AIPA
Autorità per l'Informatica
nella Pubblica Amministrazione

Spedizione in abbonamento postale - art. 2 comma 20/C legge 662/96 - filiale di Roma

iQuaderni

Supplemento al N. 9-10/1999 di Informazioni

2

Linee guida per la definizione di un piano per la sicurezza

Ottobre 1999

n. 2
ottobre 1999

i Quaderni

sommario

3 PREMESSA

4 INTRODUZIONE

6 OBIETTIVI DEL PRESENTE DOCUMENTO

7 CONTESTO NORMATIVO DI RIFERIMENTO

8 IL PROCESSO DELLA SICUREZZA DEL SISTEMA INFORMATIVO AUTOMATIZZATO

9 ANALISI DEI RISCHI

13 DEFINIZIONE DELLE POLITICHE DI SICUREZZA

16 GESTIONE DEL RISCHIO

18 IL PIANO OPERATIVO

31 VERIFICA DELLA SICUREZZA DEI SISTEMI INFORMATIVI AUTOMATIZZATI

34 INTRODUZIONE E DIFFUSIONE DELLA CULTURA DELLA SICUREZZA INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE

36 ORGANIZZAZIONE FUNZIONALE DELLA GESTIONE DELLA SICUREZZA DEI SISTEMI INFORMATIVI AUTOMATIZZATI NELLE PUBBLICHE AMMINISTRAZIONI

39 GRUPPO DI LAVORO

40 BIBLIOGRAFIA

43 APPENDICE 1 - NORMATIVA

73 APPENDICE 2 - VIRUS INFORMATICI

i Quaderni n. 2 ottobre 1999
Supplemento al n. 9-10/1999
di Informazioni
Periodico bimestrale
dell'Autorità
per l'informatica nella
Pubblica Amministrazione

Anno I - nuova serie
Registrato al Tribunale di Roma
n.173/99 del 14 aprile 1999

Direttore responsabile
Franco Tallarita
(tallarita@aipa.it)
Coordinamento redazionale
Giampiero Bellucci
(bellucci@aipa.it)

Quaderno a cura
del Gruppo di Lavoro
AIPA - ANASIN
ASSINFORM - ASSINTEL

Redazione
Ufficio documentazione
e pubblicazioni
Autorità per l'Informatica
nella Pubblica Amministrazione
Via Solferino, 15
00185 Roma
Tel. (39) 06 852641
Fax (39) 06 8413311
e-mail: documentazione@aipa.it

Tutti i numeri di Informazioni
sono pubblicati nel sito
internet dell'Autorità
all'indirizzo:http://www.aipa.it

Stampa: CSR, Roma

progetto grafico:
Segni di Segni, Roma

1. Premessa

In esecuzione dei protocolli d'intesa intervenuti con le Associazioni di categoria, ANASIN, ASSINFORM e ASSINTEL, l'Autorità preso atto delle proposte formulate nell'Adunanza del 14 gennaio 1999, ha deciso la costituzione di alcuni gruppi di lavoro, tra cui quello della "sicurezza informatica".

Questo documento descrive le "Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella Pubblica Amministrazione" elaborate dal Gruppo di Lavoro congiunto costituito con deliberazione del 19 marzo 1999 del Presidente dell'Autorità.

Il gruppo, che ha operato dal 14 aprile al 14 luglio 1999, è stato coordinato dal prof. Ferrante Pierantoni, componente dell'Autorità.

Le Linee guida elaborate dal Gruppo di Lavoro costituiscono l'avvio di un processo di miglioramento continuo che veda la partecipazione e la condivisione delle esperienze e delle conoscenze di chi opera nel mondo delle tecnologie dell'informazione e della comunicazione.
L'evoluzione incessante delle tecnologie dell'informazione e della comunicazione richiede dinamiche rapide e continue. La loro complessità è tale da rendere necessario un *mix* di specializzazioni sempre più elevato.

Con l'estensione delle Linee guida si è iniziato pertanto a mettere a punto un linguaggio condiviso fra esperti ad elevata specializzazione appartenenti a diverse comunità e famiglie professionali. Il processo dovrà essere continuato ed ulteriormente approfondito anche in considerazione della rapidità e della complessità dell'evoluzione tecnologica sopra indicata.

2. Introduzione

Il tema della Sicurezza dei Sistemi Informativi Automatizzati (S.I.A.) nella Pubblica Amministrazione italiana assume rilevanza strategica in vista delle evoluzioni previste, in termini di efficacia ed efficienza, dai piani di riorganizzazione dei Sistemi Informativi.

La realizzazione del "Sistema Informativo Unitario delle Amministrazioni Pubbliche", nucleo principale del programma di informatizzazione dell'amministrazione pubblica italiana, contempla da un lato la predisposizione di architetture per la condivisione del patrimonio informativo, l'interoperabilità, la cooperazione tra applicazioni, l'automazione dei processi interamministrativi e, dall'altro, garantisce l'autonomia di ogni soggetto in relazione al proprio dominio.

In vista di tali evoluzioni, incentrate sulla realizzazione della Rete Unitaria delle Pubbliche Amministrazioni (RUPA), della rete G-NET e dei diversi progetti intersettoriali, il tema della Sicurezza dei Sistemi Informativi della P.A. diventa strategico al fine di garantire l'affidabilità dei processi e dei dati elaborati sia all'interno di ogni specifico dominio, sia nell'ottica di interoperabilità e di cooperazione tra le diverse Amministrazioni, sia nell'automazione dei servizi al cittadino.

Il crescente ricorso alle tecnologie dell'informazione e della comunicazione intrapreso dalla P.A. per lo snellimento, l'ottimizzazione e una maggiore efficienza dei procedimenti amministrativi, comporta una serie di nuovi rischi che, se non adeguatamente affrontati, potrebbero comportare gravi conseguenze sull'affidabilità dei dati e dei servizi. Tali rischi sono imputabili a due fattori caratteristici della tecnologia in questione: l'inaffidabilità, cioè la non garanzia di corretto funzionamento sia nelle componenti hardware sia in quelle software, e l'esposizione alle intrusioni informatiche.

In termini più operativi è bene intendere la Sicurezza del Sistema Informativo Automatizzato non solo come "protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali" ma anche come "limitazione degli effetti causati dall'eventuale occorrenza di tali cause".

Occorre inoltre considerare che la sicurezza del Sistema Informativo Automatizzato non dipende solo da aspetti tecnici, ma anche, se non principalmente, da quelli organizzativi, sociali e legali.

La sicurezza del Sistema Informativo Automatizzato deve essere pertanto vista come caratteristica "globale", in grado di fornire, dinamicamente con l'evolversi temporale delle necessità e delle tecnologie, il desiderato livello di disponibilità, integrità e confidenzialità delle informazioni e dei servizi erogati.

Viene definito sicuro un Sistema Informativo Automatizzato che soddisfi le seguenti proprietà:

- Disponibilità: l'informazione ed i servizi che eroga devono essere a disposizione degli utenti del sistema compatibilmente con i livelli di servizio.
- Integrità: l'informazione ed i servizi erogati possono essere creati, modificati o cancellati solo dalle persone autorizzate a svolgere tale operazione.
- Autenticità: garanzia e certificazione della provenienza dei dati.

- Confidenzialità o Riservatezza: l'informazione che contiene può essere fruita solo dalle persone autorizzate a compiere tale operazione.

L'approccio globale alla sicurezza richiede di considerare gli aspetti tecnici (sicurezza fisica e logica), strategici (obiettivi e *budget*), organizzativi (definizione di ruoli, procedure, formazione), economici (analisi dei costi) ed infine legali (leggi e raccomandazioni, normative).

La progettazione di un Sistema Informativo Automatizzato sicuro richiede una buona esperienza nel settore e la valutazione di una serie di elementi solitamente ignorati durante la predisposizione di un sistema che non abbia pretese di sicurezza.

In particolare si ritiene necessario verificare preliminarmente, ogni qual volta si debba trattare di sistemi sicuri, la validità, a livello generale, dei seguenti assunti:

1. tutti i componenti, HW e SW, sono "*fail safe*", tali cioè che ogni loro malfunzionamento o messa fuori operazione non comporti una diminuzione della sicurezza di esercizio, eventualmente anche attraverso una messa fuori uso della particolare stazione interessata;
2. le responsabilità dell'esercizio e dei controlli interni di sicurezza sono affidate a persone distinte e collocate nella struttura organizzativa in modo tale che in alcun modo il responsabile dell'esercizio possa influire sulla carriera/retribuzione del responsabile dei controlli interni di sicurezza;
3. sono adeguate le procedure per l'accertamento della qualità delle verifiche effettuate dal responsabile dei controlli interni di sicurezza sull'operato del *team* di gestione;
4. è sempre possibile individuare, inequivocabilmente, in un apposito "*activity log file*", l'autore di una qualsiasi operazione;
5. è garantita, al di là di ogni dubbio, l'integrità di questo *log file* e la sua disponibilità nel tempo per il periodo concordato;
6. è sempre possibile ripristinare il sistema di fronte a guasti od eventi, naturali o dolosi, allo stato in cui si trovava, prima del verificarsi dell'evento stesso, in un certo tempo concordato a priori tra le parti;
7. è garantita l'integrità del SW, ad ogni livello, dal sistema operativo alle applicazioni, e dei relativi *file* di configurazione;
8. è convincente il programma dei test di penetrazione, sia interna che esterna, effettuati periodicamente, secondo la frequenza concordata;
9. sono adeguate le procedure per l'effettuazione delle varie operazioni di manutenzione e per il trattamento dei supporti di memorizzazione di massa obsoleti;
10. è convincente il programma di accertamento della qualità dei controlli sull'aggiornamento continuo del HW e del SW, del controllo della completa sincronizzazione delle versioni, aggiornate tempestivamente, dello stesso SW, all'aggiornamento delle varie "*patches*" distribuite dai fornitori per chiudere i vari "buchi", man mano che vengono scoperti.

Va inoltre ricordato che una serie di leggi emanate in questi ultimi anni obbliga i fornitori e gli utenti di servizi informatizzati al rispetto di alcune regole e alla messa in opera di una serie di contromisure atte a prevenire o minimizzare i rischi di un incidente informatico. L'adozione di tali contromisure non è più lasciata alla discrezione delle singole Amministrazioni, ma, in alcuni casi, è un obbligo di legge.

3. Obiettivi del presente documento

La sicurezza dei Sistemi Informativi Automatizzati[1] è un requisito fondamentale per il corretto sviluppo dei programmi di automazione della P.A. ed è necessario che tutte le P.A. realizzino le migliori condizioni di sicurezza, al fine di garantire l'affidabilità delle informazioni trattate e l'efficacia ed efficienza dei servizi erogati.

A tale scopo, nell'ambito del contesto normativo esistente, vengono fornite indicazioni su come affrontare le problematiche della Sicurezza dei Sistemi Informativi Automatizzati e su come realizzare e gestire adeguate misure di protezione.

In particolare, le presenti Linee Guida in materia di sicurezza dei Sistemi Informativi Automatizzati hanno l'obiettivo di:
a) incrementare la consapevolezza di rischi e insidie che possono coinvolgere la gestione e l'utilizzo dei sistemi informativi automatizzati;
b) indicare possibili percorsi tecnici ed organizzativi di salvaguardia per prevenire situazioni di pericolo per le risorse e per chi se ne avvale, nonché per affrontare e risolvere eventuali problemi insorgenti al verificarsi di eventi lesivi del patrimonio informativo;
c) supportare la creazione, nell'ambito delle Amministrazioni Pubbliche, di strutture in grado di disegnare, pianificare, implementare e gestire misure di protezione corrispondenti alle esigenze degli specifici contesti di competenza;
d) incrementare l'utilizzo delle risorse informative disponibili su supporto informatico ed accessibili per via telematica con le imprescindibili garanzie di sicurezza;
e) chiarire dal punto di vista normativo gli obblighi delle Amministrazioni in merito all'adozione di misure di sicurezza.
Le soluzioni di sicurezza adottate e da adottare a tutela dei sistemi informativi automatizzati hanno l'obiettivo di:
a) assicurare la protezione degli interessi dei soggetti, pubblici e privati, che fanno affidamento sui sistemi informativi della Pubblica Amministrazione;
b) evitare eventi pregiudizievoli che possano danneggiare disponibilità, riservatezza e integrità del patrimonio informativo disponibile su sistemi di elaborazione e tramite reti di connessione telematica.

1 Nel presente documento si intende per Sistema Informativo Automatizzato il sistema costituito dai dati, dalle applicazioni, dalle risorse tecnologiche, dalle risorse umane, dalle regole organizzative e dalle procedure deputate alla acquisizione, memorizzazione, elaborazione, scambio, ritrovamento e trasmissione delle informazioni.

4. Contesto normativo di riferimento[2]

La legislazione italiana relativa alla sicurezza informatica poggia su tre leggi fondamentali, che, nell'ambito di queste linee guida, possono costituire la griglia di riferimento normativo:

• D. Lgs. 29 dicembre 1992, n. 518, che modifica la legge n. 633 del 1941, relativa al diritto d'autore, integrandola con norme relative alla tutela giuridica dei programmi per elaboratore.
• Legge 23 dicembre 1993, n. 547, che modifica il codice penale italiano introducendo i cosiddetti "*computers crimes*".
• Legge 31 dicembre 1996, n. 675, che disciplina il trattamento dei dati personali.
È da considerare lo sforzo del legislatore nel prendere in considerazione tutti gli aspetti inerenti alla sicurezza informatica, definendo e cercando di tutelare i beni informatici e telematici.

Lo sviluppo dei sistemi informatici e informativi nella P.A. espone le amministrazioni, i suoi utenti e i propri responsabili a rischi di coinvolgimento sia penale che patrimoniale. Occorre, pertanto, adeguare le rispettive politiche di sicurezza cercando di limitare tali rischi, predisponendo, in ossequio alle norme vigenti, adeguate contromisure di carattere tecnico, organizzativo e normativo. Nella predisposizione delle politiche di sicurezza occorre anche tenere presente la normativa in materia di semplificazione e trasparenza delle procedure d'accesso ai dati delle P.A. così come articolate nelle leggi:

• Legge 7 agosto 1990, n. 241 – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
• Legge 15 marzo 1997, n. 59 – Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa;
• Legge 15 maggio 1997, n. 127 – Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e controllo;
• Legge 16 giugno 1998, n. 191 – Modifiche ed integrazioni alle leggi: n. 59 del 15/3/1997 e n. 127 del 15/5/1997, nonché norme in materia di formazione del personale dipendente e di lavoro a distanza nelle pubbliche amministrazioni.

In Appendice 1 è raccolta una sintesi delle principali normative in materia di sicurezza dei Sistemi Informativi Automatizzati.

2 Successivamente alla conclusione dei lavori del Gruppo, è stato emanato il D.P.R. 28 luglio 1999 n. 318, "Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675".

5. Il Processo della Sicurezza del Sistema Informativo Automatizzato

Il tema della Sicurezza del Sistema Informativo Automatizzato richiede, al fine della realizzazione di un sistema di sicurezza efficace ed efficiente, l'indirizzamento progettuale di un Piano Aziendale della Sicurezza, che consenta di disegnare, pianificare, implementare e gestire le opportune contromisure di natura fisica, logica ed organizzativa.

L'articolazione progettuale del Piano di Sicurezza secondo l'approccio globale prevede l'esecuzione delle seguenti attività:

- Analisi del Rischio
- Definizione delle Politiche di Sicurezza
- Gestione del Rischio
- Il Piano Operativo
- Audit
- Formazione
- Organizzazione

L'esecuzione di tali attività consente, da un lato, di realizzare il sistema di sicurezza del Sistema Informativo Automatizzato e, dall'altro, di avviare un processo di gestione del sistema stesso caratterizzato dalla ciclicità necessaria per il controllo ed il mantenimento dei livelli di sicurezza nel tempo.
Nel seguito del documento verranno illustrate le principali attività per indirizzare la realizzazione e la gestione della Sicurezza del Sistema Informativo Automatizzato.

6. Analisi dei rischi

Questo modulo costituisce la fase di partenza delle attività di progettazione del piano aziendale della sicurezza.
Le attività raggruppate al suo interno sono da considerarsi momenti diversi di una medesima macro-fase di progettazione, e contribuiscono alla definizione di quello che nella terminologia *Information Technology Security Evaluation Criteria* (ITSEC) è definito essere il *Security Target*.
L'esecuzione di tale modulo consente di:

- acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo;
- avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.

Le attività di tale modulo progettuale prevedono tipicamente l'esecuzione di:

6.1 Identificazione dei beni da proteggere

Il primo passo da compiere nella definizione di un piano di sicurezza è l'individuazione degli elementi del sistema informativo automatizzato che necessitano protezione e delle minacce a cui gli stessi possono essere sottoposti. Nello svolgimento di tale fase devono essere presi in considerazione tutti gli aspetti possibili senza trascurare il benché minimo dettaglio; ossia bisogna tenere sotto controllo ogni fattore, sia tecnologico che umano.
Anche se alcune cose sembrano ovvie, è opportuno procedere ad una elencazione di tutte le possibili componenti che hanno un impatto con il problema sicurezza. Occorre analizzare, inoltre, anche le relazioni che le singole componenti hanno fra loro e, più in generale, con il resto dell'ambiente.
Occorre, cioè, rappresentare e classificare non solo le componenti, ma anche come queste sono relazionate tra di loro, sia fisicamente che logicamente, definendo un disegno completo del Sistema Informatico.
Si tratta di specificare quale è il patrimonio informativo in termini di dati e risorse elaborative che sarà oggetto del Piano della Sicurezza.
Viene di seguito proposta, in linea con la RFC 2196, una possibile classificazione dei beni che costituiscono il Patrimonio Informativo da proteggere.

6.1.1 Risorse Hardware

Rientrano in questa categoria: CPU, terminali, *workstation*, personal computer, stampanti, *disk drive*, linee di comunicazione, *server*, *router*. Le principali minacce a cui questi dispositivi sono sottoposti sono: mal funzionamenti dovuti a guasti o sabotaggi, mal funzionamenti dovuti a eventi naturali, quali allagamenti e incendi, furti e intercettazione.
Quest'ultima minaccia interessa gli apparati di rete, cioè le linee di comunicazione, i *router* e i *server*. È infatti possibile per eseguire il

monitoraggio indebito o l'alterazione della trasmissione di dati effettuata da questi apparati, sia che questa avvenga tra terminali, tra computer, tra stazioni di lavoro periferiche e sistemi centrali di elaborazione. Un altro caso può riguardare i video, intercettando le onde elettromagnetiche da questi emesse per ricostruirne remotamente l'immagine.

6.1.2 Risorse Software

Rientrano in questa categoria i Sistemi Operativi e Software di Base (*utilities*, diagnostici), Software Applicativi, Gestori di basi di dati, Software di rete, programmi in formato sorgente e oggetto, ecc. Le minacce principali legate all'uso di questi prodotti sono:

- la presenza di errori involontari commessi in fase di progettazione e/o implementazione che consentono ad utenti non autorizzati l'esecuzione di operazioni e programmi riservati a particolari categorie di utenti;
- la presenza di codice malizioso inserito volontariamente dai programmatori dell'applicazione stessa, al fine di poter svolgere operazioni non autorizzate sul sistema o per danneggiare lo stesso. Rientrano in questa categoria di minacce i virus, i *trojan horse*, le bombe logiche, le *backdoor*;
- attacchi di tipo *denial of service* vengono generalmente portati a servizi di rete, ma sono facilmente estendibili a un qualunque servizio. Si tratta di attacchi non distruttivi, il cui obiettivo è saturare la capacità di risposta di un servizio con l'obiettivo ultimo di renderlo inutilizzabile agli altri utenti del sistema.

Particolare importanza ricoprono anche i formati sorgente delle applicazioni, che possono essere oggetto di furto per un'eventuale rivendita ad altre organizzazioni o di modifica per l'inserimento di codice malizioso.

6.1.3 Dati

Intendiamo con ciò il contenuto degli archivi, delle Basi di dati, dati di transito, copie storiche, *file* di *log*, ecc.

Le minacce a cui i dati sono sottoposti sono legate alle debolezze dei sistemi operativi e delle applicazioni che operano sulle macchine su cui risiedono e sono riconducibili a due categorie:

- accesso non autorizzato, cioè la possibilità per utenti esterni o interni di visualizzare informazioni riservate a particolari categorie di utenti;
- modifiche deliberate o accidentali, cioè la possibilità per utenti non autorizzati di modificare o cancellare dati a loro "non appartenenti", oppure errori commessi da utenti autorizzati che inavvertitamente procedono alla modifica o cancellazione di informazioni significative.

6.1.4 Le Risorse Professionali

Intendiamo appartenenti a questa categoria gli amministratori di sistemi, i sistemisti, i programmatori, gli operatori, gli utenti finali, i manutentori hardware e software, i consulenti ecc. È questa una categoria alquanto particolare in quanto può essere oggetto di minacce che compromettono la sicurezza del sistema, ma può a sua volta costituire una minaccia per la sicurezza del sistema.

Nel primo caso il personale può essere oggetto di attacchi così detti di *social engineering* in cui estranei cercano attraverso varie strategie di ottenere informazioni utili ad attaccare il sistema quali le password degli utenti, il contenuto dei *file* di configurazione, gli indirizzi IP delle macchine e così via.

Il personale, per contro, diventa una minaccia quando matura motivi di rivalsa nei confronti dell'amministrazione e quando ha una scarsa consapevolezza del problema sicurezza.

6.1.5 Documentazioni Cartacee

Si intende appartenente a questa categoria la documentazione relativa ai programmi, all'hardware, ai sistemi, alle procedure di gestione, ecc.

Le principali minacce a cui tali elementi sono sottoposti sono la distruzione e/o l'alterazione ad opera di eventi naturali, di azioni accidentali e di comportamenti intenzionali.

6.1.6 Supporti di memorizzazione

Si tratta dei supporti su cui vengono tenute le copie dei sw installati, le copie dei *file* di *log* e dei *back-up*.

Le principali minacce a tali dispositivi, oltre a quelle già menzionate per i dispositivi cartacei, sono:

- il deterioramento nel tempo;
- l'inaffidabilità del mezzo fisico che in alcuni casi può presentare difetti di costruzione che ne compromettono il buon funzionamento nel tempo;
- l'evoluzione tecnologica e del mercato.

6.2 Classificazione dei beni e loro valutazione

Ai fini della Sicurezza è fondamentale procedere alla classificazione dei beni in funzione degli elementi di integrità, riservatezza e disponibilità.

Tale classificazione consentirà quindi di attribuire ai diversi beni un valore in funzione di una serie di scenari di impatto significativi ai fini della sicurezza.

La valutazione dei beni è indispensabile per capire la strategicità degli stessi all'interno del Sistema Informativo e per poter quindi successivamente valutare il livello di esposizione al rischio.

Sono disponibili diverse metodologie di valutazione dei beni, alcune basate su principi quantitativi (costo di ripristino, costo per elaborazione tramite risorse alternative,...), altre basate su principi qualitativi (perdita di immagine, violazione di assetti legislativi, perdita di efficacia/efficienza nell'operatività,...).

È opportuno che la metodologia prescelta consenta di valutare tutti i possibili scenari di impatto che caratterizzano il patrimonio informativo dell'amministrazione, e quindi, di effettuare valutazioni che tengano in considerazione sia gli impatti quantitativi che quelli qualitativi.

Nel caso dei Sistemi della PA il criterio puramente economico dovrà essere bilanciato da altre valutazioni più pertinenti al ruolo della PA stessa.

I criteri per la valorizzazione in linea di massima dovranno tener conto, pertanto, in ordine decrescente, di parametri quali:

- rischio per la sicurezza dello Stato e\o dei cittadini;
- interruzione di pubblico servizio;
- alterazione di pubblico servizio;
- sottrazione ed alienazione di patrimonio pubblico;
- danneggiamento di patrimonio pubblico.

6.3 Valutazione delle Minacce e delle Vulnerabilità dei beni

L'individuazione delle minacce e delle vulnerabilità cui sono esposti i beni del patrimonio informativo è fondamentale per valutare successivamente l'esposizione al rischio.

La valutazione delle minacce e delle vulnerabilità prende in considerazione molte tipologie di potenziali problemi, ognuna delle quali può interessare differenti parti del sistema.

