



Comitato tecnico nazionale
sulla sicurezza informatica e
delle telecomunicazioni nelle
pubbliche amministrazioni

Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione

MARZO 2004

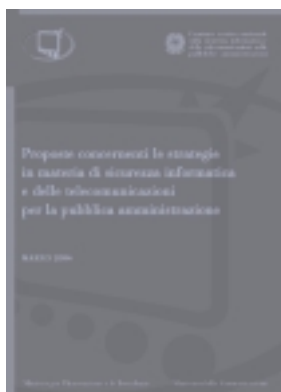
Questo documento contiene le proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione, così come richiesto dall'articolo 2, comma 1 del decreto istitutivo del Comitato per la Sicurezza. Ad esso potranno seguire ulteriori aggiornamenti, in previsione del compiersi delle attività descritte nel documento.

Si ringraziano i Componenti del Comitato Tecnico Nazionale, i signori Danilo Bruschi, Franco Guida, Carlo Sarzana di Sant'Ippolito, Giorgio Tonelli per l'intenso impegno profuso nella redazione di questo documento. Si ringraziano inoltre i coordinatori delle attività del Comitato, i signori Vincenzo Merola e Giovanni Rellini Lerz. Un ringraziamento particolare al signor Vittorio Stelo, primo Presidente del Comitato, per gli indirizzi organizzativi dati alla fase propedeutica alla produzione di questo rapporto.

Il Presidente
Claudio Manganelli

sommario

marzo
2004



marzo 2004
Comitato tecnico nazionale
sulla sicurezza informatica
e delle telecomunicazioni
nelle pubbliche amministrazioni

a cura
della Segreteria Tecnica
del Comitato

Via Isonzo, 21b
00198 Roma
Tel. (39) 06 85264.211
Fax (39) 06 85264.371

Stampa: C.S.R., Roma

progetto grafico:
Segni di Segni, Roma

1

PREMESSE E LINEE ISPIRATRICI

1.1 Introduzione	3
1.2 Le iniziative del Governo	4
1.3 Il Comitato	5
1.4 Le proposte del Comitato per il Piano Nazionale e il modello organizzativo	6
1.5 Premesse finali	6
1.6 Cenni sulla regolamentazione normativa ed amministrativa in tema di sicurezza ICT nei sistemi informatici pubblici	6
1.6.1 Premessa	6
1.6.2 Le prime iniziative normative	7
1.6.3 Sicurezza informatica e protezione dei dati personali	8
1.6.4 Le linee guida in tema di sicurezza informatica	9
1.6.5 Spunti per eventuali iniziative normative in materia di sicurezza informatica	9
1.7 Cenni sulle iniziative internazionali in tema di sicurezza informatica	10

15

PROPOSTE PER UN SISTEMA DI GOVERNO DELLA SICUREZZA ICT NELLA PA

2.1 Modello organizzativo	17
2.1.1 Il Centro Nazionale per la Sicurezza Informatica	17
2.1.2 Le funzionalità del Centro Nazionale per la Sicurezza Informatica	18
2.1.3 Le struttura del Centro Nazionale per la Sicurezza Informatica	20
2.1.4 Rapporti con le altre istituzioni	23
2.1.5 L'Unità di gestione degli attacchi informatici	24
2.1.6 L'Unità di formazione	30

2.2 Ruoli delle singole amministrazioni: le unità locali	32
2.3 Il “processo della sicurezza ICT” nella PA	35
2.3.1 Adozione di una metodologia di analisi del rischio	36
2.3.2 Adozione di un piano di Business Continuity	36
2.3.3 Stesura di capitolati per l’acquisizione di sistemi/prodotti ICT dotati di funzionalità di sicurezza	37
2.3.4 Gestione del personale	37
2.3.5 Sicurezza nell’accesso di terze parti ai sistemi ICT della PA	37
2.3.6 Outsourcing	38
2.3.7 Il ricorso alle certificazioni di sicurezza nella PA	38
2.4 Documenti di riferimento	40
2.5 Elenco dei meccanismi di sicurezza standardizzati da ISO/IEC/JTC1/SC27	41

3.1 Linee guida per l’analisi dei rischi	45
3.1.1 Considerazioni generali	45
3.1.2 Requisiti di conformità della metodologia	46
3.1.3 Logiche per sviluppare la richiesta di offerta	46
3.2 Linee guida per lo sviluppo di un piano di Business Continuity	50
3.2.1 Premessa	50
3.2.2 Lo scopo del Business Continuity Management	50
3.2.3 Le componenti del Business Continuity Management	51
3.2.4 Il ciclo del Business Continuity Management	51
3.2.5 Le strategie per il Business Continuity Management	51
3.2.6 Le linee guida all’elaborazione dei piani del Business Continuity Management	52
3.2.7 Disaster Recovery Plan	55



