INAIL
ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO

PASSAGGI
TRA LE AREE
E ALL'INTERNO DELLE AREE

Materiale Didattico

LA SICUREZZA INFORMATICA

CONSULENZA PER
L'INNOVAZIONE TECNOLOGICA

SERVIZIO FORMAZIONE

Redattori Carmela DE PADOVA
Carlo ISGRO'

Revisione 28 settembre 2012

INDICE

PAG.

1 INTRODUZIONE

Il problema della sicurezza, nel campo dell'informatica, è nato con la nascita della elaborazione dati e, per molti anni, è rimasto latente come un pericolo di cui si conosceva l'esistenza, ma che data la scarsa consistenza delle minacce e dei possibili danni che esse potevano causare, si riusciva a controllare quasi totalmente con l'esperienza e col buon senso del "*buon padre di famiglia".*
I vecchi paradigmi della elaborazione dati, però, si sono rapidamente evoluti e, da uno scenario che vedeva:

- la centralizzazione delle informazioni;
- la centralizzazione delle elaborazioni;
- l'accesso alle informazioni attraverso terminali "stupidi";

si è passati ad uno scenario completamente diverso che vede:

- la distribuzione delle informazioni;
- la distribuzione delle elaborazioni;
- l'accesso tramite sistemi tecnologici intelligenti e sempre più interconnessi.

L'avvento di questo nuovo scenario ha portato fuori dalle aziende il patrimonio informativo e lo ha posto su delle reti, più o meno sicure, incrementando possibili vulnerabilità di cui ci si è resi conto solo dopo aver subito dei danni a volte irreparabili.
Ciò ha portato in primo piano un problema che è diventato *il problema* di questo periodo e che ha mobilitato il mondo dell'informatica in senso globale perché è globale il pericolo che incombe e imperversa.
Questo cambiamento radicale ha fatto esplodere il **problema sicurezza** che ha assunto, negli ultimi tempi, un'importanza vitale accentuata dall'avvento delle reti pubbliche o aziendali (INTERNET, INTRANET e INFRANET).
Inoltre le reti sono evolute ed il perimetro non è più così ben definito; la banda è aumentata e il sistema Internet rappresenta senz'altro il più complesso problema esistente.
Queste nuove tecnologie consentono lo scambio rapido delle informazioni, tutti comunicano con tutti, ma le comunicazioni avvengono in chiaro, l'autenticazione degli utenti spesso è debole, basata normalmente su password, non sempre c'è autenticazione del server, le connessioni geografiche avvengono tramite linee condivise o router di terzi, inoltre il software contiene molti "bachi".
Questa vulnerabilità ha fatto nascere una serie di nemici, che per fini propri o solo per recare danno, si inseriscono nelle reti e apportano una varietà di attacchi ai nostri archivi o ai nostri sistemi causando danni economici o di immagine a volte irrimediabili.
Il nemico può essere al di fuori della nostra organizzazione o all'interno o, e questo è l'approccio più corretto, ***IL NEMICO è OVUNQUE***.

È importante quindi individuare i potenziali nemici, i potenziali attacchi, le contromisure da mettere in atto.
La sicurezza dei sistemi informativi richiede un impegno finanziario, umano e tecnologico costante per evolversi ed adattarsi ai sempre nuovi pericoli.
Nell'universo ICT, come in tutte le aree di produzione di qualsiasi tipo, oramai è affermata la visione della sicurezza divisa in tre grandi aree: la sicurezza organizzativa e procedurale, la sicurezza logica e la sicurezza fisica. Ma cosa sono ?

La **Sicurezza ORGANIZZATIVA** comprende:
- politiche per la sicurezza
- norme e procedure per la sicurezza;
- piani per la sicurezza;
- organigramma (ruoli e responsabilità) per la sicurezza;
- formazione del personale

La **Sicurezza LOGICA** comprende:
- identificazione e autenticazione, controllo accessi logici;
- autorizzazione;
- encription / firme digitali, ecc.;
- barriere sw di protezione;
- antivirus, antispam, antispyware, antimalware e simili;
- monitoring saltuari e periodici;
- protezione perimetrale (firewal, intrusion detection, ecc.).

La **Sicurezza FISICA** comprende:
- protezione degli edifici e delle aree interne;
- protezione dai furti, dagli incendi;
- protezione dall'indisponibilità di alimentazione elettrica;
- protezione fisica della rete;
- protezione supporti; separazione fisica supporti / data base
- back-up / recovery;
- business continuity e disaster recovery.

Nei paragrafi successivi viene illustrato il Codice per la protezione dei dati personali, le politiche per la sicurezza, l'analisi dei rischi, e vengono approfondite la Sicurezza organizzativa e la Sicurezza logica (cos'è, come si applica, a cosa si applica, e soprattutto quali sono i requisiti principali). La Sicurezza fisica è trattata in parte nell'ultimo paragrafo.

2 QUADRO NORMATIVO

2.1 GENERALITÀ

Le azioni del legislatore nel campo della sicurezza informatica e della documentazione amministrativa, in questi ultimi anni, sono state sempre più puntuali, attraverso un susseguirsi di decreti legislativi, leggi e regolamenti, alcuni dei quali sono poi confluiti in testi unici.

2.2 RIFERIMENTI NORMATIVI

a) Per quanto concerne la **normativa nazionale**:
- D.Lgs. 7 marzo 2005, n. 82 "*Codice dell'amministrazione digitale*" e successive modifiche ed integrazioni;
- D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e successive modifiche ed integrazioni;
- D.P.R. 445 del 28/12/2000 "*Testo Unico in materia di documentazione amministrativa*" e successive modifiche ed integrazioni;
- Direttiva del Presidente del Consiglio dei Ministri, 16 gennaio 2002, "*Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali*";

b) Per quanto concerne la **normativa comunitaria**:
- Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche);
- Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

c) Per quanto concerne i **provvedimenti del Garante privacy**:
- Provvedimento Generale del 27 novembre 2008, come modificato in base al Provvedimento del 25 giugno 2009: "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
- Provvedimento Generale del 13 ottobre 2008: "*Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali*";
- Provvedimento Generale del 1 Marzo 2007: "*Linee guida del Garante per posta elettronica e Internet*";
- Provvedimento del 9 marzo 2005: "*Etichette intelligenti (Rfid): le garanzie per il loro uso*".

d) Per quanto concerne le **raccomandazioni e standard**:
- Standard UNI CEI ISO/IEC 27001:2006 "*Tecnologia delle informazioni – Tecniche di sicurezza –Sistemi di gestione della sicurezza delle informazioni – Requisiti";*
- Raccomandazioni del Consiglio dell'OCSE, 25 luglio 2002, "*Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti di informazione*".

2.3 DEFINIZIONI

Per quanto concerne le definizioni e alcune terminologie richiamate nel presente documento si fa riferimento a quelle contenute nell'art. 1 del Codice dell'Amministrazione Digitale (CAD) di cui al D.Lgs.

n.82/2005 e a quelle contenute nell'art. 4 del Codice in materia di protezione dei dati personali di cui al D.Lgs. n.196/2003.

3 PRIVACY

3.1 PRINCIPI COMUNITARI

La direttiva 95/46/CE è la normativa a livello europeo sulla tutela dei diritti e delle libertà delle persone fisiche e del diritto alla vita privata, che stabilisce i principi relativi al trattamento dei dati personali e alla libera circolazione all'interno dell'Unione Europea.
Tali principi riguardano, in particolare, la qualità dei dati, la legittimazione del trattamento, le categorie particolari di trattamenti, l'informazione delle persone interessate dal trattamento dei dati, il diritto di accesso ai dati, il diritto di opposizione ai trattamenti di dati, la riservatezza e la sicurezza dei trattamenti, la notificazione dei trattamenti ad un'autorità di controllo.

3.2 CODICE DELLA PRIVACY

3.2.1 Introduzione

Il primo gennaio 2004 è entrato in vigore il Decreto Legislativo n. 196 del 30 Giugno 2003, denominato "Codice in materia di protezione dei dati personali" (nel seguito Codice).
Componendo in maniera organica le innumerevoli disposizioni relative alla privacy, il Codice riunisce in un unico contesto la legge n.675/96 e gli altri decreti legislativi, regolamenti e codici deontologici che si sono succeduti in questi anni. Contiene anche importanti innovazioni che tengono conto della "giurisprudenza" del Garante e della direttiva dell'Unione Europea sulla riservatezza nelle comunicazioni elettroniche (direttiva 2002/58/CE).
Il Testo unico, ispirato all'introduzione di nuove garanzie per i cittadini, alla razionalizzazione delle norme esistenti e alla semplificazione degli adempimenti, conferma e aggiorna la disciplina in materia di sicurezza dei dati personali e dei sistemi informatici e telematici introdotta in precedenza e sostituisce la legge "madre" sulla protezione dei dati, n. 675 del 1996.
Finalità della nuova disciplina è la garanzia che il trattamento dei dati personali debba essere svolto nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali (art. 2, c. 1).

Il **Codice è diviso in tre parti**:

- la **parte I** è dedicata alle disposizioni generali, riordinate in modo tale da trattare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato;
- la **parte II**, speciale, è dedicata a specifici settori; questa sezione, oltre a disciplinare aspetti in parte inediti

(informazione giuridica, notificazioni di atti giudiziari, dati sui comportamenti debitori), completa anche la disciplina attesa da tempo per il settore degli organismi sanitari e quella dei controlli sui lavoratori;
- la **parte III** affronta la materia delle tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante.

Il Testo è corredato da tre allegati:
- **l'allegato A** che contiene i Codici deontologici (Giornalistici, scopi storici, statistici e ricerca scientifica, ecc.),
- **l'allegato B** "Disciplinare tecnico in materia di misure minime di sicurezza" che disciplina tassativamente le modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con o senza strumenti elettronici
- **l'allegato C** che disciplina i trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia.

3.2.2 Trattamento dei dati

Il trattamento dei dati è qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, che hanno per oggetto dati personali.
Le operazioni comprendono la raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione di dati, anche se non registrati in una banca di dati.
I trattamenti effettuati per gestire la propria agenda elettronica o cartacea, oppure una rubrica, o la propria posta personale non rientrano nell'ambito di applicazione delle norme sulla privacy
Alcuni trattamenti, come ad es. quelli effettuati per ragioni di giustizia, scopi di difesa o sicurezza dello Stato, per prevenzione e perseguimento di reati, sono soggetti solo in parte all'applicazione delle disposizioni sulla privacy.

3.2.3 Tipologie di dati

Dato personale
Dato personale è qualsiasi informazione che riguardi persone fisiche identificate o che possono essere identificate anche attraverso altre informazioni, ad esempio, attraverso un numero o un codice identificativo.
Sono, ad esempio, dati personali: nome e cognome o indirizzo, codice fiscale, ma anche un'immagine, la registrazione della voce di una persona, la sua impronta digitale, i dati sanitari, i dati bancari, ecc..
La persona può essere infatti identificata anche attraverso altre informazioni (ad es., associando la registrazione della voce di una

persona alla sua immagine, oppure alle circostanze in cui la registrazione è stata effettuata: luogo, ora, situazione).

Dato sensibile

Dato sensibile è un dato personale che, per la sua natura, richiede particolari *cautele*: sono dati sensibili quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'adesione a partiti, sindacati o associazioni, lo stato di salute e la vita sessuale delle persone.

Ma quali sono queste particolari cautele? I soggetti privati possono operare solo in base alle autorizzazioni del Garante e al consenso scritto degli interessati. I soggetti pubblici non devono richiedere il consenso, ma possono svolgere solo determinati trattamenti per rilevanti finalità di interesse pubblico, che dovranno disciplinare in dettaglio con propri Regolamenti.

Per quanto riguarda specificamente il trattamento dei dati sullo stato di salute in ambito sanitario pubblico e privato, esiste una particolare disciplina secondo la quale tale trattamento può essere svolto, di regola, soltanto con il consenso dell'interessato, se ciò serve per tutelare la sua salute o l'incolumità fisica. Per alcune specifiche esigenze di tutela della salute di terzi o della collettività (prevenzione e cure di malattie, ricerca medica ed epidemiologica, interventi in materia di igiene e sanità pubblica ecc.) gli "esercenti le professioni sanitarie" e gli organismi sanitari pubblici (ASL, Enti ospedalieri, medici-chirurghi) possono trattare i dati sanitari anche senza il consenso dei pazienti interessati, ma nel rispetto delle prescrizioni contenute in un'autorizzazione del Garante (n.2/2000). È bene fare riferimento alla disciplina per il trattamento dei dati sensibili prevista negli artt. 20, 22 e 26 del Codice.

