ISTITUTO NAZIONALE DI FISICA NUCLEARE

GRUPPO DI LAVORO PER L'ATTUAZIONE DELLA NORMATIVA IN TEMA DI SICUREZZA INFORMATICA.

- Relazione di attività -

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

Nel contesto internazionale, tra le altre, recenti sono le *"OECD Guidelines for the Security of Information Sistems and Networks"* adottate, appunto, dall'OCSE, in forma di raccomandazione, il 25 luglio scorso e dirette, seppur in modo non vincolante, a tutti i soggetti che detengono, sviluppano, gestiscono ed usano i sistemi informatici. Tali raccomandazioni si possono riassumere nella 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 efficace e costantemente aggiornata progettazione e gestione della sicurezza.

Principi similari sono stati indicati, in ambito nazionale, 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 ad indicare linee di condotta per la sicurezza dei sistemi informatici e 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, 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) predisposizione di una proposta di Documento Programmatico sulla Sicurezza, di cui all'art. 6 del DPR 28 luglio 1999 n. 318, circa il trattamento dei dati personali sensibili;

b) 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.

Documento Programmatico sulla Sicurezza.

Con decreto del Presidente della Repubblica 29 luglio 1999 n. 318, il legislatore ha 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 personali effettuato sia mediante strumenti elettronici, che con mezzi diversi.

Tale provvedimento - come del resto l'intero complesso normativo dettato dalla legge n. 675/96 sulla tutela dei dati personali - pone particolare attenzione nel garantire sicurezza al trattamento di particolari categorie di dati: i cc.dd. dati personali sensibili ed i dati giudiziari.

Sono definiti **dati sensibili** quelli *"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"*, (art. 22 legge n. 675/96).

Sono **dati giudiziari** quelli contenuti nel casellario giudiziale art. 24 legge n. 675/96 (pronunce di condanna o proscioglimento in materia penale, misure detentive, ecc...).

Il DPR n. 318/99, dopo aver individuato alcune attività da compiere per garantire la sicurezza dei dati personali, ha previsto la necessità, per ogni Titolare del trattamento dei dati (e l'Istituto Nazionale di Fisica Nucleare é Titolare del trattamento ai sensi di questa normativa) di predisporre un documento programmatico sulla sicurezza da aggiornare con cadenza annuale, 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 quattro punti indicati, si è ritenuto di predisporre una proposta di Documento Programmatico che desse conto delle misure tecniche adottate e dirette a garantire la sicurezza di questa particolare tipologia di dati e che in questo fosse in grado di rispettare, con maggior aderenza possibile, le 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 p.e. alle diverse modalità di tutela delle aree adottate nei Laboratori Nazionali o nelle Sezioni istituite presso sedi universitarie), possono essere differenziate in relazione alle tipicità di ciascuna Struttura.

Si è ritenuto opportuno corredare il documento di apposite istruzioni per la compilazione al fine di rendere più agevole il compito di coloro che in sede locale si occuperanno della stesura definitiva.

L'individuazione dei soggetti che dovranno provvedere a tale incombente sarà rimessa ai Direttori delle Strutture, i quali, in attuazione della normativa sulla privacy, con apposita deliberazione del Consiglio Direttivo, sono stati indicati come Responsabili del trattamento dei dati. Sembra comunque consigliabile che i compilatori del Documento Programmatico siano tratti 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.

Regolamento per l'uso delle risorse di calcolo e reti

Il secondo obiettivo, come detto sopra, era individuato, inizialmente, nella predisposizione di un Regolamento per l'uso delle risorse di calcolo che, traendo ispirazione da alcuni documenti già redatti in alcune Strutture (p.e. Bologna e Laboratori di Frascati), provvedesse ad indicare in modo uniforme per tutte le articolazioni dell'Istituto, le linee di condotta per un corretto uso dei mezzi informatici.

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 indicata, 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 Policy di sicurezza informatica;
- alla individuazione di ruoli e responsabilità in materia di sicurezza;
- alla indicazione di norme e procedure specifiche;
- alla organizzazione della sicurezza con individuazione di apposite professionalità;
- alle metodologie adottate per efficaci analisi dei rischi informatici;
- alla esistenza e sviluppo di programmi di formazione diretti a sensibilizzare e rendere consapevole il personale sulle tematiche di sicurezza.

La fase operativa invece, che dovrebbe essere definita progettata e realizzata nell'arco temporale orientativo di 12 mesi e per la quale viene prevista per le Amministrazioni un'attività di supporto da parte dei singoli Ministeri si articola 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 indichino, coerentemente con la carta della sicurezza, le direttive da seguire 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: regole da aggiornare frequentemente sulla base di cambiamenti organizzativi e tecnologici;
- **Specifiche procedure**, a supporto della gestione operativa e che riguardano:
  - 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 quindi opportuno, anziché limitarsi a predisporre il regolamento di condotta di cui al disegno originario, individuare l'insieme dei documenti necessari a comporre il sistema complessivo di gestione della sicurezza.

Data la natura giuridica della direttiva, quale provvedimento che nel dettare linee di condotta, salvaguarda, comunque, l'autonomia dei destinatari, che possono darvi attuazione adeguandone i principi alle proprie peculiarità organizzativo-gestionali, si è ritenuto opportuno riunire in un unico documento, che viene proposto 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 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 dirette a tutti gli utenti delle risorse di calcolo INFN che individuassero, in modo 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 adottare al fine di salvaguardare la sicurezza del sistema informatico oltre che dei dati ed informazioni trattati.

Proprio perchè 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, esprimendo concetti 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, sono stati poi predisposti al fine di individuare le **Specifiche Procedure** a supporto della gestione operativa delle contromisure tecnologiche adottate per le finalità di sicurezza.

In questi documenti vengono indicate le misure adottate dall'Ente per garantire la System security 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.

Viene 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.