Proposte concernenti le strategie
in materia di sicurezza informatica
e delle telecomunicazioni
per la pubblica amministrazione

Premesse e linee ispiratrici

1. Premesse e linee ispiratrici

1.1 Introduzione

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 impongono una rigorosa attenzione agli aspetti legati alla sicurezza. Questo fattore vale per tutto lo scenario delle applicazioni informatiche e di telecomunicazioni, in particolare per la PA. Infatti, la diffusione dell'utilizzo delle reti presenta ormai coefficienti di crescita esponenziali e le applicazioni su reti aperte sono divenute una realtà non più esclusiva del mondo imprenditoriale, bensì una necessità gestionale e di colloquio delle Pubbliche Amministrazioni, tra loro, con le imprese, con i cittadini.

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 P.A. 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.

Si ponga infine attenzione al fatto che il tema della sicurezza nell’e-government accomuna tutta la PA, centrale e locale. Al proposito si ricorda che il Comitato tecnico della commissione permanente per l’Innovazione e le Tecnologie, nel documento “L’e-government per un federalismo efficiente” dell’aprile 2003, identifica le regole per l’uso sicuro dei servizi di e-government:

1. assicurazione dell’integrità e la riservatezza delle informazioni che transitano in rete;
2. affidabilità e certificazione delle fonti di erogazione dei servizi;
3. consultazione esclusiva delle informazioni di carattere personale da parte del legittimo proprietario dei dati;
4. minor numero possibile di informazioni di carattere personale richieste all’utente nell’interazione con i sistemi di e-government e utilizzo di queste informazioni esclusivamente per verificare il diritto ad accedere ai servizi;
5. concessione dell’abilitazione all’accesso ai servizi solo in funzione di specificità dell’utente (cittadinanza, appartenenza a categorie professionali, ecc.) attestate dagli organismi competenti.

1.2 Le iniziative del Governo

L’istituzione del Ministro per l’Innovazione e le Tecnologie ed i piani di finanziamento di numerosi progetti di e-government da questo approvati, destinati a far crescere il livello di efficienza degli Enti locali, dalle Regioni, alle Province, ai Comuni grandi, medi e piccoli, sino alle Comunità montane, confermano l’intenso impegno delle PPAА nella razionalizzazione dei processi amministrativi e nella volontà di avviare un dialogo più snello ed efficace con i cittadini. Affinché si compia con pieno successo l’opera di realizzazione dell’impianto di e-government é indispensabile consolidare l’azione governativa anche sugli aspetti della sicurezza ICT.

Si consideri anche il fatto che aspetti tecnologici fondamentali per la realizzazione dell’e-government, quali la larga banda e l’open source, non hanno possibilità di diffusione se non accompagnati da una adeguata infrastruttura di sicurezza.

Il Ministro dell’Innovazione e delle Tecnologie si è già fatto promotore di importanti iniziative atte ad avviare un vero e proprio sistema di sicurezza per l’e-government:

- la direttiva sulla sicurezza ICT, emanata con direttiva del Presidente del Consiglio dei Ministri 16 gennaio 2002, contiene i requisiti minimi per il raggiungimento dei quali tutte le amministrazioni devono attrezzarsi dopo aver effettuato una autovalutazione sul proprio livello di sicurezza ICT;
- il Comitato Tecnico Nazionale sulla Sicurezza ICT, (nel seguito Comitato), istituito con Decreto Interministeriale del Ministro delle Comunicazioni e del Ministro per l’Innovazione e le Tecnologie nel luglio 2002, che ha il compito di raggiungere gli obiettivi di sicurezza attraverso le seguenti fasi funzionali:
 - esame della situazione della P.A. rispetto ai temi della sicurezza;
 - elaborazione e diffusione di linee guida;

- stesura di progetti di attuazione dei principi fissati;
- realizzazione e controllo dell'avanzamento dei progetti;
- fornitura di consulenza e supporto alla realizzazione.
- l'approvazione del decreto per l'istituzione di uno schema nazionale per la certificazione di sicurezza secondo gli standard ITSEC e Common Criteria di prodotti e sistemi ICT che non trattino informazioni relative al segreto di stato, avvenuta in data 29 ottobre 2003.

