Istituto di Scienza e Teonologie dell'Informazione "Alessandro Faedo"
Sicurezza Informatica di Istituto: Politica e Organizzazione

A cura di Carlo Carlesi

Indice

Introduzione

I sistemi informatici e la rete telematica sono strumenti fondamentali per la "missione" dell' Istituto di Scienza e Tecnologie dell'Informazione "Alessandro Faedo" (di seguito ISTI) e rappresentano un sostanziale investimento di risorse sia in termini umani che finanziari.
La sicurezza informatica, e' piu' che una necessita' e richiede di essere affrontata in modo omogeneo e funzionale alle diverse realta' presenti nell'ISTI per conciliare diverse esigenze:

- proteggere i propri investimenti
- rispettare le normative legali vigenti in tema di sicurezza dei sistemi per il trattamento automatico dell'informazione (information technology system o sistemi IT)
- preservare la propria immagine istituzionale.

Nel contesto di questo documento, con il termine "sicurezza informatica" (di seguito sicurezza IT), si intendono tutte le attivita' riguardanti la protezione dei sistemi informatici, delle apparecchiature di rete e delle informazioni digitali mantenute e gestite su supporti elettronici. In termini piu' operativi la sicurezza IT ha il duplice scopo di:

- proteggere il "patrimonio informativo" dal rischio di danneggiamenti a causa del verificarsi di una minaccia,
- limitare gli effetti causati dall'eventuale occorrenza di un rischio.

Sono considerate potenziali minacce i rischi derivanti da:

- guasti "hardware",
- errori "software",
- errori umani,
- cause accidentali e imprevedibili (allagamento, incendio),
- esposizione agli "incidenti informatici"
    - virus & worms
    - intrusioni e/o accesso non autorizzato alle informazioni
    - falsificazione di documenti digitali o di identita'
    - uso illecito delle risorse

Aspetti della sicurezza

Partendo dal concetto che non esiste una sicurezza "assoluta", la sicurezza informatica, ha l'obiettivo principale di garantire, riducendo i rischi, un adeguato grado di protezione del bene mediante opportune misure di sicurezza che si concretizzano sotto vari aspetti:

- tecnici (sicurezza fisica, logica),
- organizzativi (definizione di ruoli, procedure formazione),
- strategici ed economici (obiettivi e analisi dei costi)
- legali (leggi, normative e raccomandazioni).

Aspetti Tecnici

Sicurezza fisica

La "Sicurezza fisica" riguarda la protezione fisica delle risorse e la definizione di misure atte a mantenere un ambiente di lavoro protetto che impedisca perdite di informazione e di patrimonio intellettuale di proprieta' dell'ente. Le misure di sicurezza si riferiscono alle protezioni perimetrali dell'istituto, al controllo dell'accesso fisico ai sistemi personali e multi-utente (metodi di autenticazione, password e file di log), all'accesso a sistemi e servizi via rete (filtri a livello di router di rete, firewall ecc). Obiettivo della sicurezza fisica e' quello di prevenire e ridurre il rischio di accessi fisici o virtuali non autorizzati alle risorse, perdita di informazioni e danni o interruzione di servizi (posta elettronica, accesso a sistemi informativi ecc).

Sicurezza logica

Il campo di applicazione della “Sicurezza Logica” riguarda principalmente la protezione dell’informazione e, di conseguenza, la capacità di salvaguardare la riservatezza, l’integrità e la disponibilità dell'informazione (elaborata su sistemi informativi, memorizzata su supporti di varia natura o trasmessa attraverso canali di comunicazione) e la capacità di contrastare efficacemente ogni minaccia sia di tipo accidentale sia di tipo intenzionale proveniente dall’interno o dall’esterno alla propria organizzazione.