Le categorie delle minacce possono essere raggruppate nelle seguenti aree:

- penetrazione logica;
- penetrazione nelle reti di comunicazione;
- guasti tecnici delle apparecchiature;
- errori umani;
- minacce fisiche.

Vulnerabilità e minacce dovrebbero essere classificate in termini qualitativi e poi correlate ai beni per individuare gli impatti e determinare quindi la misura del rischio in relazione ai diversi servizi informativi.

6.4 Individuazione dell'esposizione al Rischio

La misura del rischio cui è esposto il sistema informativo automatizzato viene determinata dalla combinazione dei seguenti elementi:

- il valore dei beni (dati e risorse elaborative)
- il livello delle minacce ai suddetti beni
- il livello di vulnerabilità dei suddetti beni.

Tipicamente la misura del rischio viene formalizzata attraverso una matrice di correlazione che consente di evidenziare, per ogni minaccia considerata, le criticità relative ai singoli beni ed al servizio informativo nel suo complesso, in funzione degli impatti relativi agli elementi di integrità, riservatezza e disponibilità considerati. L'analisi di tale matrice consente di evidenziare l'entità del rischio associata ai diversi beni e di capire quali sono i principali problemi, in termini di minacce e vulnerabilità, che minano la sicurezza del sistema informativo automatizzato dell'Amministrazione.

6.5 Individuazione dell'insieme delle contromisure da realizzare per innalzare il livello di Sicurezza dei Sistemi Informativi Automatizzati

L'Analisi dei Rischi si conclude tipicamente con l'individuazione di un insieme di possibili contromisure, di natura fisica, logica ed organizzativa, che potrebbero essere adottate al fine di abbattere l'entità del rischio precedentemente individuata.

Dopo la definizione dei livelli di criticità è quindi possibile definire, per ciascuna componente del sistema informativo automatizzato e per ciascuna delle minacce a cui è sottoposto, il livello di rischio che si potrebbe ritenere accettabile.

Anche in questo caso una matrice delle contromisure da attuare dovrebbe contenere almeno le seguenti categorie per singola minaccia:

- vulnerabilità;
- danno potenziale;
- probabilità dell'evento;
- rischio per l'Amministrazione;
- costo di ripristino;
- priorità nell'implementazione dei meccanismi di sicurezza;
- contromisure urgenti, ordinarie, future.

Questo insieme di contromisure, in questa fase del progetto, ha una valenza sostanzialmente indicativa, in quanto la scelta dello specifico *mix* di contromisure da adottare è subordinata all'indirizzamento delle successive fasi di progetto:

- individuazione degli obiettivi di Sicurezza (Politiche di Sicurezza);
- strategia di Gestione del Rischio, ovvero valutazione del rischio da abbattere e del rischio residuo ritenuto accettabile.

7. Definizione delle Politiche di Sicurezza

Un aspetto fondamentale della realizzazione di un Piano per la sicurezza è la definizione delle politiche di sicurezza che l'Amministrazione intende adottare.
Tali Linee dovranno essere coerenti con le normative vigenti in tema di sicurezza, con le politiche di sicurezza informatica definite a livello di Governo e, in particolare, con gli indirizzi espressi in materia dall'AIPA.
Attraverso lo sviluppo di questa fase progettuale si definiscono gli obiettivi di Sicurezza del Sistema Informativo, in linea con la missione istituzionale dell'Amministrazione e soprattutto in linea con gli obiettivi legati ai livelli di servizio.
Inoltre dovrà essere posta adeguata attenzione, al fine del contenimento dei costi, a definire misure di sicurezza coerenti con il "valore" del patrimonio informativo da proteggere.
Di fatto l'individuazione della politica di sicurezza aziendale determina il modello logico della sicurezza dell'Amministrazione fissandone gli obiettivi. L'individuazione degli obiettivi aziendali di Sicurezza si tradurrà in obiettivi di Sicurezza del Sistema Informativo, sostanziandosi con la formalizzazione di norme organizzative e standard di riferimento.

La definizione delle Politiche di Sicurezza aziendale verrà condotta ai fini dell'individuazione di criteri generali basati sulla nozione di rischio e indipendenti dalla tecnologia correntemente in uso. È fondamentale che i responsabili dell'Amministrazione prendano atto dei rischi individuati nella fase precedente (cap. 5, Analisi dei Rischi) e definiscano un'adeguata risposta in termini di politiche e relativi livelli di spesa.

La sicurezza deve essere considerata, inoltre, da tutti i dipendenti, una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione.
Un sistema di sicurezza, per poter raggiungere i migliori risultati funzionali, va visto globalmente, negli aspetti fisici, logici e organizzativi, come un insieme di misure e strumenti hardware, software, organizzativi e procedurali integrati fra loro, volti a ridurre la probabilità di danni a un livello accettabilmente basso e ad un costo ragionevole.

Le Politiche di Sicurezza si basano sul principio che le risorse informatiche (dati, risorse hardware, software, ecc.) sono un patrimonio che deve essere protetto dal momento in cui viene creato/installato, durante il suo utilizzo, fino al momento in cui viene distrutto.
Sono approvate e emanate dai vertici dell'Amministrazione e si applicano a tutti i dipendenti.
Inoltre, dovrebbero essere portate a conoscenza (per le parti di pertinenza) delle società

esterne (es. *software house*, consulenti, ecc.) che interagiscono con l'Amministrazione, le quali dovrebbero accettarne i contenuti ed impegnarsi a rispettarle.
Le Politiche di Sicurezza devono essere periodicamente aggiornate per riflettere eventuali nuovi indirizzi e/o evoluzioni e normative in materia di sicurezza.
Le Politiche di Sicurezza dovrebbero almeno indirizzare i seguenti aspetti:

• Classificazione delle informazioni: le informazioni, in qualsiasi forma esse si presentino (posta elettronica, archivi informatici, programmi, ecc.), devono essere protette con normative e misure tecniche commisurate sia alla importanza che esse rappresentano per l'Amministrazione (riservatezza, criticità, ecc.), sia a specifici requisiti. Le Politiche dovrebbero stabilire i criteri generali secondo i quali le informazioni dovrebbero essere classificate (es: informazioni riservate o informazioni vitali per l'attività dell'Amministrazione, informazioni ad uso interno, dati personali o altri dati critici, informazioni non classificate).

• Protezione fisica delle risorse: l'obiettivo è la definizione di misure di sicurezza per la predisposizione e il mantenimento di un ambiente di lavoro protetto che impedisca perdite di informazioni e di patrimonio intellettuale di proprietà, promuova la protezione delle risorse informatiche presenti e la riduzione dei rischi di interruzione dei servizi informatici.
Tale obiettivo viene raggiunto attraverso misure di controllo crescenti, correlate ai rischi e al valore dei beni e delle informazioni presenti nell'ambiente. Ne fanno parte le seguenti componenti:
– la classificazione delle aree aziendali (es: aree riservate, aree interne, aree pubbliche);
– l'accesso controllato alle aree considerate critiche;
– la sicurezza fisica (impianti) e la sorveglianza di queste aree;
– la tempestiva rilevazione di eventuali incidenti di sicurezza.

• Protezione logica delle informazioni: anche le misure di sicurezza logica dovranno essere commisurate al livello di classificazione delle informazioni. Ne fanno parte i seguenti aspetti:
– il controllo degli accessi alle informazioni;
– il mantenimento della loro integrità e riservatezza;
– la sicurezza nella trasmissione e nelle comunicazioni all'interno dell'Amministrazione e con l'esterno Internet, altre Amministrazioni, ecc.);
– la sicurezza delle stazioni di lavoro e dei personal computer;
– la sicurezza nel processo di sviluppo delle applicazioni informatiche;
– la sicurezza nella gestione operativa delle installazioni informatiche;
– la tempestiva rilevazione di eventuali incidenti di sicurezza.

• Norme per il Personale: tutti i dipendenti concorrono alla realizzazione della Sicurezza; pertanto, dovranno proteggere le informazioni assegnate loro per lo svolgimento dell'attività lavorativa nel rispetto di quanto stabilito dalle Politiche almeno in termini di:
– utilizzo delle risorse informatiche;
– accesso ai sistemi e ai dati;
– uso della *password*.

• Piano di Continuità Operativa: l'obiettivo è quello di garantire la continuità del servizio informatico e la disponibilità delle informa-

zioni (aggiornate), evitando o limitando i danni al patrimonio informativo a fronte di una emergenza. A tale scopo dovrà essere previsto da ogni Amministrazione un Piano di Ripristino delle informazioni e delle operazioni che contenga gli aspetti organizzativi e normativi, le modalità e le risorse di *backup* necessarie (centro di calcolo, risorse hardware, software, personale, ecc.) alla ripresa delle attività a seguito di una emergenza che impedisca la normale erogazione del servizio informatico.

• Gestione degli incidenti: i rischi informatici devono essere sempre costantemente controllati e monitoritati. Devono essere definite le responsabilità e le modalità con cui gestire eventuali incidenti di sicurezza.

• Sviluppo e manutenzione dei sistemi hardware e software utilizzati nel realizzare il piano di Sicurezza: occorre regolare le procedure con cui il software dovrà essere aggiornato e/o modificato e gli apparati sostituiti o riparati.

• Gestione e formalizzazione delle procedure di raccolta e analisi delle transazioni e/o trasmissioni effettuate utilizzando il Sistema Informativo Automatizzato, nel caso in cui la normativa vigente preveda la possibilità di dispute legali che abbiano come oggetto di contesa queste operazioni.

L'applicazione delle Politiche di Sicurezza all'interno dell'Amministrazione richiede la definizione di un insieme di regole che fanno riferimento alle tecnologie usate, alle metodologie, alle procedure di implementazione e ad altri elementi specifici dell'ambiente e sistema informativo. È richiesto il rispetto degli Standard da parte delle funzioni interessate.

In linea generale le regole dovrebbero indirizzare:
• identificazione e autenticazione degli utenti;
• *userid* (*naming convention*, assegnazione, ecc.);
• *password* (regole di assegnazione, lunghezza, sintassi, scadenza, ecc.) o altri strumenti di autenticazione (es. *smart card*);
• definizione e protezione delle risorse;
• protezione e personalizzazione del software di base;
• classificazione, protezione e accessi alle risorse utente;
• crittografia (algoritmi, distribuzione, ecc.);
• registrazione, conservazione e consultazione dei *log*;
• individuazione di tentativi di intrusione;
• autorità di System e Security Administration;
• ecc.

L'applicazione delle Politiche di Sicurezza all'interno dell'Amministrazione richiede, inoltre, la definizione di Processi che descrivano gli specifici passi operativi che le persone devono seguire per raggiungere gli obiettivi che sono stati stabiliti dalle Politiche.
I Processi sono indispensabili per la gestione di tutti gli oggetti legati alla sicurezza, quali le utenze, le password, le chiavi di crittografia, i certificati digitali, i *log*, gli allarmi, ecc.

Alcuni dei principali processi gestionali riguardano:
• definizione e cancellazione di *userid*;
• assegnazione di privilegi;
• assegnazione delle password;
• autorizzazioni di accesso ai dati/transazioni;
• gestione chiavi di crittografia;
• richiesta/gestione/rinnovo certificati digitali;
• analisi e gestione dei *log.*

8. Gestione del Rischio

L'attività di Gestione del Rischio ha il compito di definire gli obiettivi di Sicurezza del Sistema Informativo Automatizzato in termini di:

- rischio da abbattere;
- rischio residuo ritenuto accettabile.

Tale definizione dovrebbe essere operata ai massimi livelli dell'Amministrazione poiché è una scelta che necessita la ponderazione di molteplici elementi:

- obiettivi di missione istituzionale;
- garanzie dei livelli di servizio;
- conformità agli assetti legislativi e normativi;
- eventuali vincoli di natura contrattuale;
- piani di evoluzione del Sistema Informativo;
- vincoli tecnologici;
- disponibilità economica.

La sicurezza deve essere quindi vista in termini relativi come il "giusto" compromesso tra i "costi della sicurezza" ed i "costi della non sicurezza", frutto della ponderazione degli elementi precedentemente indicati.

Una volta definito il livello di Sicurezza da raggiungere, e quindi il rischio residuo ritenuto accettabile, è possibile procedere all'individuazione della strategia di gestione del rischio (*Risk Management*).

Tale strategia dovrà contemplare le opportune indicazioni in relazione alle ipotesi di:

- trasferimento del rischio;
- abbattimento del rischio.

Per trasferimento del rischio si intende generalmente la sottoscrizione di polizze assicurative che possono coprire alcuni rischi generalmente legati alla distruzione fisica di sistemi. Tali polizze garantiscono una copertura finanziaria per i danni fisici ed i costi di riacquisto dei sistemi, ma non rappresentano certamente una copertura rispetto ai rischi di perdita di integrità, riservatezza e disponibilità del patrimonio informativo nel suo complesso.

Per abbattimento del rischio si intende l'adozione di un insieme di contromisure di natura fisica, logica ed organizzativa che possono fornire protezione in differenti maniere:

- ridurre la minaccia;
- ridurre la vulnerabilità;
- ridurre l'impatto di eventi accidentali;
- rilevare un evento accidentale;
- aiutare nel *recovery* di un evento accidentale.

Nella strategia di abbattimento del rischio è fondamentale la valutazione del rapporto costi/benefici.

Riportiamo, a titolo esemplificativo, alcuni degli elementi che vengono utilizzati per determinare se il costo dei meccanismi di protezione bilancia il valore del bene a rischio:

- Il reddito netto del bene/processo da proteggere indica il reddito generato dall'utilizzo del bene/processo da proteggere. Qualora tale dato non sia facilmente ottenibile, come nel caso di un servizio pubblico di rilascio certificati, altri parametri possono essere adottati, quali il numero di utenti che usano il bene/processo in questione moltiplicato per un fattore

che indichi qual è il ricavo che l'utente ottiene dall'uso del suddetto bene/processo.

• La perdita annuale attesa dovuta alla perdita del bene/processo da proteggere indica una stima del danno creato nel momento in cui si attuano le minacce a cui lo stesso è sottoposto. Nel computo di tale stima vanno conteggiati il danno all'immagine, violazioni normative esistenti, mancato profitto, ecc.

• Le soluzioni di sicurezza disponibili devono essere valutate in relazione a una serie di parametri: il costo di sviluppo, il costo di implementazione complessivo, il costo di manutenzione e di supporto annuale, il contributo dell'utente all'implementazione dell'opzione di sicurezza (il contributo iniziale, il canone annuale, il numero di utenti paganti), le minacce coperte dalla singola soluzione. Queste informazioni sono utili per valutare il costo totale della soluzione, che può essere suddiviso in totale iniziale e totale di manutenzione annuale. In generale si considera il costo totale su cinque anni, che è il periodo di ammortamento in genere considerato per questo tipo di soluzioni.

• L'efficacia delle soluzioni identificate valuta la copertura delle soluzioni rispetto alle minacce. L'utente definisce la percentuale di efficacia della soluzione nell'eliminazione della minaccia (0% indica che l'opzione non elimina la minaccia, 100% indica che l'opzione elimina totalmente la minaccia) e quindi se ne valuta la media per singola soluzione.

• L'impatto che la misura di sicurezza ha sugli utenti del servizio per cui viene approntata. Per stimare il livello di accettazione della soluzione da parte degli utenti finali vanno considerati una serie di parametri quali: come la soluzione impatta sul modo di operare dell'utente, il numero di utenti coinvolti, quali inconvenienti potrebbe causare (ritardi, difficoltà, ecc.), eventuali incrementi nei costi del servizio.

• Il livello di accettazione della misura di sicurezza da parte dei propri dipendenti. Gli indicatori che possono essere considerati per valutare questo fattore sono: il numero di dipendenti coinvolti, gli inconvenienti che tale soluzione potrebbe causare al loro modo usuale di operare (ritardi, difficoltà, ecc.), il grado di preparazione e il tempo a disposizione dei dipendenti per implementare efficacemente questa soluzione.

• La facilità di implementazione della misura di sicurezza. Gli indicatori utilizzati per esprimere tale valore sono in genere: il tempo necessario per implementare la soluzione, eventuali alterazioni che la stessa apporterà al processo, la disponibilità di risorse per implementare la soluzione efficacemente e l'approvazione della direzione riguardo l'importanza della stessa.

Tutti i parametri di cui sopra devono inoltre essere raggruppati in un quadro di valutazione globale che, combinato con il *budget* di spesa previsto e il livello di rischio predeterminato, consentirà di scegliere la soluzione di sicurezza più appropriata.

Comunque, la decisione finale se una contromisura debba essere implementata o meno, resta una decisione della direzione. Può essere accettabile per la direzione stabilire che una particolare contromisura non debba essere implementata, con la conseguente accettazione implicita del livello di rischio, ma la decisione dovrebbe essere documentata e spiegata.

L'individuazione della specifica strategia di abbattimento del rischio costituirà l'*input* per consentire lo sviluppo del piano operativo di implementazione delle contromisure.

9. Il Piano Operativo

Definite quali sono le risorse da proteggere, le strategie di abbattimento del rischio ed il livello di rischio ritenuto accettabile, si procede con la stesura del piano operativo.

Questo passo operativo consente di determinare, tra l'insieme delle contromisure (funzioni di sicurezza) di natura fisica, logica ed organizzativa individuate, quali siano le più idonee, verificarne la fattibilità, stabilirne le priorità di attuazione valorizzandone le mutue interdipendenze per una copertura dei rischi sulla base degli obiettivi posti dalle Politiche.

L'*output* sarà costituito da un piano operativo la cui esecuzione sarà regolata dalle priorità espresse dall'Amministrazione e dai tempi relativi all'evoluzione complessiva del S.I.

Il piano conterrà:

• l'individuazione dell'insieme delle attività di sviluppo della sicurezza;
• il Piano Generale di attuazione;
• le sinergie tra i diversi interventi;
• le possibili alternative di realizzazione;
• l'indicazione di tempi, risorse (materiali ed economiche) e competenze.

Le attività di sviluppo sono generalmente raggruppabili all'interno delle seguenti aree:

– Sicurezza Fisica
– Sicurezza Logica
– Sicurezza Organizzativa
– Piano di Continuità Operativa

Vengono di seguito riportate, per ogni area di intervento, le principali contromisure attuabili.

Si sottolinea che gli aspetti della Sicurezza Organizzativa sono essenziali sia per la Sicurezza Fisica che per la Sicurezza Logica e verranno approfonditi al punto 9.3 seguente.

9.1 Sicurezza Fisica

Il ruolo della sicurezza fisica è quello di proteggere le persone che operano sui sistemi, le aree e le componenti del Sistema Informativo. I requisiti di sicurezza fisica possono variare considerevolmente in funzione delle dimensioni e dell'organizzazione del Sistema Informativo. Generalmente le contromisure di sicurezza fisica possono essere ricondotte alle seguenti:

Sicurezza di area

La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi IT. Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza delle *computer room* rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

Sicurezza delle apparecchiature hardware

La sicurezza delle apparecchiature è riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali e dall'altro alla sicurezza degli impianti di alimentazione e di condizionamento. Anche la manutenzio-

ne dell'hardware rientra in questa area, come pure la protezione da manomissione o furti.

9.2 Sicurezza Logica

La sicurezza logica è una componente particolarmente critica della Sicurezza del Sistema Informativo.

Il campo di applicazione della Sicurezza Logica riguarda principalmente la protezione dell'informazione, e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.

Le contromisure di Sicurezza Logica sono quindi da intendersi come l'insieme di misure di sicurezza di carattere tecnologico (*Information and Communication Technology*) e di natura procedurale ed organizzativa (vedi punto 9.3) che concorrono nella realizzazione del livello di sicurezza da raggiungere.

A causa della eterogeneità dei sistemi, delle reti e delle applicazioni che caratterizzano l'architettura dei Sistemi Informativi della PA, la realizzazione della Sicurezza Logica deve essere pensata in termini architetturali in funzione della realizzazione di uno specifico Sistema di Sicurezza Logica [3].

La realizzazione di tale architettura di sicurezza dovrà essere basata sull'individuazione di:

– Servizi di Sicurezza: sono le funzioni di sicurezza che il sistema dovrà garantire su tutte le piattaforme ed a tutti i livelli di elaborazione. ISO individua i seguenti servizi di sicurezza:

- Autenticazione
- Controllo Accessi
- Confidenzialità
- Integrità
- Non Ripudio

– Meccanismi di Sicurezza: rappresentano le modalità tecniche attraverso le quali è possibile realizzare i servizi di sicurezza. ISO individua i seguenti meccanismi di sicurezza:

- Cifratura
- Firma Digitale
- Meccanismi per il controllo degli accessi
- Integrità dei dati
- Meccanismi per l'autenticazione
- *Traffic Padding* ovvero saturazione del traffico in rete
- Controllo Instradamento
- Notarizzazione

La definizione dell'architettura di sicurezza logica deve rispondere ai seguenti punti:

- Quali funzioni di sicurezza devono essere garantite e per quali beni ?
- Con quali meccanismi di sicurezza è conveniente realizzare tali funzioni ?
- In quali livelli dell'architettura del sistema informatico devono essere collocati i diversi meccanismi ?

L'individuazione delle funzioni di sicurezza da garantire si evince dalla precedente attività di analisi dei rischi, politiche di sicurezza e gestione del rischio.

L'individuazione dei meccanismi di sicurezza da utilizzare e la loro collocazione ai diversi livelli dell'architettura del sistema informatico è invece oggetto di una importante attività di progettazione. Tale attività richiede notevole esperienza tecnica e progettuale ed è opportuno che sia condotta da personale esperto e qualificato. Sostanzialmente si tratta di effettuare:

- Analisi dei meccanismi attualmente in uso, verifica della loro congruenza con gli obiettivi di sicurezza, valutazione della loro efficacia ed efficienza;
- Valutazione della allocazione di tali meccanismi all'interno dell'architettura in relazione ai beni da proteggere;

3 Per Sistema di Sicurezza Logica si intende il sottosistema di sicurezza finalizzato alla implementazione dei requisiti di sicurezza nelle architetture informatiche, dotato quindi di meccanismi opportuni e di specifiche funzioni di gestione e controllo.

• Analisi e verifica dell'utilizzo degli attuali meccanismi di sicurezza e della loro manutenzione;
• Valutazione dell'introduzione di nuovi meccanismi in funzione di nuovi beni da proteggere e nuovi servizi di sicurezza da realizzare;
• Integrabilità dei nuovi meccanismi con quelli attualmente in uso;
• Garanzia del mantenimento del livello di sicurezza;
• Efficacia ed efficienza dell'architettura di sicurezza nel suo complesso;
• Scalabilità, gestibilità e controllo dell'architettura di sicurezza nel suo complesso;
• Alternative in relazione alle diverse architetture elaborative presenti nel S.I.A.;
• Procedure di implementazione, gestione e controllo;
• Accettabilità della soluzione da parte dell'utente;
• Formazione per i gestori e gli utenti;
• Tempi di implementazione;
• Costi di implementazione e di gestione.

Nell'ambito della definizione di un'architettura di sicurezza vengono in generale prese in considerazione alternative diverse per l'implementazione di una stessa funzionalità. La scelta dell'opzione da rendere esecutiva viene fatta solo dopo un'analisi costi/benefici, come precedentemente illustrato.

Di seguito riportiamo, a titolo esemplificativo, le categorie di strumenti tecnologici più utilizzati per far fronte ai principali rischi legati alla sicurezza logica.

9.2.1 Il controllo degli accessi ai sistemi di elaborazione

Il controllo degli accessi consiste nel garantire che tutti gli accessi agli oggetti del sistema informativo avvengano esclusivamente secondo modalità prestabilite. Il controllo accessi può essere visto come un sistema caratterizzato da soggetti (utenti, processi) che accedono a oggetti (applicazioni, dati, programmi) mediante operazioni (lettura, aggiornamento, esecuzione). Funzionalmente è costituito da:
• un insieme di politiche e di regole di accesso che stabiliscono le modalità (lettura, aggiornamento, ecc.) secondo le quali i vari soggetti possono accedere agli oggetti;
• un insieme di procedure di controllo (meccanismi di sicurezza) che verificano se la richiesta di accesso è consentita o negata, in base alle suddette regole (validazione della richiesta).