1.3 Il Comitato

Senza voler riportare l'intero contenuto del Decreto istitutivo del Comitato, è però il caso di ricordare le funzioni previste nel Decreto all'articolo 2, "Funzioni del Comitato":

1. Il Comitato, al fine del raggiungimento di un livello di sicurezza nelle informazioni conforme a criteri standard internazionali e per garantire integrità e affidabilità dell'informazione, formula le proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la pubblica amministrazione, in particolare ai fini della redazione:
 - a) del Piano nazionale della sicurezza delle tecnologie dell'informazione e comunicazione della pubblica amministrazione, di cui verifica annualmente lo stato di avanzamento, identificando le eventuali misure correttive;
 - b) della predisposizione del modello organizzativo nazionale di sicurezza ICT per la pubblica amministrazione, del quale verifica la relativa attivazione e applicazione.
2. Il Comitato formula, inoltre, proposte in materia di regolamentazione della certificazione e valutazione della sicurezza, nonché ai fini della predisposizione di criteri di certificazione e delle linee guida per la certificazione di sicurezza ICT per la pubblica amministrazione, sulla base delle normative nazionali, comunitarie e internazionali di riferimento.
3. Il Comitato elabora linee guida per la predisposizione delle intese con il Dipartimento della funzione pubblica in ordine alla formazione dei dipendenti pubblici in tema di sicurezza ICT."

Il presente documento contiene le proposte di cui al punto 1. sopra citato. Si sottolinea anche che, su proposta del Comitato, sono stati già stanziati i fondi dal Comitato dei Ministri per la Società dell'informazione nella riunione del 18 marzo 2003 per le due seguenti iniziative:

- un progetto di "CERT per la Pubblica Amministrazione";
 - un "Centro di formazione e sensibilizzazione del personale della PA",
- e che il Comitato intende anche promuovere alcune altre iniziative concrete, di supporto all'attuazione del Piano, così come richiesto nel Decreto; in particolare:
- la produzione di linee guida sulla sicurezza informatica, redatte con il contributo non solo dei responsabili informatici della PA, ma anche con quello delle associazioni rappresentative delle imprese e dei cittadini;
 - la promozione di incontri periodici con la PA, con provider internet, con realtà rilevanti di banche, finanza, assicurazioni, commercio e industria, al fine di armonizzare il sistema sicurezza ICT italiano, sfruttando le più riuscite esperienze e capacità di tutte le realtà nazionali;
 - la determinazione di alcuni obiettivi operativi relativi ad aspetti urgenti e sentiti dagli utenti ICT, come l'abuso di spamming e dei cookie.

1.4 Le proposte del Comitato per il Piano Nazionale e il modello organizzativo

Nella prima parte di questo documento, "Proposte per un sistema di governo della sicurezza ICT nella PA", vengono presentate una serie di indicazioni relative alla costituzione di una infrastruttura organizzativa, che possa farsi carico a livello nazionale di coordinare un processo di "messa in sicurezza" delle PPAA, unitamente ad una serie di indicazioni in merito alle iniziative di tipo legislativo che dovrebbero essere intraprese nel settore.

La seconda parte di questo documento, "Linee guida per l'attuazione della sicurezza ICT nella PA", contiene l'indicazione di una serie di attività da intraprendere con estrema urgenza per avviare il suddetto processo.

Il Comitato ritiene, nella situazione contingente del livello di sicurezza rilevato da un primo ciclo di incontri con i responsabili dei sistemi informativi della PAC, che le indicazioni contenute nel presente documento, siano le più urgenti. L'evolversi della situazione attuale dovrà ovviamente riflettersi in adeguamenti e revisioni successive del documento stesso.

1.5 Premesse finali

Il Comitato ha preventivamente definito i seguenti punti, relativamente al Piano Nazionale che verrà realizzato sulla base delle proposte:

1. area di competenza del Piano:

- amministrazioni dello Stato;
- aziende ed amministrazioni autonome dello Stato;
- Enti pubblici non economici nazionali;

2. requisiti attuativi del Piano:

- la verifica del rispetto del Piano sarà effettuata attraverso un monitoraggio.

I tempi e i modi di realizzazione del Piano e del modello organizzativo sono stati volutamente lasciati indefiniti, ritenendo il Comitato che siano oggetti specifici delle fasi realizzative.

Il Piano e il modello organizzativo acquisteranno natura normativa con decreto legislativo su iniziativa del Ministro Stanca, di concerto con il Ministro Gasparri in base all'art. 10 della legge 29-07-2003 n° 229.