Più in dettaglio:

• salvaguardare la riservatezza dell'informazione significa ridurre a livelli accettabili il rischio che un'entità (persona fisica procedura/programma software) possa, volontariamente o involontariamente, accedere all'informazione stessa senza esserne autorizzata;

• salvaguardare l'integrità dell'informazione significa ridurre a livelli accettabili il rischio che possano avvenire cancellazioni o modifiche di informazioni a seguito di interventi di entità non autorizzate o del verificarsi di fenomeni non controllabili (come il deteriorarsi dei supporti di memorizzazione, la trasmissione dei dati su canali non protetti, i guasti degli apparati, gli incendi, gli allagamenti ecc.) e prevedere adeguate procedure di recupero delle informazioni (piani di back-up ecc.);

• salvaguardare la disponibilità dell'informazione significa ridurre a livelli accettabili il rischio che possa essere impedito l'accesso alle informazioni a seguito di azioni compiute da entita’ non autorizzate interne o esterne (intrusori informatici) o del verificarsi di fenomeni non controllabili del tipo già visto al punto precedente.

Aspetti Organizzativi

Gli aspetti organizzativi della sicurezza riguardano una serie di norme e procedure atte a regolamentare il processo della sicurezza rispetto a:

- la definizione di ruoli, compiti e responsabilita' per la gestione di tutte le fasi del processo sicurezza;
- l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate.

Aspetti Strategici

Gli aspetti strategici della sicurezza informatica riguardano essenzialmente il livello di sicurezza che l'Istituto si propone di raggiungere e i tempi e i modi con cui si intende raggiungerlo.

Aspetti legali

Gli aspetti legali riguardano il contesto normativo di riferimento.
Nel presente lavoro, si e' pertanto tenuto conto della legislazione italiana relativa alla sicurezza informatica e in particolarre delle leggi fondamentali che costituiscono la griglia di riferimento normativo.

1. Dlgs n. 518/1992 che modifica il regio decreto n. 633/1941, relativo al diritto di autore, integrandolo con norme relative alla tutela giuridica dei programmi per elaboratore.
2. Legge n. 547/1993 che modifica il codice penale italiano introducendo i cosidetti "computer crimes".
3. Legge delega n. 127/2001 Codice in materia di protezione dei dati personali, DL n. 196/2003
4. DL n.72/2004 - Interventi per contrastare la diffusione telematica abusiva di materiale audiovisivo.

Organizzazione del documento

Il presente documento propone il modello organizzativo generale di infrastruttura necessaria sia per la formulazione delle Politiche di sicurezza, sia per l'attuazione della sicurezza stessa ed e' il risultato finale di una serie di incontri, da me condotti su questo specifico tema, con tutte le parti interessate di Istituto, ovvero i Responsabili dei Centri, Laboratori e Servizi, e i rispettivi Referenti Informatici.
Desidero qui, ringraziare, tutti coloro che hanno partecipato agli incontri e che hanno contribuito allo sviluppo di questo documento e in particolare Renzo Beltrame per l'attenta rilettura di questo e altri documenti correlati.
A completamento e integrazione di quanto presentato di seguito, sono in via di sviluppo due linee di documentazione (di seguito sezioni) che saranno mantenute volutamente separate:

AUP: Politiche di sicurezza;
Piano di attuazione della sicurezza.

La sezione "Politiche di sicurezza" o AUP "Acceptable Use Policy" e' una raccolta di normative strutturata per argomenti che riporta i principi generali ovvero la Politica dell'ISTI per quel dato argomento.
La sezione "Piano di attuazione della sicurezza" descrive le metodologie applicate per il raggiungimento della sicurezza dei sistemi e delle informazioni, in sintonia con quanto disposto nelle Politiche; in questa sezione e' definito il piano generale di sicurezza applicabile a tutti i sistemi e i piani specifici per particolari applicazioni e/o sistemi che

richiedono, per la loro natura, speciali misure di sicurezza.

La sicurezza non e' una attivita' da intraprendere una volta tanto (one-time activity) ma un processo dinamico di gestione dei rischi in grado, con l'evolversi temporale delle necessita' e delle tecnologie, di rinnovarsi per garantire il desiderato livello di sicurezza in termini di disponibilita', integrita', autenticita' e confidenzialita' delle informazioni e dei servizi erogati.