Per garantire quanto sopra esposto, è indispensabile prevedere un meccanismo che costringa ogni utente ad autenticarsi (cioè dimostrare la propria identità) prima di poter accedere ad un calcolatore; il meccanismo sinora più usato a tale scopo è quello delle password. Si concede all'utente una coppia user-id e password al livello del sistema operativo e/o per ogni applicazione (di solito in numero limitato) al cui accesso quell'utente è abilitato. Si arriva molto presto alla constatazione che il meccanismo delle password non è però sufficientemente adeguato a garantire il livello di sicurezza richiesto nella fase di autenticazione. I problemi principali legati all'uso delle password sono: la scelta di password estremamente facili da indovinare da parte degli utenti e la possibilità di intercettarle quando transitano in rete.

Per far fronte a questi problemi sono stati individuati dei meccanismi di autenticazione forte, che consentono di rendere molto più sicura una qualunque fase di autenticazione. Tali meccanismi sono basati sul riconosci-

mento di un attributo posseduto dall'utente, che può essere:

• una caratteristica fisica, quale l'impronta digitale, la forma della mano, l'iride, la retina, o una caratteristica comportamentale, quale la firma, la voce (in questo caso parliamo di dispositivi di autenticazione biometrici);

• una password generata dinamicamente da un apposito dispositivo personalizzato per ciascun utente (in questo caso parliamo di *one-time password*);

• un certificato digitale che attesta l'identità dell'utente, solitamente memorizzato su *smart card*.

I certificati digitali con particolare riferimento a quelli di tipo X.509, dal nome dello standard internazionale che ne definisce il contenuto, sono, tra i meccanismi di autenticazione, quelli che hanno visto il maggior numero di implementazioni in questo ultimo periodo. La loro importanza è legata anche al fatto che lo stesso meccanismo può essere utilizzato per realizzare la firma digitale di documenti. Questo sarà, molto probabilmente, il meccanismo di autenticazione che sostituirà nei prossimi anni le password. In seguito richiamiamo brevemente i principi di funzionamento su cui si basano.

I certificati digitali sono il frutto dei risultati della più recente branca della crittografia, la crittografia a chiave asimmetrica. Al fine di utilizzare tali meccanismi è necessario fare riferimento ad una PKI (*Public Key Infrastructure*) cioè una infrastruttura che emette dei certificati digitali e che provvede alla loro gestione (pubblicazione in rete, revoca, sospensione e aggiornamento).

In tale scenario ogni utente viene fornito di una coppia di chiavi (pubblica e privata) che lo identificano. La chiave pubblica viene inserita in un certificato digitale emesso dalla PKI che ne attesta inequivocabilmente l'appartenenza all'utente stesso, e viene diffuso pubblicamente dalla PKI. La chiave privata viene invece custodita segretamente dall'utente.

L'uso appropriato di questa coppia di chiavi consente lo svolgimento di una fase di autenticazione forte, fase che viene solitamente realizzata automaticamente con il minimo coinvolgimento dell'utente grazie all'uso di *smart card*.

Il ricorso ai certificati digitali consente anche la realizzazione di funzionalità estremamente importanti in ambito sicurezza informatica, quali l'autenticità e l'integrità dei messaggi, la non ripudiabilità e la confidenzialità, che verranno richiamate di seguito.

Un meccanismo di sicuro interesse nell'ambito di strumenti per il controllo degli accessi è rappresentato dai sistemi di *Single Sign-On* (SSO). Tali strumenti sono realizzati per facilitare la gestione degli accessi in quei sistemi in cui l'utente si trova di fronte ad una moltitudine eterogenea di *workstation*, server ed applicazioni, e si vede costretto ad effettuare la fase di autenticazione (*log-in*) ogni qualvolta deve modificare server o applicazione su cui operare. In tali situazioni un sistema di *Single Sign-On* (SSO) presenta all'utente una singola istanza iniziale di identificazione / autenticazione forte; è poi il SSO che sfruttando un *Security Information Base* interno fornisce automaticamente le *log-in* di tutte le applicazioni (o sistemi) al cui uso l'utente è abilitato. Il sistema di SSO gestisce in proprio, ed automaticamente, le *log-in* (nuova attribuzione, rinnovo o cancellazione) mediante colloquio diretto con i sistemi o le applicazioni.

Oltre alla fase di identificazione e autenticazione dell'utente, indipendentemente dal meccanismo di autenticazione utilizzato, si

deve provvedere al controllo dell'accesso agli oggetti del sistema informativo. I sistemi operativi sono spesso dotati di meccanismi di sicurezza interni che controllano se la richiesta di accesso è consentita o negata. Come è già avvenuto per i mainframe, l'utilizzo di appositi strumenti di controllo accesso esterno, amministrabili in modo semplice e sicuro, agevolano il compito del gestore della sicurezza logica. Tali strumenti, oltre ad agevolare, l'amministrazione della sicurezza, attraverso semplici definizioni di regole di accesso agli oggetti (es.: *file*, *directory*, comandi), sono anche in grado di offrire un livello di sicurezza maggiore.

9.2.2 Antivirus

I computer virus sono i rappresentanti più noti di una categoria di programmi scritti per generare intenzionalmente una qualche forma di danneggiamento a un computer o ad una rete, indicati con il termine generico di codice maligno.

In allegato 2 vengono descritti, a titolo di esempio, alcuni degli aspetti fondamentali per la definizione di un'architettura antivirus.

Considerato che un virus informatico può dar luogo a:

a) danni all'hardware

b) danni al software

c) danneggiamento di dati (integrità)

d) perdita di tempo impiegato a ripristinare le funzioni del sistema

e) infezione di altri sistemi

è necessario che le Amministrazioni attribuiscano la debita priorità all'adozione di iniziative a difesa attivando una protezione sistematica dei propri sistemi informatici e dei dati in essi custoditi e gestiti contro la minaccia rappresentata da virus, macro virus e *worm*.

Tali "programmi" sono in grado, senza alcun intervento dell' utente, di:

a) "infettare" altri programmi, cioè creare copie di se stessi su altri programmi presenti nel sistema;

b) insediarsi nella tabella di partizione e nel settore di *boot* del disco rigido, dove attendono il verificarsi di un determinato evento per poter assumere il controllo di alcune funzioni del sistema operativo, con il fine di svolgere azioni dannose per cui sono stati programmati;

c) inserire operazioni automatizzate (c.d. macroistruzioni) in documenti di testo, di archivio o di calcolo, dagli effetti indesiderati e nocivi;

d) autoreplicarsi all'interno del sistema al fine di saturarlo.

Le azioni di danneggiamento possono andare dalla modifica del contenuto di alcuni *file* residenti sull'hard disk, alla completa cancellazione dello stesso, cosi come all'alterazione del contenuto del video o alla impostazione hardware della tastiera

La miglior difesa contro i virus informatici consiste nel definire un'architettura antivirus composta da regole comportamentali e da procedure operative, a protezione dell'intero sistema informatico.

Tutti gli utenti del sistema sono tenuti a conoscere e rispettare le regole emesse dall'Amministrazione e l'amministratore di sistema è tenuto a mantenere costantemente operative e aggiornate le procedure software predisposte.

9.2.3 Controllo del software

Tra i principali punti di debolezza di un sistema informatico vanno sicuramente annoverati il sistema operativo e le applicazioni. Spesso attraverso lo sfruttamento di errori (*bug*) presenti in questi programmi un estraneo riesce a

guadagnare un accesso al sistema. Le contromisure da adottare in questo caso sono essenzialmente di due tipi:
- l'aggiornamento costante dei prodotti non appena viene scoperto un *bug* che compromette la sicurezza del sistema. Tale procedura è nota come installazione di *patch*;
- la verifica periodica dell'installazione e della configurazione dei prodotti software. Un errore anche minimo in questa fase può trasformare un prodotto che dovrebbe contribuire a migliorare la sicurezza di un sistema, come ad esempio un *firewall*, nel prodotto che compromette ogni misura.

Numerose *mailing list*, gruppi di discussione e siti sono già attivi da tempo sull'argomento. Tutti gli amministratori di rete dovrebbero costantemente monitorare queste fonti di informazioni e aggiornare i sistemi operativi. Ogni aggiornamento del software dovrebbe essere registrato in una specifica base dati.
Sono disponibili dei *tool* in grado di verificare automaticamente eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete. Questi prodotti sono noti con il generico termine di *Network Scanner*. Anche per questi prodotti il livello di sofisticazione cresce di anno in anno.

9.2.4 Strumenti per la Riservatezza ed Autenticità dei Dati

I dati conservati in un sistema informatico devono essere protetti da letture e/o modifiche da parte di utenti non autorizzati. Due sono i momenti principali in cui tali dati devono essere difesi: l'accesso in locale e la trasmissione in rete.
Nel caso in cui i dati da proteggere risiedono su basi di dati è necessario ricorrere a prodotti che implementino politiche di autorizzazione per l'accesso, ai dati possibilmente legati a meccanismi di autenticazione forte degli utenti.
Per la protezione di dati conservati su *file* si possono utilizzare strumenti, genericamente chiamati *crypto file system*, che, utilizzando tecniche crittografiche, consentano di cifrare il contenuto dei *file*, in modo che lo stesso contenuto possa essere "letto" solo da utenti in possesso di un particolare codice, garantendo quindi la riservatezza dei dati.
Se l'Amministrazione dispone anche di una PKI, è possibile utilizzare i suddetti strumenti anche per apporre firme digitali ad interi file, garantendo in questo modo l'autenticità e l'integrità degli stessi.o in fase di trasmissione si può utilizzare uno schema unico basato sulla cifratura dei dati stessi.
Il principale strumento per la Riservatezza dei dati è l'utilizzo di PKI, cioè infrastrutture che permettono di utilizzare in modo semplice e su vasta scala una serie di funzionalità consentite dalla crittografia a chiave pubblica, quali: la firma digitale, il non ripudio dei messaggi, l'autenticazione, la confidenzialità e l'integrità. I principali compiti di una PKI sono l'emissione dei certificati digitali, la gestione di un archivio costantemente in rete che contiene tutti i certificati emessi, la sospensione e la revoca dei certificati e la gestione degli archivi dei certificati sospesi e revocati.
La diffusione di tali strutture consente di migliorare notevolmente la sicurezza delle comunicazioni e dei sistemi.

9.2.5 Strumenti per la Disponibilità dei dati

I dati di un sistema sono sottoposti a una serie di rischi che ne minacciano continuamente la disponibilità. Questi rischi vanno dai mal funzionamenti hardware agli atti di vandalismo

perpetrati da intrusi informatici. È possibile ridurre al minimo gli effetti, spesso disastrosi, di tali eventi, predisponendo una serie di accorgimenti tecnologici, come:

- sistemi RAID (*Redundant array of inexpensive disks*): si tratta di hard disk multipli, visti però dal sistema operativo come un singolo disco. La principale proprietà di questi dispositivi è quella di garantire la disponibilità e l'integrità dei dati anche nel caso di guasto hardware di uno dei dischi che compongono il sistema;
- *back-up*: si tratta di una serie di procedure attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema su dispositivi opportuni. In caso di guasto hardware dei dischi è quindi possibile "ripristinare" il sistema nello stesso stato in cui si trovava nel momento dell'ultimo *back-up*.

Il problema principale in questo caso è legato al fatto che anche i dispositivi di *back-up* possono guastarsi. Vanno quindi individuate delle strategie di *back-up* che, in funzione delle quantità di dati da memorizzare e delle caratteristiche del sistema, cerchino di minimizzare i rischi derivanti da guasti hardware e consentano, in caso di rottura dei dischi di un sistema, di ripristinare la situazione più aggiornata possibile. Le politiche di *back-up* devono essere organizzate in maniera tale da poter disporre di uno storico e poter così recuperare lo stesso dato in più stadi. I *back-up* dovrebbero essere automatizzati e giornalieri e la gestione dei supporti dovrebbe scongiurare i disastri derivanti da cause fisiche (incendi, allagamenti).

È importante quindi predisporre armadi a isolamento termico e/o magnetico, nonché copie multiple dei *back-up* da tenersi in luoghi differenti e distanti tra loro.

9.2.6 Sicurezza delle reti di telecomunicazione

Il crescente utilizzo di reti di telecomunicazioni locali e geografiche risponde all'esigenza di migliorare l'efficacia e l'efficienza dei procedimenti amministrativi, ma nello stesso tempo espone i Sistemi Informativi Automatizzati e le informazioni trattate a molteplici attacchi alla disponibilità, integrità e riservatezza.

Anche se alcuni concetti della sicurezza delle reti sono comuni ad altre aree della sicurezza dei SIA, si è ritenuto opportuno comunque trattarli esplicitamente in questa sezione, data la rilevanza che la problematica della sicurezza delle reti riveste. La sicurezza della rete deve principalmente garantire, da un lato, l'utilizzo della risorsa trasmissiva ai soli utenti autorizzati e nelle specifiche modalità abilitate, e, dall'altro, che i dati contenuti in una comunicazione non possano essere:

- divulgati o alterati nel momento appena precedente al loro invio ad un destinatario;
- intercettati (attivamente o passivamente) quando sono trasmessi sui mezzi trasmissivi, compromettendo la loro integrità e/o riservatezza;
- conosciuti da utenti non autorizzati quando giungono a destinazione.

La protezione delle informazioni in rete dovrebbe indirizzare, in funzione delle Politiche di Sicurezza, i seguenti servizi:

Controllo del traffico di rete
Riservatezza
Integrità
Autenticazione
Non Ripudio

Vengono di seguito illustrati i principali contenuti di ognuno dei servizi di sicurezza sopra menzionati e fornite alcune indicazioni relativamente alle principali misure di sicurezza da adottare.

Controllo del traffico di rete

Il controllo degli accessi alla rete ha l'obiettivo di garantire che la rete sia utilizzata esclusivamente dall'utenza autorizzata e nelle modalità definite dai profili di abilitazione (ovvero quali servizi di rete è possibile usare e come).

In relazione alla crescente interconnessione di reti utilizzanti il protocollo TCP/IP (Internet per prima) la problematica di controllo degli accessi alla rete è diventata particolarmente critica a causa della intrinseca vulnerabilità del protocollo medesimo.

Per questo motivo sarebbe opportuno implementare misure efficaci di identificazione ed autenticazione dell'utente e di controllo degli accessi ai servizi di rete per far sì che in ogni rete interconnessa vengano rispettati i relativi requisiti di sicurezza definiti dalle specifiche politiche.

Tra le principali misure di sicurezza per controllare l'accesso alle reti basate su protocollo TCP/IP è di primario riferimento l'utilizzo di dispositivi *Firewall*.

I *Firewall* sono dei sistemi hardware e software dislocati nei punti di interconnessione tra reti TCP/IP distinte, ad esempio tra la rete interna ed Internet o tra la rete intranet dell'amministrazione e la RUPA, che hanno il compito di controllare gli accessi alle risorse di rete interconnesse.

Tale controllo è effettuato filtrando i messaggi in transito e facendo passare solo quelli che rispondono ai requisiti definiti dalle politiche di sicurezza del Sistema Informativo Automatizzato.

Per la protezione dalla diffusione di software "maligno" tra le reti interconnesse, sarebbe opportuno che il *Firewall* disponesse di opportune funzioni antivirus.

L'efficacia dei sistemi *Firewall* è strettamente correlata alla corretta configurazione e gestione dei diritti di privilegio, che devono essere accuratamente definiti dalle Politiche di Sicurezza e correttamente implementati.

Ai fini della verifica dell'efficacia e dell'efficienza della soluzione *Firewall* implementata è molto importante la verifica, sia della corretta implementazione, che dell'adeguata gestione. Tale verifica va effettuata prima del rilascio in esercizio del sistema *Firewall* ed ogni qualvolta intervengano modifiche al Sistema Informativo Automatizzato. La verifica viene eseguita attraverso la conduzione di test di penetrazione del sistema di Sicurezza, nonché attraverso la valutazione di adeguatezza delle procedure di gestione in essere.

Riservatezza

La riservatezza sulla rete ha l'obiettivo di contrastare i cosiddetti attacchi passivi, ovvero quelli tesi a carpire in modo non autorizzato il contenuto di informazioni, o l'ubicazione degli interlocutori o la struttura del sistema telematico.

A seconda dei requisiti di sicurezza definiti dalle politiche, i servizi della riservatezza potranno essere:

- Riservatezza dei dati: protezione di tutti i dati trasmessi e ricevuti.
- Riservatezza della Connessione: protegge solo i dati di una particolare connessione selezionandoli in funzione degli indirizzi di rete o altro.
- Riservatezza dei campi selezionati: per garantire la riservatezza di particolari informazioni che risiedono in specifici campi.
- Riservatezza del flusso di traffico: per proteggere informazioni sulla quantità o la direzione del traffico dati.

Il meccanismo attualmente più diffuso per

garantire la confidenzialità del traffico di rete è costituito dalla VPN (*Virtual private network*). Si tratta di un meccanismo che consente la cifratura del traffico tra due punti di una rete in modo trasparente rispetto all'utente stesso. Requisito fondamentale per realizzare una VPN è che le due entità coinvolte siano tra loro compatibili nello svolgimento della suddetta funzione. Una volta predisposta una VPN tra due punti della rete, tutti i pacchetti di informazione tra questi punti vengono cifrati/decifrati dai due dispositivi in questione automaticamente, senza nessun intervento dell'utente che viene però garantito sulla riservatezza delle informazioni trasmesse.

Integrità

Il servizio di integrità ha l'obiettivo di proteggere dai cosiddetti attacchi attivi verificando in fase di ricezione se sono state apportate modifiche alle singole unità dei dati o alla sequenza delle stesse.

A seconda dei requisiti di sicurezza definiti dalle politiche i servizi dell' integrità potranno essere:

• Integrità della connessione "con recupero": realizza l'integrità dei dati effettuando, se ci sono state violazioni di integrità, la ritrasmissione dei dati originali (se il protocollo di comunicazione supporta la ritrasmissione);

• Integrità della Connessione "senza recupero": il servizio rileva l'occorrenza della violazione dell'integrità ma non effettua la ritrasmissione;

• Integrità della connessione per campi selezionati: assicura l'integrità di specifici campi preselezionati.

Autenticazione

Il servizio garantisce l'entità ricevente sull'autenticità dell'entità mittente e dei dati ricevuti e può essere implementato in due modalità:

• Autenticazione per entità di pari livello: garantisce la mutua autenticazione tra entità di pari livello interconnesse durante la fase iniziale del colloquio e nel corso del trasferimento dei dati;

• Autenticazione della sorgente dei dati: garantisce al ricevente l'autenticità dell'identità del mittente per ogni pacchetto inviato in trasmissione.

Non Ripudio

Il servizio di non ripudio serve per fornire la prova incontestabile di un'avvenuta spedizione o di un'avvenuta ricezione di dati in rete.

Assume due modalità:

• Non ripudio dell'origine: prova chi è il mittente di una spedizione;

• Non ripudio della destinazione: prova che la spedizione è arrivata ad uno specifico destinatario. Generalmente il servizio di non ripudio è richiesto laddove bisogna avere garanzie di avvenuta spedizione/ricezione di flussi telematici e salvaguarda dalle minacce di *misrouting*.

Crittografia

Per l'implementazione dei servizi di sicurezza sopra descritti, Riservatezza, Integrità, Autenticazione e Non Ripudio, è importante l'utilizzo della crittografia ed in particolare della Firma Digitale. Questo significa realizzare la sicurezza dei servizi di rete attraverso un'infrastruttura tecnologica di crittografia a Chiave Pubblica (PKI), come evidenziato nel paragrafo 9.2.1, basata su diversi servizi:

• Certificazione (*Certification Authority*);

• Registrazione (*Registration Authority*);

• *Time Stamping*;

• Notariato.

La realizzazione dell'architettura di sicurezza basata su crittografia a chiave pubblica (PKI) consentirebbe inoltre di realizzare sistemi di sicurezza in grado di erogare servizi, sia alla rete (meccanismi di *Virtual Private Networking*), che alle applicazioni, che agli utenti.

Il meccanismo attualmente più diffuso per garantire la confidenzialità del traffico di rete è costituito dalla VPN (*Virtual private network*). Si tratta di un meccanismo che consente la cifratura del traffico tra due punti di una rete in modo trasparente rispetto all'utente stesso. Requisito fondamentale per realizzare una VPN è che le due entità coinvolte siano tra loro compatibili nello svolgimento della suddetta funzione. Una volta predisposta una VPN tra due punti della rete tutti i pacchetti di informazione tra questi punti vengono cifrati/decifrati dai due dispositivi in questione automaticamente, senza nessun intervento dell'utente che viene però garantito sulla riservatezza delle informazioni trasmesse.

L'adozione della Firma Digitale quale strumento di identificazione ed autenticazione dell'utente sarà la principale misura di sicurezza sia per l'integrazione in RUPA sia per lo sviluppo dei servizi *on-line* ai cittadini.

La realizzazione della Sicurezza della rete richiede l'esecuzione di una serie di attività complesse orientate, oltre che alle misure di sicurezza logica precedentemente descritte, anche alle misure, sia di sicurezza fisica (protezione fisica degli apparati di trasmissione), che di carattere organizzativo (procedure di gestione della crittografia).

Dovranno in particolare essere sviluppate le seguenti attività:

- Politiche di Sicurezza della rete (*Network Security:* Esigenze e Regole);
- Requisiti di Sicurezza della Rete (Controllo degli Accessi, Riservatezza, Integrità, Autenticazione e Non Ripudio);
- Meccanismi tecnologici di implementazione (Crittografia);
- Norme e Procedure per la realizzazione e la Gestione della infrastruttura di Sicurezza basata su Crittografia.

9.3 Sicurezza Organizzativa

Il Processo della Sicurezza dei Sistemi Informativi Automatizzati richiede che, accanto all'adozione di misure tecnologiche precedentemente illustrate, vengano definite una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi del processo medesimo.

Gli aspetti organizzativi della Sicurezza dei Sistemi Informativi Automatizzati riguardano principalmente:

- La definizione di ruoli, compiti e responsabilità 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.

In relazione al primo aspetto, con riferimento alle funzioni organizzative definite nel capitolo 12, dovranno essere identificati una serie di ruoli, compiti e responsabilità per le specifiche attività del processo della Sicurezza.

Ogni Amministrazione, in relazione alla propria particolare struttura organizzativa e ruoli del personale, definirà specifici compiti e responsabilità.

In relazione al secondo aspetto vengono di seguito indicate le principali procedure organizzative che dovrebbero essere emanate ed adottate per la Sicurezza dei Sistemi Informativi Automatizzati:

- Procedure di Gestione delle Contromisure di Sicurezza Logica;

• Procedure di Gestione specifiche per la Sicurezza della Rete;
• Procedure di Controllo dei Sistemi di Sicurezza;
• Procedure di Controllo del Ciclo di Vita del Software;
• Procedure di Controllo per la Gestione delle Operazioni;
• Procedure per la Gestione degli Incidenti;
• Procedure per la Continuità Operativa;
• Procedure per il Personale.

Una serie di aspetti che devono essere regolamentati dalle procedure di Sicurezza sono, ad esempio:

- Documenti: Accesso ai documenti, Conservazione dei documenti, Consegna documenti, Distruzione;
- Utilizzo del software: installazione, licenze d'uso, modalità d'uso;
- Password: Modalità di assegnazione, gestione ed utilizzo, validità nel tempo;
- I virus informatici: Misure preventive, Regole operative, Norme sull'utilizzo dei programmi antivirus;
- La posta elettronica: Norme generali, Utilizzo corretto, Attivazione del servizio;
- Le risorse informatiche: Generalità, Diritto d'Uso, Autorizzazioni, Dismissione, Installazione delle postazioni, Ergonomia e salute del lavoratore, Sicurezza ambientale, Protezione da furti, Blocco fisico dell'apparato, Blocco dell'avvio da disco floppy, Protezioni logiche della risorsa;
- I Supporti rimovibili, magnetici e ottici: Supporto di memorizzazione fisso o rimovibile, Distruzione dei supporti magnetici e ottici;
- La rete: Gli utenti di rete, Directory condivise, Monitoraggio e Gestione, Backup Centralizzato di rete, Utilizzo della rete;
- Sicurezza dei Personal Computer portatili;
- Comportamenti illegali;
- Norme disciplinari;
- Riferimenti Normativi.

Un ulteriore aspetto inerente alla Sicurezza Organizzativa è quello concernente i controlli sulla consistenza e sulla affidabilità degli apparati.

