CARTA DELLA SICUREZZA INFORMATICA

Premessa

L'Istituto Nazionale di Fisica Nucleare (INFN) è un ente pubblico nazionale di ricerca a carattere non strumentale con autonomia scientifica, organizzativa, finanziaria e contabile ai sensi dell'art. 33 della Costituzione e dell'art. 8 della legge 9 maggio 1989 n. 168. L'INFN ha un Servizio di Presidenza in Roma ed è articolato nelle seguenti Strutture:

- Amministrazione Centrale, sita in Frascati (RM);
- 4 Laboratori Nazionali, siti in Legnaro (PD), Assergi (AQ), Frascati (RM) e Catania;
- 1 Centro Nazionale, sito in Bologna;
- 20 Sezioni, site in Torino, Milano, Milano Bicocca, Pavia, Padova, Trieste, Ferrara, Bologna, Genova, Pisa, Firenze, Perugia, Roma, Roma-Tor Vergata, Roma 3, Napoli, Bari, Lecce, Catania, Cagliari, di norma presso i Dipartimenti di Fisica delle rispettive Università.

Attualmente esistono inoltre 11 Gruppi Collegati (Trento, Udine, Brescia, Alessandria, Parma, Siena, L'Aquila, Sanità, Salerno, Cosenza e Messina), ciascuno afferente ad una Struttura.

Istituzionalmente l'INFN svolge attività di ricerca teorica e sperimentale nel campo della fisica nucleare, subnucleare e astroparticellare. A tal fine utilizza risorse informatiche in grado di garantire l'acquisizione, la gestione e l'elaborazione di una consistente mole di dati scientifici di assoluta rilevanza per l'Ente.

Per la natura delle attività dell'INFN, le risorse informatiche e i dati scientifici risultano distribuiti anche al di fuori delle Strutture di cui sopra. Risorse informatiche sono peraltro utilizzate anche per lo svolgimento dell'attività organizzativa e gestionale dell'Istituto, in connessione alle quali l'INFN effettua anche il trattamento di dati personali.

Dato il particolare rilievo che i sistemi informatici assumono nel perseguimento dei propri fini istituzionali, l'INFN considera tali sistemi, le informazioni da questi gestite e i dati scientifici parte integrante del proprio patrimonio. È pertanto obiettivo di assoluta priorità, per l'Istituto Nazionale di Fisica Nucleare, salvaguardare la sicurezza del proprio sistema informatico e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni, prodotte, raccolte o comunque trattate, da ogni minaccia intenzionale od accidentale, interna od esterna all'Ente.

In tale contesto si intende per

- *tutela della riservatezza*, la riduzione del rischio che una qualsiasi entità possa accedere alle informazioni senza esserne autorizzata;
- *tutela dell'integrità:* la riduzione del rischio che i dati o le informazioni siano modificati o distrutti;

- *tutela della disponibilità:* la riduzione del rischio che l'accesso ai dati ed alle informazioni possa essere impedito ai soggetti autorizzati.

Il riferimento alla riduzione del rischio, e non alla eliminazione dello stesso, è dovuto alla consapevolezza della impossibilità di raggiungere in ambito informatico, come del resto in natura, una condizione di sicurezza assoluta.

I rischi e le minacce al Sistema Informatico

Il Sistema Informatico dell'INFN è composto dalle apparecchiature (quali elaboratori, stampanti e apparati di rete), dal software e dai dati utilizzati dall'INFN per le sue attività istituzionali.

La predisposizione di adeguate misure di sicurezza richiede consapevolezza dei rischi e delle minacce cui può essere sottoposto un sistema: a tal fine l'INFN ha effettuato un'analisi dei potenziali eventi lesivi.

Si intende per *minaccia* un qualsiasi evento non desiderato, sia volontario che accidentale, idoneo ad arrecare danno, direttamente o indirettamente, al Sistema Informatico.