1. Politica della sicurezza: Scopi e finalità

Tutelare adeguatamente un "bene informatico", significa mantenere un costante equilibrio tra il livello di rischio accettabile e il corrispondente grado di protezione necessario a limitarlo, coniugando correttamente l'esigenza di tutelare il "valore" del bene con la necessita' di assicurare efficienza ed efficacia ai processi che lo producono.
Questo documento ha l'obiettivo di definire il livello di sicurezza informatica idoneo alla missione istituzionale dell'ISTI ed e' stato formulato in funzione della complessita' della rete telematica e delle diverse esigenze informatiche dei Laboratori, dei Centri e dei Servizi, che necessitano di un "ambiente di rete" aperto ma sicuro.
In particolare vengono individuate le responsabilita' (ruoli) considerati fondamentali per assicurare la tutela del patrimonio informativo e creare l'infrastruttura di base necessaria al ciclo di vita del processo di gestione della sicurezza.

Le politiche di sicurezza informatica dell'ISTI, esplicitano quindi gli obiettivi, i principi guida, le regole e l'ambito di applicazione di tali principi senza entrare nel merito delle soluzioni tecnologiche; tema che sara' affrontato nella preparazione del "Piano di attuazione della Sicurezza Informatica". In particolare la documentazione relativa alle procedure attuative per il raggiungimento degli obiettivi sarà mantenuta volutamente separata dalla documentazione delle politiche in quanto oggetto di maggiori e più frequenti revisioni e aggiornamenti.

2 Definizione delle politiche di sicurezza informatica

Attraverso questo documento, la Direzione dell'ISTI definisce i ruoli, le responsabilita' e le modalita' d'uso delle risorse informatiche, della rete locale e di Internet e diffonde a tutta la struttura i principi fondamentali di sicurezza che intende adottare e conseguire, informando tutti gli utenti riguardo alle normative di base e le regole che disciplinano l'uso dei servizi telematici di Istituto.

2.1 Obiettivo delle Politiche di Sicurezza

Nessuna iniziativa di sicurezza e' tale da garantire, con assoluta certezza, l'assenza di rischi informatici. Pertanto l'obiettivo e' quello di contenere questi rischi a un livello ritenuto accettabile per mezzo di un insieme di misure di protezione organizzative, operative e tecnologiche finalizzate a:

- Assicurare l'integrita' e la disponibilita' delle informazioni;
- Consentire l'accesso, in aderenza agli aspetti legislativi vigenti in materia di riservatezza delle informazioni, ai soli addetti per i quali le informazioni in questione effettivamente attengono in virtu' delle funzioni dagli stessi esercitate;
- Definire le responsabilita' generali e specifiche per la gestione della sicurezza informatica;
- Definire le procedure di gestione e mantenimento dei rapporti relativi agli "incidenti informatici";
- Fornire l'evidenza dell'utilizzo delle risorse informatiche e delle informazioni;
- Garantire la riservatezza dei dati personali;
- Garantire la continuita' e la disponibilita' dei servizi;
- Identificare, autenticare e autorizzare tutti gli utilizzatori dei sistemi informatici;
- Prevenire e rilevare l'introduzione di virus o altre forme di software malizioso;
- Salvaguardare i diritti della proprieta' intellettuale.

2.2 Responsabilita' delle politiche di sicurezza

Le politiche di sicurezza informatica, sono formulate sulla base dell'analisi del rischio, del livello di sicurezza atteso e dei requisiti derivanti dalle norme vigenti.

Le modalita' per rendere operative le politiche verranno definite da apposite norme e procedure predisposte dal gruppo di lavoro "Supporto Sicurezza Informatica" (di seguito SSI) che si occupera' piu' in generale di tutte le attivita' inerenti la gestione della sicurezza dell'ISTI. Il gruppo di lavoro "SSI" e' diretto dal responsabile della "Sicurezza Infornatica"

La Direzione dell'ISTI definisce annualmente l'impegno finanziario messo a disposizione per l'attuazione, l'applicazione e la verifica delle politiche.

Il responsabile della "Sicurezza Informatica" di seguito RSI, rende conto almeno una volta all'anno, alla Direzione, del progresso ottenuto nell'attuazione delle politiche di sicurezza.