È necessario prendere tutte le precauzioni affinché i computer e tutti gli apparati utilizzati per l'erogazione dei servizi non siano un punto di criticità del sistema. Al di là di tutti quelli che sono i già presenti controlli sul materiale che va acquistato è importante creare una banca dati di tutte le dotazioni HW, SW e di trasmissione dati della P.A. È importante che questo comune archivio venga tenuto aggiornato con le sostituzioni, riparazioni e con i consumi delle apparecchiature.

Questa banca dati dei sistemi informativi, se correttamente gestita, darebbe una visione storica e precisa del patrimonio arricchita di informazioni estremamente utili e statistiche sul grado di affidabilità e uso dei sistemi; sarebbe di conseguenza di grande aiuto nei processi di acquisto ed in quelli di pianificazione degli investimenti e delle scorte e materiali di consumo.

Nell'acquisto delle apparecchiature bisognerebbe prevedere sistemi di protezione elettrica delle stesse, quali stabilizzatori di corrente e apparecchiature UPS.

Per HW impiegato in attività di fondamentale importanza, ai fini del conseguimento degli obiettivi istituzionali, è importante prevedere la necessità di utilizzare apparati che si avvicinino ad un concetto di garantire la massima ridondanza ed affidabilità (*Fault Tolerance*).

Oltre a regolamentare il comportamento dei propri utenti è necessario anche regolamentare quello di utenti esterni (ad esempio consu-

lenti e fornitori) che operano con il Sistema Informativo Automatizzato o comunque che sono abilitati a connettersi con esso.

9.4 Piano di Continuità Operativa

Il piano di continuità operativa rappresenta l'aspetto della Sicurezza principalmente orientata a garantire la continuità e la disponibilità dei Sistemi Informativi Automatizzati rispetto a danneggiamenti causati da eventi accidentali, sabotaggi, disastri naturali.

In considerazione del fatto che i Piani di Continuità in genere richiedono investimenti significativi per la loro realizzazione, è importante che vengano definiti, tenendo continuamente presente un corretto rapporto costi/benefici, nei limiti della loro effettiva necessità.

L'obiettivo del Piano di Continuità Operativa è quello di ripristinare i servizi informatici entro un tempo prestabilito, in funzione dei livelli di servizio attesi, e di rendere minime le perdite causate dall'interruzione dell'attività.

Ciò vuol dire che il Piano di Continuità Operativa non deve essere inteso come misura alternativa a quelle di prevenzione, ma a completamento di queste ultime, al fine di:

• garantire la continuità dei principali processi assicurando l'erogazione dei servizi essenziali;

• limitare gli impatti degli eventi a carattere distruttivo sulla posizione finanziaria.

Il Piano di Continuità Operativa si occupa del controllo delle interruzioni di operatività al fine di prevenirne e minimizzarne l'impatto, individuando un insieme specifico di contromisure di sicurezza in grado di sostenere le operazioni critiche di missione istituzionale anche attraverso infrastrutture alternative.

Lo scopo è quello di raggiungere e mantenere un sistema di operazioni che risponda alle Politiche della Continuità, che quindi prevenga i rischi e, in caso di accadimento dell'evento distruttivo, ne limiti l'impatto sulla continuità dei servizi.

A tal fine sarebbe opportuno attivare un processo di sviluppo e mantenimento di specifici piani che includano misure di identificazione e riduzione del rischio orientate a limitare le conseguenze di un impatto dannoso e ad assicurare un rapido ripristino delle operazioni essenziali.

Il processo di pianificazione della Continuità Operativa dovrebbe essere visto come un quadro di riferimento per la gestione di più procedure di ripristino orientate a coprire scenari di impatto differenziati in relazione ai diversi eventi dannosi: dalla semplice caduta di alimentazione fino agli eventi catastrofici che richiedono un vero e proprio Piano di *Disaster Recovery*. La Continuità Operativa è un processo continuo che si articola in attività di analisi, progetto, attuazione e manutenzione di un piano che deve contemplare:

• identificazione e classificazione per priorità di ripristino dei processi e servizi critici;

• determinazione dei potenziali impatti di indisponibilità rispetto ai diversi scenari di danneggiamento;

• identificazione delle responsabilità ed adozione di contromisure tecniche ed organizzative;

• documentazione dei processi e delle procedure concordate (di emergenza, di continuità, di ripristino);

• formazione specifica di tutto il personale sui processi e le procedure della Continuità Operativa;

• test, Manutenzione ed aggiornamento del Piano.

La realizzazione del Piano di Continuità Operativa si basa quindi su contromisure di carattere sia tecnologico che organizzativo che indicano cosa fare, con quali risorse, e quali procedure seguire in condizioni di emergenza che rendano i Sistemi Informativi Automatizzati parzialmente o totalmente indisponibili.

I principali aspetti tecnologici riguardano:

• il recupero dei supporti di *back-up*;

• il recupero delle transazioni perse;

• IT *Disaster Recovery* nel caso di impatto per evento catastrofico.

In questo ultimo caso la principale contromisura di carattere tecnologico consiste nel centro di *back-up* che può essere realizzato in uno dei seguenti modi:

• Predisponendo una struttura tipo "scatola vuota" (in inglese: *Empty Shell*) di proprietà dell'Amministrazione, o di tipo consortile o in service;

• Raddoppiando il centro ed integrandolo in rete;

• Creando un centro di *recovery* che può essere di proprietà dell'azienda, o di tipo consortile o in *service*.

Dovrà inoltre essere predisposta una struttura di commutazione che in caso di emergenza sia in grado di commutare l'utenza dal sistema principale a quello di *back-up*.

I principali aspetti organizzativi, come accennato nel precedente paragrafo, riguardano la definizione del piano dettagliato di chi fa cosa dal momento della dichiarazione dello stato di emergenza a tutto il periodo (anche diversi mesi) durante il quale il centro primario potrebbe rimanere fuori servizio.

Nulla deve essere lasciato al caso, il piano dovrà quindi comprendere:

• l'assegnazione delle responsabilità individuali

• le procedure di rilevamento e segnalazione;

• il Piano di gestione dell'emergenza;

• l'organizzazione della ripartenza dei servizi essenziali (ripartenza automatica);

• il Piano di gestione della comunicazione verso le Direzioni, le altre Amministrazioni, il pubblico;

• corsi di Sensibilizzazione e Formazione periodici;

• la manutenzione del Piano: organizzazione di test regolari e revisioni di tutte le contromisure, le procedure ed i *recovery plan*.

L'attività di manutenzione del piano riveste particolare importanza per evitare che il sistema stesso divenga rapidamente obsoleto ed inefficace a causa della:

• Evoluzione tecnologica dei sistemi hardware e software sia del proprio Sistema Informativo Automatizzato che, eventualmente, del Centro di Back-up;

• Evoluzione organizzativa e logistica dell'Amministrazione;

• Caduta di attenzione delle persone coinvolte;

• Cambiamento delle persone che occupano i ruoli interessati.

Se il piano non segue tempestivamente questi cambiamenti perde di efficacia in breve tempo. L'unico modo per verificare che la manutenzione sia effettuata in modo adeguato è quello di programmare prove reali o almeno "di carico" almeno due volte all'anno.

10. Verifica della Sicurezza dei Sistemi Informativi Automatizzati

La verifica dell'efficacia e della validità nel tempo delle misure di sicurezza adottate è punto fondamentale di tutto il processo per la sicurezza dei SIA.
Infatti, in un contesto tecnologico in rapidissima evoluzione, è necessario avere le massime garanzie circa l'adeguatezza delle misure di sicurezza adottate nei confronti del sempre più vasto, articolato ed aggiornato panorama delle minacce possibili.
Per quanto sopra le attività di verifica dovranno consistere in due attività distinte, sia per compiti, che per organizzazione.
La prima – Monitoraggio – è l'attività di verifica continua della efficacia delle misure di sicurezza realizzate ed è effettuata, sotto la responsabilità della struttura che progetta e realizza le misure di sicurezza, durante la progettazione, implementazione ed esercizio delle misure stesse (vedi cap. 12).
La seconda – Audit di sicurezza – è un'attività di verifica effettuata da una struttura esterna alla struttura che ha implementato le misure di sicurezza, e potrà avvenire in modo estemporaneo e non prevedibile (vedi cap. 12).
Si riporta, nel seguito, una breve descrizione dei contenuti delle attività sopra indicate:

10.1 Monitoraggio delle misure di sicurezza

È necessario anche prevedere un controllo continuo delle misure di sicurezza. Tutto ciò per poter intercettare il più presto possibile eventuali attacchi ai danni del sistema, non previsti in fase di definizione delle contromisure o resi possibili da errori presenti o commessi in fase di installazione delle misure di sicurezza e degli apparati hw e sw ad esse collegati. Questa fase viene solitamente definita *monitoring* o monitoraggio.
Il metodo principale per effettuare il monitoraggio è costituito dalla raccolta ed analisi dei file di "log" (*log file*), cioè file in cui i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono tutte le principali operazioni svolte dagli utenti per loro tramite.
Attraverso questa analisi, che nelle organizzazioni complesse deve essere necessariamente effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi riusciti o meno di accesso al sistema e l'esecuzione di operazioni sospette. Vista l'importanza di questi file viene spesso suggerito di allocare gli stessi su dispositivi non riscrivibili.

10.2 Audit delle misure di sicurezza

Definito il piano di sicurezza, ultimato il piano operativo e dopo aver emanato le norme comportamentali è necessario verificare con periodicità fissa, ed inoltre con verifiche casuali non annunciate, che tutte le misure implementate, sia quelle tecnologiche che quelle organizzative, e la loro attuazione siano consistenti con gli indirizzi definiti nel

piano operativo. Più precisamente deve essere verificato che le misure tecnologiche implementate e il loro effettivo dispiegamento svolgano correttamente le funzionalità per cui sono state adottate.

I test specifici di verifica delle misure tecnologiche possono essere effettuati con l'ausilio dei moderni strumenti automatizzati di "*network scanning*" che stanno acquistando attualmente livelli sempre più elevati di affidabilità e copertura; essi consistono comunque in un'approfondita analisi del sistema in esame, con lo scopo di individuare il livello di *release* e di *patches* dei sistemi operativi, dei *middleware*, degli applicativi installati e la configurazione dei relativi parametri di sicurezza, per confrontare poi queste informazioni con un database di "*security flaws*" denunciate dai produttori o individuati dalla comunità internazionale degli utenti.

È particolarmente importante affiancare a queste attività una serie di attacchi di tipo intrusivo (test di penetrabilità), che prevedono, ad esempio, tentativi esaustivi di individuazione delle password. E' utile per questi test l' impiego di "*ethical hackers*", che abbiano una esperienza consolidata di penetrazione dei sistemi informatici, e che possano operare sia dall'interno che dall'esterno del Sistema Informativo oggetto della verifica.

Per quanto riguarda le misure organizzative, va verificato il loro effettivo rispetto da parte di tutti gli utenti coinvolti.

Tali verifiche, che vengono generalmente indicate come audit di sicurezza, e che sono distinte dalle attività di monitoraggio indicate al paragrafo 10.1, per ovvii motivi debbono essere svolte da personale che non abbia responsabilità di gestione del sistema informatico oggetto della verifica.

Gli audit di sicurezza, richiedendo un notevole livello di specializzazione tecnica e comportando un elevato grado di imparzialità e di indipendenza dalle organizzazioni aziendali coinvolte, possono essere effettuati in *outsourcing* da organizzazioni esterne specializzate.

Data la particolare delicatezza di queste attività, le organizzazioni esterne incaricate devono essere scelte per comprovata competenza ed esperienza professionale specifica, avallata da certificazioni, referenze e riconoscimenti verificabili.

Gli audit di sicurezza devono essere pianificati ed eseguiti secondo uno schema formale, che può variare da organizzazione ad organizzazione, ma che comprendono comunque alcune fasi principali:

- Attività preliminari;
- Preparazione;
- Audit;
- Report;
- Action item.

a) Attività preliminari

Viene svolta l'analisi del sistema oggetto dell'audit. In particolare si rivisitano le scelte iniziali operate in fase di predisposizione del piano per la sicurezza quali l'analisi dei rischi e l'adozione delle contromisure. Valutando la qualità del lavoro svolto e cercando di individuare eventuali errori commessi.

Le attività preliminari sono volte a definire l'ambito generale in cui si svolge l'audit e comprendono:

- verificare l'adeguatezza delle Politiche di sicurezza adottate, confrontandole anche con le "*best practices*" note ed accettate;
- verificare l'analisi dei rischi su cui si basano le Politiche di sicurezza adottate.

b) Preparazione
È una fase volta a connotare tecnicamente la verifica che si intende effettuare e a predisporre organizzativamente l'operazione. Vengono definiti una serie di parametri quali: il tipo di audit, gli strumenti tecnologici da utilizzare. Si procede inoltre a pianificare i test in modo tale che non possano in alcun modo compromettere l'integrità dei sistemi nonché creare il minor disturbo possibile alle attività operative. Inoltre dovranno essere richieste tutte le autorizzazioni necessarie allo svolgimento dell'audit.
Occorre quindi:
- determinare il tipo di audit: host, network, firewall;
- stabilire il livello di severità: alta, normale, leggera;
- determinare l'ambito di sicurezza: perimetrale e/o interna;
- scegliere gli strumenti tecnologici da utilizzare;
- pianificare i test in orari di minor disturbo sulle attività del sistema;
- prepararsi a risolvere gli eventuali inconvenienti indotti dalla esecuzione dei test.

c) Audit
Consiste nella effettiva esecuzione delle verifiche sul sistema informatico. Vengono utilizzati i vari strumenti tecnologici definiti nella fase precedente e si procede inoltre con le interviste al personale per verificare la conoscenza ed il rispetto delle regole comportamentali previste.
Si procede infine alla verifica della documentazione esistente (inventario, schemi topologici, procedure di emergenza, file di log), ricercando in primo luogo la presenza di allarmi o almeno di tracce dei tentativi di penetrazione effettuati durante il test.
Alcune delle anomalie da ricercare riguardano:
- i tentativi multipli falliti di accesso;
- lo stesso utente che accede da postazioni differenti;
- attività fuori orario;
- un numero elevato e fallito di accesso a file.

d) Report
È la fase di preparazione dell'output, cioè della documentazione di quanto riscontrato.
È una fase fondamentale in quanto l'obiettivo primario dell'audit è quello di documentare più accuratamente possibile le criticità riscontrate.
Si estraggono dai dati raccolti solo quelli maggiormente significativi e si preparano i vari report, con vari livelli di dettaglio e di formulazione a seconda dei destinatari.

e) Action Item
In questa fase vengono date indicazioni in merito alle azioni necessarie per risolvere gli eventuali problemi di sicurezza riscontrati, si procede inoltre all'utilizzo dei risultati ottenuti per rivisitare il piano di sicurezza iniziale.
Anche per l'audit di sicurezza sono disponibili alcuni strumenti automatici, programmi software, che eseguono dei test generali o specifici, basati su una base dati di problemi noti di vulnerabilità per le configurazioni individuate.

11. Introduzione e diffusione della cultura della Sicurezza Informatica nella Pubblica Amministrazione

Assicurare la miglior sicurezza dei Sistemi Informativi Automatizzati presenta particolari problematiche d'ordine culturale, sociale ed organizzativo oltre che legale e tecnico, per questo è anche necessario elaborare ed attuare specifici processi di formazione, sensibilizzazione e corresponsabilizzazione.

11.1 Sensibilizzazione e corresponsabilizzazione

La sensibilizzazione alle tematiche della sicurezza informatica ed a costanti comportamenti coerenti con le politiche e le disposizioni date in merito, deve interessare tutte le risorse umane dell'Amministrazione, anche quelle non direttamente interessate dalla formazione predetta, ad ogni livello di responsabilità ed attività.

Ciò al fine di diffondere una cultura generalizzata della sicurezza, che consenta tra l'altro di favorire la miglior efficacia ed efficienza delle misure prese oltre che di sopperire ad eventuali mancanze delle stesse.

Presentazioni, opuscoli, seminari, riunioni dei Dirigenti con i propri collaboratori, a solo titolo d'esempio, possono rappresentare opportunità per raggiungere quest'obiettivo.

Per la corresponsabilizzazione, si deve prevedere di:

• Coinvolgere i Dirigenti e rappresentanze degli addetti in tutte le fasi di definizione del piano per la sicurezza (analisi e gestione dei rischi, politiche, piano operativo e audit);

• Effettuare interventi di richiamo e se necessario adottare gli adeguati provvedimenti disciplinari in caso di inadempienze e/o superficialità in tema di sicurezza informatica.

Analoghi processi devono essere previsti con eventuali partner e per i collaboratori esterni, privati e pubblici, persone fisiche e giuridiche, che interagiscono in modo significativo con l'Amministrazione.

Infine, occorre informare e sensibilizzare su queste tematiche anche gli utenti finali dei servizi erogati dall'Amministrazione.

11.2 Formazione

L'introduzione di un sistema di sicurezza, come di qualunque altro elemento che modifichi le modalità lavorative all'interno di una qualsiasi realtà, ha sicuramente un forte impatto sull'organizzazione.

La formazione interviene in due momenti ben precisi del processo di introduzione di un sistema di sicurezza:

• Sensibilizzazione sulle problematiche della sicurezza e sulla loro importanza (vedi punto precedente);

• Conoscenza delle misure di sicurezza da adottare e da gestire ai diversi livelli di responsabilità.

Dunque anche i fruitori della formazione saranno di diversa tipologia: è fondamentale riuscire a sensibilizzare i manager delle

Amministrazioni affinché questi riescano a trasmettere i principi fondamentali del sistema all'interno delle loro realtà.
Per raggiungere i suoi obiettivi il programma di formazione deve essere concepito in modo tale da:
• Rendere consapevoli i partecipanti sull'importanza delle scelte aziendali;
• Coinvolgere i partecipanti sulle problematiche inerenti alla sicurezza;
• Responsabilizzare i partecipanti sulle attività da eseguire per garantire il mantenimento di un livello di sicurezza accettabile.
Occorre quindi progettare due tipologie di corsi, distinte a seconda dei destinatari: il primo, indirizzato alla direzione, deve prevedere cenni sulla normativa, indicazioni sulle Politiche di Sicurezza, analisi dei rischi; l'altro, indirizzato al personale operativo, deve fornire indicazioni precise sui comportamenti da adottare, sia nelle operazioni quotidiane, che nelle situazioni di emergenza.

I corsi saranno progettati dalle singole amministrazioni in base alle diverse esigenze ed ai diversi sistemi di sicurezza sviluppati, in funzione del diverso patrimonio informativo da proteggere e del diverso grado di informatizzazione raggiunto; in generale non potranno mancare riferimenti a:
• Normativa vigente;
• Definizione delle responsabilità;
• Elenco delle vulnerabilità: spesso non c'è la consapevolezza dei rischi che si possono correre, vale quindi la pena individuare i punti di vulnerabilità del sistema, sia nell'ottica della prevenzione che nell'individuazione di possibili incidenti;
• Regole comportamentali che comprendono la gestione degli accessi (password,…);
• I possibili rischi: virus, intercettazioni, intrusioni, ecc.;
• Firma digitale;
• Audit dei sistemi di sicurezza: su questo argomento è necessario sensibilizzare il personale che dovrà affrontare le verifiche da parte di personale specializzato.

Le Amministrazioni devono tener presente che le attività relative alla sicurezza non rappresentano un appesantimento del lavoro quotidiano, ma una volta che entrano nel ciclo standard delle operazioni da compiere, contribuiscono a garantire il personale dal rischio di perdere o comunque compromettere parte del lavoro fatto.

La formazione, se ben orientata, progettata e realizzata, può essere lo strumento più efficace per realizzare la diffusione delle politiche, degli obiettivi e dei piani dell'Amministrazione in tema di sicurezza e per minimizzare quella componente, sempre presente, che consiste nella resistenza al cambiamento.
Inoltre è necessario rivedere ed aggiornare annualmente i Piani di formazione in relazione alle mutate esigenze dell'Amministrazione ed allo sviluppo delle tecnologie (di attacco alla Sicurezza e di difesa).

12. Organizzazione funzionale della gestione della sicurezza dei Sistemi Informativi Automatizzati nelle pubbliche amministrazioni

La messa in sicurezza di un sistema informativo automatizzato richiede lo svolgimento di una serie di attività a diversi livelli. In questa sezione viene fornito uno schema di riferimento utilizzabile per classificare e organizzare sistematicamente tali attività. La messa in sicurezza dei sistemi e la protezione del patrimonio informativo si può ricondurre, da un punto di vista organizzativo, a tre specifiche funzioni:

1. Definizione delle Politiche in tema di Sicurezza Informatica;
2. Progettazione, implementazione e gestione delle misure di sicurezza in attuazione delle Politiche di cui al punto precedente;
3. Verifica e controllo della corretta attuazione e dell'efficienza delle misure di sicurezza adottate (Audit di sicurezza);

I contenuti delle tre funzioni sopra individuate, e la conseguente collocazione in termini organizzativi, sono riassunti nei successivi paragrafi.

12.1 Definizione delle Politiche in tema di Sicurezza Informatica

Tale funzione è di carattere eminentemente strategico in quanto definisce le finalità e gli obiettivi delle politiche di sicurezza che l'Amministrazione intende adottare.

Tali indicazioni dovranno essere coerenti con le normative vigenti in tema di sicurezza, con le politiche di sicurezza Informatica definite a livello di Governo ed, in particolare, con gli indirizzi espressi in materia dall'AIPA.

Inoltre dovrà essere posta adeguata attenzione, al fine del contenimento dei costi, a definire misure di sicurezza coerenti con il "valore" del patrimonio informativo da proteggere.

È una funzione di indirizzo che dovrà fornire chiare linee operative per lo sviluppo, la gestione ed il controllo delle misure di sicurezza da adottare.

12.2 Progettazione, implementazione e gestione delle misure di sicurezza in attuazione delle Politiche di cui al punto precedente

Tale funzione ha il compito di progettare, realizzare e mantenere in efficienza misure di sicurezza tali da soddisfare le linee strategiche di indirizzo definite dalla funzione di cui al punto precedente.

Il compito di proporre, sviluppare e mantenere aggiornate le misure di sicurezza è di rilevante responsabilità e richiede alta professionalità e profonda conoscenza dell'Amministrazione.

I principali compiti di tale funzione sono riconducibili a:

- Definire i requisiti di sicurezza da adottare per proteggere il complesso degli archivi, delle procedure e dei sistemi informatici esistenti, sulla base delle linee di cui al punto precedente. In particolare dovranno essere definiti diversi livelli di requisiti funzionali in relazione alla "valorizzazione " del patrimonio informativo da proteggere;

• Definire un'architettura di sicurezza che soddisfi i requisiti di cui sopra e che armonizzi le misure di sicurezza con le architetture informatiche esistenti od in corso di implementazione;
• Realizzare la progettazione esecutiva del Sistema di sicurezza da realizzare, con particolare riferimento alla:
- Identificazione degli elementi da proteggere,
- Identificazione delle minacce a cui detti elementi sono sottoposti,
- Analisi e mappa dei rischi,
- Analisi costi \ benefici,
• Implementazione del Sistema di sicurezza progettato e definito;
• Pianificazione ed esecuzione di test del sistema di sicurezza attraverso adeguate prove di penetrazione;
• Definizione ed attuazione di Piani e strumenti di monitoraggio continuo della sicurezza;
• Aggiornamento periodico del Sistema di sicurezza per renderlo sempre adeguato alle nuove minacce;
• Manutenzione del Sistema di sicurezza per assicurarne costante efficienza e disponibilità;
• Supporto alla formazione del personale dell'Amministrazione (dirigenza, addetti, utenti) in tema di sicurezza;
• Emanazione di procedure interne inerenti alla sicurezza (regolamentazione degli accessi fisici e logici agli archivi ed ai sistemi informativi, norme operative di utilizzo e gestione dei sistemi, gestione delle *password*, ecc.).

12.3 Verifica e controllo della corretta attuazione e dell'efficienza delle misure di sicurezza adottate (Audit di sicurezza)

Tale funzione ha il compito di controllare le misure di sicurezza adottate, verificandone l'efficacia e la coerenza con le Politiche di Sicurezza definite dal vertice dell'Amministrazione.
Per le sue specifiche attività, è una funzione che richiede autonomia operativa ed un alto livello di conoscenze tecniche, nonché la necessità di un costante aggiornamento sulle evoluzioni del mercato e delle tecnologie.

