Proposta per l'organizzazione della Sicurezza Informatica dell'ISTI

Carlo Carlesi

Situazione attuale

- Non esiste un'organizzazione della sicurezza
- Non sono ben chiare le responsabilità
- Non c'è "coscienza" di quelle che sono le leggi in vigore e le raccomandazioni europee per l'IT

Scopo dell'incontro

- Presentare la proposta di organizzazione della sicurezza ai responsabili dei Centri, Laboratori e Servizi
  - Richiedere il loro esplicito appoggio all'iniziativa
  - Richiedere il loro contributo alla definizione delle politiche
  - Individuare i referenti tecnici per l'analisi dei rischi, la definizione e la gestione dei piani di attuazione

Considerazioni Generali

- Perchè la sicurezza è necessaria
  - proteggere i propri investimenti
  - rispettare le normative legali vigenti in tema di sicurezza informatica (information technology system o sistemi IT)
  - preservare la propria immagine istituzionale.

Considerazioni Generali

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

Aspetti tecnici (sicurezza fisica, logica)

- Sicurezza Fisica
  - Le misure di sicurezza si riferiscono alle protezioni perimetrali dell'istituto, al controllo dell'accesso fisico ai sitemi 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 etc).
- Sicurezza logica
  - salvaguardare l'integrità dell'informazione
  - salvaguardare la riservatezza dell'informazione
  - salvaguardare la disponibilità dell'informazione

Aspetti Organizzativi

- Definizione di ruoli, compiti e responsabilita'
  - Chi fa:
    - Cosa
    - Quando
    - Come
    - Perchè

Aspetti legali & etici

- Individuazione delle attivita' soggette a normative
- Rispetto delle normative in vigore
  - Testo unico, "privacy", "spamming", "child pornography" etc
- Conformita' a standard internazionali e raccomandazioni in materia di sicurezza IT
  - ISO/IEC 17799
  - Common Criteria for information technology
  - Raccomandazioni della "Commissione delle Comunita' Europee"

Il processo sicurezza

- La sicurezza si ottiene attraverso tre fasi fondamentali:
  - Organizzazione della sicurezza
  - Definizione delle politiche di sicurezza
  - Piani attuativi delle politiche

Organizzazione della sicurezza

- Proposta di infrastruttura organizzativa
  - Presidi organizzativi della sicurezza
  - Ruolo operativo della sicurezza
  - Modello organizzativo della sicurezza
  - Modello gerarchico delle responsabilita'

Organizzazione della sicurezza

- Presidi organizzativi della sicurezza
  - Propretario (Resposabile Centro, Laboratorio e Servizio)
  - Referente informatico
  - Referente applicativo
  - Referenti locali della sicurezza (amministratori sistemi)
  - Utenti
  - Gruppo di lavoro SSI “Supporto Sicurezza Informatica”

Organizzazione della sicurezza

- Proprietario del bene informativo
  - Responsabile Centro, Laboratorio e Servizio
  - Ha il compito e la responsabilità di stabilire il livello di sensibilità e valore strategico dei propri beni in termini di:
    - Riservatezza, integrità e disponibilità (delle informazioni)
    - Criticità ed esposizione ai rischi informatici (dei sistemi)
    - Costi economici e perdita di immagine a seguito di un possibile incidente informatico
  - Ha la responsabilità di approvare le misure di sicurezza ritenute opportune sulla base del rischio valutato

Organizzazione della sicurezza

- Referente Informatico
  - La persona che su delega del “Proprietario” provvede a:
    - Identificare i beni informativi
      - Sistemi hardware e software
      - Tipologia di dati/informazioni
    - Evidenziare le eventuali vulnerabilità (infrastruttura)
    - Valutare i possibili rischi a cui sono esposti i beni
    - Proporre le contromisure di sicurezza ritenute necessarie
  - Collabora e si avvale del supporto dei
    - Referenti applicativi
    - Referenti locali della sicurezza (Amministratori dei sistemi)
    - Gruppo di lavoro” Supporto Sicurezza Informatica”

Organizzazione della sicurezza

- Referente Applicativo
  - La persona che ha di fatto ha la responsabilità dell'analisi e sviluppo di applicazioni e/o progetti (Project leader)
  - Ha la responsabilità di supportare il Referente Informatico per:
    - Analisi dei rischi informatici connessi all'applicazione
    - Classificare il tipo di informazioni/dati trattati
    - Valutare il livello di criticità e attribuire un valore all'applicazione
    - Segnalare eventuali obblighi da ripettare