2.3 Ambito delle politiche di sicurezza

L'ambito di applicazione delle politiche di sicurezza IT riguarda tutte le attivita' che richiedono e/o sono svolte con l'uso di sistemi informatici e telematici. Schematicamente possiamo riassumere che:

Le misure di sicurezza si applicano alle risorse, ovvero:

- Alle informazioni contenute nei sistemi informatici di Istituto
- Al "hardware" e al "software" che compone ogni singolo sistema informatico incluse memorie, supporti magnetici e supporti di telecomunicazione;
- All'ambiente fisico in cui le risorse sono ubicate;

Le regole di sicurezza riguardano gli utilizzatori, ovvero:

- Il personale interno;
- I collaboratori che interagiscono con i laboratori, i centri e i servizi;
- I fornitori di servizi;
- Gli interlocutori esterni che a qualunque titolo interagiscono con i sistemi informatici d' Istituto;

I requisiti di sicurezza si applicano ai processi e alle applicazioni che riguardano

- I servizi telematici Intranet/Internet;
- La fruizione di servizi informatici interni ed esterni;
- L'erogazione di servizi informatici interni ed esterni.

3 Organizzazione e infrastruttura della sicurezza

Le politiche generali approvate dalla Direzione sono attuate da tutti i componenti dei Servizi, dei Centri, dei Laboratori con il supporto del gruppo di lavoro SSI.

L'attuazione delle politiche si ottiene non solo con il rispetto delle norme e delle procedure ma di fatto stabilendo dei presidi organizzativi e assegnando responsabilita' specifiche per quanto attiene l'organizzazione della sicurezza delle singole risorse.

3.1 Presidi organizzativi della sicurezza

I ruoli che seguono sono fondamentali per assicurare una infrastruttura organizzativa in grado di consentire una corretta gestione del processo continuo di impostazione, di mantenimento, di valutazione e di revisione della sicurezza IT a tutti i livelli dell'Istituto.

3.1.1 Proprietario

Ciascun bene informativo (inteso come insieme di risorse tecnologiche e di informazioni) deve poter essere ricondotto a un *Proprietario* ben definito, il cui compito e' quello di manifestare le esigenze relative allo sviluppo, implementazione ed integrazione del bene informativo oggetto delle proprie attivita'.
Nell'ottica della sicurezza IT, il *Proprietario* e' identificato con il Responsabile del Servizio, Laboratorio o Centro che, avvalendosi della collaborazione del *Referente Informatico*, definisce il livello di sensibilita' del bene informativo in termini di riservatezza, integrita'e disponibilita'; ne stabilisce il valore e ne determina il livello di rischio.
E' anche responsabilita' del *Proprietario* scegliere e approvare, le contromisure di sicurezza, ritenute più opportune per ridurlo oppure accettarlo o trasferirlo all'esterno.

3.1.2 Referente Informatico

Il *Referente Informatico* e' colui che, su delega del *Proprietario* e con il supporto del gruppo di lavoro SSI, identifica e classifica le informazioni per livello di sensibilita' e, secondo criteri concordati, al fine di soddisfare le esigenze di

protezione risultanti dall'analisi comparata tra il valore del bene informativo e il costo delle contromisure di sicurezza necessarie. Inoltre per ogni applicazione informatizzata (progetto/attività) di interesse, deve valutare le eventuali situazioni di rischio dovute dall'eventuale esposizione ai pericoli della rete pubblica (se necessario e richiesto), proponendo al *Proprietario* le relative contromisure di sicurezza da adottare.

3.1.3 Utente finale

Gli Utenti sono tutte quelle persone, interne o esterne all'ISTI che hanno necessita' di utilizzare le informazioni e le risorse telematiche per svolgere i compiti loro assegnati. Ogni utente e' tenuto, in generale, a svolgere, a conoscere e rispettare tutte le norme di sicurezza in vigore; in particolare deve farsi identificare e autenticare. Ogni utente che dispone di una macchina (personal computer) o di un "accesso" a un sistema multi-utente è responsabile dell'uso che viene fatto di tale risorsa. In particolare la responsabilità del contenuto dei materiali prodotti e diffusi attraverso la rete è delle persone che li producono e diffondono.