I principali compiti di tale funzione sono riconducibili a:
• controllare la coerenza delle misure di sicurezza adottate con gli standard nazionali e\o internazionali e le normative vigenti in materia;
• eseguire audit periodici sui livelli di sicurezza realizzati;
• definire Piani di attacco ai Sistemi informativi Automatizzati, sulla base anche delle evoluzione tecnologica e delle nuove minacce che nel tempo si presentano;
• simulare attacchi estemporanei ed imprevedibili ai Sistemi informativi (tali, comunque, da non creare danni ai Sistemi stessi);
• proporre eventuali modifiche\implementazioni ai Sistemi di sicurezza sulla base dei controlli \test effettuati.

12.4 Collocazione Organizzativa delle tre Funzioni della Sicurezza

In considerazione delle attività sopra indicate si ritiene necessario, da un punto di vista organizzativo, rendere le tre funzioni sopra indicate tra loro indipendenti.
In particolare è necessario garantire la completa indipendenza strutturale ed organizzativa tra la funzione di Implementazione e Gestione (punto 12.2) e la funzione di Auditing (punto 12.3).

12.5 Strutture di supporto alla Sicurezza informatica

Un altro aspetto inerente alla gestione della Sicurezza informatica è la possibilità di creare "centri di competenza in materia di sicurezza informatica" che possano supportare le Amministrazioni nella definizione ed attuazione delle loro politiche di sicurezza.

È inoltre da auspicare la creazione di un "osservatorio permanente sulla sicurezza informatica" che possa avere strette connessioni con le Aziende e\o le loro Associazioni per monitorare il continuo sviluppo tecnologico del mercato e costituire, così, punto di riferimeto per le maggiori problematiche del settore
L'osservatorio dovrebbe avere la missione di:

- rendere più trasparente e comprensibile il mercato;
- contribuire allo sviluppo di una maggiore consapevolezza del problema della sicurezza nella PA e di una maggiore connessione tra PA e le imprese specialistiche del settore.

E dovrebbe espletare le proprie attività in tema di:

- attività di ricerca sul tema della sicurezza;
- sviluppo ed utilizzo di metodologie innovative di ricerca;
- creazione e sviluppo di un *network* di relazioni internazionali con altri Osservatori nonché con industrie ed enti di provata esperienza nel settore.

13. Gruppo di lavoro

Coordinatore

Ferrante PIERANTONI	AIPA

Componenti

Leonardo ANGELONE	AIPA	Vincenzo MEROLA	AIPA
Andrea APARO	esperto	Luca MISSORI	ANASIN
Luciano ARRIGO	ANASIN	Elio MOLTENI	ASSINTEL
Paolo BALLACCI	ASSINFORM	Alessandro MUSUMECI	ANASIN
Danilo BRUSCHI	esperto	Massimo NAVA	ASSINFORM
Giovanni CAPORALE	AIPA	Giuseppe NERI	ASSINFORM
Giorgio COMUNELLO	esperto	Piercarlo RAPETTI	ASSINTEL
Raffaella D'ALESSANDRO	esperto	Umberto RAPETTO	AIPA
Massimo FUBINI	esperto	Giampiero SARACINO	ANASIN
Francesco LIVERANI	esperto	Mario TERRANOVA	AIPA-CT
Giacomo MASIELLO	esperto		

14. Bibliografia

- Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonized Criteria, Vers. 1.2, Giugno 1991, Commission of the European Communities, Directorate-General XIII, Rue de la Loi 200, B-1049, Brussels,Belgium
- Information Technology Security Evaluation Manual (ITSEM) Vers. 1.0, Settembre 1993, Commission of the European Communities, Directorate-General XIII, Rue de la Loi 200, B-1049, Brussels, Belgium
- BS 7799: Code of Practice for Information Security Management, British Standard Institute, Giugno 1995
- AIPA - Studio di fattibilità - La Rete unitaria della Pubblica Amministrazione. - 1996
- AIPA - Proposta di architettura applicativa della Rete unitaria della P.A. - 1997
- AIPA - Linee guida per la realizzazione di studi di fattibilità - 1997
- AIPA - Studio di prefattibilità per la individuazione delle infrastrutture necessarie a favorire lo sviluppo della cooperazione applicativa tra Amministrazioni - 1998
- AIPA - Gara per la fornitura del servizio trasmissivo di trasporto e per la fornitura dei servizi di interoperabilità della Rete unitaria delle Pubbliche Amministrazioni -1998
- AIPA - Piano Triennale per l'Informatica della Pubblica Amministrazione 1999-2001

NORMATIVA DI RIFERIMENTO

- Direttiva del Consiglio delle Comunità Europee 91/250/CEE del 14 maggio 1991 (G.U.C.E. 17.5.1991, n. L 122)
- Raccomandazione del Consiglio dell'Unione Europea 95/144/CE del 7 aprile 1995 (G.U.C.E. 26.4.1995, n. 93)
- Direttiva del Parlamento europeo e del Consiglio 95/46/CE del 24 ottobre 1995 (G.U.C.E. 23.11.95, n.281)
- Direttiva del Parlamento Europeo e del Consiglio 96/9/CE dell' 11 marzo 1996 (G.U.C.E. 27.3.1996, n.77)

- Legge 1 aprile 1981, n. 121 (G.U.R.I. 10.4.1981, n. 100, S.O.)
- Decreto del Presidente del Consiglio dei Ministri 15 febbraio 1989 (G.U.R.I. 10.3.1989, n.58)
- Legge 7 agosto 1990, n. 241 (GURI 18.8.1990, n. 192)
- Decreto legge 3 maggio 1991, n.143 (G.U.R.I. 8.5.1991, n.106), convertito con modificazioni dalla legge 5 luglio 1991, n. 197 (G.U.R.I. 6.7.1991, n.157)
- Decreto legge 13 maggio 1991, n. 152 (G.U.R.I. 13.5.1991, n. 110), converito con modificazioni dall'art. 1, c.1 della legge 12 luglio 1991, n.203 (G.U.R.I. 12.7.1991, n.162)
- Decreto legge 8 giugno 1992, n. 306 (G.U.R.I. 8.6.1992, n.133), convertito con modificazioni dalla legge 7 agosto 1992, n. 356 (G.U.R.I. 7.8.1992, n. 185)
- Decreto del Presidente della Repubblica 27 giugno 1992, n. 352 (G.U.R.I. 29.7.1992, n.177)
- Decreto legislativo 29 dicembre 1992, n. 518 (G.U.R.I. 31.12.1992, n.306, S.O.)
- Decreto legislativo 3 febbraio 1993 n. 29 (G.U.R.I. 6.2.1993, n. 30, S.O.)
- Decreto legislativo 12 febbraio 1993, n. 39 (G.U.R.I. 20.2.1993, n. 42)
- Legge 23 dicembre 1993, n. 547 (G.U.R.I. 30.12.1993, n. 305)
- Legge 31 dicembre 1996, n. 675 (G.U.R.I. 8.1.1997, n. 5, S.O.)
- Legge 15 marzo 1997, n.59 (G.U.R.I. 17.3.1997, n. 63, S.O.)
- Legge 15 maggio 1997, n. 127 (G.U.R.I. 17.5.1997, n. 113, S.O.)
- Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (G.U.R.I. 13.3.1998, n. 60)
- Legge 16 giugno 1998, n.191 (G.U.R.I. 20.6.1998, n.142, S.O.)
- Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999 (G.U.R.I. 15.4.1999, n. 87)
- Decreto legislativo 6 maggio 1999, n.169 (G.U.R.I. 15.6.1999, n. 138)
- Decreto del Presidente della Repubblica 28 luglio 1999, n. 318 (G.U.R.I. 14.9.1999, n. 216)

- ISO-IS-7498-2: Information Processing Systems - Open Systems Interconnections - Basic Reference Model Part 2: Security Architecture.
- ISO/IEC 9594-8/ITU-T Recommendation X.509 "Information Technology - Open System Interconnection: The Directory Authentication Framework " 1997
- ISO-IS-15408: Information Technology - Security Techniques - Evaluation Criteria for IT Security (Common Criteria) - 1999

AIPA
Autorità per l'Informatica nella Pubblica Amministrazione

Linee Guida

per la definizione di un piano

per la Sicurezza

APPENDICE 1

NORMATIVA

Legge 22 aprile 1941, n. 633 p. 45

(Integrata dal D.Lgs. 29/12/92 n. 518 e dal D.Lgs. 6/5/99 n. 169)

Decreto legislativo 6 maggio 1999 n.169 p. 63

Legge 1 aprile 1981 n.121 p. 64

D.P.C.M. 15 febbraio 1989 p. 66

Legge 23 dicembre 1993 n. 547 p. 67

Questa appendice riporta un estratto di alcune delle disposizioni di legge in tema di sicurezza dei sistemi informativi automatizzati.
Sono state tralasciate le parti non rilevanti delle singole normative.

Un elenco più ampio delle disposizioni in materia è riportato nel capitolo 14.

Legge 22 aprile 1941 n. 633

Integrata dal D.Lgs. 29 dicembre 1992 n. 518 e dal D.Lgs. 6 maggio 1999 n. 169

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

TITOLO I
Disposizioni sul diritto d'autore

Capo I - Opere protette

1. Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione.
Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, nonché le banche di dati che per scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.

2. In particolare sono comprese nella protezione:
1) le opere letterarie, drammatiche, scientifiche, didattiche, religiose, tanto se in forma scritta quanto se orale;
2) le opere e le composizioni musicali, con o senza parole, le opere drammatico-musicali e le variazioni musicali costituenti di per sé opera originale;
3) le opere coreografiche e pantomimiche, delle quali sia fissata la traccia per iscritto o altrimenti;
4) le opere della scultura, della pittura, dell'arte del disegno, della incisione e delle arti figurative similari, compresa la scenografia, anche se applicata all'industria, sempreché il loro valore artistico sia scindibile dal carattere industriale del prodotto al quale sono associate;
5) i disegni e le opere dell'architettura;
6) le opere dell'arte cinematografica, muta o sonora, sempreché non si tratti di semplice documentazione protetta ai sensi delle norme del capo quinto del titolo secondo;
7) le opere fotografiche e quelle espresse con procedimento analogo a quello della fotografia sempre che non si tratti di semplice fotografia protetta ai sensi delle norme del capo V del titolo II;
8) i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore. Restano esclusi dalla tutela accordata dalla presente legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso.
9) Le banche di dati di cui al secondo comma dell'articolo 1, intese come raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche di dati non si estende al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto.

3. Le opere collettive, costituite dalla riunione di opere o di parti di opere, che hanno carattere di creazione autonoma, come risultato della scelta e del coordinamento ad un determinato fine letterario, scientifico, didattico, religioso, politico od artistico, quali le enciclopedie, i dizionari, le antologie, le riviste e i giornali, sono protette come opere originali indipendentemente e senza pregiudizio dei diritti di autore sulle opere o sulle parti di opere di cui sono composte.

4. Senza pregiudizio dei diritti esistenti sull'opera originaria, sono altresì protette le elaborazioni di carattere creativo dell'opera stessa, quali le traduzioni in altra lingua, le trasformazioni da una in altra forma letteraria od artistica, le modificazioni ed aggiunte che costituiscono un rifacimento sostanziale dell'opera originaria, gli adattamenti, le riduzioni, i compendi, le variazioni non costituenti opera originale.

5. Le disposizioni di questa legge non si applicano ai testi degli atti ufficiali dello Stato e delle Amministrazioni pubbliche, sia italiane che straniere.

Capo II - Soggetti del diritto

6. Il titolo originario dell'acquisto del diritto di autore è costituito dalla creazione dell'opera, quale particolare espressione del lavoro intellettuale.

7. È considerato autore dell'opera collettiva chi organizza e dirige la creazione dell'opera stessa.
È considerato autore delle elaborazioni l'elaboratore, nei limiti del suo lavoro.

8. È reputato autore dell'opera, salvo prova contraria, chi è in essa indicato come tale nelle forme d'uso, ovvero, è annunciato come tale nella recitazione, esecuzione, rappresentazione o radio-diffusione dell'opera stessa. Valgono come nome lo pseudonimo, il nome d'arte, la sigla o il segno convenzionale, che siano notoriamente conosciuti come equivalenti al nome vero .

9. Chi abbia rappresentato, eseguito o comunque pubblicato un'opera anonima, o pseudonima, è ammesso a far valere i diritti dell'autore, finché non sia rivelato. Questa disposizione non si applica allorché si tratti degli pseudonimi indicati nel secondo comma dell'articolo precedente.

10. Se l'opera è stata creata con il contributo indistinguibile ed inscindibile di più persone, il diritto di autore appartiene in comune a tutti i coautori.
Le parti indivise si presumono di valore eguale, salvo la prova per iscritto di diverso accordo.
Sono applicabili le disposizioni che regolano la comunione. La difesa del diritto morale può peraltro essere sempre esercitata individualmente da ciascun coautore e l'opera non può essere pubblicata, se inedita, né può essere modificata o utilizzata in forma diversa da quella della prima pubblicazione, senza l'accordo di tutti i coautori. Tuttavia in caso di ingiustificato rifiuto di uno o più coautori, la pubblicazione, la modificazione o la nuova utilizzazione dell'opera può essere autorizzata dall'autorità giudiziaria, alle condizioni e con le modalità da essa stabilite.

11. Alle amministrazioni dello Stato, alle Province ed ai Comuni, spetta il diritto di autore sulle opere create e pubblicate sotto il loro nome ed a loro conto e spese.
Lo stesso diritto spetta agli enti privati che non perseguano scopi di lucro, salvo diverso accordo con gli autori delle opere pubblicate, nonché alle accademie e agli altri enti pubblici culturali sulla raccolta dei loro atti e sulle loro pubblicazioni.

Capo III - Contenuto e durata del diritto di autore

Sezione I - Protezione della utilizzazione economica dell'opera

12. L'autore ha il diritto esclusivo di pubblicare l'opera.
Ha altresì il diritto esclusivo di utilizzare economicamente l'opera in ogni forma e modo originale, o derivato, nei limiti fissati da questa legge, ed in particolare con l'esercizio dei diritti esclusivi indicati negli articoli seguenti.
È considerata come prima pubblicazione la prima forma di esercizio del diritto di utilizzazione.

12-bis.1. Salvo patto contrario, il datore di lavoro è titolare del diritto esclusivo di utilizzazione economica del programma per elaboratore o della banca di dati creati dal lavoratore dipendente nell'esecuzione delle sue mansioni o su istruzioni impartite dallo stesso datore di lavoro .

13. Il diritto esclusivo di riprodurre ha per oggetto la moltiplicazione in copie dell'opera con qualsiasi mezzo, come la copiatura a mano, la stampa, la litografia, la incisione, la fotografia, la fonografia, la cinematografia ed ogni altro procedimento di riproduzione.

14. Il diritto esclusivo di trascrivere ha per oggetto l'uso dei mezzi atti a trasformare l'opera orale in opera scritta o riprodotta con uno dei mezzi indicati nell'articolo precedente.

15. Il diritto esclusivo di eseguire, rappresentare o recitare in pubblico ha per oggetto la esecuzione, la rappresentazione o la recitazione, comunque effettuate, sia gratuitamente che a pagamento, dell'opera musicale, del-

l'opera drammatica, dell'opera cinematografica, di qualsiasi altra opera di pubblico spettacolo e dell'opera orale. Non è considerata pubblica la esecuzione, rappresentazione o recitazione dell'opera entro la cerchia ordinaria della famiglia, del convitto, della scuola o dell'istituto di ricovero, purché non effettuata a scopo di lucro.

15 - bis.1. (omissis)
2. Con decreto del Presidente del Consiglio dei ministri da emanare ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentite le competenti Commissioni parlamentari, sono stabiliti i criteri e le modalità per l'individuazione delle circostanze soggettive ed oggettive che devono dar luogo alla applicazione della disposizione di cui al primo periodo del comma 1. In particolare occorre prescrivere:
a) l'accertamento dell'iscrizione da almeno due anni dei soggetti ivi indicati ai registri istituiti dall'articolo 6 della legge 11 agosto 1991, n. 266;
b) le modalità per l'identificazione della sede dei soggetti e per l'accertamento della quantità dei soci ed invitati, da contenere in un numero limitato e predeterminato;
c) che la condizione di socio sia conseguita in forma documentabile e con largo anticipo rispetto alla data della manifestazione di spettacolo;
d) la verifica che la manifestazione di spettacolo avvenga esclusivamente a titolo gratuito da parte degli artisti, interpreti o esecutori, ed a soli fini di solidarietà nell'esplicazione di finalità di volontariato.

16. 1. Il diritto esclusivo di diffondere ha per oggetto l'impiego di uno dei mezzi di diffusione a distanza, quali il telegrafo, il telefono, la radio, la televisione ed altri mezzi analoghi e comprende la comunicazione al pubblico via satellite e la ritrasmissione via cavo.

16-bis.1. Ai fini della presente legge si intende per:
a) satellite: qualsiasi satellite operante su bande di frequenza che, a norma della legislazione sulle telecomunicazioni, sono riservate alla trasmissione di segnali destinati alla ricezione diretta del pubblico o riservati alla comunicazione individuale privata purché la ricezione di questa avvenga in condizioni comparabili a quelle applicabili alla ricezione da parte del pubblico;
b) comunicazione al pubblico via satellite: l'atto di inserire sotto il controllo e la responsabilità dell'organismo di radiodiffusione operante sul territorio nazionale i segnali portatori di programmi destinati ad essere ricevuti dal pubblico in una sequenza ininterrotta di comunicazione diretta al satellite e poi a terra. Qualora i segnali portatori di programmi siano diffusi in forma codificata, vi è comunicazione al pubblico via satellite a condizione che i mezzi per la decodificazione della trasmissione siano messi a disposizione del pubblico a cura dell'organismo di radiodiffusione stesso o di terzi con il suo consenso. Qualora la comunicazione al pubblico via satellite abbia luogo nel territorio di uno stato non comunitario nel quale non esista il livello di protezione che per il detto sistema di comunicazione al pubblico stabilisce la presente legge:
1) se i segnali ascendenti portatori di programmi sono trasmessi al satellite da una stazione situata nel territorio nazionale, la comunicazione al pubblico via satellite si considera avvenuta in Italia. I diritti riconosciuti dalla presente legge, relativi alla radiodiffusione via satellite, sono esercitati nei confronti del soggetto che gestisce la stazione;
2) se i segnali ascendenti sono trasmessi da una stazione non situata in uno Stato membro dell'Unione europea, ma la comunicazione al pubblico via satellite avviene su incarico di un organismo di radiodiffusione situato in Italia, la comunicazione al pubblico si considera avvenuta nel territorio nazionale purché l'organismo di radiodiffusione vi abbia la sua sede principale. I diritti stabiliti dalla presente legge, relativi alla radiodiffusione via satellite, sono esercitati nei confronti del soggetto che gestisce l'organismo di radiodiffusione;
c) ritrasmissione via cavo: la ritrasmissione simultanea, invariata ed integrale, per il tramite di un sistema di ridistribuzione via cavo o su frequenze molto elevate, destinata al pubblico, di un'emissione primaria radiofonica o televisiva comunque diffusa, proveniente da un altro Stato membro dell'Unione europea e destinata alla ricezione del pubblico.

17.1. Il diritto esclusivo di distribuzione ha per oggetto il diritto di mettere in commercio, di porre in circolazione o comunque a disposizione del pubblico, con qualsiasi mezzo ed a qualsiasi titolo, l'opera o gli esemplari di essa e comprende, altresì, il diritto esclusivo di introdurre, a fini di distribuzione, nel territorio degli

Stati dell'Unione europea le riproduzioni fatte negli Stati extracomunitari.
2. Non costituisce esercizio del diritto esclusivo di distribuzione la consegna gratuita, effettuata o consentita dal titolare di esemplari delle opere a fini promozionali ovvero a fini di insegnamento o di ricerca scientifica.

18. Il diritto esclusivo di tradurre ha per oggetto tutte le forme di modificazione, di elaborazione e di trasformazione dell'opera previste nell'art. 4.
L'autore ha altresì il diritto di pubblicare le sue opere in raccolta. Ha infine il diritto esclusivo di introdurre nell'opera qualsiasi modificazione.

18-bis. 1. Il diritto esclusivo di noleggiare ha per oggetto la cessione in uso degli originali, di copie o di supporti di opere, tutelate dal diritto d'autore, fatta per un periodo limitato di tempo ed ai fini del conseguimento di un beneficio economico o commerciale diretto o indiretto.
2. Il diritto esclusivo di dare in prestito ha per oggetto la cessione in uso degli originali, di copie o di supporti di opere, tutelate dal diritto d'autore, fatta da istituzioni aperte al pubblico, per un periodo di tempo limitato, a fini diversi da quelli di cui al comma 1.
3. L'autore ha il potere esclusivo di autorizzare il noleggio o il prestito da parte di terzi.
4. I suddetti diritti e poteri non si esauriscono con la vendita o con la distribuzione in qualsiasi forma degli originali, di copie o di supporti delle opere.
5. L'autore, anche in caso di cessione del diritto di noleggio ad un produttore di fonogrammi o di opere cinematografiche o audiovisive o sequenze di immagini in movimento, conserva il diritto di ottenere un'equa remunerazione per il noleggio da questi a sua volta concluso con terzi. Ogni patto contrario è nullo. In difetto di accordo da concludersi tra le categorie interessate quali individuate dall'articolo 16, primo comma, del regolamento, detto compenso è stabilito con la procedura di cui all'articolo 4 del decreto legislativo luogotenenziale 20 luglio 1945, n. 440 .
6. I commi da 1 a 4 non si applicano in relazione a progetti o disegni di edifici e ad opere di arte applicata.

19. I diritti esclusivi previsti dagli articoli precedenti sono fra loro indipendenti.
L'esercizio di uno di essi non esclude l'esercizio esclusivo di ciascuno degli altri diritti.
Essi hanno per oggetto l'opera nel suo insieme ed in ciascuna delle sue parti .

Sezione II - Protezione dei diritti sull'opera a difesa della personalità dell'autore (Diritto morale dell'autore)

20. Indipendentemente dai diritti esclusivi di utilizzazione economica dell'opera, previsti nelle disposizioni della sezione precedente, ed anche dopo la cessione dei diritti stessi, l'autore conserva il diritto di rivendicare la paternità dell'opera e di opporsi a qualsiasi deformazione, mutilazione od altra modificazione, ed a ogni atto a danno dell'opera stessa, che possano essere di pregiudizio al suo onore o alla sua reputazione .

(omissis)

21. L'autore di un'opera anonima e pseudonima ha sempre il diritto di rivelarsi e di far conoscere in giudizio la sua qualità di autore. Nonostante qualunque precedente patto contrario, gli aventi causa dell'autore che si sia rivelato ne dovranno indicare il nome nelle pubblicazioni, riproduzioni, trascrizioni, esecuzioni, rappresentazioni, recitazioni e diffusioni o in qualsiasi altra forma di manifestazione o annuncio al pubblico.

22. I diritti indicati nei precedenti articoli sono inalienabili.
Tuttavia l'autore che abbia conosciute ed accettate le modificazioni della propria opera non è più ammesso ad agire per impedirne l'esecuzione o per chiederne la soppressione.

23. Dopo la morte dell'autore il diritto previsto nell'art. 20 può essere fatto valere, senza limite di tempo, dal coniuge e dai figli, e, in loro mancanza, dai genitori e dagli altri ascendenti e dai discendenti diretti; mancando gli ascendenti ed i discendenti, dai fratelli e dalle sorelle e dai loro discendenti.

(omissis)

24. Il diritto di pubblicare le opere inedite spetta agli eredi dell'autore o ai legatari delle opere stesse, salvo che l'autore abbia espressamente vietata la pubblicazione o l'abbia affidata ad altri.
Qualora l'autore abbia fissato un termine per la pubblicazione, le opere inedite non possono essere pubblicate prima della sua scadenza.
Quando le persone indicate nel primo comma siano più e vi sia tra loro dissenso, decide l'autorità giudiziaria, sentito il Pubblico Ministero. È rispettata, in ogni caso, la volontà del defunto, quando risulti da scritto.
Sono applicabili a queste opere le disposizioni contenute nella sezione seconda del capo secondo del titolo terzo.