Dato giudiziario

Dati giudiziari sono i dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione). Rientrano in questa categoria anche la qualità di imputato o di indagato. Per una elencazione completa dei dati definiti giudiziari si veda la definizione contenuta nell'art. 4, comma 1, lettera e del Codice.

3.2.4 Soggetti coinvolti

Titolare del trattamento

Titolare del trattamento è la persona fisica, l'impresa, l'ente, l'associazione, ecc. cui fa capo effettivamente il trattamento di dati personali che ha il potere decisionale sugli scopi e sulle modalità del trattamento medesimo (comprese le misure di sicurezza).

Chi è il titolare? Nei casi in cui il trattamento sia svolto da una società o da una pubblica amministrazione per titolare va intesa l'entità nel suo complesso e non l'individuo o l'organo che l'amministra o la

rappresenta (presidente, amministratore delegato, legale rappresentante pro-tempore, sindaco, direttore generale ecc.). I casi in cui il trattamento può essere imputabile ad un individuo riguardano semmai liberi professionisti o ditte individuali.

Responsabile (del trattamento)
Responsabile del trattamento è la persona, la società, l'ente, l'associazione o l'organismo cui il titolare affida, anche all'esterno, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati. La designazione del responsabile è facoltativa con possibilità di nominare, sulla base di motivata esperienza, capacità e affidabilità, una pluralità di responsabili sia interni che esterni all'organizzazione (persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo).
Il titolare stabilisce un meccanismo di vigilanza periodica sull'attività svolta dal responsabile, per la verifica del rispetto da parte di quest'ultimo delle disposizioni in materia di trattamento, compreso il profilo della sicurezza e delle istruzioni impartite.

Incaricato (del trattamento)
Incaricato del trattamento è la persona (dipendente, collaboratore, ecc.) che per conto del titolare elabora o utilizza materialmente i dati personali sulla base delle istruzioni ricevute dal titolare medesimo (e/o dal responsabile, se designato).
La nomina è obbligatoria e per iscritto e individua puntualmente l'ambito di trattamento consentito. La designazione può essere individuale o, nel caso di organizzazioni complesse, anche per unità organizzativa se è individuato per iscritto l'ambito di trattamento consentito agli addetti all'unità medesima.

Interessato
L'interessato al trattamento è la persona fisica cui si riferiscono i dati personali (quindi, se un trattamento riguarda, ad es., l'indirizzo, il codice fiscale ecc. di Mario Rossi, Mario Rossi è l'interessato).

3.2.1 Punti rilevanti

Ecco, in sintesi, alcuni dei punti rilevanti del testo, che in molte parti recepisce e codifica le numerose pronunce emanate e i pareri forniti in questi anni dal Garante.

Sanità
In ambito sanitario è stata semplificata l'informativa da rilasciare agli interessati e il consenso al trattamento dei dati con un'unica dichiarazione resa al medico di famiglia o all'organismo sanitario (il consenso vale anche per la pluralità di trattamenti a fini di salute erogati da distinti reparti e unità dello stesso organismo, nonché da più strutture ospedaliere e territoriali).
Per il settore sanitario vengono inoltre codificate misure per il rispetto dei diritti del paziente: distanze di cortesia, modalità per appelli in

sale di attesa, certezze e cautele nelle informazioni telefoniche e nelle informazioni sui ricoverati, estensione delle esigenze di riservatezza anche agli operatori sanitari non tenuti al segreto professionale.
Per le prescrizioni mediche viene prevista anche la possibilità di non rendere sempre e in ogni caso immediatamente identificabili in farmacia gli intestatari di ricette.
Per i dati genetici viene previsto il rilascio di un'apposita autorizzazione da parte del Garante, sentito il Ministro della salute.
Per quanto riguarda le cartelle cliniche sono previste particolari misure per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati (comprese le informazioni relative ai nascituri), ma anche specifiche cautele per il rilascio delle cartelle cliniche a persone diverse dall'interessato.

Lavoro
Viene confermata l'elaborazione di un codice di deontologia e buona condotta che dovrà fissare regole per l'informativa ed il consenso anche degli annunci per finalità di occupazione (selezione del personale) e della ricezione dei curricula.
Il Codice affronta anche la questione dei controlli a distanza con la riaffermazione di quanto sancito dall'articolo 4 dello Statuto dei lavoratori (legge 300/1970).
Il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.

Trattamento dati personali in ambito giudiziario
Vengono meglio garantiti i diritti della personalità delle parti. Il Codice prevede anche che l'interessato possa chiedere, nel processo, di apporre sulla sentenza un'annotazione con la quale si avvisa che, in caso di pubblicazione su riviste giuridiche o su supporti elettronici o di diffusione telematica, devono essere omessi i dati dell'interessato. La versione della sentenza così pubblicata va sempre "criptata" quando si tratta di minori.
Con disposizione espressa si attribuisce maggiore tutela ai minori non solo nel processo penale, ma anche nei procedimenti civili e amministrativi.

Pubblica amministrazione
Il Codice innova anche, raccogliendo indicazioni del Garante, nella materia della notificazione degli atti giudiziari e degli atti amministrativi e impone la regola della busta chiusa per i casi di notifica effettuata a persona diversa dal destinatario.
Viene sancita espressamente la necessità per gli enti pubblici di approvare regolamenti per i trattamenti dei dati sensibili, ma solo con il parere conforme del Garante.

Liste elettorali
Le liste elettorali non possono essere più usate per promozione commerciale, ma solo per scopi collegati alla disciplina elettorale e

per finalità di studio ricerca statistica, scientifica o storica o a carattere socio assistenziale.

Telecomunicazioni

I cittadini potranno scegliere se essere inseriti nell'elenco telefonico e con quali modalità comparire sull'elenco: potranno decidere, in particolare, se far usare i loro numeri telefonici e indirizzi anche per informazioni commerciali o solo per comunicazioni interpersonali.
Vengono previste misure per combattere il fenomeno delle chiamate di disturbo.
Confermato il diritto a ricevere, su richiesta, fatture dettagliate (con le ultime tre cifre "in chiaro") in caso di contestazione.

Spamming

L'invio di messaggi attraverso sistemi automatizzati (Sms, Mms, fax, posta elettronica) richiede il consenso degli interessati.
Il cliente deve essere informato della possibilità di opporsi a "messaggi indesiderati".

Internet, videosorveglianza, direct marketing, credito al consumo

Per settori così delicati il Codice conferma la previsione di appositi codici deontologici che fissano regole specifiche.

Sanzioni

Il Codice prevede sanzioni pecuniarie e penali aumentate per chi viola la privacy, in particolare per l'uso dei dati senza consenso degli interessati, per il mancato adempimento nei confronti di un provvedimento del Garante, per la mancata informativa agli interessati sull'uso che si intende fare dei loro dati.

Misure di sicurezza

Vengono rafforzate, in un quadro di evoluzione tecnologica, le misure di sicurezza contro i rischi di distruzione, intrusione o uso improprio. Alle precauzioni già previste nella normativa precedente (password, codici identificativi, antivirus etc.) se ne aggiungono altre come: password di non meno di otto caratteri, autenticazione informatica, sistemi di cifratura, procedure per il ripristino dei dati.

Notificazione

È stata semplificata la notificazione, ovvero l'atto con cui l'impresa, il professionista o la pubblica amministrazione segnala all'Autorità i trattamenti di dati che intende effettuare. La notifica dovrà essere effettuata solo in particolari casi di trattamento di dati sensibili (specie se sanitari) con determinate modalità d'uso, ma anche per trattamenti particolarmente a rischio, effettuati con strumenti elettronici, nel campo della profilazione dei consumatori, oppure in relazione a procedure di selezione del personale e ricerche di marketing, nonché in ipotesi di utilizzo di informazioni commerciali e relative alla solvibilità. Diminuiscono le ipotesi di notifica obbligatoria e vengono snellite anche le modalità di presentazione: solo per via

telematica, seguendo le indicazioni del Garante sull'utilizzo della firma digitale.

Consenso
Resta sostanzialmente confermata la necessità del consenso, ma sono previste rispetto alla precedente disciplina alcune ipotesi di esonero per settori specifici, in cui il trattamento può essere effettuato senza consenso (art. 24 del Codice).
Il consenso è la libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (v. titolare).

Informativa
Rimane fermo l'adempimento dell'informativa agli interessati prima di procedere al trattamento dei dati. Il Garante può, comunque, individuare modalità semplificate in particolare per i servizi telefonici di assistenza e informazione al pubblico (*call center*).
L'informativa, che deve essere fornita dal titolare verbalmente o per iscritto, deve ad esempio precisare sinteticamente e in modo colloquiale quali sono gli scopi e le modalità del trattamento, se l'interessato è obbligato o no a fornire i dati, quali sono le conseguenze se i dati non vengono forniti, a chi possono essere comunicati o diffusi i dati, quali sono i diritti degli interessati, ecc..

3.2.2 Altre disposizioni

La normativa afferma e rafforza, rispetto alla precedente, i **principi fondamentali di necessità** (i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità (art. 3) del trattamento) e **di pertinenza, correttezza e non eccedenza** dei dati personali che devono essere trattati in modo lecito e corretto, raccolti e registrati per scopi determinati e legittimi, esatti e aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati.
La nuova disciplina riconosce priorità ai diritti degli interessati definendo i poteri del **diritto di accesso ai dati personali** e altri diritti (art. 7). L'esercizio dei diritti può essere effettuato con richiesta rivolta senza formalità al titolare o al responsabile anche per il tramite dell'incaricato (art. 8, c. 1) e può aver luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativo a giudizi, opinioni od altri apprezzamenti di tipo soggettivo. La richiesta rivolta al titolare o al responsabile può essere trasmessa mediante lettera raccomandata, fax o posta elettronica (art. 9, c. 1).

Il trattamento dei **dati sensibili** da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite (art. 20, c. 1).
In caso di disposizione di legge che specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici con atto di natura regolamentare (art. 20, c. 2).
Il trattamento di **dati giudiziari** da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili (art. 21, c. 1).
I **dati idonei a rivelare lo stato di salute e la vita sessuale** sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.
I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici (art. 22, c. 7). Il nuovo Codice conferma, rispetto alla precedente legge, la necessità di acquisire il **consenso** espresso dall'interessato per il trattamento di dati personali da parte di privati o di enti pubblici economici (art. 23, c. 1).

Il Codice conferma ed evidenzia con maggiore chiarezza rispetto alla precedente disciplina due distinti **obblighi di sicurezza**:

a) l'obbligo più generale di ridurre al minimo determinati rischi (art. 31)

I dati personali oggetto di trattamento devono essere custoditi e controllati per contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dei casi consentiti o altrimenti trattati in modo illecito. Resta in vigore l'obbligo di adottare **misure idonee** di sicurezza per fronteggiare le predette evenienze.
Come in passato, l'inosservanza di questo obbligo rende il trattamento illecito anche se non si determina un danno per gli interessati, ed espone a **responsabilità civile** per danno anche non patrimoniale qualora, davanti al giudice ordinario, non si dimostri di aver adottato tutte le misure idonee ad evitarlo (artt. 15 e 152 del Codice);

b) nell'ambito del predetto obbligo più generale, il dovere di adottare in ogni caso le "misure minime" (art. 33)

Il nuovo Codice rafforza l'obbligo di adottare le **misure minime** di sicurezza contro i rischi di distruzione, intrusione o uso improprio, volte ad assicurare comunque un livello minimo di protezione dei dati personali.

il Codice conferma l'impianto secondo il quale l'omessa adozione delle misure minime di sicurezza prescritte, le cui modalità sono specificate tassativamente nell'allegato B) del Codice, espone a **responsabilità penale** anche per colpa costituendo reato (art. 169 del Codice, che prevede l'arresto sino a due anni o l'eventuale "ravvedimento operoso").
La **notificazione del trattamento** (art. 37 del Codice), ovvero l'atto con cui l'impresa, il professionista o la pubblica amministrazione segnala all'Autorità Garante i trattamenti di dati che intende effettuare, non è più obbligatoria; essa non deve essere effettuata fatti salvi i casi particolari di trattamento espressamente previsti all'art. 37.
La presentazione è prevista **solo per via telematica**, seguendo le indicazioni del Garante quanto all'utilizzo della firma digitale.

