolare attenzione nel garantire sicurezza al trattamento dei personali sensibili e giudiziari, definiti i primi quali dati *“idonei a rivelare l’origine razziale od etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l’adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati idonei a rivelare lo stato di salute e la vita sessuale”*, ed i secondi quelli contenuti nel casellario giudiziale (pronunce di condanna o proscioglimento in materia penale, misure detentive, ecc...)

Il DPR n. 318/99, disponeva che ogni Titolare del trattamento dei dati (quale è l’Istituto Nazionale di Fisica Nucleare) redigesse un Documento Programmatico sulla Sicurezza (DPS) da aggiornare con cadenza annuale e diretto a definire, con riferimento al trattamento dei dati sensibili:

a) i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza;

b) i criteri e le procedure per assicurare l’integrità dei dati;

c) i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi i criteri per le restrizioni di accesso per via telematica;

d) l’elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento (cioè tutti coloro che materialmente trattano dati personali) dei rischi individuati e dei modi di prevenire danni.

Con riferimento ai punti indicati, è stata formulata una proposta di Documento Programmatico che desse conto delle misure tecniche dirette a garantire la sicurezza di questa particolare tipologia di dati ed in grado di tener conto delle realtà peculiari esistenti in ciascuna Struttura.

A tal fine è sembrato opportuno proporre un documento nella forma del *template*, nel quale ad alcune parti che risultano omogenee in tutte le articolazioni dell’Istituto e che pertanto rimangono invariate, se ne aggiungono altre che, suscettibili di variazione in relazione alle diverse realtà locali (si pensi, per esempio, alle diverse modalità di tutela delle aree adottate nei Laboratori Nazionali o nelle Sezioni istituite presso sedi universitarie), possano essere differenziate in relazione alle particolarità di ciascuna Struttura.

Nell’intento di rendere più agevole il compito di coloro che in sede locale si sarebbero occupati della stesura definitiva del DPS, il documento è stato corredato di istruzioni per la compilazione fornite attraverso l’invio alle Strutture di un DPS esemplificativo già predisposto da una Struttura campione.

L’individuazione dei soggetti che avrebbero dovuto provvedere a tale incombente è stata rimessa ai Direttori delle Strutture, individuati, con apposita deliberazione del Consiglio Direttivo, Responsabili del trattamento dei dati personali, consigliando, comunque, che i compilatori del Documento Programmatico venissero individuati tra da unità di personale addette ai Centri di Calcolo, coadiuvati dai Responsabili amministrativi per gli aspetti più strettamente inerenti l’individuazione delle tipologie di dati sensibili e le modalità operative di gestione degli stessi.

Successivamente con l’entrata in vigore – il primo gennaio 2004 – del Codice in materia di tutela dei dati personali di cui al D.Lgs. 30 giugno 2003 n. 196, che ha abrogato la legge n. 675/96 ed i connessi provvedimenti regolamentari di attuazione, si è reso necessario provvedere ad un aggiornamento del Documento Programmatico sulla Sicurezza. Il nuovo Codice, infatti, conservava la prescrizione per i Titolari del trattamento di provvedere alla redazione del DPS, ma ne rivedeva i parametri, integrando alcuni profili, descritti ora, nell’Allegato B al Codice recante il *“Disciplinare tecnico in materia di misure minime di sicurezza”*.

Per tali motivi si è provveduto ad una rielaborazione dell’originario *template* di DPS.

Peraltro, poiché il Codice, nel suo contenuto normativo originario, disponeva che la redazione del nuovo DPS dovesse essere effettuata dai Titolari entro il 31 marzo 2004, la rivisitazione del *template* ha avuto come parametri di riferimento esclusivamente le norme di cui all’Allegato B sopra citato e – in conformità a quanto richiesto dalla legge - nel febbraio 2004 si è data indicazione ai Direttori delle Strutture di provvedere alla nuova redazione.

In seguito, in prossimità del 31 marzo dello stesso anno, il Legislatore è intervenuto con successivi provvedimenti di proroga di tale termine, posticipando l’originaria scadenza prima al 30 giugno 2004 e poi, sempre in prossimità del compimento del termine, di semestre in semestre sino al prossimo 31 dicembre 2005.

Nel giugno 2004, peraltro, l’Autorità Garante per la tutela dei dati personali ha dettato delle linee guida per la redazione del Documento Programmatico sulla Sicurezza.

Dal momento che la stessa Autorità definiva non vincolanti le proprie linee guida, che le stesse non offrivano indicazioni sostanzialmente diverse da quelle recepite nella rielaborazione del *template* e che la gran parte delle Strutture aveva provveduto tempestivamente alla prima scadenza ad adempiere agli obblighi connessi alla redazione del DPS, si è ritenuto che fornire ulteriori indicazioni per una nuova predisposizione del Documento avrebbe concretizzato una duplicazione di attività amministrativa.

Non sembra escludersi tuttavia che, prevedendo il punto 19 dell’Allegato B al Codice che il DPS sia redatto ogni anno, entro il 31 marzo, con riferimento al 2006 non sia opportuno provvedere ad una nuova revisione del Documento che tenga conto anche delle indicazioni fornite dal Garante.