Per utente finale si intende:

- personale dipendente;
- dottorandi;
- laureandi;
- contrattisti;
- collaboratori, fornitori e altro personale formalmente autorizzato ad accedere alle risorse informatiche di Istituto.

3.1.4 Supporto Sicurezza Informatica (SSI)

Il gruppo di lavoro "SSI" e' un gruppo di lavoro dinamico che si costituisce a fronte di una precisa direttiva emanata con la politica della sicurezza.
Il gruppo e' costituito da esperti interni con competenze in:

- tecnologie informatiche,
- tecnologie telematiche (rete internet),
- sviluppo applicazioni e servizi telematici,
- problematiche ambientali e conoscenza dell'ambiente della ricerca.

Fanno parte del SSI, i Referenti Informatici, che partecipano al gruppo di lavoro, ognuno per il proprio settore di responsabilita' e competenza.
Possono partecipare inoltre, "esperti" esterni chiamati a dare il proprio contributo in termini di analisi e soluzioni tecniche a fronte di specifici problemi.
Il gruppo e' coordinato e diretto dal RSI.

3.2 Ruolo Operativo della sicurezza

Il RSI ha la responsabilita' di mettere in atto le direttive di sicurezza approvate dalla Direzione e di rendere conto della loro applicazione.

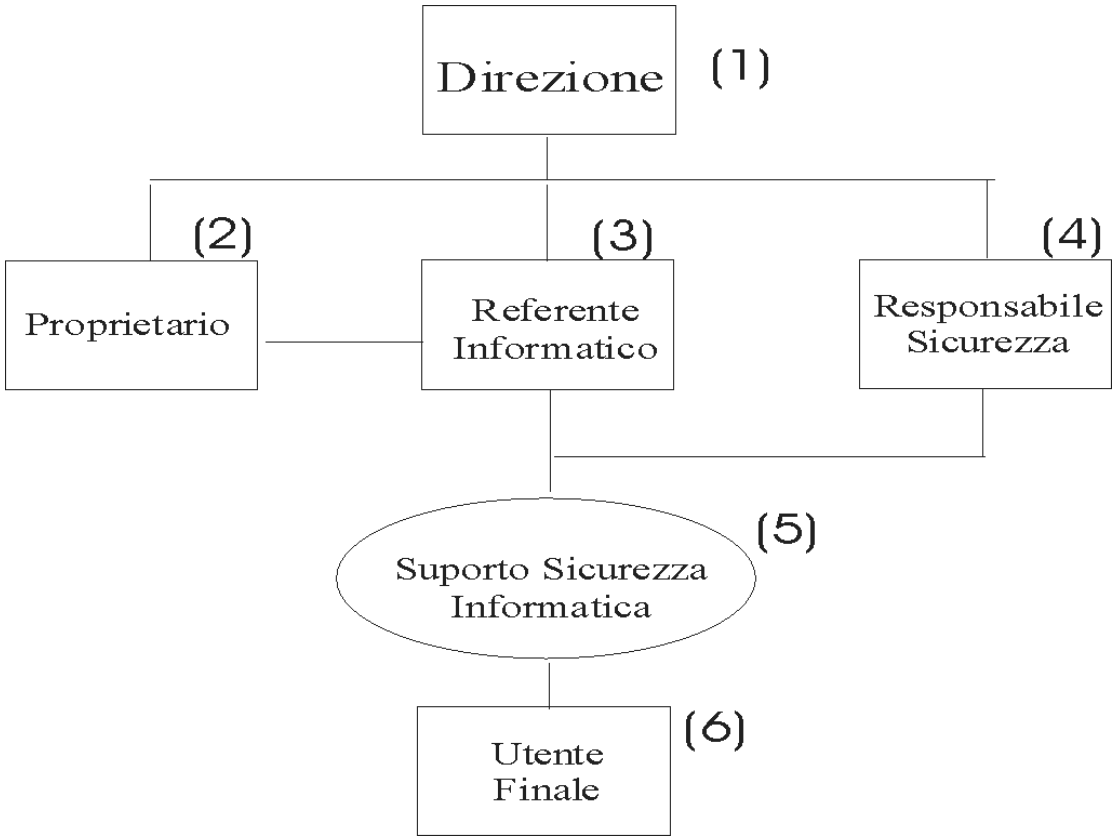
A questo scopo deve assicurare, con la collaborazione e il supporto dei responsabili dei presidi organizzativi precedentemente citati, la realizzazione del "Piano di Sicurezza Informatica".