3.2.3 Misure minime di sicurezza

Le **misure minime** sono definite dal Codice (art. 4, c. 3, lett a) come il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 del Codice.
Il Codice, come dovrà avvenire periodicamente in base all'evoluzione tecnologica (art. 36), ha aggiornato rispetto alla precedente normativa l'elenco delle "misure minime", le cui modalità di applicazione, sulla base di alcune prescrizioni di ordine generale (artt. 33-35), sono indicate analiticamente nelle regole incluse nell'allegato B) del medesimo Testo.
Analogamente a quanto avveniva in passato, le misure minime sono diverse a seconda che il trattamento sia effettuato o meno con strumenti elettronici, oppure riguardi dati sensibili o giudiziari.
Il trattamento di dati personali effettuato con **strumenti elettronici** (art. 35) è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) **autenticazione informatica** (definita come l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità, art. 4, c. 3 lett. c);
b) **adozione di procedure di gestione delle credenziali di autenticazione** (definiti come i dati e i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica art. 4, c. 3 lett. d);
c) **utilizzazione di un sistema di autorizzazione** (definito come l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente, art. 4, c. 3, lett. g);

d) **aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito** ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) **protezione degli strumenti elettronici e dei dati** rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) **adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi**;
g) **tenuta di un aggiornato documento programmatico sulla sicurezza** (soppresso dal D.L. 9 febbraio 2012, n. 5);
h) **adozione di tecniche di cifratura o di codici identificativi** per determinati trattamenti di dati idonei a rivelare lo **stato di salute o la vita sessuale** effettuati da organismi sanitari.

Il trattamento di dati personali effettuato **senza l'ausilio di strumenti elettronici** (art. 36) è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Il disciplinare tecnico di cui all'allegato B) relativo alle misure minime, sarà aggiornato periodicamente (art. 36) con decreto del Ministro della Giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.
Oltre alle precauzioni già previste nella normativa precedente (password, codici identificativi, antivirus etc.), se ne aggiungono altre come: password di non meno di otto caratteri, autenticazione informatica, sistemi di cifratura, procedure per il ripristino dei dati.

3.2.4 Documento programmatico sulla sicurezza

La precedente disciplina prevedeva, in caso di trattamento di dati sensibili o relativi a determinati provvedimenti giudiziari effettuati mediante elaboratori accessibili con una rete di telecomunicazioni disponibili al pubblico, l'obbligo di predisporre e aggiornare il Documento Programmatico sulla Sicurezza (DPS) almeno annualmente.
Anche la vigente disciplina aveva mantenuto l'obbligo di predisporre e aggiornare il DPS entro il 31 marzo di ogni anno, secondo le

prescrizioni contenute nel "Disciplinare tecnico in materia di misure minime di sicurezza" Allegato B) al Codice, sino all'entrata in vigore del Decreto Legge 9 febbraio 2012, n. 5 (convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35).
L'art. 45 del citato Decreto Legge ha soppresso dagli adempimenti in materia di misure minime di sicurezza l'obbligo della tenuta di un aggiornato documento programmatico sulla sicurezza, abrogazione che riguarda solo il documento e non l'adozione delle altre misure di sicurezza, da quelle minime (dalle password al backup) a quelle idonee, che rimangono in ogni caso obbligatorie.

3.3 PROVVEDIMENTI DEL GARANTE

3.3.1 Etichette intelligenti

Le etichette intelligenti sono dei minuscoli chip a radiofrequenza basati sulla tecnologia *Rfid* (*RadioFrequency Identification*) con circuiti in grado di contenere informazioni, di elaborarle e di trasmetterle. I chip si attivano quando entrano nel campo elettromagnetico generato da appositi lettori in grado di comunicare con l'etichetta.
Tramite le etichette *Rfid* si possono avere immediate informazioni su un prodotto, come la data di confezionamento o la scadenza, seguire i percorsi di un oggetto nella catena produttiva, conoscere in tempo reale le consistenze di un magazzino, facilitare l'accesso sui mezzi di trasporto o a determinati luoghi, effettuare rapidamente l'inventario dei libri in una biblioteca, identificare un bene dalla produzione allo smaltimento. I sistemi di pagamento a pedaggio automatici, come sulle autostrade, per esempio, si basano sulla tecnologia *Rfid*.
I sistemi *Rfid* possono essere utilizzati, a precise condizioni, per l'ingresso in determinati luoghi, per verificare l'identità di una persona (come avverrà con i nuovi passaporti elettronici) o per tutelare la salute delle persone (microchip sottopelle).
Alcuni usi sproporzionati di questa tecnologia potrebbero però violare il diritto alla protezione dei dati personali e determinare forme di controllo sulle persone. Con l'uso di sistemi *Rfid* sempre più evoluti si potrebbero infatti raccogliere dati sulle abitudini dei consumatori e seguire perfino gli spostamenti delle persone senza che esse se ne accorgano.
Il Garante segue con attenzione lo sviluppo di queste tecnologie e ha adottato anche un primo provvedimento generale con il quale ha indicato accorgimenti e cautele per rendere il loro impiego conforme alle norme sulla privacy.
Nel Provvedimento del Garante del 9 marzo 2005 sono state individuate garanzie per i cittadini e prescrizioni per chi intende produrre e utilizzare "etichette intelligenti":

- quando entriamo in un negozio o in un supermercato dobbiamo essere informati che si usano etichette *Rfid* e sono attivi i sistemi per "leggerle";

- su oggetti e prodotti dotati di etichette intelligenti deve essere apposta una specifica informativa;
- deve sempre essere garantito il diritto di asportare, disattivare o interrompere gratuitamente e in maniera agevole il funzionamento delle etichette *Rfid*.
- le *Rfid* non devono rimanere attive oltre la barriera/cassa dell'esercizio commerciale;
- per la verifica di accessi ad aree aziendali particolarmente riservate occorre rispettare i divieti sanciti dallo Statuto dei lavoratori riguardo all'utilizzo di strumenti per il controllo a distanza dei lavoratori.

3.3.2 Internet

Navigando in rete si lasciano molte tracce. L'uso illecito o non corretto dei dati personali da parte di terzi potrebbe mettere in pericolo la nostra privacy. Esistono però diversi mezzi per garantirci una navigazione sicura in Internet.
Il Codice affida all'autorità giudiziaria e al Garante nuovi compiti per svolgere controlli, esaminare controversie, bloccare o vietare trattamenti illeciti.
Occorre sapere che:

- L'indirizzo e-mail è un dato personale e potrebbe essere utilizzato per scopi diversi da quelli per i quali è stato reso noto fornendolo, ad esempio, in una chat line, in un forum o in un newsgroup. Il fatto che sia accessibile in rete non significa che sia liberamente utilizzabile da chiunque.
- Qualcuno potrebbe usare l'indirizzo di posta elettronica per fare spamming, intasando la casella di messaggi informativi o pubblicitari non richiesti.
- I siti web che si visitano potrebbero inviare cookies a insaputa dell'utente. Questi file, se da un lato rendono più veloce la navigazione, dall'altro possono consentire, ad esempio, al gestore del sito di riconoscere l'utente ad ogni successiva connessione e tracciarne il profilo.
- Durante la navigazione le informazioni che si rilasciano per effettuare un'operazione o visitare un sito potrebbero essere conservate per lunghi periodi, anche oltre la durata necessaria del servizio richiesto, e successivamente, utilizzate a insaputa dell'utente.

3.3.3 Lavoro: Linee guida per posta elettronica e Internet

Il Provvedimento Generale del Garante del 1 marzo 2007 prescrive ai datori di lavoro privati e pubblici di adottare la misura necessaria a garanzia degli interessati riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori, indicando chiaramente le modalità di uso degli strumenti

messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli.
Tale provvedimento indica inoltre, ai medesimi datori di lavoro, le seguenti **linee guida** a garanzia degli interessati per ciò che riguarda:

a) l'adozione e la pubblicizzazione di un **disciplinare interno**;
b) l'adozione di **misure di tipo organizzativo** affinché:
   - si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori;
   - si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet;
   - si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;
c) l'adozione di **misure di tipo tecnologico**, e segnatamente:
   I. **rispetto alla "navigazione" in Internet**:
      - l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
      - la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni;
      - il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;
      - l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
      - la graduazione dei controlli;
   II. **rispetto all'utilizzo della posta elettronica**:
      - la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;
      - l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
      - la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;
      - consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e

informato il lavoratore interessato alla prima occasione utile;
- l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
- la graduazione dei controlli;

Il Provvedimento **vieta ai datori di lavoro** privati e pubblici di effettuare trattamenti di dati personali mediante sistemi *hardware* e *software* che mirano al **controllo a distanza di lavoratori**, svolti in particolare mediante:

a) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
b) la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
d) l'analisi occulta di computer portatili affidati in uso;

Il Provvedimento individua i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati.

3.3.4 Amministratori di sistema

La figura dell'amministratore di sistema e delle altre figure assimilabili dal punto di vista dei rischi connessi alla privacy (*amministratore di basi di dati, amministratore di reti e di apparati di sicurezza e amministratore di sistemi software complessi*), riveste particolare rilevanza per la sicurezza dei sistemi, delle banche dati e per la corretta gestione delle reti telematiche, in quanto la funzione svolta comporta la concreta capacità di accedere a tutti i dati dei sistemi informativi ovvero ai dati che transitano sulle reti aziendali ed istituzionali.
Attività tecniche quali il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la gestione e manutenzione hardware e software comportano, in molti casi, un'effettiva capacità di azione su informazioni che va considerata, a tutti gli effetti, alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.
Tenuto conto della particolare criticità di tale ruolo[1], il Garante per la protezione dei dati personali ha emanato il 27 novembre 2008 un

[1] Il personale preposto alla gestione o manutenzione dei sistemi informatici, infatti, svolge un'attività particolarmente critica che si presta a possibili azioni non previste o illeciti che si configurano come specifici reati. Ci si riferisce, in particolare,

Provvedimento Generale con il quale ha prescritto ai titolari di trattamenti effettuati con strumenti elettronici accorgimenti e misure circa le attribuzioni delle funzioni di amministratori di sistema (o assimilate).
Tra gli accorgimenti previsti si citano, ad esempio, la designazione individuale per iscritto degli amministratori di sistema (o assimilati), l'obbligo di attivare il tracciamento dei loro accessi ai sistemi e di provvedere alla verifica periodica del loro operato, la redazione dell'elenco degli amministratori.
Il conferimento degli incarichi è effettuato in base al criterio del *need to know*, o criterio di necessità, cioè tramite la assegnazione di diritti di accesso strettamente inerenti le mansioni da svolgere e per il solo periodo di tempo necessario, ed in base al criterio di separazione (*segregation of duty*), o criterio di pertinenza, in modo che il personale preposto alla gestione operativa di sistemi operativi, database ed applicazioni non sia anche responsabile dei meccanismi di controllo della sicurezza (per esempio la gestione dei file di log o dei sistemi di controllo degli accessi).

3.3.5 Riutilizzo e distruzione dei supporti di memorizzazione

Il Provvedimento del Garante del 13 ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" estende le misure previste dalle regole 21 e 22[2] dell'Allegato B al D. Lgs. 196/2003 a tutti i supporti contenenti dati personali, indipendentemente dalla loro tipologia.
In particolare, il Provvedimento pone l'accento sulla necessità per i titolari che dismettono apparati elettronici o supporti (PC, *hard-disk, floppy disk, pen drive, cd-rom, dvd,* ecc.) di adottare idonei accorgimenti e misure volti a prevenire accessi non consentiti ai dati personali contenuti nelle apparecchiature destinate ad essere reimpiegate o riciclate, ovvero smaltite.
Per prevenire l'acquisizione indebita di dati è necessario operare in diversi modi e tempi a seconda delle circostanze:

- preventivamente, con tecniche di memorizzazione sicura con attivazione di funzionalità crittografiche proprie del sistema

---

all'abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615-ter) e di frode informatica (art. 640-ter e D.Lgs. 70/2003), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (articoli 635-bis e ter, D.Lgs 70/2003) e di danneggiamento di sistemi informatici e telematici (articoli 635-quater e quinques) di recente modifica.

[2] 21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

operativo; è bene proteggere i file usando una password di cifratura, oppure memorizzare i dati su hard disk o su altri supporti magnetici usando sistemi di cifratura automatica al momento della scrittura;
- immediatamente prima della cessione o dismissione dell'apparato elettronico, con strumenti software di cancellazione sicura delle informazioni registrate (a condizione che l'apparato sia funzionante);
- al momento della cessione o dismissione, con distruzione dei supporti mediante il ricorso a sistemi di punzonatura o deformazione meccanica o di vera e propria distruzione fisica del dispositivo di memorizzazione (usata per i supporti ottici come i cd-rom e i dvd) o di demagnetizzazione ad alta intensità che azzera tutte le aree di memoria elettronica e rende l'apparato inutilizzabile.