Sezione III - Durata dei diritti di utilizzazione economica dell'opera

25. I diritti di utilizzazione economica dell'opera durano tutta la vita dell'autore e sino al termine del cinquantesimo anno solare dopo la sua morte.

26. Nelle opere indicate nell'art. 10, nonché in quelle drammatico-musicali, coreografiche e pantomimiche, la durata dei diritti di utilizzazione economica spettanti a ciascuno dei coautori o dei collaboratori si determina sulla vita del coautore che muore per ultimo.
Nelle opere collettive la durata dei diritti di utilizzazione economica spettante ad ogni collaboratore, si determina sulla vita di ciascuno. La durata dei diritti di utilizzazione economica dell'opera come un tutto è di cinquant'anni dalla prima pubblicazione, qualunque sia la forma nella quale la pubblicazione è stata effettuata, salve le disposizioni dell'art. 3, per le riviste, i giornali e le altre opere periodiche.

27. Nelle opere anonime o pseudonime, fuori del caso previsto nel capoverso dell'art. 8, la durata dei diritti di utilizzazione economica è di cinquant'anni a partire dalla prima pubblicazione, qualunque sia la forma nella quale essa è stata effettuata.
Se prima della scadenza di detto termine l'autore si è rivelato o la rivelazione è fatta dalle persone indicate dall'art. 23 o da persone autorizzate dall'autore, nelle forme stabilite dall'articolo seguente, si applica il termine di durata determinato nell'art. 25 .

27-bis. (omissis)

28. Per acquistare il beneficio della durata normale dei diritti esclusivi di utilizzazione economica, la rivelazione deve essere fatta mediante denuncia all'ufficio della proprietà letteraria, scientifica ed artistica presso il Ministero della cultura popolare , secondo le disposizioni stabilite nel regolamento.
La denuncia di rivelazione è pubblicata nelle forme stabilite da dette disposizioni ed ha effetto, a partire dalla data del deposito della denuncia, di fronte ai terzi che abbiano acquistati diritti sull'opera come anonima o pseudonima.

29. La durata dei diritti esclusivi di utilizzazione economica spettanti, a termini dell'art. 11, alle amministrazioni dello Stato, alle Province, ai Comuni, alle accademie, agli enti pubblici culturali nonché agli enti privati che non perseguano scopi di lucro, è di vent'anni a partire dalla prima pubblicazione, qualunque sia la forma nella quale la pubblicazione è stata effettuata. Per le comunicazioni e le memorie pubblicate dalle accademie e dagli altri enti pubblici culturali, tale durata è ridotta a due anni, trascorsi i quali, l'autore riprende integralmente la libera disponibilità dei suoi scritti.

30. Quando le parti o i volumi di una stessa opera siano pubblicati separatamente, in tempi diversi, la durata dei diritti di utilizzazione economica, che sia fissata ad anni, decorre per ciascuna parte o per ciascun volume dall'anno di pubblicazione. Le frazioni di anno giovano all'autore.
Se si tratta di opera collettiva, periodica, quale la rivista o il giornale, la durata dei diritti è calcolata egualmente a partire dalla fine di ogni anno dalla pubblicazione dei singoli fascicoli o numeri.

31. Nelle opere pubblicate per la prima volta dopo la morte dell'autore, che non ricadono nella previsione dell'articolo 85-ter, la durata dei diritti esclusivi di utilizzazione economica è di settant'anni a partire dalla morte dell'autore .

32. Fermo restando quanto stabilito dall'articolo 44, i diritti di utilizzazione economica dell'opera cinematografica o assimilata durano sino al termine del settantesimo anno dopo la morte dell'ultima persona sopravvissuta fra le seguenti persone: il direttore artistico, gli autori della sceneggiatura, ivi compreso l'autore del dialogo, e l'autore della musica specificamente creata per essere utilizzata nell'opera cinematografica o assimilata.

32-bis. I diritti di utilizzazione economica dell'opera fotografica durano sino al termine del settantesimo anno dopo la morte dell'autore.

32-ter. I termini finali di durata dei diritti di utilizzazione economica previsti dalle disposizioni della presente sezione si computano, nei rispettivi casi, a decorrere dal 1° gennaio dell'anno successivo a quello in cui si verifica la morte dell'autore o altro evento considerato dalla norma.

Capo IV - Norme particolari ai diritti di utilizzazione economica di talune categorie di opere

Sezione I - Opere drammatico-musicali, composizioni con parole, opere coreografiche e pantomimiche.

(omissis)

Sezione II - Opere collettive, riviste e giornali

38. Nell'opera collettiva, salvo patto in contrario, il diritto di utilizzazione economica spetta all'editore dell'opera stessa, senza pregiudizio del diritto derivante dall'applicazione dell'art. 7.
Ai singoli collaboratori dell'opera collettiva è riservato il diritto di utilizzare la propria opera separatamente, con la osservanza dei patti convenuti e, in difetto, delle norme seguenti.

39. Se un articolo è inviato alla rivista o giornale, per essere riprodotto, da persona estranea alla redazione del giornale o della rivista e senza precedenti accordi contrattuali, l'autore riprende il diritto di disporre liberamente quando non abbia ricevuto notizia dell'accettazione nel termine di un mese dall'invio o quando la riproduzione non avvenga nel termine di sei mesi dalla notizia dell'accettazione.
Trattandosi di articolo fornito da un redattore, il direttore della rivista o giornale ne può differire la produzione anche al di là dei termini indicati nel comma precedente. Decorso però il termine di sei mesi dalla consegna del manoscritto, l'autore può utilizzare l'articolo per riprodurlo in volume o per estratto separato, se si tratta di giornale, ed anche in altro periodico, se si tratta di rivista.

40. Il collaboratore di opera collettiva che non sia rivista o giornale ha diritto, salvo patto contrario, che il suo nome figuri nella riproduzione della sua opera nelle forme d'uso.Nei giornali questo diritto non compete, salvo patto contrario, al personale della redazione.

41. Senza pregiudizio della applicazione della disposizione contenuta nell'art. 20, il direttore del giornale ha diritto, salvo patto contrario, di introdurre nell'articolo da riprodurre quelle modificazioni di forma che sono richieste dalla natura e dai fini del giornale.
Negli articoli da riprodursi senza indicazione del nome dell'autore, questa facoltà si estende alla soppressione o riduzione di parti di detto articolo.

42. L'autore dell'articolo, o altra opera, che sia stato riprodotto in un'opera collettiva ha diritto di riprodurlo in estratti separati o raccolti in volume, purché indichi l'opera collettiva dalla quale è tratto e la data di pubblicazione.
Trattandosi di articoli apparsi in riviste o giornali, l'autore, salvo patto contrario, ha altresì il diritto di riprodurli in altre riviste o giornali.

43. L'editore o direttore della rivista o del giornale non ha obbligo di conservare o di restituire i manoscritti degli articoli non riprodotti, che gli siano pervenuti senza sua richiesta.

Sezione III - Opere cinematografiche

(omissis)

Sezione IV - Opere radiodiffuse

(omissis)

Sezione V - Opere registrate su apparecchi meccanici

61. L'autore ha il diritto esclusivo, ai sensi delle disposizioni contenute nella sezione prima del capo terzo di questo titolo:
1) di adattare e di registrare l'opera sopra il disco fonografico, la pellicola cinematografica, il nastro metallico o sopra altra analoga materia o apparecchio meccanico riproduttore di suoni o di voci;
2) di riprodurre, di distribuire, di noleggiare, di dare in prestito, nonché il potere esclusivo di autorizzare il noleggio ed il prestito degli esemplari dell'opera così adattata o registrata ;
3) di eseguire pubblicamente e di radiodiffondere l'opera mediante l'impiego del disco o altro istrumento meccanico sopraindicato, nonché di autorizzarne la comunicazione al pubblico via satellite e la ritrasmissione via cavo .
La cessione del diritto di riproduzione o del diritto di distribuzione non comprende, salvo patto contrario, la cessione del diritto di esecuzione pubblica o di radiodiffusione, nonché l'autorizzazione alla comunicazione al pubblico via satellite o alla ritrasmissione via cavo. Per quanto riguarda la radiodiffusione, il diritto di autore resta regolato dalle norme contenute nella precedente sezione.

62. Gli esemplari del disco fonografico o di altro analogo apparecchio riproduttore di suoni o di voci, nel quale l'opera dell'ingegno è stata registrata, non possono essere messi in commercio se non portino stabilmente apposte, sul disco o apparecchio, le indicazioni seguenti:
1) titolo dell'opera riprodotta;
2) nome dell'autore;
3) nome dell'artista interprete od esecutore. I complessi orchestrali o corali sono indicati col nome d'uso;
4) data della fabbricazione.

63. Il disco o altro apparecchio analogo devono essere fabbricati od utilizzati in modo che venga rispettato il diritto morale dell'autore, ai termini degli artt. 20 e 21 di questa legge.
Si considerano lecite le modificazioni dell'opera richieste dalle necessità tecniche della registrazione.

(omissis)

Sezione VI - Programmi per elaboratore

64-bis. 1. Fatte salve le disposizioni dei successivi articoli 64-ter e 64-quater, i diritti esclusivi conferiti dalla presente legge sui programmi per elaboratore comprendono il diritto di effettuare o autorizzare:
a) la riproduzione, permanente o temporanea, totale o parziale, del programma per elaboratore con qualsiasi mezzo o in qualsiasi forma. Nella misura in cui operazioni quali il caricamento, la visualizzazione, l'esecuzione, la trasmissione o la memorizzazione del programma per elaboratore richiedano una riproduzione, anche tali operazioni sono soggette all'autorizzazione del titolare dei diritti;
b) la traduzione, l'adattamento, la trasformazione e ogni altra modificazione del programma per elaboratore, nonché la riproduzione dell'opera che ne risulti, senza pregiudizio dei diritti di chi modifica il programma;
c) qualsiasi forma di distribuzione al pubblico, compresa la locazione, del programma per elaboratore originale o di copie dello stesso. La prima vendita di una copia del programma nella Comunità Economica Europea da parte del titolare dei diritti, o con il suo consenso, esaurisce il diritto di distribuzione di detta copia all'interno della Comunità, ad eccezione del diritto di controllare l'ulteriore locazione del programma o di una copia dello stesso .

64-ter. 1.Salvo patto contrario, non sono soggette all'autorizzazione del titolare dei diritti le attività indicate nell'art. 64-bis, lettere a) e b), allorché tali attività sono necessarie per l'uso del programma per elaboratore conformemente alla sua destinazione da parte del legittimo acquirente, inclusa la correzione degli errori.
2. Non può essere impedito per contratto, a chi ha il diritto di usare una copia del programma per elaboratore di effettuare una copia di riserva del programma, qualora tale copia sia necessaria per l'uso.
3. Chi ha il diritto di usare una copia del programma per elaboratore può, senza l'autorizzazione del titolare

dei diritti, osservare, studiare o sottoporre a prova il funzionamento del programma, allo scopo di determinare le idee ed i princìpi su cui è basato ogni elemento del programma stesso, qualora egli compia tali atti durante operazioni di caricamento, visualizzazione, esecuzione, trasmissione o memorizzazione del programma che egli ha il diritto di eseguire. Le clausole contrattuali pattuite in violazione del presente comma e del comma 2 sono nulle .

64-quater. 1. L'autorizzazione del titolare dei diritti non è richiesta qualora la riproduzione del codice del programma di elaboratore e la traduzione della sua forma ai sensi dell'art. 64-bis, lettere a) e b), compiute al fine di modificare la forma del codice, siano indispensabili per ottenere le informazioni necessarie per conseguire l'interoperabilità, con altri programmi, di un programma per elaboratore creato autonomamente purché siano soddisfatte le seguenti condizioni:
a) le predette attività siano eseguite dal licenziatario o da altri che abbia il diritto di usare una copia del programma oppure, per loro conto, da chi è autorizzato a tal fine;
b) le informazioni necessarie per conseguire l'interoperabilità non siano già facilmente e rapidamente accessibili ai soggetti indicati alla lettera a);
c) le predette attività siano limitate alle parti del programma originale necessarie per conseguire l'interoperabilità.
2. Le disposizioni di cui al comma 1 non consentono che le informazioni ottenute in virtù della loro applicazione:
a) siano utilizzate a fini diversi dal conseguimento dell'interoperabilità del programma creato autonomamente;
b) siano comunicate a terzi, fatta salva la necessità di consentire l'interoperabilità del programma creato autonomamente;
c) siano utilizzate per lo sviluppo, la produzione o la commercializzazione di un programma per elaboratore sostanzialmente simile nella sua forma espressiva, o per ogni altra attività che violi il diritto di autore.
3. Le clausole contrattuali pattuite in violazione dei commi 1 e 2 sono nulle .
4. Conformemente alla convenzione di Berna sulla tutela delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, le disposizioni del presente articolo non possono essere interpretate in modo da consentire che la loro applicazione arrechi indebitamente pregiudizio agli interessi legittimi del titolare dei diritti o sia in conflitto con il normale sfruttamento del programma .

Sezione VII - Banche di dati

64-quinquies. 1. L'autore di un banca di dati ha il diritto esclusivo di eseguire o autorizzare:
a) la riproduzione permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsiasi forma;
b) la traduzione, l'adattamento, una diversa disposizione e ogni altra modifica;
c) qualsiasi forma di distribuzione al pubblico dell'originale o di copie della banca di dati; la prima vendita di una copia nel territorio dell'Unione europea da parte del titolare del diritto o con il suo consenso esaurisce il diritto di controllare, all'interno dell'Unione stessa, le vendite successive della copia;
d) qualsiasi presentazione, dimostrazione o comunicazione in pubblico, ivi compresa la trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma;
e) qualsiasi riproduzione, distribuzione, comunicazione, presentazione o dimostrazione in pubblico dei risultati delle operazioni di cui alla lettera b).

64-sexies. 1. Non sono soggetti all'autorizzazione di cui all'articolo 64-quinquies da parte del titolare del diritto:
a) l'accesso o la consultazione della banca di dati quando abbiano esclusivamente finalità didattiche o di ricerca scientifica, non svolta nell'ambito di un'impresa, purché si indichi la fonte e nei limiti di quanto giustificato dallo scopo non commerciale perseguito. Nell'ambito di tali attività di accesso e consultazione, le eventuali operazioni di riproduzione permanente della totalità o di parte sostanziale del contenuto su altro supporto sono comunque soggette all'autorizzazione del titolare del diritto;
b) l'impiego di una banca di dati per fini di sicurezza pubblica o per effetto di una procedura amministrativa o giurisdizionale.
2. Non sono soggette all'autorizzazione dell'autore le attività indicate nell'articolo 64-quinquies poste in essere da parte dell'utente legittimo della banca di dati o di una sua copia, se tali attività sono necessarie per

l'accesso al contenuto della stessa banca di dati e per il suo normale impiego; se l'utente legittimo è autorizzato ad utilizzare solo una parte della banca di dati, il presente comma si applica unicamente a tale parte.
3. Le clausole contrattuali pattuite in violazione del comma 2 sono nulle ai sensi dell'articolo 1418 del codice civile.
4. Conformemente alla Convenzione di Berna per la protezione delle opere letterarie e artistiche, ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, le disposizioni di cui ai commi 1 e 2 non possono essere interpretate in modo da consentire che la loro applicazione arrechi indebitamente pregiudizio al titolare del diritto o entri in conflitto con il normale impiego della banca di dati.

Capo V - Utilizzazioni libere

65. Gli articoli di attualità, di carattere economico, politico, religioso, pubblicati nelle riviste o giornali, possono essere liberamente riprodotti in altre riviste o giornali, anche radiofonici, se la riproduzione non è stata espressamente riservata, purché si indichino la rivista o il giornale da cui sono tratti, la data e il numero di detta rivista o giornale e il nome dell'autore, se l'articolo è firmato.

66. I discorsi sopra argomenti di interesse politico od amministrativo, tenuti in pubbliche assemblee o comunque in pubblico, possono essere liberamente riprodotti nelle riviste o giornali, anche radiofonici, purché si indichino la fonte, il nome dell'autore e la data e luogo in cui il discorso fu tenuto.

67. Opere o brani di opere possono essere riprodotti nelle procedure giudiziarie od amministrative ai fini del giudizio, purché si indichino la fonte o il nome dell'autore.

68. È libera la riproduzione di singole opere o brani di opere per uso personale dei lettori, fatta a mano con mezzi di riproduzione non idonei a spaccio o diffusione dell'opera nel pubblico.
È libera la fotocopia di opere esistenti nelle biblioteche, fatta per uso personale o per i servizi della biblioteca.
È vietato lo spaccio di dette copie nel pubblico e, in genere ogni utilizzazione di concorrenza con i diritti di utilizzazione economica spettanti all'autore .

(omissis)

TITOLO II

Capo I - Diritti relativi alla produzione di dischi fonografici e di apparecchi analoghi

(omissis)

Capo I-bis - Diritti dei produttori di opere cinematografiche o audiovisive o seguenze di immagini in movimento

(omissis)

Capo II - Diritti relativi all'emissione radiofonica e televisiva

(omissis)

Capo III - Diritti degli artisti interpreti e degli artisti esecutori

(omissis)

Capo III-bis - Diritti relativi ad opere pubblicate o comunicate al pubblico per la prima volta successivamente alla estinzione dei diritti patrimoniali d'autore

(omissis)

Capo III-ter - Diritti relativi ad edizioni critiche e scientifiche di opere di pubblico dominio

(omissis)

Capo IV - Diritti relativi a bozzetti di scene teatrali

(omissis)

Capo V - Diritti relativi alle fotografie

87. Sono considerate fotografie, ai fini dell'applicazione delle disposizioni di questo capo, le immagini di persone o di aspetti, elementi o fatti della vita naturale e sociale, ottenute col processo fotografico o con processo analogo, comprese le riproduzioni di opere dell'arte figurativa e i fotogrammi delle pellicole cinematografiche.
Non sono comprese le fotografie di scritti, documenti, carte di affari, oggetti materiali, disegni tecnici e prodotti simili.

88. Spetta al fotografo il diritto esclusivo di riproduzione, diffusione e spaccio della fotografia, salve le disposizioni stabilite dalla sezione seconda del capo sesto di questo titolo, per ciò che riguarda il ritratto e senza pregiudizio, riguardo alle fotografie riproducenti opere dell'arte figurativa, dei diritti di autore sulla opera riprodotta.
Tuttavia se l'opera è stata ottenuta nel corso e nell'adempimento di un contratto di impiego o di lavoro, entro i limiti dell'oggetto e delle finalità del contratto, il diritto esclusivo compete al datore di lavoro. La stessa norma si applica, salvo patto contrario, a favore del committente quando si tratti di fotografia di cose in possesso del committente medesimo e salvo pagamento a favore del fotografo, da parte di chi utilizza commercialmente la riproduzione, di un equo corrispettivo.
(omissis)

89. La cessione del negativo o di analogo mezzo di riproduzione della fotografia comprende, salvo patto contrario, la cessione dei diritti previsti nell'articolo precedente, sempreché tali diritti spettino al cedente.

90. Gli esemplari della fotografia devono portare le seguenti indicazioni:
1) il nome del fotografo, o, nel caso previsto nel primo capoverso dell'art. 88, della ditta da cui il fotografo dipende o del committente;
2) la data dell'anno di produzione della fotografia;
3) il nome dell'autore dell'opera d'arte fotografata.
Qualora gli esemplari non portino le suddette indicazioni, la loro riproduzione non è considerata abusiva e non sono dovuti i compensi indicati agli artt. 91 e 98 a meno che il fotografo non provi la mala fede del riproduttore.

91. a riproduzione di fotografie nelle antologie ad uso scolastico ed in generale nelle opere scientifiche o didattiche è lecita, contro pagamento di un equo compenso, che è determinato nelle forme previste dal regolamento. Nella riproduzione deve indicarsi il nome del fotografo e la data dell'anno della fabbricazione, se risultano dalla fotografia riprodotta.
La riproduzione di fotografie pubblicate su giornali od altri periodici, concernenti persone o fatti di attualità od aventi, comunque, pubblico interesse, è lecita contro pagamento di un equo compenso.
Sono applicabili le disposizioni dell'ultimo comma dell'art. 88

92. Il diritto esclusivo sulle fotografie dura vent'anni dalla produzione della fotografia.

Capo VI - Diritti relativi alla corrispondenza epistolare ed al ritratto

Sezione I - Diritti relativi alle corrispondenze epistolari

93. Le corrispondenze epistolari, gli epistolari, le memorie familiari e personali e gli altri scritti della medesima natura, allorché abbiano carattere confidenziale o si riferiscano alla intimità della vita privata, non possono essere pubblicati, riprodotti od in qualunque modo portati alla conoscenza del pubblico senza il consenso dell'autore, e, trattandosi di corrispondenze epistolari e di epistolari, anche del destinatario .

Dopo la morte dell'autore o del destinatario occorre il consenso del coniuge o dei figli, o, in loro mancanza, dei genitori; mancando il coniuge, i figli e i genitori, dei fratelli e delle sorelle, e, in loro mancanza, degli ascendenti e dei discendenti fino al quarto grado. Quando le persone indicate nel comma precedente siano più e vi sia tra loro dissenso, decide l'autorità giudiziaria, sentito il Pubblico Ministero. È rispettata, in ogni caso, la volontà del defunto quando risulti da scritto.

94. Il consenso indicato all'articolo precedente non è necessario quando la conoscenza dello scritto è richiesta ai fini di un giudizio civile o penale o per esigenza di difesa dell'onore o della reputazione personale o familiare.

95. Le disposizioni degli articoli precedenti si applicano anche alle corrispondenze epistolari che costituiscono opere tutelate dal diritto di autore ed anche se cadute in dominio pubblico. Non si applicano agli atti e corrispondenze ufficiali o agli altri atti e corrispondenze che presentano interesse di Stato.

(omissis)

Capo VII - Diritti relativi ai progetti di lavori dell'ingegneria

99. All'autore di progetti di lavori di ingegneria, o di altri lavori analoghi, che costituiscano soluzioni originali di problemi tecnici, compete, oltre al diritto esclusivo di riproduzione dei piani e disegni dei progetti medesimi, il diritto ad un equo compenso a carico di coloro che realizzano il progetto tecnico a scopo di lucro senza il suo consenso.
(omissis)

Capo VIII - Protezione del titolo, delle rubriche, dell'aspetto esterno dell'opera, degli articoli e di notizie - Divieto di taluni atti di concorrenza sleale

100. Il titolo dell'opera, quando individui l'opera stessa, non può essere riprodotto sopra altra opera senza il consenso dell'autore.
Il divieto non si estende ad opere che siano di specie o carattere così diverso da risultare esclusa ogni possibilità di confusione.
È vietata egualmente, nelle stesse condizioni, la riproduzione delle rubriche che siano adoperate nella pubblicazione periodica in modo così costante da individuare l'abituale e caratteristico contenuto della rubrica.
Il titolo del giornale, delle riviste o di altre pubblicazioni periodiche non può essere riprodotto in altre opere della stessa specie o carattere, se non siano decorsi due anni da quando è cessata la pubblicazione del giornale.

101. La riproduzione di informazioni e notizie è lecita purché non sia effettuata con l'impiego di atti contrari agli usi onesti in materia giornalistica e purché se ne citi la fonte.
Sono considerati atti illeciti:
a) la riproduzione o la radiodiffusione, senza autorizzazione, dei bollettini di informazioni distribuiti dalle agenzie giornalistiche o di informazioni, prima che siano trascorse sedici ore dalla diramazione del bollettino stesso e, comunque, prima della loro pubblicazione in un giornale o altro periodico che ne abbia ricevuto la facoltà da parte dell'agenzia. A tal fine, affinché le agenzie abbiano azione contro coloro che li abbiano illecitamente utilizzati, occorre che i bollettini siano muniti dell'esatta indicazione del giorno e dell'ora di diramazione;
b) la riproduzione sistematica di informazioni o notizie, pubblicate o radiodiffuse, a fine di lucro, sia da parte di giornali o altri periodici, sia da parte di imprese di radiodiffusione.

102. È vietata come atto di concorrenza sleale, la riproduzione o imitazione sopra altre opere della medesima specie, delle testate, degli emblemi, dei fregi, delle disposizioni di segni o caratteri di stampa e di ogni altra particolarità di forma o di colore nell'aspetto esterno dell'opera dell'ingegno, quando detta riproduzione o imitazione sia atta a creare confusione di opera o di autore.