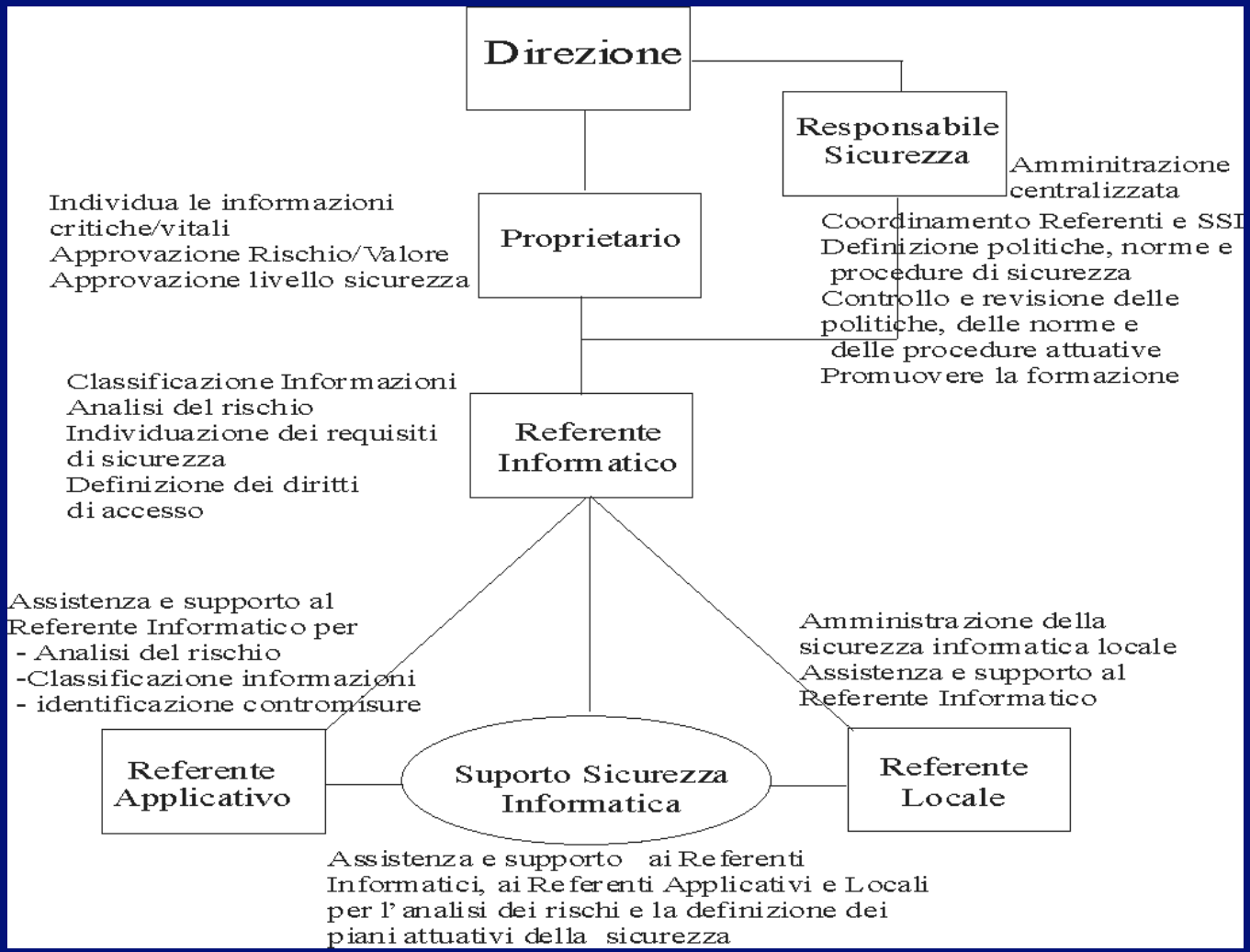
Organizzazione della sicurezza

- Referente locale della sicurezza
  - La persona che ha di fatto ha l'amministrazione di un dato sistema informatico.
  - Ha il compito e la responsabilità di:
    - Mantenere il sistema operativo aggiornato in termini di "Patch" di sicurezza periodicamente rilasciate dai produttori
    - Controllare periodicamente lo stato del sistema (file di log etc.)
    - Gestire il controllo e le modalità di accesso al sistema e alle informazioni
    - Segnalare al SSI/RSI eventuali incidenti informatici o situazioni di rischio
    - Provvedere all'applicazione e attuazione dei piani di sicurezza
    - Collaborare alla revisione periodica delle procedure
    - Identificare e segnalare nuove vulnerabilità

Organizzazione della sicurezza

- Supporto Sicurezza Informatica (SSI)
  - Il gruppo e' costituito da esperti interni con competenze in:
    - tecnologie informatiche
    - tecnologie telematiche (rete internet)
    - sviluppo applicazioni e servizi telematici
    - problematiche ambientali (profonda conoscenza dell'ambiente della ricerca)

Modello organizzativo della sicurezza



Modello gerarchico delle responsabilita'