La semplice cancellazione dei file o la formattazione dell'hard disk, infatti, non sempre realizzano una vera cancellazione delle informazioni registrate, che rimangono spesso fisicamente presenti e tecnicamente recuperabili.

4 GENERALITÀ SULLA SICUREZZA INFORMATICA

4.1 PREMESSA

Come accennato in precedenza, i fattori di crescita ed evoluzione dell'ICT, con particolare riguardo allo sviluppo di reti di interconnessione tra i sistemi informativi, e la sua diffusione in uno spettro di applicazioni sempre più vasto hanno imposto una rigorosa attenzione agli aspetti legati alla sicurezza.
Internet sta divenendo sempre più il sistema di scambio di informazioni, di accesso alle grandi banche dati, di esecuzione di transazioni e disposizioni finanziarie, di sviluppo di attività professionali e, parallelamente si sta evidenziando la sua attuale fragilità.
A fianco di eventi distruttivi motivati da vandalismo, azioni di cyber terrorismo, puro esibizionismo cibernetico, si verificano molti attacchi rivolti a carpire informazioni, per scopi di concorrenza commerciale piuttosto che per attuare frodi informatiche. Non vanno dimenticate le troppo abusate forme di attacco a sistemi informatici e di comunicazione, che sono finalizzate principalmente a compromettere il corretto funzionamento di un sistema o a carpire informazioni commerciali o informazioni relative alle abitudini di vita di un utente, quali *spyware*, *cookies*, *sniffing*, *tracking*, *hijacking*, sino a raggiungere intollerabili azioni invasive delle caselle di posta elettronica come lo *spamming*.
In questo scenario la sicurezza informatica deve essere un elemento fondamentale nel processo di avvicinamento, tramite la tecnologia, del cittadino e delle istituzioni private (i "clienti" dell'e-government)

alla PA. Infatti, aldilà della disponibilità di servizi, è necessario fornire al "cittadino" precise garanzie in relazione al rispetto delle principali proprietà di sicurezza dei servizi stessi, al fine di assecondare quelle attività di coinvolgimento e di collaborazione tra "cittadino" e PA, che sono alla base di ogni processo di e-government.
Queste considerazioni impongono la ricerca delle necessarie garanzie. La prima è quella di poter dialogare con servizi della PA che offrano:

- un elevato grado di sicurezza, in termini di riservatezza, integrità disponibilità e autenticità;
- il trattamento dei dati personali e la gestione delle transazioni fatte secondo i dettami delle direttive europee e della normativa sulla protezione dei dati personali;
- una chiara informazione sulle modalità da seguire per richiedere controlli ed azioni correttive e rivolgere reclami.

La seconda garanzia è quella di una visione unitaria della sicurezza in rete che può derivare solo da una stretta cooperazione tra le istituzioni, le imprese e i maggiori protagonisti della *high-tech* e dei servizi ICT al fine di disporre:

- di standard semplici e sicuri;
- dello sviluppo e della diffusione di tecnologie che contribuiscano a migliorare la sicurezza dei prodotti e dei servizi;
- di norme di base, chiare ed omogenee tra loro, corredate dalle necessarie ed applicate sanzioni amministrative e penali;
- di una azione di autoregolamentazione fondata su convinti e rispettati codici deontologici;
- di infrastrutture che possano assecondare il processo di "messa in sicurezza" delle risorse e delle attività, in ambito nazionale, della società dell'informazione.

4.2 CONCETTI BASE

Tutti i piani di e-government si pongono l'obiettivo di semplificare i procedimenti amministrativi e burocratici per fornire servizi ai cittadini affrancandoli dagli obblighi di conoscere il modello organizzativo dello Stato, l'amministrazione competente e la documentazione necessaria per il servizio richiesto. Questo obiettivo sarebbe difficilmente raggiungibile se non si potesse confidare su adeguati livelli di sicurezza dei sistemi informativi.
La sicurezza delle informazioni è il mantenimento delle **proprietà** di:

- **Riservatezza**: disponibilità e comunicazione dell'informazione solo a chi è autorizzato;
- **Integrità**: tutela dell'accuratezza e della completezza delle informazioni (non compromissione dell'informazione);
- **Disponibilità**: accessibilità e utilizzabilità dell'informazione.

Possono essere, inoltre, coinvolte altre proprietà quali *l'autenticità*, la *responsabilità*, il *non ripudio* e *l'affidabilità.*

Affinché un utente possa fruire, attraverso un'interfaccia omogenea ("front office"), di servizi inter-amministrativi che richiedono l'attuazione di procedimenti presso amministrazioni diverse ("back office"), è necessario:

- garantire l'autenticazione dell'utente e l'autorizzazione all'erogazione del servizio (processi di "**autorizzazione**"), richiesto (processi di "**attivazione**");
- eseguire tali procedimenti amministrativi presso le amministrazioni di competenza (processi di "esecuzione");
- fornire i risultati all'utente (processi di "**erogazione**");
- gestire gli aggiornamenti delle informazioni, conseguenti all'erogazione del servizio, presso le diverse Amministrazioni coinvolte (processi di "**fall back**");
- tracciare tutte le azioni significative che concorrono all'erogazione del servizio (processi di "**tracciatura o logging**"),
- fornire adeguata assistenza attraverso strutture di call center e di help desk (processi di "**assistenza utente**").

5 SICUREZZA ORGANIZZATIVA

5.1 ORGANIZZAZIONE DELLA SICUREZZA

La Direttiva del Presidente del Consiglio dei Ministri del 16/1/2002 ha fornito alcune indicazioni per assistere le PP.AA. (Amministrazioni dello Stato, aziende ed amministrazioni autonome dello Stato, enti pubblici non economici nazionali) nell'individuazione delle misure di protezione che debbono essere realizzate e gestite con assoluta priorità, al fine di supportare le medesime sia nell'applicazione degli adempimenti normativi vigenti (D.Lgs 196/03), sia nel contrastare eventuali minacce.
In linea con la Direttiva sopra menzionata, il corretto svolgimento delle azioni di prevenzione, protezione e contrasto deve avvenire tramite la definizione delle seguenti logiche organizzative:

- **Presidio globale**: sicurezza, analisi e gestione del rischio, controllo delle informazioni/servizi critici sono concetti che stanno assumendo una importanza sempre maggiore. Deve essere quindi assicurata una visione unitaria e strategica a livello dell'intera organizzazione (es. ente pubblico), anche attraverso l'eventuale istituzione di un "Comitato per la sicurezza", in grado di valutare sia il rischio operativo complessivo, sia le necessarie misure di sicurezza.
- **Corretta responsabilizzazione**: la valutazione del rischio e la realizzazione della sicurezza necessaria devono essere garantite dai ruoli dell'organizzazione che hanno a disposizione le effettive leve di responsabilità e di autonomia/delega, nonché di conoscenza dell'operatività per prendere decisioni chiave quali: classificare e valorizzare il bene, riconoscere un certo grado di esposizione al rischio, definire un conseguente livello di

protezione, monitorare la coerenza dei comportamenti con le politiche stabilite.

- **Bilanciamento rischio/sicurezza**: essere in sicurezza significa operare avendo ottenuto una ragionevole riduzione delle probabilità di accadimento di una determinata minaccia la cui presenza espone il bene ad un certo rischio. Qualsiasi investimento per la realizzazione di contromisure di sicurezza deve essere quindi rigorosamente collegabile al margine di riduzione del rischio ottenibile mettendo in campo quelle contromisure.
- **Separazione dei compiti**: vale per il processo della sicurezza il principio che "chi esegue non verifica", distinguendo tra monitoraggio e verifica della sicurezza. Per monitoraggio si intende l'attività di controllo continuo degli indicatori di performance, sicurezza e rischio, svolte dalla funzione/ruolo che realizza le misure di sicurezza, mentre per verifica si intende l'attività di controllo saltuaria che si sviluppa attraverso un vero e proprio audit da parte di una funzione/ruolo (Auditing) diversa da quella/o che ha realizzato la sicurezza.

Al fine di assicurare un corretto presidio organizzativo della sicurezza e consentire così sia una corretta gestione (security management system), sia una efficace diffusione e crescita della "cultura" della sicurezza, occorre definire la "rete di responsabilità" che equivale ad identificare chiaramente delle figure professionali nell'ambito della organizzazione.
Quanto espresso fin qui, in termini di "organizzazione della sicurezza", è di fatto applicabile a vari ambiti (sicurezza delle informazioni, sicurezza del lavoro, ecc.).
L'organizzazione della sicurezza, in particolare, si esplica nella definizione di "politiche generali" per la sicurezza e di un insieme (congruente con le dimensioni e complessità dell'organizzazione presa in esame) di "politiche specifiche" per la tematica di interesse.
Pertanto, se analizziamo l'ambito della sicurezza delle informazioni e, più in dettaglio, la sicurezza ICT, intendendo per essa la sicurezza di tutte le "risorse" di cui si avvale il patrimonio informativo di una specifica organizzazione, è auspicabile che sia definita e formalizzata la "politica per la sicurezza ICT".
Questo in quanto l'adozione e la gestione delle più appropriate misure di sicurezza ICT nell'ambito di un'organizzazione richiede alla stessa la rivisitazione e l'adeguamento di una serie di processi e funzioni dando vita a quello che viene solitamente definito come il processo della sicurezza ICT. Queste misure correttive sono generalmente introdotte in maniera graduale e sono definite proprio in un documento noto come **Politica di sicurezza ICT.**
La definizione di questo documento è quindi un requisito irrinunciabile per la predisposizione e la buona riuscita di un processo di "messa in sicurezza" di un'organizzazione. A tale proposito vale la pena

ricordare che nell'ambito di un'organizzazione una politica di sicurezza può essere sviluppata a diversi livelli:

- a livello dell'intera organizzazione, in questo caso il documento raccoglierà tutte le prescrizioni che si ritiene debbano valere in qualsiasi parte dell'organizzazione stessa; può essere utile precisare che, pur essendo d'alto livello, questo documento non deve necessariamente limitarsi a contenere prescrizioni molto generali. È infatti anche possibile includere in tale politica eventuali specifiche tecniche dettagliate che si desideri siano soddisfatte da tutti i sistemi ICT dell'organizzazione;
- a livello di singole componenti, nel caso di un'organizzazione molto complessa (come ad es. un ente pubblico), può essere conveniente sviluppare ulteriori politiche di sicurezza valide per parti dell'organizzazione. In genere tale convenienza sussiste quando è possibile individuare un dominio sufficientemente ampio entro il quale si debbano adottare modalità di gestione e protezione omogenee che non siano già previste nella politica di sicurezza dell'intera organizzazione.

Nelle politiche di sicurezza fin qui citate, che si possono considerare di tipo organizzativo, non sono trattate in modo completo le modalità secondo le quali i singoli sistemi ICT devono gestire e proteggere le informazioni da essi trattate. A tale scopo devono infatti essere sviluppate ulteriori politiche di sicurezza valide per sistemi ICT specifici e/o per classi di essi. Nelle politiche di sicurezza di tipo organizzativo, tuttavia, vengono generalmente fornite indicazioni circa le modalità secondo le quali si ritiene che le politiche dei sistemi ICT debbano essere sviluppate.

Riguardo alle figure professionali "chiave" coinvolte nella attuazione delle politiche di sicurezza si citano, in particolare:

1. Responsabile della sicurezza ICT

È il soggetto cui compete la definizione delle soluzioni tecniche, in attuazione delle direttive impartite direttamente, ad esempio, dagli Organi nel caso degli enti pubblici o dal Ministro o su indicazione del Comitato per la sicurezza ICT. La definizione delle soluzioni tecniche deve essere eseguita dal Responsabile della sicurezza ICT sviluppando opportune politiche di sicurezza dei sistemi ICT che trattano le informazioni e applicazioni utilizzate nell'ambito dell'organizzazione.
Per le PP.AA. tale sviluppo deve essere eseguito partendo dalle indicazioni contenute nella politica di sicurezza della PA e nella eventuale politica di sicurezza dell'Amministrazione e si deve avvalere di una metodologia di analisi e gestione del rischio, come descritto nel seguito. Il Responsabile della sicurezza ICT ha il compito di fornire al Responsabile dei sistemi informativi le definizioni relative alle soluzioni tecniche al fine della loro realizzazione e del monitoraggio del loro corretto funzionamento.

2. Responsabile dei sistemi informativi

Nell'ambito della PA è il referente istituito dal decreto legislativo n.39/93, cui compete la pianificazione degli interventi di automazione, l'adozione delle cautele e delle misure di sicurezza, la committenza delle attività da affidare all'esterno. Il Responsabile dei sistemi informativi può nominare suoi assistenti in numero proporzionato alla complessità dei servizi informatici gestiti dall'Amministrazione.