Le minacce più comuni si individuano come segue:

- *danneggiamenti:* eventi di origine naturale o derivante da comportamenti umani, in grado di arrecare danno;
- *furti:* appropriazione da parte di terzi di hardware, software, dati e informazioni appartenenti all'Ente;
- *frodi o malversazioni:* azioni poste in essere attraverso inganni, raggiri o contraffazioni e dirette ad ottenere profitti illeciti, personali o di terzi;
- *manipolazioni di dati o programmi:* azioni dirette a modificare, in modo non autorizzato, i dati ed i programmi;
- *perdita di privacy e riservatezza:* eventi accidentali o deliberati, idonei a determinare l'accesso ad informazioni riservate da parte di soggetti non autorizzati;
- *divulgazioni di dati e/o programmi:* azioni ritenute intermedie tra gli atti di frode e il furto poste in essere non attraverso la sottrazione del bene, ma mediante copia non autorizzata dello stesso e successiva divulgazione;
- *uso illecito di risorse hardware e software:* utilizzazione non autorizzata o abusiva delle risorse informatiche dell'Ente;
- *malfunzionamenti del sistema:* eventi strettamente connessi al sistema in grado di compromettere l'affidabilità e la continuità dei servizi;
- *inagibilità dei locali:* condizioni di impraticabilità dei locali in cui sono posti gli archivi offline o dove sono svolte le attività;
- *minacce provenienti da Internet e dalle reti:* aggressioni al sistema informatico determinate o agevolate dal collegamento degli elaboratori a reti informatiche quali ad esempio:
  - azioni dirette ad utilizzare i difetti e le debolezze dei protocolli di trasmissione dei dati; ad es.: *denial of service*, insieme di tecniche per provocare malfunzionamenti o blocchi del sistema informatico;
  - azioni dirette ad utilizzare difetti esistenti nei meccanismi di autenticazione e autorizzazione;

- azioni dirette ad inserirsi in una rete locale senza la necessaria autorizzazione, in particolare nel caso di reti wireless, per le quali è necessario prevedere configurazioni particolarmente curate a causa delle difficoltà di circoscrizione geografica;
- azioni dirette a sfruttare difetti ed errori del software (*bug*) o ad usare funzionalità non note agli utilizzatori (*backdoor*);
- furto di password*;*
- *virus e worm informatici:* programmi eseguibili capaci di riprodursi copiando loro stessi all'insaputa e senza l'autorizzazione dell'utente: attualmente costituiscono una tra le più diffuse minacce al sistema informatico;
- *phishing:* il tentativo di ottenere l'accesso a informazioni personali e riservate mediante l'utilizzo di messaggi di posta elettronica, opportunamente creati per apparire autentici.

Obiettivi di sicurezza

In relazione alle minacce indicate ed ai conseguenti potenziali rischi, l'INFN ritiene necessario adottare idonee misure dirette a garantire la sicurezza del sistema informatico nel suo complesso; misure che attengono secondo la tripartizione convenzionalmente accolta:

- la sicurezza fisica,
- la sicurezza logica,
- la sicurezza organizzativa.

Sicurezza fisica

Con riferimento a tale aspetto, connesso alla protezione dei locali, delle risorse umane e delle componenti hardware e software che costituiscono il sistema informatico aziendale, l'INFN prevede:

- *un servizio di vigilanza* presso ciascuno dei quattro Laboratori Nazionali ed apposite convenzioni con le Università per tutelare la sicurezza dei luoghi nelle Strutture situate presso le sedi universitarie, al fine di ridurre il rischio di furti e danneggiamenti connessi a condotte umane volontarie;
- *sistemi anti-intrusione* con procedure d'ingresso controllato nei locali che ospitano i centri di calcolo ed in quelli ove sono posti server ed elaboratori mediante i quali vengono trattati dati personali, al fine di ridurre il rischio di furto, danneggiamento, perdita della riservatezza e divulgazione specialmente per i dati e le informazioni per le quali la legge richiede una particolare riservatezza (dati personali sensibili e giudiziari del Decreto Legislativo 196/03 – Codice in materia di tutela dei dati personali);
- la predisposizione di *dispositivi antincendio* e di *continuità elettrica* in modo tale da ridurre il rischio di danneggiamenti e malfunzionamenti di quelle parti del sistema ritenute critiche al fine di garantire l'espletamento delle attività istituzionali dell'Ente.
- l'adozione altresì di particolari misure di protezione per le risorse distribuite al di fuori delle Strutture dell'Ente.

Sicurezza logica

Rappresenta una forma di tutela direttamente connessa alla protezione dei dati e delle informazioni e si esplica in misure tecnologiche dirette a garantire servizi di autenticazione, controllo accessi, confidenzialità, integrità e non ripudio.