RSI ha inoltre il compito di:

- Assicurare l'amministrazione centralizzata del processo sicurezza
- Definire le politiche di sicurezza da sottoporre alla Direzione per l'approvazione e curarne l'evoluzione;
- Definire le norme e le procedure operative di sicurezza;
- Gestire e mantenere aggiornata e disponibile in linea tutta la documentazione relativa alle politiche e alla loro attuazione;
- Gestire e mantenere i rapporti relativi agli "incidenti informatici";
- Coordinare e organizzare l'attività del gruppo di lavoro SSI;
    - Promuovere e assistere i Referenti Informatici nell'analisi dei rischi;
    - Assistere i Referenti Informatici, per quanto attiene l'interpretazione delle norme e l'applicazione di specifiche metodologie operative;
- Proporre e seguire la realizzazione dei piani di azione per il miglioramento del livello di sicurezza;
- Provvedere ad azioni di monitoraggio e controllo con strumenti di rilevamento di potenziali vulnerabilita' e di prevenzione delle intrusioni per valutare l'efficienza e l'efficacia delle misure di sicurezza in atto;
- Valutare in collaborazione con il gruppo di lavoro SSI i prodotti di sicurezza di mercato e Open Source;
- Condurre e coordinare la revisione periodica delle politiche;
- Promuovere, le azioni di formazione e sensibilizzazione alla sicurezza per il personale attraverso comunicazioni via e-mail e seminari tecnico-divulgativi.

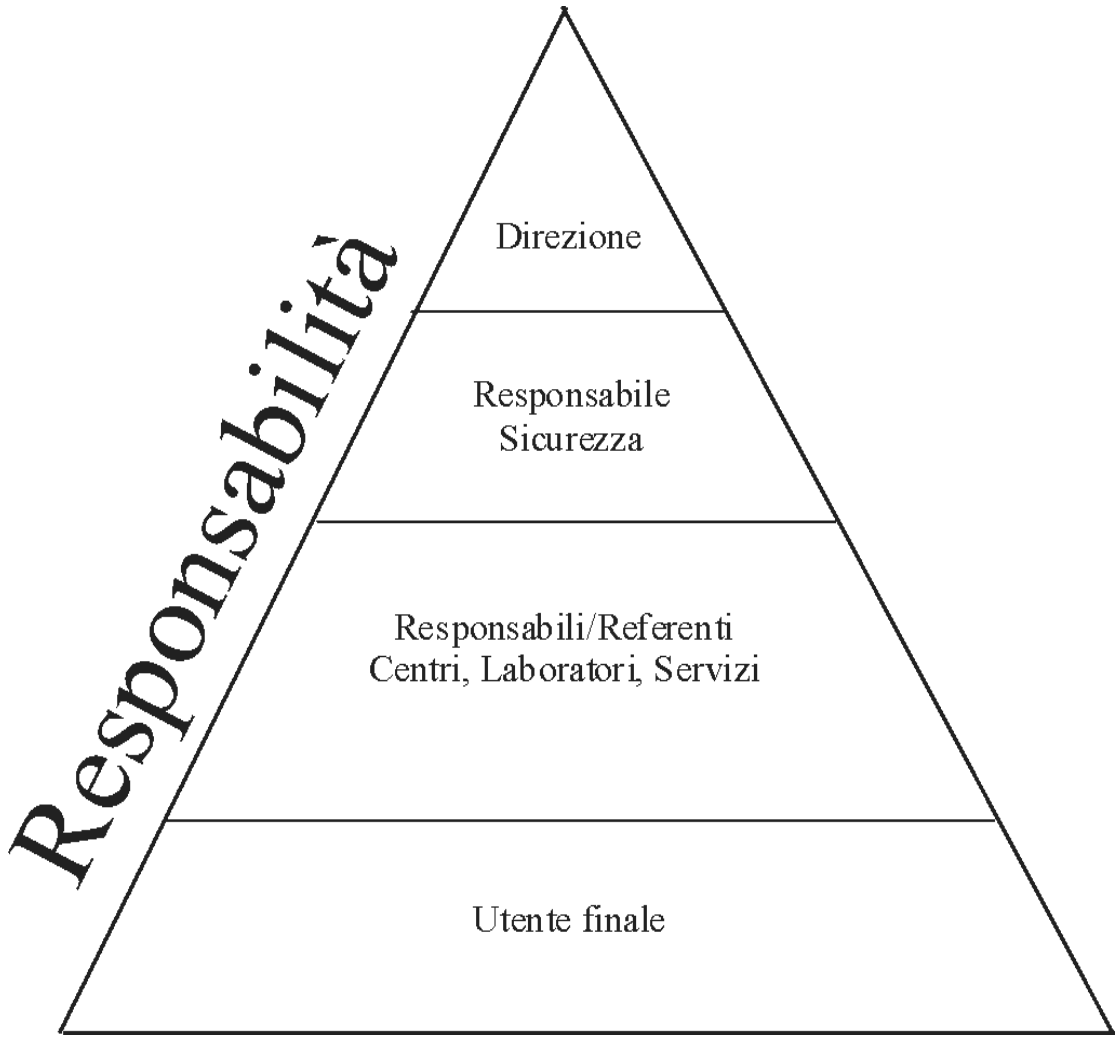
3.3 Modello Organizzativo della sicurezza informatica