3. Gestore esterno

È il fornitore di servizi che opera sotto il controllo del responsabile dei sistemi informativi.
Nel caso in cui i fornitori svolgano servizi critici dal punto di vista della sicurezza è estremamente importante che l'organizzazione (Amministrazione dello Stato, ente pubblico, ecc.) si cauteli adeguatamente, esplicitando chiaramente nei contratti gli obblighi e le responsabilità che il Gestore esterno deve assumersi nel fornire il servizio e mantenendo il più possibile un controllo sugli aspetti di maggiore criticità che caratterizzano il servizio stesso.

4. Proprietario dei dati e delle applicazioni

È ciascun responsabile/referente dell'organizzazione (ad es., per gli enti pubblici, Direttore Centrale, Direttore Regionale, ecc.) per la sfera di informazioni di diretta competenza o trattamento.

5. Addetto alle verifiche di sicurezza ICT

Svolge un'attività di controllo saltuaria che si sviluppa attraverso un vero e proprio audit. Tale audit deve mirare a verificare la completa e corretta realizzazione delle soluzioni tecniche ed il recepimento di tutte le indicazioni contenute nella politica di sicurezza della PA, nella eventuale politica di sicurezza dell'organizzazione (Amministrazione dello Stato, ente pubblico, ecc.) e nelle Politiche di sicurezza dei sistemi ICT. Ove necessario, l'addetto alle verifiche di sicurezza ICT potrà avvalersi di tecniche di penetration testing al fine di verificare la resistenza dei sistemi ICT dell'organizzazione ad eventuali attacchi. In base al principio della separazione dei compiti enunciato nella direttiva sulla sicurezza ICT, l'addetto alle verifiche di sicurezza ICT non può essere chi ha il compito di installare, configurare e aggiornare le soluzioni tecniche definite dal Responsabile della sicurezza ICT. Nei casi in cui sia richiesto un livello di sicurezza più elevato alle verifiche periodiche eseguite dai soggetti che ricoprono questo ruolo dovrà essere aggiunta l'effettuazione di vere e proprie certificazioni della sicurezza ICT.
L'addetto alle verifiche di sicurezza ICT può nominare suoi assistenti in numero proporzionato alla complessità dei servizi informatici gestiti dall'organizzazione.

5.2 GESTIONE DELLA SICUREZZA

In generale, per **Politica di sicurezza** s'intende l'insieme delle leggi, regole e pratiche che governano la gestione e protezione delle "risorse" dell'organizzazione, all'interno del dominio di validità della politica stessa.
A tale scopo la direttiva citata in precedenza prevede, ad esempio, di calare sull'organizzazione un sistema di gestione della sicurezza (security management system) composto da:

- Carta della sicurezza, che definisce gli obiettivi e le finalità delle politiche di sicurezza, le strategie di sicurezza scelte dall'organizzazione nonché il modello organizzativo ed i processi per attuarle.
- Politiche generali di sicurezza, che indicano, coerentemente con la Carta della sicurezza, le direttive da seguire per lo sviluppo, la gestione, il controllo e la verifica delle misure di sicurezza da adottare; devono essere modificate al verificarsi di cambiamenti di scenario.
- Politiche specifiche di sicurezza (norme), focalizzate sull'emissione di normative afferenti argomenti rilevanti per l'organizzazione, il personale, i sistemi e aggiornate frequentemente sulla base dei cambiamenti organizzativi e tecnologici.
- Specifiche procedure, a supporto della gestione operativa delle contromisure tecnologiche adottate, riguardanti ad esempio:
    - la gestione della "system security";
    - la gestione della "setwork security";
    - il ciclo di vita del software;
    - la gestione operativa;
    - la continuità del servizio;
    - la gestione degli incidenti;
    - il controllo e il monitoraggio del sistema di sicurezza;
    - la sicurezza del personale.

Alla luce di quanto sopra e come già indicato nel precedente paragrafo, al fine di garantire una efficace protezione del patrimonio informativo, occorre definire una "Politica di sicurezza ICT" per gestire in modo specifico la protezione di particolari informazioni/servizi che si avvalgono di infrastrutture tecnologiche e di applicazioni informatiche.
Per poter sviluppare adeguate e specifiche politiche di sicurezza ICT occorre adottare una **metodologia di analisi e gestione del rischio** inteso come quel processo necessario per identificare i rischi di sicurezza e determinarne la loro portata. In altri termini l'analisi e gestione del rischio è quel processo che definisce le esigenze di sicurezza ICT di un'organizzazione, supportando la scelta delle misure di controllo più appropriate.

Naturalmente tutti gli sforzi devono essere compiuti affinché gli incidenti informatici non abbiano a verificarsi, adottando le opportune contromisure sia a livello tecnico sui sistemi ICT sia a livello organizzativo.
Nei casi, tuttavia, in cui l'incidente finisce ugualmente per verificarsi è estremamente importante che sia stato sviluppato e che sia pienamente operativo un piano che garantisca il più possibile la continuità dei servizi offerti dai sistemi ICT colpiti dall'incidente.
A tale scopo è necessario che sia adottato un **piano di business continuity** (contingency plan). Lo scopo di questo piano è quello di individuare tutte le misure (tecnologiche e organizzative) atte a garantire la continuità dei processi dell'organizzazione in funzione del loro valore e della qualità dei prodotti/servizi erogati tramite il supporto dell'infrastruttura di ICT, prevenendo e minimizzando l'impatto di incidenti intenzionali o accidentali e dei conseguenti possibili danni.
Inoltre deve essere ampiamente diffusa la **cultura della sicurezza** e deve permeare nella organizzazione, a tutti i livelli, la consapevolezza che ciascuno contribuisce a garantire la sicurezza; per questo deve essere adottato un **piano di formazione per la sicurezza** le cui sessioni devono essere erogate in funzione dei ruoli e delle responsabilità assegnate.

6 ANALISI E GESTIONE DEL RISCHIO

6.1 GENERALITÀ

Il rischio è la possibilità che una azione o una scelta (inclusa quella di non agire) porti ad una perdita o ad un danno o ad un evento indesiderabile o ad un impatto negativo.
L'analisi e gestione del rischio (risk management) è il processo mediante il quale si analizza, si misura o si stima il rischio e, successivamente, si sviluppano strategie per governarlo.
In ambito ICT, si tratta di identificare, analizzare e valutare i rischi potenziali sul patrimonio informativo e informatico dell'organizzazione e di determinare le azioni da intraprendere e le modalità per il trattamento dei rischi.
L'analisi e gestione del rischio è un processo fondamentale per la pianificazione, realizzazione e gestione di qualsiasi sistema di sicurezza ICT.
Infatti, senza una costante valutazione del valore del patrimonio informativo, dell'intensità delle minacce attuali e potenziali, delle vulnerabilità del sistema e dei potenziali impatti tangibili e intangibili sull'attività dell'organizzazione, risulta impossibile definire un sistema di sicurezza veramente equilibrato e bilanciato rispetto ai rischi ed ai danni/perdite che potrebbero verificarsi.

Il processo di analisi e gestione del rischio si compone di due macro-fasi:

- **analisi e valutazione del rischio** (risk assessment) che consente di identificare i rischi potenziali per l'organizzazione e di determinarne la probabilità di accadimento, l'impatto conseguente e le possibili salvaguardie da introdurre per mitigare questo impatto;
- **gestione del rischio** (risk treatment) che consente di creare una strategia di protezione per la riduzione dei rischi ritenuti non accettabili da parte dell'organizzazione, identificando le azioni da intraprendere, le responsabilità e le priorità nella gestione del rischio in base a quanto emerso dalla fase di valutazione.

Ii risultati dell'analisi e valutazione del rischio aumentano la consapevolezza dell'organizzazione verso la necessità di protezione dei propri beni supportando la scelta delle più adeguate misure di sicurezza. Dopo aver valutato i rischi si analizzano le misure di protezione già in atto e quelle ipotizzate e si rieseguono le fasi previste nella valutazione al fine di determinare la situazione ottimale di "gestione del rischio".

Diamo alcune definizioni utili al processo:

- per **asset** si intende qualunque "bene" materiale (ad es. le risorse tecnologiche) o immateriale (ad es. le informazioni) che abbia un valore per l'organizzazione;
- per **minaccia** s'intende una possibile causa di incidente indesiderato che può comportare danni ad un sistema o a una organizzazione;
- per **vulnerabilità** s'intende una debolezza di un asset o gruppo di asset che può essere attualizzata da una minaccia.

6.2 ANALISI E VALUTAZIONE DEL RISCHIO

Il processo di analisi e valutazione del rischio (risk assessment) si compone di due fasi:

- **analisi dei rischi** che consente di identificare le cause e stimare i rischi cui l'organizzazione è soggetta (analisi minacce, analisi vulnerabilità, ecc.);
- **valutazione dei rischi** che valuta la significatività e l'accettabilità dei rischi identificati (con misure in essere e da adottare).

Le metodologie di supporto alla conduzione di tali attività sono molteplici.
Nel seguito viene descritta, nelle sue linee generali, la metodologia più comunemente usata anche dai tools informatici che supportano queste attività.

Dopo aver "censito" i beni fondamentali il primo passo procedurale dell'attività di analisi dei rischi riguarda l'analisi delle **minacce** cui tali beni sono soggetti. Conseguentemente è necessario:

- individuare e descrivere l'associazione asset/minacce;
- valutarle riguardo alla frequenza, probabilità e gravità;
- calcolare, sulla base di indicazioni metodologiche predefinite, un indice di minaccia associato a ciascun asset.

A seguire viene condotta l'analisi delle **vulnerabilità** di ciascun asset, intesa come mancanza o carenza di contromisure adeguate a proteggere il bene. Si prosegue con:

- l'associazione scoperto/minacce (quanto l'asset è scoperto rispetto ad ogni minaccia);
- la valutazione delle vulnerabilità (rispetto a ciascuna minaccia) come quota di perdita dell'asset in caso di attuazione della minaccia.

Le associazioni tra asset/minacce e asset/vulnerabilità sono facilmente rilevabili dalla letteratura disponibile sull'argomento e sono comunque già presenti, come liste di scelta, nei tools informatici di supporto a questi processi.
Per arrivare a valutare correttamente i rischi che incombono sugli asset è necessario identificare le contromisure già in essere e rielaborare l'analisi delle vulnerabilità tenendo presente l'esistenza di tali contromisure

Pertanto, il **calcolo del rischio**, viene effettuato tenendo presente sia le contromisure esistenti, sia eventuali nuove misure pianificate per aumentare la protezione dei beni.

6.3 GESTIONE DEL RISCHIO

La gestione del rischio (risk treatment) è il processo riguardante la selezione e la realizzazione di misure per modificare il livello di rischio.
Prima di avviare il processo di analisi e valutazione del rischio è necessario che la Direzione (dell'organizzazione) stabilisca i criteri di "accettabilità" del rischio, che equivale a determinare qual'è il livello del rischio al di sotto del quale non sono necessari ulteriori interventi (massimo rischio tollerabile per ciascun asset).
La applicazione delle contromisure abbatte ovviamente il rischio. Vengono pertanto eseguiti più assessment valutando il livello di riduzione del rischio conseguente all'applicazione delle contromisure.
I passi procedurali di questa fase, quindi, sono:

- l'individuazione e la selezione delle **contromisure** a fronte delle vulnerabilità identificate;
- l'individuazione e calcolo del **rischio residuo**;
- la definizione delle regole utili a determinare **l'accettazione del rischio residuo** dopo l'applicazione delle contromisure.

6.4 REPORT ALLA DIREZIONE

Questa fase prevede l'analisi delle informazioni rilevate durante la fase di analisi e valutazione del rischio, al fine di elaborare un report per la Direzione che renda palese quali siano i maggiori rischi che minacciano il business sia di natura organizzativa che tecnologica.
Deve essere altresì formalizzato un piano di azione che assicuri che tutti i necessari miglioramenti in termini di protezione e controllo siano implementati secondo scadenze temporali.

7 SICUREZZA LOGICA

Un sistema informativo sicuro deve garantire la riservatezza, l'integrità e la disponibilità delle informazioni in esso contenute. In tale contesto il sistema informatico può essere pensato come costituito da due grosse componenti:

1. l'infrastruttura (con i relativi sistemi operativi, e sw specialistico, es. sicurezza, backup, monitoraggio, ecc.);
2. le applicazioni.