TITOLO II - bis
Disposizioni sui diritti del costitutore di una banca di dati
Diritti e obblighi dell'utente

Capo I - Diritti del costitutore di una banca di dati

102-bis. 1. Ai fini del presente titolo si intende per:

a) costitutore di una banca di dati: chi effettua investimenti rilevanti per la costituzione di una banca di dati o per la sua verifica o la sua presentazione, impegnando, a tal fine, mezzi finanziari, tempo o lavoro;

b) estrazione: il trasferimento permanente o temporaneo della totalità o di una parte sostanziale del contenuto di una banca di dati su un altro supporto con qualsiasi mezzo o in qualsivoglia forma. L'attività di prestito dei soggetti di cui all'articolo 69, comma 1, non costituisce atto di estrazione;

c) reimpiego: qualsivoglia forma di messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto della banca di dati mediante distribuzione di copie, noleggio, trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma. L'attività di prestito dei soggetti di cui all'articolo 69, comma 1, non costituisce atto di reimpiego.

2. La prima vendita di una copia della banca di dati effettuata o consentita dal titolare in uno Stato membro dell'Unione europea esaurisce il diritto di controllare la rivendita della copia nel territorio dell'Unione europea.

3. Indipendentemente dalla tutelabilità della banca di dati a norma del diritto d'autore o di altri diritti e senza pregiudizio dei diritti sul contenuto o parti di esso, il costitutore di una banca di dati ha il diritto, per la durata e alle condizioni stabilite dal presente Capo, di vietare le operazioni di estrazione ovvero reimpiego della totalità o di una parte sostanziale della stessa.

4. Il diritto di cui al comma 3 si applica alle banche di dati i cui costitutori o titolari di diritti sono cittadini di uno Stato membro dell'Unione europea o residenti abituali nel territorio dell'Unione europea.

5. La disposizione di cui al comma 3 si applica altresì alle imprese e società costituite secondo la normativa di uno Stato membro dell'Unione europea ed aventi la sede sociale, l'amministrazione centrale o il centro d'attività principale all'interno della Unione europea; tuttavia, qualora la società o l'impresa abbia all'interno della Unione europea soltanto la propria sede sociale, deve sussistere un legame effettivo e continuo tra l'attività della medesima e l'economia di uno degli Stati membri dell'Unione europea.

6. Il diritto esclusivo del costitutore sorge al momento del completamento della banca di dati e si estingue trascorsi quindici anni dal 1° gennaio dell'anno successivo alla data del completamento stesso.

7. Per le banche di dati in qualunque modo messe a disposizione del pubblico prima dello scadere del periodo di cui al comma 6, il diritto di cui allo stesso comma 6 si estingue trascorsi quindici anni dal 1° gennaio dell'anno successivo alla data della prima messa a disposizione del pubblico.

8. Se vengono apportate al contenuto della banca di dati modifiche o integrazioni sostanziali comportanti nuovi investimenti rilevanti ai sensi del comma 1, lettera a), dal momento del completamento o della prima messa a disposizione del pubblico della banca di dati così modificata o integrata, e come tale espressamente identificata, decorre un autonomo termine di durata della protezione, pari a quello di cui ai commi 6 e 7.

9. Non sono consentiti l'estrazione o il reimpiego ripetuti e sistematici di parti non sostanziali del contenuto della banca di dati, qualora presuppongano operazioni contrarie alla normale gestione della banca di dati o arrechino un pregiudizio ingiustificato al costitutore della banca di dati.

10. Il diritto di cui al comma 3 può essere acquistato o trasmesso in tutti i modi e forme consentiti dalla legge.

Capo II - Diritti e obblighi dell'utente

102-ter. 1. L'utente legittimo della banca di dati messa a disposizione del pubblico non può arrecare pregiudizio al titolare del diritto d'autore o di un altro diritto connesso relativo ad opere o prestazioni contenute in tale banca.

2. L'utente legittimo di una banca di dati messa in qualsiasi modo a disposizione del pubblico non può eseguire operazioni che siano in contrasto con la normale gestione della banca di dati o che arrechino un ingiustificato pregiudizio al costitutore della banca di dati.

3. Non sono soggette all'autorizzazione del costitutore della banca di dati messa per qualsiasi motivo a disposizione del pubblico le attività di estrazione o reimpiego di parti non sostanziali, valutate in termini qualitativi

e quantitativi, del contenuto della banca di dati per qualsivoglia fine effettuate dall'utente legittimo. Se l'utente legittimo è autorizzato ad effettuare l'estrazione o il reimpiego solo di una parte della banca di dati, il presente comma si applica unicamente a tale parte.
4. Le clausole contrattuali pattuite in violazione dei commi 1, 2 e 3 sono nulle.

TITOLO III
Disposizioni comuni

Capo I - Registri di pubblicità e deposito delle opere

103. È istituito presso il Ministero della cultura popolare[1] un registro pubblico generale delle opere protette ai sensi di questa legge.
L'Ente italiano per il diritto di autore[2] cura la tenuta di un registro pubblico speciale per le opere cinematografiche.
In detti registri sono registrate le opere soggette all'obbligo del deposito con la indicazione del nome dell'autore, del produttore, della data della pubblicazione e con le altre indicazioni stabilite dal regolamento.
Alla Società italiana degli autori ed editori è affidata, altresì, la tenuta di un registro pubblico speciale per i programmi per elaboratore. In tale registro viene registrato il nome del titolare dei diritti esclusivi di utilizzazione economica e la data di pubblicazione del programma, intendendosi per pubblicazione il primo atto di esercizio dei diritti esclusivi.
La registrazione fa fede, sino a prova contraria, della esistenza dell'opera e del fatto della sua pubblicazione.
Gli autori e i produttori indicati nel registro sono reputati, sino a prova contraria, autori o produttori delle opere che sono loro attribuite. Per le opere cinematografiche la presunzione si applica alle annotazioni del registro indicato nel secondo comma.
La tenuta dei registri di pubblicità è disciplinata nel regolamento.
I registri di cui al presente articolo possono essere tenuti utilizzando mezzi e strumenti informatici.

104. (omissis)

105. Gli autori e i produttori delle opere e dei prodotti protetti ai sensi di questa legge o i loro aventi causa devono depositare presso il Ministero della cultura popolare[1] un esemplare o copia della opera o del prodotto, nei termini e nelle forme stabilite dal regolamento.
Qualora si tratti di opera drammatico-musicale o sinfonica di cui non sia stampata la partitura d'orchestra, basterà una copia o un esemplare della riduzione per canto e pianoforte o per pianoforte solo.
Per i programmi per elaboratore la registrazione è facoltativa ed onerosa.
Per le fotografie è escluso l'obbligo del deposito, salvo il disposto del secondo comma dell'art. 92.

106. (omissis)

Capo II - Trasmissione dei diritti di utilizzazione

Sezione I - Norme generali

(omissis)

Sezione II - Trasmissione a causa di morte

(omissis)

Sezione III - Contratto di edizione

(omissis)

[1] Ora, Presidenza del Consiglio dei ministri (N.d.R.)
[2] Ora, Società italiana degli autori ed editori (N.d.R.)

Sezione IV - Contratti di rappresentazione e di esecuzione
(omissis)

Sezione V - Ritiro dell'opera dal commercio
(omissis)

Sezione VI - Diritti dell'autore sull'aumento di valore delle opere delle arti figurative
(omissis)

Capo III - Difese e sanzioni giudiziarie
Sezione I - Difese e sanzioni civili

Norme relative ai diritti di utilizzazione economica

156. Chi ha ragione di temere la violazione di un diritto di utilizzazione economica a lui spettante in virtù di questa legge, oppure intende impedire la continuazione o la ripetizione di una violazione già avvenuta, può agire in giudizio per ottenere che il suo diritto sia accertato e sia interdetta la violazione. L'azione è regolata dalle norme di questa sezione e dalle disposizioni del codice di procedura civile.

157. Chi si trova nell'esercizio dei diritti di rappresentazione o di esecuzione di un'opera adatta a pubblico spettacolo, compresa l'opera cinematografica, o di un'opera o composizione musicale, può richiedere al Prefetto della provincia, secondo le norme stabilite dal regolamento, la proibizione della rappresentazione, o della esecuzione, ogni qualvolta manchi la prova scritta del consenso da esso prestato.
Il Prefetto provvede sulla richiesta, in base alle notizie e a documenti a lui sottoposti, permettendo, o vietando la rappresentazione o l'esecuzione, salvo alla parte interessata di adire l'Autorità giudiziaria, per i definitivi provvedimenti di sua competenza.

158. Chi venga leso nell'esercizio di un diritto di utilizzazione economica a lui spettante può agire in giudizio per ottenere che sia distrutto o rimosso lo stato di fatto da cui risulta la violazione o per ottenere il risarcimento del danno.

159. La rimozione o la distruzione prevista nell'articolo precedente non può avere per oggetto che gli esemplari o copie illecitamente riprodotte o diffuse, nonché gli apparecchi impiegati per la riproduzione o diffusione, che, per loro natura, non possono essere adoperati per diversa riproduzione o diffusione.
Se una parte dell'esemplare, della copia o dell'apparecchio di cui si tratta può essere impiegata per una diversa riproduzione o diffusione, l'interessato può chiedere, a sue spese, la separazione di questa parte nel proprio interesse.
Se l'esemplare o la copia dell'opera o l'apparecchio, di cui si chiede la rimozione, o la distruzione hanno singolare pregio artistico o scientifico, il giudice ne può ordinare di ufficio il deposito in un pubblico museo.
Il danneggiato può sempre chiedere che gli esemplari, le copie e gli apparecchi soggetti alla distruzione gli siano aggiudicati per un determinato prezzo in conto del risarcimento dovutogli.
I provvedimenti della distruzione e della aggiudicazione non colpiscono gli esemplari o le copie contraffatte acquistati in buona fede per uso personale.

160. La rimozione o la distruzione non può essere domandata nell'ultimo anno della durata del diritto. In tal caso, deve essere ordinato il sequestro dell'opera o del prodotto sino alla scadenza della durata medesima. Qualora siano stati risarciti i danni derivati dalla violazione del diritto il sequestro può esser autorizzato anche ad una data anteriore a quella sopraindicata.

161. Agli effetti dell'esercizio delle azioni previste negli articoli precedenti, può essere ordinata dall'Autorità giudiziaria la descrizione, l'accertamento, la perizia od anche il sequestro di ciò che si ritenga costituire violazione del diritto di utilizzazione.
Il sequestro non può essere concesso nelle opere che risultano dal contributo di più persone, salvo i casi di particolare gravità o quando la violazione del diritto di autore è imputabile a tutti i coautori.

L'Autorità giudiziaria può anche ordinare, in casi particolarmente gravi, il sequestro dei proventi dovuti all'autore dell'opera o del prodotto contestato.
Le disposizioni di questa Sezione si applicano anche a chi mette in circolazione in qualsiasi modo, o detiene per scopi commerciali copie non autorizzate di programmi e qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale dei dispositivi applicati a protezione di un programma per elaboratore.

162. I provvedimenti previsti nel precedente articolo sono autorizzati, su ricorso della parte interessata, con decreto del Pretore del mandamento dove i provvedimenti stessi devono essere eseguiti, per qualunque valore, a meno che vi sia lite pendente fra le parti, nel qual caso sono autorizzati con decreto del Pretore o del Giudice istruttore, quando la lite pende innanzi a magistratura collegiale.
Se vi sia urgenza, i provvedimenti possono, anche in questo caso, essere autorizzati dal Pretore del mandamento dove devono eseguirsi. Con lo stesso decreto può essere imposta al richiedente la prestazione di una idonea cauzione.
Salvo il caso di pericolo nel ritardo, l'Autorità giudiziaria prima di provvedere sul ricorso, deve chiamare in camera di consiglio, per sommarie informazioni, la parte a carico della quale il provvedimento dovrebbe essere eseguito per essere sentita nel contraddittorio della parte istante.
Il decreto è notificato, prima dell'esecuzione o contemporaneamente alla esecuzione stessa, alla parte contro la quale deve essere eseguito. La esecuzione è fatta per mezzo di ufficiale giudiziario con l'assistenza, ove occorra, di uno o più periti, nominati nel decreto suddetto.
Trattandosi di pubblici spettacoli non si applicano all'esecuzione del decreto le limitazioni di giorni e di ore fissate per atti di questa natura dal codice di procedura civile .

163. Sempre quando non sia altrimenti ordinato nel decreto di sequestro, ai fini dell'esercizio della giustizia penale, i provvedimenti previsti nei precedenti articoli perdono ogni efficacia, senza bisogno di pronuncia dell'Autorità giudiziaria, qualora entro otto giorni da quello della loro esecuzione, non venga promosso davanti al giudice competente il giudizio di convalida dei provvedimenti medesimi contro colui ai danni del quale si è proceduto.

164. Se le azioni previste in questa sezione e nella seguente sono promosse da uno degli enti di diritto pubblico indicati negli artt. 180 e 184 si osservano le regole seguenti:
1) i funzionari appartenenti agli enti sopramenzionati possono esercitare le azioni di cui sopra nell'interesse degli aventi diritto senza bisogno di mandato bastando che consti della loro qualità;
2) l'ente di diritto pubblico è dispensato dall'obbligo di prestare cauzione per la esecuzione degli atti per i quali questa cautela è prescritta o autorizzata;
3) l'ente di diritto pubblico può valersi del procedimento di ingiunzione nelle condizioni previste dagli artt. 3 e 12 del R.D. 7 agosto 1936, n. 1531 secondo le disposizioni del regolamento, il quale designa il funzionario ed il pubblico ufficiale autorizzati a compiere le attestazioni e a ricevere gli atti previsti negli articoli suddetti.

165. L'autore dell'opera oggetto del diritto di utilizzazione, anche dopo la cessione di tale diritto, ha sempre la facoltà di intervenire nei giudizi promossi dal cessionario a tutela dei suoi interessi.

(omissis)

Sezione II - Difese e sanzioni penali

171. Salvo quanto previsto dall'art. 171-bis, è punito con la multa da lire 100.000 a lire 4.000.000 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:
a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nel regno esemplari prodotti all'estero contrariamente alla legge italiana;
b) rappresenta, esegue o recita in pubblico o diffonde con o senza variazioni od aggiunte, una opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende

la proiezione pubblica dell'opera cinematografica, l'esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico;
c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;
d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di produrre o di rappresentare;
e) [riproduce con qualsiasi processo di duplicazione dischi o altri apparecchi analoghi o li smercia, ovvero introduce nel territorio dello Stato le riproduzioni così fatte all'estero];
f) in violazione dell'art. 79 ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.
La pena è della reclusione fino ad un anno o della multa non inferiore a lire 1.000.000 se i reati di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

171-bis. 1. Chiunque abusivamente duplica a fini di lucro, programmi per elaboratore, o, ai medesimi fini e sapendo o avendo motivo di sapere che si tratta di copie non autorizzate, importa, distribuisce, vende, detiene a scopo commerciale, o concede in locazione i medesimi programmi, è soggetto alla pena della reclusione da tre mesi a tre anni e della multa da L. 1.000.000 a L. 10.000.000. Si applica la stessa pena se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale dei dispositivi applicati a protezione di un programma per elaboratore. La pena non è inferiore nel minimo a sei mesi di reclusione e la multa a L. 3.000.000 se il fatto è di rilevante gravità ovvero se il programma oggetto dell'abusiva duplicazione, importazione, distribuzione, vendita, detenzione a scopo commerciale o locazione sia stato precedentemente distribuito, venduto o concesso in locazione su supporti contrassegnati dalla Società italiana degli autori ed editori ai sensi della presente legge e del relativo regolamento di esecuzione approvato con R.D. 18 maggio 1942, n. 1369.
1-bis. Chiunque, al fine di trarne profitto, riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64 - quinquies e 64 - sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102 - bis e 102 - ter è soggetto alla pena della reclusione da tre mesi a tre anni e della multa da lire un milione a lire dieci milioni. La pena non è inferiore nel minimo a sei mesi di reclusione e a lire tre milioni di multa se il fatto è di rilevante gravità ovvero se la banca di dati oggetto delle abusive operazioni di riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, estrazione o reimpiego sia stata distribuita, venduta o concessa in locazione su supporti contrassegnati dalla Società italiana degli ed editori ai sensi della presente legge e del relativo regolamento di esecuzione approvato con *R.D. 18 maggio 1942, n.1369*.
2. La condanna per i reati previsti ai commi 1 e 1-bis comporta la pubblicazione della sentenza in uno o più quotidiani e in uno o più periodici specializzati.

171-ter. 1. È punito con la reclusione da tre mesi a tre anni e con la multa da lire cinquecentomila a lire sei milioni chiunque:
a) abusivamente duplica o riproduce a fini di lucro, con qualsiasi procedimento, opere destinate al circuito cinematografico o televisivo, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere cinematografiche o audiovisive o sequenze di immagini in movimento;
b) pur non avendo concorso alla duplicazione o riproduzione, pone in commercio, concede in noleggio o comunque in uso a qualunque titolo a fine di lucro, detiene per gli usi anzidetti, introduce a fini di lucro nel territorio dello Stato, proietta in pubblico o trasmette per il mezzo della televisione le duplicazioni o riproduzioni abusive di cui alla lettera a);
c) vende o noleggia videocassette, musicassette od altro supporto contenente fonogrammi o videogrammi di opere cinematografiche o audiovisive o sequenze di immagini in movimento, non contrassegnati dalla Società italiana degli autori ed editori (S.I.A.E.) ai sensi della presente legge e del regolamento di esecuzione.
2. La pena non è inferiore nel minimo a sei mesi e la multa a lire un milione se il fatto è di rilevante gravità.

3. La condanna per i reati previsti ai commi 1 e 2 comporta la pubblicazione della sentenza in uno o più quotidiani ed in uno o più periodici specializzati.
3-bis. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai commi 1 e 2 sono versati all'Ente nazionale di previdenza e assistenza per i pittori e scultori, musicisti, scrittori e autori drammatici.

171-quater. Salvo che il fatto costituisca più grave reato, è punito con l'arresto sino ad un anno o con l'ammenda da lire un milione a lire dieci milioni chiunque, abusivamente ed a fini di lucro:
a) concede in noleggio o comunque concede in uso a qualunque titolo, originali, copie o supporti lecitamente ottenuti di opere tutelate dal diritto di autore;
b) esegue la fissazione su supporto audio, video o audiovideo delle prestazioni artistiche di cui all'art. 80.

172. Se i fatti preveduti nell'articolo 171 sono commessi per colpa la pena è della sanzione amministrativa sino a lire 2.000.000.
Con la stessa pena è punito chiunque:
a) esercita l'attività di intermediario in violazione del disposto degli artt. 180 e 183;
b) non ottempera agli obblighi previsti negli artt. 153 e 154;
c) viola le norme degli artt. 175 e 176.

173. Le sanzioni previste negli articoli precedenti si applicano quando il fatto non costituisce reato più grave previsto dal codice penale o da altre leggi.

174. Nei giudizi penali regolati da questa sezione la persona offesa, costituitasi parte civile, può sempre chiedere al giudice penale l'applicazione dei provvedimenti e delle sanzioni previsti dagli artt. 159 e 160.

TITOLO IV
Diritto demaniale

(omissis)

TITOLO V
Enti di diritto pubblico per la protezione e l'esercizio dei diritti di autore

(omissis)

TITOLO VI
Sfera di applicazione della legge

185. Questa legge si applica a tutte le opere di autori italiani, dovunque pubblicate per la prima volta, salve le disposizioni dell'art. 189.Si applica egualmente alle opere di autori stranieri, fuori delle condizioni di protezione indicate per la prima volta in Italia.Può essere applicata ad opere di autori stranieri, fuori delle condizioni di protezione indicate nel comma precedente, quando sussistano le condizioni previste negli articoli seguenti.

186. Le convenzioni internazionali per la protezione delle opere dell'ingegno regolano la sfera di applicazione di questa legge alle opere di autori stranieri.Se le convenzioni contengono un patto generico di reciprocità o di parità di trattamento, detto patto è interpretato secondo le norme di equivalenza di fatto delle due protezioni stabilite negli articoli seguenti. .

187. In difetto di convenzioni internazionali, le opere di autori stranieri che non rientrano nelle condizioni previste nel secondo comma dell'articolo 185 godono della protezione sancita da questa legge, a condizione che lo Stato di cui è cittadino l'autore straniero conceda alle opere di autori italiani una protezione effettivamente equivalente e nei limiti di detta equivalenza.

Se lo straniero, è apolide o di nazionalità controversa, la norma del comma precedente è riferita allo Stato nel quale l'opera è stata pubblicata per la prima volta .

188. L'equivalenza di fatto, osservate le norme che seguono, è accertata e regolata con decreto reale da emanarsi a norma dell'art. 3, n. 1, della L. 31 gennaio 1926, n. 100 .
La durata della protezione dell'opera straniera non può in nessun caso eccedere quella di cui l'opera gode nello Stato di cui è cittadino l'autore straniero.
Se la legge di detto Stato abbraccia nella durata della protezione un periodo di licenza obbligatoria, l'opera straniera è sottoposta in Italia ad una norma equivalente.
Se la legge di detto Stato sottopone la protezione alla condizione dell'adempimento di formalità, di dichiarazioni di riserva o di depositi di copie dell'opera o ad altre formalità qualsiasi, l'opera straniera è sottoposta in Italia a formalità equivalenti determinate col decreto reale.
Il decreto reale può altresì sottoporre la protezione dell'opera straniera allo adempimento di altre particolari formalità o condizioni.

189. Le disposizioni dell'art. 185 si applicano all'opera cinematografica, al disco fonografico o apparecchio analogo, ai diritti degli interpreti, attori o artisti esecutori, alla fotografia ed alle opere della ingegneria, in quanto si tratti di opere o prodotti realizzati in Italia o che possano considerarsi nazionali a termini di questa legge o di altra legge speciale.
In difetto della condizione sopraindicata sono applicabili a dette opere, diritti o prodotti, le disposizioni degli artt. 186, 187 e 188.

TITOLO VII
Comitato consultivo permanente per il diritto di autore

(omissis)

TITOLO VIII
Disposizioni generali transitorie e finali

196. È considerato come luogo di prima pubblicazione, il luogo dove sono esercitati per la prima volta i diritti di utilizzazione previsti negli artt. 12 e seguenti di questa legge.
Nei riguardi delle opere dell'arte figurativa, del cinema, del disco fonografico o di altro apparecchio analogo riproduttore di suoni o di voci, della fotografia o di ogni altra opera identificata dalla sua forma materiale, si considera come equivalente al luogo della prima pubblicazione il luogo della fabbricazione.

197. (omissis)

198. (omissis)

199. - bis. 1. Le disposizioni della presente legge si applicano anche ai programmi creati prima della sua entrata in vigore, fatti salvi gli eventuali atti conclusi e i diritti acquisiti anteriormente a tale data.

(omissis)

Decreto legislativo 6 maggio 1999, n. 169

Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati.

(omissis)

7. Disposizioni finali e transitorie. - 1. Le disposizioni del titolo I della legge 22 aprile 1941, n. 633, si applicano anche alle banche di dati create prima del 1° gennaio 1998 e che entro la data di entrata in vigore del presente decreto soddisfino i requisiti di cui all'articolo 2 del decreto medesimo, fatti salvi gli eventuali atti conclusi e i diritti acquisiti anteriormente. La stessa disposizione si applica anche alle banche di dati create dal 1° gennaio 1998 fino alla data di entrata in vigore del presente decreto.
2. Le disposizioni del capo I del titolo II-bis della legge 22 aprile 1941, n. 633, si applicano anche alle banche di dati costituite completamente nei 15 anni precedenti il 1° gennaio 1998 e che alla data di entrata in vigore del presente decreto soddisfino i requisiti di cui all'articolo 5 del decreto medesimo, fatti salvi gli eventuali atti conclusi e i diritti acquisiti anteriormente. La stessa disposizione si applica anche alle banche di dati costituite completamente dal 1° gennaio 1998 fino alla data di entrata in vigore del presente decreto.
3. Per le banche di dati di cui al comma 2, primo periodo, il termine di cui all'articolo 102-bis, comma 5, della legge 22 aprile 1941, n. 633, decorre dal 1° gennaio 1998.
4. Il presente decreto non osta all'applicazione delle disposizioni concernenti, in particolar modo, il diritto d'autore, i diritti connessi o altri diritti od obblighi preesistenti su dati, opere o altri elementi inseriti in una banca di dati, brevetti, marchi commerciali, disegni e modelli industriali, la protezione dei beni appartenenti al patrimonio nazionale, le norme sulle intese e sulla concorrenza sleale, il segreto industriale, la sicurezza, la riservatezza, la tutela dei dati di carattere personale ed il rispetto della vita privata, l'accesso ai documenti pubblici o il diritto dei contratti.