(**Responsabilita' e compiti principali**)



1) Approva le Politiche di Sicurezza e i Piani Attuativi
2) Individua le informazioni critiche e vitali. Approva l'analisi dei rischi
3) Classifica le informazioni ed effettua l'analisi dei rischi formulando le contromisure ritenute adeguate con il supporto di SSI
4) Promuove e coordina la definizione delle Politiche di Sicurezza e dei Piani Attuativi. Coordina le attività dei Referenti Informatici e del SSI per l'analisi dei rischi. Provvede alla revisione periodica delle procedure e al monitoraggio dell'efficacia delle misure di sicurezza
5) Fornisce assistenza e supporto per le attività di analisi dei rischi e la definizione delle procedure e dei piani attuativi della sicurezza
6) Provvede all'attuazione delle procedure guidate per la sicurezza informatica locale e al rispetto delle norme in vigore

3.4 Modello gerarchico della responsabilita'


Responsabilità
Direzione
Responsabile
Sicurezza
Responsabili/Referenti
Centri, Laboratori, Servizi
Utente finale

BIBLIOGRAFIA

Legge n.547/1993, "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica", G.U. serie generale n.305 del 30 dicembre 1993

AIPA – Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella pubblica amministrazione [1999]

Common Criteria for Information Technology Security Evaluation, CCIMB-99-031, [August 1999]

ISO/IEC 17799 – International Standard (Information technology – Code of pratice for information security management) [ISO 2000]

AIPA –La sicurezza dei servizi in rete
-requisiti, modelli, metodi e strumenti- [novembre 2001];

Decisione-Quadro del Consiglio relativa agli attacchi contro i sistemi di informazione, COM(23002)173 definitivo, 2002/0086(CNS), [Aprile 2002]

Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione
Verso una cultura della sicurezza [2002]

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(Legge delega n. 127/2001; G.U. N. 174 2003; DL n. 196/2003)

Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)
(Codice in materia di protezione dei dati personali art.34 e Allegato B, regola 19, del d.lg. n.196/2003)

CNIPA – Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione [Marzo 2004]

DL n.72/2004 - Interventi per contrastare la diffusione telematica abusiva di materiale audiovisivo [Aprile 2004]