7.1 SICUREZZA DEL SOFTWARE

La sicurezza delle applicazioni su base locale o in rete impone una rigorosa riflessione sui meccanismi di produzione del software e sulla univocità dello stesso.
Per le applicazioni in rete, si tratta di esigenze relativamente recenti per le quali il modello di riferimento non è ancora pienamente consolidato. Attualmente, si continua ad arricchire il profilo funzionale raccogliendo il numero maggiore di comportamenti sistemici o architetturali sulla base dell'esperienza che progressivamente viene a consolidarsi.

7.2 PRODUZIONE E CERTIFICAZIONE DEL SOFTWARE

L'osservazione sui metodi di produzione e distribuzione del software fa emergere le seguenti osservazioni:

- la strutturale debolezza della catena produttiva (progettazione, stesura delle specifiche, costruzione del prototipo, controllo dei risultati attesi, rilascio della versione finale alla data prevista);
- la necessita di misurare l'errore nel meccanismo di produzione.

Si tratta di elementi che si può provare a tenere sotto controllo, ma che non possono essere rimossi e con cui bisogna convivere per contenere gli effetti indesiderati. Allo stato attuale delle esperienze consolidate, appare necessario utilizzare un modello di certificazione del meccanismo di produzione software e del software consolidato da immettere nel circuito distributivo.
Attualmente vi sono opinioni differenti sui meccanismi di certificazione del software. Spesso rispecchiano l'opinione aziendale dei produttori e non la condivisione di un modello comportamentale.

Appare utile ritenere che il software vada certificato ad ogni sua nuova emissione o successiva modificazione; anche se la nuova certificazione impone costi aggiuntivi e tempi più lunghi di rilascio.

7.3 AUTENTICAZIONE DEL SOFTWARE

I processi di autenticazione del software consentono all'utente di accertarsi che l'applicazione con cui sta interagendo è proprio quella che eroga i servizi di cui vuole usufruire. Questa funzionalità è importante quando i servizi sono erogati su reti telematiche aperte.
L'autenticazione dell'utente abbinata all'autenticazione della applicazione prende il nome di ***mutua autenticazione***
Tale controllo può essere effettuato verificando che il codice in questione sia digitalmente firmato e che il firmatario sia persona o organizzazione, con i quali l'Amministrazione o l'ente ha rapporti di fiducia. in caso contrario, viene interdetto l'accesso al codice.
Le funzionalità precedenti si possono ottenere interamente o in parte con le seguenti tecnologie:

- sicurezza a livello di trasporto (**IPSEC**);
- sicurezza a livello di sessione (protocollo **SSL**);
- sicurezza applicativa (sicurezza **end to end**).

7.4 PROPRIETÀ DI UN'APPLICAZIONE SICURA

La definizione di sistema sicuro più referenziata è quella che fa riferimento alle proprietà di confidenzialità, integrità e disponibilità. In particolare, un sistema o un'applicazione sicura devono garantire il soddisfacimento delle suddette proprietà per poter essere definite tali. Nella definizione delle specifiche di un'applicazione sicura è quindi necessario definire i suddetti requisiti.
In specifico, tra le proprietà più utilizzate vi sono l'autenticità, la tracciabilità e la non ripudiabilità.

7.4.1 Confidenzialità o riservatezza

Un'applicazione soddisfa la proprietà di confidenzialità quando è in grado di garantire che le risorse di cui dispone sono accessibili in lettura solo da persone autorizzate. Per confidenzialità di un'applicazione si intende quindi la ***capacità di un'applicazione di non consentire ad utenti non autorizzati l'accesso ad informazioni sensibili.*** La confidenzialità viene referenziata, anche, come segretezza, riservatezza o privacy. Solitamente però il termine **privacy** viene utilizzato per definire la ***protezione di informazioni personali.*** Il sistema più sicuro per garantire la confidenzialità dei dati è quella di operare sugli stessi una serie di trasformazioni crittografiche in modo da renderli effettivamente accessibili solo a chi possiede le relative chiavi di decifratura.

7.4.2 Integrità

Genericamente, potremmo dire che per integrità si intende la ***capacità di un sistema di prevenire operazioni di "modifica" (scrittura, cancellazione, modifica, …) non autorizzate.***
Applicato ai dati il termine integrità sta a significare che i dati sono nello stato in cui li ha lasciati l'ultima computazione correttamente eseguita, e che non hanno subito manipolazioni, modifiche o cancellazioni non autorizzate.
Per garantire l'integrità delle informazioni nell'ambito di un sistema informatico si ricorre generalmente a particolari tecniche crittografiche.
Tali tecniche consistono nel calcolo di un'impronta di un certo file ad un certo istante di tempo, alla sua memorizzazione su di un supporto rimovibile ed alla verifica periodica tra l'impronta del file nel suo formato corrente e l'impronta memorizzata.

7.4.3 Disponibilità

Per disponibilità di una risorsa o di un'applicazione si intende la ***capacità della stessa di poter essere accessibile e utilizzabile a ogni richiesta inoltrata da un utente autorizzato***. La proprietà di disponibilità è utilizzata, con significati diversi, anche in altri settori ed in particolare nell'ambito dei sistemi critici.
Nel contesto della sicurezza informatica, garantire la disponibilità di una risorsa significa prendere tutte le misure precauzionali affinché un intruso non sia in grado di accedere alla risorsa stessa.
Recentemente diversi host delle rete Internet sono stati vittime di attacchi noti come **Denial of Service (DOS)**, che hanno di fatto disabilitato l'accesso a questi host da parte di utenti autorizzati.

7.4.4 Non Ripudiabilità

La non ripudiabilità è una proprietà che caratterizza transazioni eseguite in rete tra due parti e ***fa sì che l'originario di una transazione non possa negare la paternità della stessa.***
Applicato ad un sistema di posta elettronica questo significa che, se il sistema gode della proprietà di non ripudiabilità, colui che invia un messaggio non possa negare in tempi successivi i seguenti due elementi:

a. di averlo effettivamente inviato;
b. il contenuto dello stesso.

7.4.5 Vulnerabilità

Quando si eroga un sevizio in rete, il sistema informativo soggiacente è per definizione vulnerabile agli attacchi derivanti da utenti che, intenzionalmente o inavvertitamente, sfruttano bachi di sicurezza che possono derivare dai sistemi di supporto e/o nelle applicazioni stesse oppure dalla natura intrinseca dell'architettura di sistema e delle risorse utilizzate.

7.5 MINACCE

Diversi sono i tipi di attacchi e diversi gli scopi per i quali vengono perpetrati. Di seguito indichiamo i più noti cercando, oltre alla definizione, di indicare le possibili cause di vulnerabilità.

1 **Autorizzativo -** Intrusione attraverso l'impersonificazione.

Un intruso cerca di raggirare il processo di autenticazione e presentarsi al front office con una falsa identità.
Se l'attacco riesce l'intruso potrà usufruire di alcuni tipi di informazioni anche senza esserne autorizzato.
Le tecniche più usate per effettuare l'impersonificazione vanno dal password guessing sino allo sfruttamento di bachi presenti nel sistema operativo degli host.

2 **Attivazione -** Intrusione attraverso l'impersonificazione.

Anche in questi casi il problema principale con cui confrontarsi è quello dell'impersonificazione anche se diverso è il dominio di riferimento rispetto a quello del processo autorizzativo. Nel processo di attivazione infatti, l'autenticazione anziché avvenire tra utente finale e amministrazione, avviene tra amministrazione e amministrazione. Si possono quindi adottare dei meccanismi che ne rendono più difficile lo "scavalcamento".

3 **Esecuzione -** Abuso di privilegi.

Va evitato, attraverso un controllo degli accessi, che un processo autorizzato ad accedere ad un certo insieme di dati possa anche accedere ad altre informazioni per il cui accesso non ha ottenuto autorizzazioni.

4 **Erogazione -** Intercettazione delle informazioni.

Vanno implementate tecniche di crittografia o comunque tecniche atte a garantire la riservatezza delle informazioni nei riguardi di soggetti non autorizzati a conoscerne il contenuto.

5 **Fall back -** Affidabilità (autenticità) della fonte e integrità dell'informazione trasmessa.

È necessario premunirsi affinché le sorgenti da cui provengono le informazioni siano state preventivamente autenticate e che l'informazione trasmessa non sia stata in qualche modo manipolata ma corrisponda esattamente a quella trasmessa dalla fonte originale.

6 **Tracciabilità -** Distruzione del logging.

È necessario premunirsi affinché i file dove sono contenuti questi dati della tracciabilità dell'evento (chi, come e quando) non siano modificati, rimossi o compromessi.

Tutti i processi sopra menzionati, possono essere a loro volta oggetto di attacchi del tipo Denial of Service (DOS), miranti a renderli praticamente inutilizzabili attraverso l'inoltro di un numero molto elevato di richieste false.

7.6 TECNOLOGIE

Dopo aver descritto quali debbano essere le proprietà richieste a qualunque applicazione sicura, è necessario estendere la descrizione dei principali meccanismi utilizzati in ambito applicativo per garantire il soddisfacimento delle suddette proprietà.
Tali meccanismi sono:

- identificazione/autenticazione;
- controllo degli accessi;
- *User accountability* (*tracciabilità degli utenti*).

Va sottolineata la non esaustività della suddetta lista, che contiene comunque gli elementi fondamentali per la realizzazione di una qualunque applicazione sicura.

7.6.1 Identificazione

Processo attraverso il quale una risorsa dichiara la propria identità nell'ambito di un sistema o di un'applicazione.
Nel caso di utenti umani è solitamente espressa attraverso uno **USERID** e specificata in un campo "*login name*" o "nome utente". Viene solitamente richiesta ogni volta che l'utente vuole accedere ad una risorsa gestita dal sistema o dall'applicazione, e viene assegnata all'utente quando lo stesso viene per la prima volta registrato nel sistema o tra gli utenti dell'applicazione.
Potenzialmente una persona può avere diverse identità in funzione della risorsa a cui accede, anche se, almeno all'interno di un circuito chiuso, sarebbe preferibile, anche per motivi di tracciabilità, assegnare lo stesso USERID ad un utente.

7.6.2 Autenticazione

È il processo attraverso cui, in una comunicazione tra due parti (uomo-macchina, macchina-macchina, uomo-applicazione, applicazione-macchina, ecc.) una parte verifica la veridicità dell'identità conclamata dall'altra parte. In alcune situazioni può essere necessario che tale verifica d'identità sia reciproca. In questi casi si parla di mutua autenticazione.
Il processo di autenticazione viene svolto basandosi su alcune proprietà che si conoscono essere possedute dalla controparte. Tipicamente i parametri utilizzati per svolgere tale fase sono:

- un segreto condiviso tra le due parti;
- un particolare oggetto in possesso della parte da autenticare;
- una caratteristica personale in possesso della parte da autenticare.

Sistemi di autenticazione basati sul primo parametro sono chiamati sistemi di autenticazione debole. I sistemi invece che utilizzano almeno uno degli altri parametri sono chiamati sistemi di autenticazione forte.

7.6.2.1 Autenticazione debole

Questo è il caso più generale e riconducibile all'uso di una **Password** o codice di accesso. Con il diffondersi delle reti di calcolatori si è giunti molto presto alla constatazione che il meccanismo delle password non è sufficientemente adeguato per garantire il livello di sicurezza richiesto nella fase di autenticazione. I motivi principali della sua non adeguatezza non risiedono nel meccanismo stesso, ma più che altro nel modo con cui vengono gestite le password dagli agenti che le utilizzano: i protocolli di rete e gli utenti.
D'altro canto, è stato definitivamente accertato che gli utenti costretti ad utilizzare le password per accedere a risorse di calcolo, scelgono password estremamente facili da indovinare. A tale proposito sono stati realizzati dei programmi che forniti di appositi dizionari tentano di indovinare le password degli utenti dei sistemi. L'uso di tali programmi in centri di calcolo di università, aziende, enti pubblici consente tipicamente di individuare almeno il 20% delle password degli utenti di tali sistemi.
Esistono alcune tecniche per limitare i danni, ad esempio:

- limitare il numero dei tentativi di utilizzo di quella password (bancomat);
- assegnare alla password un periodo temporale di validità;
- imporre una lunghezza minima o comunque dei vincoli nel formato della password (almeno sette caratteri non tutti alfanumerici o numerici, ecc.);
- assegnare una password, anziché farla scegliere all'utente;
- assegnare password monouso o one time password;
- crittografare la password durante la sua trasmissione e/o registrazione su file.

7.6.2.2 Autenticazione forte

Per far fronte ai problemi derivanti dall'uso di meccanismi di autenticazione debole sono stati predisposti dei meccanismi che sono in grado di rendere molto più sicura una qualunque fase di autenticazione. Tali meccanismi sono basati principalmente su sistemi di crittografia asimmetrica o sul meccanismo one time password.