A tali fini l'INFN raccomanda un'attenta valutazione del software installato sui sistemi e promuove l'implementazione di meccanismi e strumenti di sicurezza, quali:

- strumenti di protezione specifica delle reti locali: *firewall*;
- strumenti di *Intrusion Detection*;
- *Virtual Private Network* (VPN);
- meccanismi di controllo degli accessi ed autenticazione;
- strumenti per la tutela della riservatezza e autenticità dei dati: crittografia e firma elettronica;
- strumenti per l'integrità e disponibilità dei dati: sistemi di backup;
- programmi antivirus.

Sicurezza organizzativa

E' relativa all'individuazione delle procedure dirette alla implementazione, gestione e controllo delle misure di sicurezza adottate e si concretizza:

a) nell'individuazione di ruoli, funzioni e responsabilità coinvolte nella realizzazione e gestione del sistema di sicurezza, con riferimento alla tutela sia dei dati di carattere scientifico sia dei dati personali, conformemente a quanto disposto dal Codice in materia di tutela dei dati personali;

b) nell'individuazione delle procedure da seguire per conservare in sicurezza il sistema informatico, regolamentando la condotta degli utenti.

Con riferimento al punto a) l'articolazione organizzativa in ciascuna Struttura prevede:

- il *Direttore di Struttura*, cui compete la responsabilità di assicurare il funzionamento scientifico, organizzativo ed amministrativo della Struttura nel rispetto degli indirizzi approvati dal Consiglio Direttivo; egli è individuato, con riferimento al trattamento dei dati personali, responsabile del trattamento ai sensi dell'art. 29 del D.Lgs. n. 196/03;
- il *Servizio di Calcolo e Reti*, cui competono la gestione delle risorse di calcolo centrali, i collegamenti in rete all'interno ed all'esterno della Struttura, nonché la cura, installazione e sviluppo delle stesse e l'assistenza agli utenti per l'accesso alle risorse ed alla rete; ha inoltre competenza in materia di sicurezza su ogni risorsa di calcolo comunque afferente alla propria Struttura; nell'ambito di ciascun Servizio di Calcolo è individuato almeno un referente per il *Computer Security Incident Response Team* (CSIRT);
- l'*Amministratore di sistema* con il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione;
- gli *Utenti*, soggetti che hanno accesso alle risorse di calcolo e ai servizi di rete, in relazione alle funzioni ed attività che sono chiamati a svolgere nell'ambito dell'Istituto; gli utenti autorizzati al trattamento dei dati personali sono individuati come *incaricati del trattamento* ai sensi dell'art. 30 del D.Lgs. n. 196/03.

In ciascuna Struttura possono essere individuati uno o più *Referenti* per le questioni informatiche, che svolgono un ruolo di interfaccia tra il gruppo di utenti che rappresentano e il Servizio di Calcolo.

Per quanto attiene il punto b), l'individuazione delle procedure viene formalizzata attraverso *policy* e specifici regolamenti di condotta, periodicamente aggiornati in relazione all'evoluzione tecnologica del settore.

Compiti di coordinamento nell'individuazione delle politiche di sicurezza e nell'adozione delle conseguenti misure sono affidati alla Commissione Calcolo e Reti, che provvede anche all'organizzazione dello CSIRT.

L'INFN attribuisce particolare rilievo alla costante sensibilizzazione degli utenti ad un uso corretto delle risorse informatiche, attraverso attività di formazione ed aggiornamento, dirette a creare, al di là di competenze specialistiche proprie dei soggetti tenuti alla gestione del sistema, un patrimonio comune di conoscenze informatiche relativamente alle nozioni basilari di protezione, manutenzione ed uso degli elaboratori.

Verifica dell'adeguatezza delle misure di sicurezza

L'INFN verifica periodicamente l'adeguatezza ed efficacia delle misure di sicurezza adottate provvedendo ad adeguare le stesse alla particolare evoluzione tecnologica del settore, al fine di mantenere elevato il livello di protezione e ridurre, quindi, il livello di rischio.

L'attività di verifica viene attuata mediante procedure di *monitoraggio* e di *audit* ed in particolare:

- attraverso un sistema di *monitoraggio* effettuato da responsabili interni che eseguono un controllo costante dell'effettivo funzionamento del sistema informatico e delle misure di sicurezza, adottando tutte le misure necessarie ad incrementarne il livello di efficacia;
- attraverso la previsione di un'attività di *audit*, quale controllo saltuario svolto da soggetti *diversi* dai responsabili interni, al fine di ottenere un giudizio imparziale circa la qualità delle misure di sicurezza approntate ed in grado di evidenziarne eventuali debolezze od errori.