(omissis)

Legge 1 aprile 1981 n. 121

Nuovo ordinamento dell'Amministrazione della pubblica sicurezza

(omissis)

Art. 6 - Coordinamento e direzione unitaria delle forze di polizia.
Il dipartimento della pubblica sicurezza, ai fini dell'attuazione delle direttive impartite dal Ministro dell'interno nell'esercizio delle attribuzioni di coordinamento e di direzione unitaria in materia di ordine e di sicurezza pubblica, espleta compiti di:
a) classificazione, analisi e valutazione delle informazioni e dei dati che devono essere forniti anche dalle forze di polizia in materia di tutela dell'ordine, della sicurezza pubblica e di prevenzione e repressione della criminalità e loro diramazione agli organi operativi delle suddette forze di polizia;
b) ricerca scientifica e tecnologica, documentazione, studio e statistica;
c) elaborazione della pianificazione generale dei servizi d'ordine e sicurezza pubblica;
d) pianificazione generale e coordinamento delle pianificazioni operative dei servizi logistici e amministrativi di carattere comune alle forze di polizia;
e) pianificazione generale e coordinamento delle pianificazioni operative della dislocazione delle forze di polizia e dei relativi servizi tecnici;
f) pianificazione generale e coordinamento delle pianificazioni finanziarie relative alle singole forze di polizia;
g) mantenimento e sviluppo delle relazioni comunitarie e internazionali.
(omissis)

Art. 7 - Natura e entità dei dati e delle informazioni raccolti.
Le informazioni e i dati di cui all'articolo 6, lettera a), devono riferirsi a notizie risultanti da documenti che comunque siano conservati dalla pubblica amministrazione o da enti pubblici, o risultanti da sentenze o provvedimenti dell'autorità giudiziaria o da atti concernenti l'istruzione penale acquisibili ai sensi dell'articolo 165-ter del codice di procedura penale o da indagini di polizia.
In ogni caso è vietato raccogliere informazioni e dati sui cittadini per il solo fatto della loro razza, fede religiosa od opinione politica, o della loro adesione ai princìpi di movimenti sindacali, cooperativi, assistenziali, culturali, nonché per la legittima attività che svolgano come appartenenti ad organizzazioni legalmente operanti nei settori sopraindicati.
Possono essere acquisite informazioni relative ad operazioni o posizioni bancarie nei limiti richiesti da indagini di polizia giudiziaria e su espresso mandato dell'autorità giudiziaria, senza che possa essere opposto il segreto da parte degli organi responsabili delle aziende di credito o degli istituti di credito di diritto pubblico.
Possono essere altresì acquisiti le informazioni e i dati di cui all'articolo 6 in possesso delle polizie degli Stati appartenenti alla Comunità economica europea e di quelli di confine, nonché di ogni altro Stato con il quale siano raggiunte specifiche intese in tal senso.
Possono essere inoltre comunicati alle polizie indicate al precedente comma le informazioni e i dati di cui all'articolo 6, che non siano coperti da segreto istruttorio.

Art. 8.- Istituzione del Centro elaborazione dati.
È istituito presso il Ministero dell'interno, nell'ambito dell'ufficio di cui alla lettera a) dell'articolo 5, il Centro elaborazione dati, per la raccolta delle informazioni e dei dati di cui all'articolo 6, lettera a), e all'articolo 7.
Il Centro provvede alla raccolta, elaborazione, classificazione e conservazione negli archivi magnetici delle informazioni e dei dati nonché alla loro comunicazione ai soggetti autorizzati, indicati nell'articolo 9, secondo i criteri e le norme tecniche fissati ai sensi del comma seguente.
Con decreto del Ministro dell'interno è costituita una commissione tecnica, presieduta dal funzionario preposto all'ufficio di cui alla lettera a) dell'articolo 5, per la fissazione dei criteri e delle norme tecniche per l'espletamento da parte del Centro delle operazioni di cui al comma precedente e per il controllo tecnico sull'osservanza di tali criteri e norme da parte del personale operante presso il Centro stesso. I criteri e le norme tecniche predetti divengono esecutivi con l'approvazione del Ministro dell'interno.

Art.9 - Accesso ai dati ed informazioni e loro uso.
L'accesso ai dati e alle informazioni conservati negli archivi automatizzati del Centro di cui all'articolo precedente e la loro utilizzazione sono consentiti agli ufficiali di polizia giudiziaria appartenenti alle forze di polizia, agli ufficiali di pubblica sicurezza e ai funzionari dei servizi di sicurezza, nonché agli agenti di polizia giudiziaria delle forze di polizia debitamente autorizzati ai sensi del secondo comma del successivo articolo 11 .
L'accesso ai dati e alle informazioni di cui al comma precedente è consentito all'autorità giudiziaria ai fini degli accertamenti necessari per i procedimenti in corso e nei limiti stabiliti dal codice di procedura penale.
È comunque vietata ogni utilizzazione delle informazioni e dei dati predetti per finalità diverse da quelle previste dall'articolo 6, lettera a). È altresì vietata ogni circolazione delle informazioni all'interno della pubblica amministrazione fuori dei casi indicati nel primo comma del presente articolo.

(omissis)

Art.12 - Sanzioni.
Il pubblico ufficiale che comunica o fa uso di dati ed informazioni in violazione delle disposizioni della presente legge, o al di fuori dei fini previsti dalla stessa, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a tre anni.
Se il fatto è commesso per colpa, la pena è della reclusione fino a sei mesi.

(omissis)

D.P.C.M. 15 febbraio 1989

Coordinamento delle iniziative e pianificazioni degli investimenti in materia di automazione nelle amministrazioni pubbliche

(omissis)

ART. 6.

1. La documentazione amministrativa delle amministrazioni pubbliche è redatta in modo da permetterne la memorizzazione e la ricerca con procedure automatizzate.

2. Con successivo decreto del Ministro per la funzione pubblica, saranno definiti standards operativi ai fini dell'adeguamento delle procedure di redazione dei documenti e degli atti di cui al presente articolo, sulla base degli indirizzi e delle proposte di una commissione costituita con decreto del Ministro per la funzione pubblica e composta da esperti, anche estranei alla pubblica amministrazione, qualificati nella materia.

3. I programmi applicativi e i sistemi diretti a consentire il funzionamento dei mezzi elettronici di elaborazione possono essere utilizzati anche da centri elaborazione dati di amministrazioni pubbliche diverse da quella per la quale sono stati realizzati, fatti salvi i diritti di proprietà di terzi.

4. Le amministrazioni pubbliche garantiscono l'applicazione delle misure per la sicurezza dei centri elaborazione dati, la segretezza e la riservatezza dei dati contenuti negli archivi automatizzati, il numero delle copie dei programmi dei dati memorizzati da conservare, le modalità per la loro conservazione e custodia.

(omissis)

Legge 23 dicembre 1993 n. 547

Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica.

ART. 1.
1. All'articolo 392 del codice penale, dopo il secondo comma è aggiunto il seguente:
"Si ha, altresì, violenza sulle cose[1], allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento da un sistema informatico o telematico".

ART. 2.
1. L'articolo 420 del codice penale è sostituto dal seguente:
"Art. 420. - (Attentato a impianti di pubblica utilità)[2]. - Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.
La pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o ad esso pertinenti.
Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi, ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema, la pena è della reclusione da tre a otto anni".

ART. 3.
1. Dopo l'articolo 491 del codice penale è inserito il seguente:
"Art. 491-bis - (Documenti informatici)[3] - Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".

[1] **Esercizio arbitrario delle proprie ragioni con violenza sulle cose.** Agli effetti della legge penale si ha violenza sulle cose allorché la cosa viene danneggiata o trasformata o ne è mutata la destinazione.
Se un programmatore interno od esterno all'Amministrazione inserisce nel codice del programma una "bomba logica" una *backdoor*, o più in generale una qualsiasi *routine* che nel corso del tempo modifichi il normale funzionamento del programma stesso, al fine di far valere le proprie ragioni, si può applicare l'art 392.
Tutto il software sviluppato all'interno dell'Amministrazione prima dell'installazione deve essere collaudato e la documentazione consegnata dovrà corrispondere in tutto e per tutto al programma originale. Gli sviluppatori esterni dovranno garantire che il software consegnato è esente da routine atte al danneggiamento, alla trasformazione o al mutamento di destinazione. (NdR)

[2] **Danneggiamento e distruzione di sistemi informatici e di pubblica utilità.**
La norma mira a punire tutti gli atti DIRETTI a produrre l'evento dannoso e non il loro risultato. Da notare che la norma per essere applicata deve riguardare impianti di pubblica utilità che abbiano rilevanza tale che un eventuale "attentato" sia fonte di immediato pericolo per l'ordine pubblico. Il reato inteso dall'art. 420 è a forma libera, nel senso che il danno può essere provocato anche con l'attivazione di virus informatici o "bombe logiche"
Le P.A. devono predisporre una classificazione dei beni informatici (intesi come dati e come strutture) e soprattutto definire un piano di disaster recovery. (NdR)

[3] **Falsità in documenti informatici.**
Da notare che per documento informatico non si intende l'*output* di un elaborazione di dati ma il supporto informatico, qualunque esso sia. (NdR)

ART. 4.

1. Dopo l'articolo 615-bis del codice penale sono inseriti i seguenti:

"Art. 615-ter. - (Accesso abusivo ad un sistema informatico o telematico)[4]. - Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole, per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Art. 615-quater.- (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)[5]. - Chiunque, al fine di procurare a sé o ad altri un profitto, o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni.

La pena è della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

Art 615-quinquies. - (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico)[6]. - Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, aven-

[4] **La tutela del domicilio informatico.**
I sistemi informatici e telematici non sono più considerati mezzi o strumenti tramite i quali esercitare la propria attività professionale o individuale ma diventano luoghi nei quali esercitare l'attività. Per l'applicazione di questo articolo il sistema informatico deve essere protetto da misure di sicurezza.
L'acceso abusivo cui fa riferimento l'art. 615 ter è quello elettronico o informatico.
Per misure di sicurezza potremmo intendere: accorgimenti tecnici atti ad impedire l'accesso e l'utilizzo del sistema informatico da parte di persone non autorizzate. In sostanza per poter tutelare il diritto all'applicazione della norma in questione il soggetto (P.A. o Ente) deve dimostrare di avere predisposto le misure di protezione. (NdR)

[5] **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici.**
Anche in questo caso, per l'applicazione della norma occorre che il sistema sia protetto, anche se, parlando di codici d'accesso, implicitamente si suppone che il sistema abbia già misure di sicurezza.
Da notare che la norma usa l'espressione "parola chiave" che nel lessico "informatico" si usa per indicare la chiave di ricerca documentale, ovviamente la parola chiave cui fa riferimento il legislatore è la chiave logica.
Ulteriore nota all'art. 615 quater è la nozione di "procurare" cioè l'azione di chi si adopera per entrare in possesso di codici ecc… In questa definizione rientra, ampiamente, la ricerca per tentativi, effettuata dagli *hacker* e pertanto i sistemi informatici dovranno essere in grado di rilevare e successivamente monitorare i tentativi di accesso.
Da notare che da questa norma, inoltre, si può estrapolare anche la nozione del reato di ricettazione in quanto il possesso di *password* di terze persone può far pensare al loro utilizzo per trarne profitto. (NdR)

[6] **Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico o telematico.**
Da notare che progettare, realizzare o produrre programmi con le caratteristiche indicate nella norma non costituisce reato.
Anche se la norma, nel panorama internazionale, è innovativa, occorre sottolineare che programmi aventi le caratteristiche descritte dall'art. 615 quater sono insiti anche nei software di gestione dei vari sistemi operativi.
Rientra, ad esempio, nella fattispecie di reato se un utente di un sistema informatico innavvertitamente o volutamente utilizzando il comando "cancella" distrugge documenti informatici?

te per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire venti milioni".

ART. 5.
1. Nell'articolo 616 del codice penale, il quarto comma è sostituito dal seguente:
"Agli effetti delle disposizioni di questa sezione, per corrispondenza si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza".[7]

ART. 6.[8]
1. Dopo l'art. 617-ter del codice penale sono inseriti i seguenti:
"Art. 617-quater. - (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche). - Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusone da sei mesi a quattro anni.
Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.
I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni, se il fatto è commesso:
1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2) da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3) da chi esercita anche abusivamente la professione di investigatore privato.
Art. 617-quinquies. - (Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche). - Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

Il comando "cancella" che nei diversi S.O. può essere *erase*, *delete*, *kill* ecc., è in realtà una funzione o un comando interno del s.o. stesso. In questo caso è perseguibile la *software house* che ha distribuito il sistema operativo?
Naturalmente il legislatore intendeva dare una definizione atta ad identificare i programmi cosiddetti "virus". (NdR)

[7] **Violazione della corrispondenza.**
Testo integrale dell'art. 616 c.p.
"Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero in tutto o in parte la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino ad un anno o con la multa da lire sessantamila a un milione.
Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino tre anni.
Il delitto è punibile a querela della persona offesa.
Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza".
Oltre alle azioni e al reato previste dalla norma è possibile ravvisare la fattispecie di altri reati nell'utilizzo della posta elettronica:
- Invio di messaggi contenenti insulti: reato di ingiuria
- Invio di messaggi contenenti frasi diffamatorie nei confronti di un terzo: reato di diffamazione
- Invio di messaggi contenenti frasi di minaccia
- Invio di messaggi contenenti frasi denigratorie verso prodotti commerciali: concorrenza sleale. (NdR)

[8] **Le comunicazioni Informatiche o Telematiche.**
I tre articoli introdotti con l'art. 6 sono indirizzati alla protezione e alla sicurezza del sistema informatico.
Da notare che per tutti gli articoli in esame le aggravanti della pena sono applicate se il reato è commesso da un pubblico ufficiale o da un incaricato di un pubblico esercizio o dall'abuso delle funzioni di SysOp. (NdR)

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.
Art. 617-sexies. - (Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche). - Chiunque, al fine di procurare ad altri o a sé un vantaggio o di arrecare ad altri un danno, forma falsamente, ovvero altera o sopprime in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater".

ART. 7.
1. Nell'articolo 621 del codice penale, dopo il primo comma, è inserito il seguente:
"Agli effetti della disposizione di cui al primo comma è considerato documento[9] anche qualunque supporto informatico contenente dati, informazioni o programmi".

ART. 8.
1. L'articolo 623-bis del codice penale è sostituito dal seguente:
"Art. 623-bis (Altre comunicazioni e conversazioni). - Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini o altri dati".

ART. 9.
1. Dopo l'articolo 635 del codice penale è inserito il seguente:
"Art. 635-bis. - (Danneggiamento di sistemi informatici e telematici)[10]. - Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.
Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".

ART. 10.
1. Dopo l'articolo 640-bis del codice penale è inserito il seguente:
"Art. 640-ter. - (Frode informatica). - Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni.
La pena della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante".

ART. 11.
1. Dopo l'articolo 266 del codice di procedura penale è inserito il seguente:
"Art. 266-bis. - (Intercettazioni di comunicazioni informatiche o telematiche) -1. Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi".

[9] **Rivelazione del contenuto di documenti segreti.**
Affinché si ravvisi l'ipotesi di reato il documento informatico deve essere classificato come segreto e che sia, conservato, elaborato e diffuso in modalità sicura. (NdR)

[10] **Danneggiamento di sistemi informatici o telematici.**
Il reato descritto nella norma in questione si può definire "istantaneo" si consuma, quindi, nel momento in cui si verifica l'evento dannoso. Da notare che la norma sanziona non solo la distruzione o il rendere inservibili i sistemi informatici ma anche programmi, informazioni o dati altrui, si provi a pensare, cosa potrebbe accadere nel caso di un utente che abbia accesso (anche leggittimo) a basi dati condivisione e alla possibilità anche volontaria di poterle danneggiare o renderle inservibili. (NdR)

ART. 12.
1. L'articolo 268 del codice di procedura penale è così modificato:
a) dopo il comma 3 è inserito il seguente:
"3-bis. Quando si procede a intercettazione di comunicazioni informatiche o telematiche, il pubblico ministero può disporre che le operazioni siano compiute anche mediante impianti appartenenti a privati";
b) i commi 6, 7 e 8 sono sostituiti dai seguenti:
"6. Ai difensori delle parti è immediatamente dato avviso che, entro il termine fissato a norma dei commi 4 e 5, hanno facoltà di esaminare gli atti e ascoltare le registrazioni ovvero di prendere cognizione dei flussi di comunicazioni informatiche o telematiche indicati dalle parti, che non appaiano manifestamente irrilevanti, procedendo anche di ufficio allo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione. Il pubblico ministero e i difensori hanno diritto di partecipare allo stralcio e sono avvisati almeno ventiquattro ore prima.
7. Il giudice dispone la trascrizione integrale ovvero la stampa in forma intelligibile delle informazioni contenute nei flussi di comunicazioni informatiche o telematiche da acquisire, osservando le forme, i modi e le garanzie previsti per l'espletamento delle perizie. Le trascrizioni o le stampe sono inserite nel fascicolo per il dibattimento.
8. I difensori possono estrarre copia delle trascrizioni e fare eseguire la trasposizione della registrazione su nastro magnetico. In caso di intercettazione di flussi di comunicazioni informatiche o telematiche i difensori possono richiedere copia su idoneo supporto dei flussi intercettati, ovvero copia della stampa prevista dal comma 7".

ART. 13.
1. Al comma 1 dell'articolo 25-ter del decreto-legge 8 giugno 1992, n. 306 convertito, con modificazioni, dalla legge 7 agosto 1992, n.356, dopo le parole "e di altre forme di telecomunicazione" sono inserite le seguenti: "ovvero del flusso di comunicazioni relativo a sistemi informatici o telematici".
Le presente legge, munita del sigillo di Stato, sarà inserita nella Raccolta ufficiale degli atti normativi della Repubblica Italiana. È fatto obbligo a chiunque spetti di osservarla e farla osservare come legge dello Stato.

AIPA
Autorità per l'Informatica nella Pubblica Amministrazione

Linee Guida

per la definizione di un piano

per la Sicurezza

APPENDICE 2

VIRUS INFORMATICI

Fattori di incremento del rischio e comportamenti da evitare p. 75

Norme basilari di comportamento p. 75

Regole operative p. 75

Caratteristiche di base del software antivirus p. 76

Fattori di incremento del rischio e comportamenti da evitare

1. I seguenti comportamenti, comportano un incremento dei livelli di rischio informatico:

a) riutilizzo di dischetti già adoperati in precedenza;
b) uso di *software* gratuito (o *shareware*) prelevato da siti Internet o in allegato a riviste o libri;
c) uso di dischetti preformattati;
d) collegamento in rete, nel quale il *client* avvia solo applicazioni residenti nel proprio disco rigido;
e) collegamento in rete, nel quale il *client* avvia anche applicazioni residenti sul disco rigido del *server*;
f) uso di modem per la posta elettronica e prelievo di *file* da BBS o da servizi commerciali in linea o da banche dati;
g) ricezione di applicazioni e dati dall'esterno, Amministrazioni, fornitori, ecc.;
h) utilizzo dello stesso computer da parte di più persone;
i) collegamento in Internet con *download* di *file* eseguibili o documenti di testo da siti web o da siti FTP;
l) collegamento in Internet e attivazione degli *applets* di Java o altri contenuti attivi;
m) *file attached* di posta elettronica.

Norme basilari di comportamento

Al fine di evitare problemi correlati ad infezioni informatiche, dovranno essere rispettate almeno le seguenti prescrizioni:

a) i *floppy disk*, sia quando vengono forniti sia quando vengono ricevuti, devono essere sottoposti a scansione da parte del programma antivirus;
b) è obbligatorio sottoporre a controllo tutti i *floppy disk* di provenienza incerta prima di eseguire o caricare uno qualsiasi dei *file* in esso contenuti;
c) non si deve utilizzare il proprio "disco sistema" su di un altro computer se non in condizione di "protezione in scrittura";
d) proteggere in "scrittura" tutti i propri *floppy disk* di sistema o contenenti programmi eseguibili;
e) se si utilizza un computer che necessita di un *"bootstrap"* da *floppy*, usare un *floppy disk* protetto in scrittura;
f) non attivare mai da *floppy* un sistema basato su *hard disk* a meno di utilizzare un disco di sistema, protetto in scrittura e sicuramente non infetto;
g) limitare la trasmissione di *file* eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computer in rete;
h) non utilizzare i *server* di rete come stazioni di lavoro;
i) non aggiungere mai dati o *file* ai *floppy disk* contenenti programmi originali.

Regole operative

1. Tutti i computer dell'Amministrazione devono essere dotati di programmi antivirus.
2. L'Amministrazione deve assicurarsi che i computer delle società esterne, qualora interagiscano con proprio sistema informatico, siano dotati di adeguate misure di protezione antivirus.
3. Il personale delle ditte addette alla manutenzione dei supporti informatici devono usare solo dischetti preventivamente controllati e certificati singolarmente ogni volta.
4. Ogni P.C. deve essere costantemente sottoposto a controllo anti-virus.
5. I dischetti provenienti dall' esterno devono essere sottoposti a verifica da attuare con un P.C. non collegato in rete (macchina da quarantena), ed inoltre devono essere individuate le aree dell'Amministrazione che, in relazione alla loro particolare attività, sono da considerare a più alto rischio nei riguardi dell'infezione da virus.
6. All'atto della individuazione di una infezione il virus deve essere immediatamente rimosso.
7. Tutti gli utenti del sistema informatico devono sapere a chi rivolgersi per la disinfezione e l'informazione dell'infezione deve essere mantenuta riservata.
8. Il personale deve essere a conoscenza che la diffusione dei virus è punita dall'art. 615 quinquies del Codice Penale.
9. Il *software* acquisito deve essere sempre controllato contro i virus e verificato perchè sia di uso sicuro prima che sia installato .

Caratteristiche di base del software antivirus

1. Il *software* antivirus deve essere sottoposto a costante e frequente aggiornamento (almeno due volte al mese) ed in particolare:

a) gli aggiornamenti devono essere resi disponibili non solo per posta ma anche tramite BBS o Internet;
b) deve essere particolarmente efficace contro i virus della nostra area geografica;
c) deve poter effettuare automaticamente una scansione ogni volta che viene avviato un programma;
d) deve poter effettuare una scansione automatica del *floppy disk* ;
e) deve accorgersi del tentativo di modificare le aree di sistema;
f) deve essere in grado di effettuare scansioni a intervalli regolari e programmati;
g) deve essere in grado di effettuare la scansione all'interno dei *file* compressi;
h) deve mantenere il livello di protezione in tempo-reale;
i) deve eseguire la scansione in tempo-reale;
l) deve poter eseguire la rimozione del codice virale in automatico;
m) in caso di impossibilità di rimozione i *file* non pulibili devono essere spostati una *subdirectory* predefinita;
n) deve essere attivo nella protezione per *Applet* di ActiveX e Java contenenti codice malizioso;
o) deve essere in grado di effettuare la rilevazione/pulizia dei virus da Macro sconosciuti;
p) deve essere in condizione di rilevare e rimuovere i virus da macro senza *file pattern* con un grado di riconoscimento superiore al 97 %;
q) deve essere in grado di riconoscere i codici virali anche in *file* compattati utilizzando qualsiasi programma di compressione e in qualsiasi ambiente operativo;

Considerato che in sistemi basati su reti locali o su reti geografiche, aumenta il pericolo di diffusione dei virus, ove possibile il sistema antivirus deve essere centralizzato e predisposto a svolgere almeno le funzioni di:

1. distribuzione degli aggiornamenti sia dei motori di scansione che degli eventuali *file "pattern"*;
2. controllo e monitoraggio degli eventi virali;
3. automatico spostamento in *directory* di "quarantena" di virus informatici risultati non pulibili;
4. avviso all'amministratore di sistema di rilevazione di virus e indicazione del *file* "infetto".