One-time password

Meccanismo basato sull'uso di password che possono essere utilizzate una sola volta. Ogni utente di un sistema viene fornito di una lista di password e ogni volta che si collega ad un calcolatore usa una password sulla lista che poi provvederà a cancellare. Al prossimo collegamento userà la password successiva presente sulla lista. ***(challenge response)***

Crittografia asimmetrica

Un'altra tecnologia per ottenere l'autenticazione forte è quella basata su sistemi di crittografia asimmetrica, le cui caratteristiche peculiari sono:la presenza di una coppia di chiavi (pubblica e privata. Questa forma di autenticazione garantisce il non ripudio e prevede la presenza di una trusted party che garantisce l'abbinamento "identità della persona / chiave pubblica assegnata" attraverso il rilascio di un certificato digitale.
La chiave privata deve essere gelosamente custodita dal suo legittimo possessore.
(In pratica c'è una chiave per crittografare, che chiunque può vedere, e una per decifrare, che conosce solo il destinatario senza necessità quindi di riceverla (scambiarla) dal mittente. In altre parole, se A vuole ricevere un messaggio segreto da B, manda a B una scatola vuota con un lucchetto aperto senza chiavi. B mette dentro il messaggio, chiude il lucchetto, e rimanda il tutto ad A, che è l'unico ad avere le chiavi. Chiunque può vedere passare la scatola, ma non gli serve a niente. A non deve correre rischi con le sue chiavi).

Smart card

La smart card è uno strumento relativamente recente e tecnologicamente giovane. Può risultare di grande utilità poiché semplifica il riconoscimento forte dell'utilizzatore da parte del sistema.
Una smart card crittografica è un piccolo elaboratore con una sua CPU e sistema operativo. Le protezioni d'accesso alla smart card, ed alle sue singole componenti, sono gestite in genere mediante i due tipi di chiavi:

1. *External Key* (key0 - keyN);
2. *Card Holder Verification* (chv1 - chv2).

La carta d'identità elettronica

La Carta d'Identità Elettronica **(**CIE - token crittografico privilegiato per la digitalizzazione dei rapporti tra Stato e cittadino) si basa su tre principi:

1. la sicurezza dello strumento;
2. l'utilizzo della carta d'identità elettronica come carta servizi;
3. l'interoperabilità a livello nazionale.

Il primo requisito risponde all'esigenza di produrre uno strumento sicuro sotto i diversi aspetti della produzione, rilascio nonché utilizzo da parte del titolare.
Il secondo requisito costituisce una novità importante rispetto alla versione attuale della carta di identità cartacea e consiste, nel rispetto della normativa vigente, nell'utilizzo del documento di identità come carta servizi, attraverso l'utilizzo di tecniche di autenticazione opportunamente combinate alla specificazione di un codice personale di identificazione (PIN).

Il terzo requisito è relativo alla necessità di dover disporre di un supporto in grado di funzionare allo stesso modo e su tutto il territorio nazionale nei confronti delle Pubbliche Amministrazioni Centrali.
Sono previste due differenti modalità di autenticazione atte a stabilire l'identità dell'utente:

- Protocollo SSL/TSL;
- Autenticazione in modalità *Challenge/Response*.

La firma digitale e la firma elettronica

La firma digitale è associata indissolubilmente al concetto di documento elettronico.
La recente normativa italiana conferisce ad un documento elettronico firmato digitalmente, utilizzando tecniche di firma asimmetrica, la stessa valenza probatoria di un documento cartaceo munito di firma olografa.
Si basa su un certificato qualificato, (quindi rilasciato da una *trusted part* detta *Certification Authority* che, per quanto previsto dalla vigente legislazione nazionale deve essere iscritta nell'elenco pubblico dei certificatori) e creata mediante un dispositivo di firma sicuro (in genere una *smart card*).
La direttiva europea e la nascita del commercio elettronico, hanno introdotto altri tipi di firma applicabili in contesti diversi da quello di un documento, come per esempio quello dei messaggi di posta elettronica: in questo caso si parla di firma elettronica.
Sia la firma digitale che quella elettronica, permettono di conseguire gli obiettivi di autenticità del mittente, di integrità dei dati firmati e di non ripudio dell'origine dei dati: cioè che il mittente non possa in una fase successiva negare di aver effettuato la trasmissione dei dati stessi.

La firma digitale e la carta di identità elettronica

Come precedentemente specificato, la carta di identità elettronica nasce come strumento di identificazione a vista (in modo analogo a quanto avviene per l'attuale versione cartacea) e può essere usata come strumento di autenticazione ai servizi e quindi come strumento di accesso. Solo successivamente all'accesso, in presenza di dati da autenticare ed in un contesto che richiede il non ripudio degli stessi, può essere utilizzata per la firma elettronica avanzata (e non digitale) in linea con quanto stabilito dalla normativa europea in materia di firma elettronica.

7.6.3 Controllo degli accessi

Per controllo degli accessi, o più precisamente sistema per il controllo degli accessi, si intende ***l'insieme di meccanismi che garantiscono che le entità che accedono a delle risorse in un sistema lo facciano nel rispetto di una serie di regole predefinite.***

Il controllo degli accessi può essere svolto a livello di sistema operativo oppure a livello di applicazione per regolamentare l'accesso ai dati.

7.6.4 Tracciabilità degli utenti

Per tracciabilità degli utenti s'intende l'insieme di meccanismi adottati per poter ricondurre inequivocabilmente ad un tempo ben individuato ed a un utente l'esecuzione di una certa azione, e quindi poter attribuire ad ogni singolo utente le proprie responsabilità.
Adottare un sistema che garantisce la tracciabilità delle utenze consente di raggiungere due obiettivi molto importanti:

- rilevare in tempo debito un'intrusione;
- prevenire azioni non autorizzate da parte di interni grazie all'effetto scoraggiante che un tale sistema può provocare sugli stessi.

7.6.5 Sicurezza nei sistemi distribuiti

Nella trattazione sinora presentata, abbiamo implicitamente supposto che le applicazioni a cui un utente accede siano tutte residenti su un unico sistema e quindi di poter gestire centralmente i vari aspetti di sicurezza coinvolti.
Lo scenario cambia radicalmente se l'utente non vuole più autenticarsi ad un singolo sistema ma vuole autenticarsi ad una rete di calcolatori, o anche se l'applicazione che l'utente sta eseguendo deve accedere ad altri host per recuperare i dati.
Vediamo alcuni aspetti nei paragrafi seguenti.

7.7 SICUREZZA DELLE RETI E DELLE APPLICAZIONI IN RETE

La sicurezza di un sistema è legata alla sicurezza delle singole componenti del sistema. In particolare il livello di sicurezza di un sistema è determinato dal livello di sicurezza della componente del sistema meno protetta. Le componenti del sistema sin qui considerato sono le applicazioni realizzate per fornire servizi agli utenti finali, ed è l'infrastruttura di rete, nel senso più generale del termine, che consente alle applicazioni di reperire i dati appropriati indipendentemente dalla loro localizzazione e soddisfare così le richieste degli utenti.
Per sicurezza della rete, intendiamo la sicurezza che attiene ad: "un insieme di host opportunamente connessi da canali di comunicazione sui quali possono operare dei servizi di sistema, che rappresentano l'interfaccia tra le applicazioni e l'host stesso."
Nel caso in cui la rete in questione sia Internet il numero di potenziale utenti del calcolatore è smisurato (un centinaio di milioni di utenti). L'esperienza di questi anni ci insegna che tutto ciò può comportare notevoli vantaggi ma anche alcuni rischi. Tra i potenziali utenti della rete si nascondono infatti persone, che per una serie di motivi, sono interessate a compromettere il buon funzionamento dei sistemi,

accedere o modificare senza l'adeguata autorizzazione, informazioni riservate.
Si dovrà, tra le altre cose, cercare di ridurre in termini ragionevoli l'esposizione al rischio della propria infrastruttura.
Il raggiungimento del suddetto obiettivo avviene facendo ricorso a opportuni strumenti tecnologici. Al di là dell'insostituibile supporto di esperti per la fase di progettazione di un sistema di sicurezza, molte attività possono essere realizzate solo attraverso l'ausilio di strumenti crittografici quali IPSEC (*Secure Internet Protocol*), SSL (*Secure Socket Layer*) e VPN (*Virtual Private Network*) e tecnologici quali *Firewall* e *Intrusion Detection System* (IDS).

7.8 SICUREZZA DEL CANALE

Affinché dei calcolatori connessi in rete possano reciprocamente scambiarsi informazioni è necessario che gli stessi adottino lo stesso protocollo di comunicazione, che è oramai parte integrante di ogni sistema operativo. Il protocollo di comunicazione (in realtà sono più protocolli) utilizzato dai calcolatori di Internet è noto come TCP/IP (*Transmission Control Protocol / Internet Protocol*) ed è costituito da diversi protocolli fra cui UDP (*User Datagram Protocol*) + TCP + IP.
Per consentire la comunicazione tra due calcolatori il TCP/IP stabilisce un "canale" di comunicazione tra il calcolatore del mittente e quello del destinatario. La trasmissione di informazioni in Internet è analoga alla trasmissione di una lettera. Per prima cosa la corrispondenza raggiunge l'ufficio postale più vicino al mittente (smistatore di primo livello); questo provvede ad inviare la corrispondenza ad un ufficio centrale, che successivamente la rinvia ad uno o più smistatori intermedi, finché la corrispondenza non arriva all'ufficio postale più vicino al destinatario, dal quale un postino provvede alla consegna. Elemento peculiare del protocollo è che la trasmissione delle informazioni non deve necessariamente seguire sempre la stessa strada, anzi è probabile che due pacchetti dati raggiungano la destinazione seguendo strade diverse. Esistono quindi molti punti in cui l'informazione trasmessa può essere intercettata, letta ed eventualmente modificata.
Questa operazione è facilitata dal fatto che le informazioni nell'ambito del protocollo TCP/IP viaggiano in chiaro, rischio che può essere evitato operando opportune trasformazioni crittografiche sulle informazioni che devono essere trasmesse. In questa sezione vedremo i prodotti più diffusi: IPSEC, SSL/TLS e VPN che consentono di operare tali trasformazioni.

7.8.1 IPSEC

È l'abbreviazione di *IP Security* ed è uno standard per ottenere connessioni basate su reti IP sicure. La sicurezza viene raggiunta attraverso la cifratura e l'autenticazione dei pacchetti IP. La sicurezza viene fornita quindi a livello di rete cui IP appartiene. La capacità di

fornire protezione a livello di rete rende questo protocollo trasparente al livello delle applicazioni che non devono essere modificate.
IPSEC nasce su iniziativa della *Internet Engineering Task Force* (IETF) e quindi come *Internet Standard*. IPSEC è un protocollo creato per aggiungere ad IP una serie di servizi supplementari di sicurezza. Nell'ambito della presente trattazione ci interessa sottolineare che IPSEC consente di operare sui messaggi in uscita da un host le seguenti operazioni:

- Cifratura dei dati contenuti nei messaggi con appositi algoritmi di crittografia;
- Autenticazione del mittente;
- Integrità dei dati.

Il punto di forza di IPSEC è quello di consentire l'esecuzione. Questo significa che è sufficiente installare IPSEC su un host affinché lo stesso possa incominciare a cifrare/autenticare il traffico di rete generato.

7.8.2 SSL/TLS

Il *Transport Layer Security* (**TLS**) e il suo predecessore *Secure Sockets Layer* (**SSL**) sono dei protocolli crittografici che permettono una comunicazione sicura e una integrità dei dati su reti TCP/IP come, ad esempio, Internet. TLS e SSL cifrano la comunicazione dalla sorgente alla destinazione (*end-to-end*) sul livello di trasporto. Diverse versioni del protocollo sono ampiamente utilizzate in applicazioni come i browser, l'E-mail, la messaggistica istantanea e il Voice over IP. TLS è un protocollo standard IETF che, nella sua ultima versione, è definito nella RFC 5246, sviluppata sulla base del precedente protocollo SSL da Netscape Corporation.
Secure Socket Layer **(SSL)** nasce in casa *Netscape Inc*., come protocollo per proteggere il traffico di rete generato dal servizio *World Wide Web.* Le specifiche della versione 3 del protocollo (SSLv3) vengono successivamente acquisite dall'IETF per la formulazione di un protocollo per la sicurezza del traffico di rete noto come *Transport Layer Security* **(TLS)** Visto il grado di somiglianza dei due protocolli entrambi sono oggi indicati come SSL/TLS.
La comunicazione via SSL/TLS tra due entità viene effettuata in due fasi:

1. una fase di *handshake*, deputata alla definizione di alcune chiavi di sessione da utilizzare con algoritmi di crittografia simmetrica necessari per garantire la riservatezza/integrità dei dati trasmessi tra le due entità;
2. una fase di preparazione e trasmissione dei dati usando i parametri definiti nella fase di *handshake*.

7.8.3 Virtual private network (VPN)

Una *Virtual Private Network* o VPN è una rete di telecomunicazioni privata instaurata tra soggetti che utilizzano un sistema di

trasmissione pubblico e condiviso come per esempio Internet. Lo scopo delle reti VPN è di dare alle aziende le stesse possibilità delle linee private in affitto ad un costo inferiore sfruttando le reti condivise pubbliche. Si può vedere una VPN come l'estensione a scala geografica di una rete locale privata aziendale che colleghi tra loro siti interni all'azienda stessa variamente dislocati su un ampio territorio.
Le VPN sono un ulteriore approccio proposto per fornire sicurezza al traffico di rete generato da un host. Il modello di sicurezza di riferimento è quello di IPSEC, in cui cioè viene stabilito un canale sicuro tra due entità che vogliono comunicare. Scopo di queste componenti è il garantire che il traffico generato tra le due entità collegate dalla VPN goda delle seguenti proprietà:

- riservatezza del contenuto dei messaggi;
- integrità dei messaggi;
- mutua autenticazione delle parti.

È possibile realizzare senza particolari sforzi una VPN tra due host provvisti del protocollo IPSEC. In questo caso è sufficiente configurare opportunamente il protocollo IPSEC sui due host.

7.9 ANTIVIRUS

Una categoria particolare di intrusioni informatiche e indubbiamente la più diffusa è costituita dai computer virus. 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 a una rete indicati con il termine generico di codice malizioso.
Un computer virus svolge due funzioni di base infetta altri programmi, cioè copia se stesso su altri programmi presenti nel sistema, svolge all'interno del sistema le azioni per cui è stato programmato. Queste azioni 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 consiste nell'installazione di un prodotto antivirus, in particolare di un prodotto del tipo TSR (*Terminate and Stay Resident*).
La migliore soluzione implementativa consiste nell'installazione di questo prodotto su ciascun calcolatore della rete interna e sui *bastion host* (Il bastion host è un server ben protetto in cui sono integrate molte misure di sicurezza ed è l'unico punto di contatto per le richieste in arrivo da Internet). Sono presenti sul mercato anche soluzioni diverse, quali ad esempio quella basata sull'installazione di un prodotto antivirus sul firewall contemporaneamente con l'eliminazione di floppy disk e CD drive da ogni calcolatore della rete, oppure l'installazione di un antivirus su tutti i server di una rete e non sui client che mantengono le caratteristiche appena descritte.

7.10 SICUREZZA DI UN WEB SERVER

Un web server è un servizio, e per estensione il computer su cui è in esecuzione, che si occupa di fornire, tramite software dedicato e su richiesta dell'utente, file di qualsiasi tipo, tra cui pagine web (successivamente visualizzabili dal browser sul PC dell'utente). Le informazioni inviate dal server web all'utente viaggiano in rete trasportate dal protocollo HTTP. L'insieme di server web dà vita al World Wide Web, uno dei servizi più utilizzati di Internet.
Nell'ambito di tale sezione intendiamo con il termine web server il programma software che implementa le funzionalità server del protocollo HTTP, come ad esempio Apache, Internet Information Service, Netscape Server.
Nell'ambito di un sito Internet i server web sono tra le componenti software più complesse, e spesso sono anche il punto più vulnerabile dell'intera infrastruttura. Tali vulnerabilità derivano sia da errori presenti nel codice del server ma anche e soprattutto da errori commessi in fase di installazione e configurazione. Va sottolineato che la presenza di tali vulnerabilità può compromettere l'integrità di un sito web indipendentemente dalla presenza di firewall e di *bastion host*, nel senso che nei confronti di vulnerabilità presenti nel web server sia firewall che *bastion host* sono nella maggioranza dei casi inefficaci.

7.10.1 Le principali misure di protezione da adottare

Il web server è indubbiamente un servizio molto critico, che per ovvie ragioni, nella stragrande maggioranza dei casi, deve anche essere un servizio pubblico. Vediamo quali sono i principi a cui attenersi per evitare di esporre troppo un web server esterno ad attacchi informatici, tenendo presente che non esistono soluzioni definitive ad attacchi come il *Denial of Service* (**DoS**).
Bisogna sviluppare delle politiche in collaborazione con specialisti del settore, che per esempio, con l'ausilio di strumenti automatici che analizzino i log di sistema per valutare se ad esempio è presente traffico IP anomalo, qualche sottorete IP sta trasferendo password errate con frequenza sospetta oppure nei log del web server ci sono delle GET (è un comando utilizzato dall'HTTP) incrementali provenienti dalla stessa origine a brevissima distanza una dall'altra.

Un'ulteriore misura precauzionale può essere costituita (questa opzione fa parte delle opzioni contrattuali previste sulla rete unitaria) dall'outsourcing in termini di hosting della propria infrastruttura web. Il contratto di outsourcing in questo caso dovrebbe garantire la certificazione periodica del sito ed un adeguato reporting sulle attività di sicurezza svolte dal personale di chi gestisce il servizio.

7.11 WEB PROXY

I *web proxy* sono delle terze parti tra client e server, in particolare intercettano richieste di client e le inviano, previa verifica, al server. I *web proxy* sono proxy specializzati a trattare i pacchetti che sono

scambiati tra un web server ed il browser. In un'organizzazione il *web proxy* può essere usato per gestire il traffico verso Internet da parte del personale interno. In tal senso il *web proxy* può essere istruito per bloccare accessi da parte di determinati utenti a determinati siti web e per effettuare una dettagliata operazione di logging.

7.12 FIREWALL

I *firewall* sono probabilmente la tecnologia di sicurezza più diffusa. Un **Internet firewall**, in particolare, è un firewall eretto con lo scopo di proteggere la rete interna di un'organizzazione (che nel seguito indicheremo anche con il termine Intranet) da Internet. In particolare, un Internet firewall:

- consente di concentrare tutti gli aspetti di protezione di una rete rispetto alle minacce che arrivano dall'esterno in un unico punto;
- può registrare tutta l'attività svolta dall'organizzazione verso Internet;
- può facilmente interdire l'uso di servizi di rete non previsti dalla politica di sicurezza del sito e in generale essere lo strumento che aiuta a rafforzare la politica di sicurezza di un'organizzazione;
- può intercettare diversi tentativi di intrusione informatica;
- può difendere da alcuni attacchi di tipo "*Denial of Service*";
- non può niente contro gli insider (cioè intrusori che operano dall'interno dell'organizzazione). I firewall servono solamente a proteggere un'intranet da attacchi esterni;
- può solo controllare il traffico che lo attraversa;
- non è una protezione completa contro i virus.

7.13 PROXY SYSTEM

In un'architettura di Internet firewall, un proxy viene posizionato tra Internet e la Intranet e controlla tutte le richieste di servizi che dalla rete interna vanno verso la rete Internet e viceversa. In base alle politiche di sicurezza del sito, decide se inoltrare o bloccare le richieste, in particolare i controlli effettuati dal proxy sono tutti quei controlli non esprimibili a livello di *packet filtering*.

7.14 INTRUSION DETECTION SYSTEM (IDS)

L'*Intrusion Detection System* o IDS è un dispositivo *software* o *hardware* (o a volte la combinazione di entrambi, sotto forma di sistemi stand-alone pre-installati e pre-configurati) utilizzato per identificare accessi non autorizzati ai computer o alle reti locali. Le intrusioni rilevate possono essere quelle prodotte da *cracker* esperti (oggi comunemente denominati *hacker*), da tool automatici o da utenti inesperti che utilizzano programmi semiautomatici.
Tipicamente un *intrusion detection system* è costituito da una serie di sensori di rete o agenti e da un analizzatore centrale, ognuno di essi

risiede su un host dedicato. Nella sua configurazione più semplice un *intrusion detection system* è costituito da un singolo *host* che contiene sia l'analizzatore che un agente di rete e viene interposto, in un'architettura di *firewall* con rete demilitarizzata, tra la rete demilitarizzata e il router interno per far si che possa controllare tutto il traffico diretto verso la rete interna.
Un *intrusion detection system* può erroneamente riconoscere una sequenza di pacchetti innocua come maligna e quindi provvedere ad attivare un falso allarme.

8 SICUREZZA FISICA

Per sicurezza fisica di un sistema informativo intendiamo l'adozione di tutte quelle soluzioni tecniche atte a ridurre al minimo sia le probabilità che si verifichino certi eventi dannosi, sia l'entità dei danni che il verificarsi di tali eventi potrebbe causare agli edifici, alle macchine, agli archivi ed a tutto quanto può compromettere la integrità fisica di tutti i componenti del sistema informativo.
Gli eventi cui ci si riferisce sono di natura molto diversa, essi comprendono infatti furti, sabotaggi, incendi casuali o dolosi, calamità naturali e così via.
In questa sezione non intendiamo affrontare le vulnerabilità e quindi le contromisure da mettere in atto per far fronte alle possibili minacce che possono interessare gli edifici e/o gli accessi fisici agli stessi.
Ci limitiamo ad elencare alcune misure senza scendere nel dettaglio ritenendo l'argomento, per quanto interessante, non di competenza di questa dispensa.

Elenchiamo quindi le misure di sicurezza fisiche e procedurali il cui scopo è quello di tenere sotto controllo gli accessi all'interno dell'edificio e delle aree interne, esse sono:

- le misure antincendio
- le misure antinondazione
- le misure antintrusione
- le misure per la protezione dell'alimentazione elettrica
- le telecamere
- le recinzione
- la guardiania
- il controllo degli ospiti
- le porte antintrusione
- le smart card o badge
- la videosorveglianza
- l'autenticazione visiva o biometria

In questa sezione daremo maggior enfasi alla così detta sicurezza **logico-fisica** nel suo aspetto informatico, considerando appartenenti a questa sezione le minacce e le contromisure riferite ai sistemi informatici, agli archivi ed ai servizi che gli stessi debbono erogare.

8.1 SICUREZZA DEGLI HOST

Gli *host* che erogano servizi direttamente verso Internet vengono chiamati *bastion host*. I *bastion host* sono, quindi, i sistemi dell'organizzazione più esposti agli attacchi informatici. Tutto ciò comporta un notevole rischio poiché questi *host* rimangono esposti ai numerosi bug che affliggono il sistema operativo e i servizi di sistema quali ad esempio il www server, FTP server ecc. ecc.
Configurazione hardware: I *bastion host* sono macchine molto critiche, è quindi necessario che le stesse siano provviste di dispositivi che ne garantiscano l'alta affidabilità (*high availability*) e siano connesse a sistemi che garantiscano la continuità dell'alimentazione elettrica.

8.2 DISASTER RECOVERY

Per *Disaster Recovery Plan* (DRP) si intendono gli aspetti tecnologici del *Business Continuity Plan* (BCP). Il DRP può essere definito nel modo seguente:"DRP si riferisce ad un piano focalizzato sull'ICT per ripristinare l'operatività di un sistema, di un'applicazione o di un centro elaborativo in un sito alternativo dopo un'emergenza (duplicazione delle macchine e degli archivi posti in locali diversi e lontani).
In particolare non ci si riferisce quindi a interruzioni minori che non richiedono rilocazione di sito.
Affinché una organizzazione possa rispondere in maniera efficiente ad una situazione di emergenza, devono essere analizzati:

- i possibili livelli di disastro;
- la criticità dei sistemi/applicazioni.

8.3 BUSINESS CONTINUITY MANGEMENT

Lo scopo del *Business Continuity Management* è garantire la continuità dei processi dell'organizzazione in funzione del loro valore e della qualità dei prodotti/servizi erogati tramite il supporto dell'infrastruttura di ICT, prevenendo e minimizzando l'impatto di incidenti intenzionali o accidentali e dei conseguenti possibili danni.
Gli eventi che potrebbero pregiudicare la continuità del business sono:

- eventi imprevisti che possono inficiare l'operatività dei sistemi (interruzione dell'alimentazione, incendi, allagamenti, ecc.);
- malfunzionamenti dei componenti hw e sw;
- errori operativi da parte del personale incaricato della gestione o da parte degli utilizzatori;
- introduzione involontaria di componenti dannosi per il sistema informativo e di rete (es. virus, cavalli di troia, bombe logiche);
- atti dolosi miranti a ridurre la disponibilità delle informazioni (sabotaggi e frodi, diffusione di virus, bombardamento di messaggi, interruzione di collegamenti, ecc.).