1.6 Cenni sulla regolamentazione normativa ed amministrativa in tema di sicurezza ICT nei sistemi informatici pubblici

1.6.1 Premessa

La formulazione delle proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni di cui all'art.2 del Decreto Interministeriale del 24 luglio 2002 rende necessario, ad avviso del Comitato, esaminare anche gli aspetti giuridico-normativi del problema. Per far ciò appare necessario tracciare una ricostruzione del quadro normativo ed amministrativo relativo alla sicurezza informatica che, allo stato, come rilevato dalla dottrina specialistica, presenta indubbi caratteri di frammentarietà e di scarsa coerenza sistematica. I capitoli che seguono cercano quindi di ricostruire, in modo necessariamente sintetico, le linee del trend normativo sviluppatosi nel corso dei decenni precedenti in modo da offrire un panorama, il più possibile completo, della situazione

concernente la materia e di consentire ai “decision makers” di valutare la situazione stessa e, eventualmente, di intervenire sul piano politico-normativo allo scopo di dettare le prescrizioni che apparissero necessarie per regolamentare la materia in modo esaustivo e coerente nell’ambito pubblico.

L’importanza della predisposizione di sistemi efficienti di sicurezza informatica relativamente al settore pubblico è stata ben sottolineata nella Direttiva del Ministro per l’innovazione e le tecnologie del 16 gennaio 2002 allorché è stato affermato che le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese e che questo patrimonio deve essere efficacemente protetto e tutelato al fine di prevenire possibili alterazioni sul significato intrinseco delle informazioni stesse¹.

1.6.2 Le prime iniziative normative

Come già accennato, la situazione normativa e regolamentare per quanto riguarda la sicurezza informatica nell’ambito pubblico presenta un aspetto non unitario essendo le varie prescrizioni, in generale, contenute in provvedimenti sparsi e non collegati tra di loro non esistendo, sino al 2001, un preciso indirizzo politico al riguardo ed un centro amministrativo di riferimento. Le stesse lodevoli iniziative in materia dell’AIPA, data la scarsa incidenza dell’azione della stessa sulle burocrazie ministeriali, poco sollecitate tradizionalmente a recepire in modo organico ed integrabile l’innovazione tecnologica, non sembrano aver avuto esiti concreti.

Un primo tentativo di mettere ordine nel settore dell’informatica pubblica è stato probabilmente quello compiuto dal Ministro per la Funzione pubblica dell’epoca con la Circolare n.51223 del 21 maggio 1990 avente come titolo “Indirizzi di normalizzazione delle tecnologie dell’informazione nella pubblica amministrazione” un paragrafo della quale era dedicato ai criteri generali per la sicurezza fisica delle installazioni e per la sicurezza logica delle applicazioni. Va ricordato anche il D.lgs.n. 39 del 12 febbraio 1993 con il quale, tra l’altro, venne creata l’AIPA che, secondo il testo dell’art.7, c.1.lett.a) aveva anche il compito di dettare i “criteri tecnici” riguardanti la sicurezza dei sistemi².

¹ Dalle audizioni svolte dal Comitato è emerso che le Amministrazioni hanno, in genere, adottato misure di sicurezza, soprattutto per quanto riguardava la protezione dei dati personali. Tuttavia, come fatto presente da alcune Amministrazioni, ed in particolare dai rappresentanti della Presidenza del Consiglio dei Ministri, nell’appunto del 12/12/2002 le cui puntualizzazioni appaiono, per così dire, emblematiche della situazione, le misure adottate ..”non comprendono ..”, gran parte della base minima citata nel documento allegato 2 della G.U del 22/3/02 ...” Inoltre nel documento citato si afferma, senza mezzi termini, che “per soddisfare adeguatamente a quanto richiesto nel tempo di un anno è comunque prevedibile che si incontrino grosse difficoltà da parte dell’Amministrazione, essendo necessario un grosso sforzo organizzativo ed economico per istituire un’organizzazione di qualità per la sicurezza ...”

In tema di sicurezza informatica e di “stato dell’arte” in materia va citata una ricerca sulla sicurezza informatica negli Enti Locali del luglio 2002 (peraltro effettuata su un campione ristretto di Comuni), dall’ANCITEL secondo cui “solo il 12% dei Comuni intervistati ha adottato sistemi di difesa derivati da una valutazione complessiva dei rischi e di una vera applicazione delle policy di sicurezza, integrando le tecniche di firewalling con quelle di intrusion detection ed antivirus centralizzato. Di contro “il 48% dichiara di utilizzare almeno una delle due tecniche sopracitate, dimostrando un certo grado di attenzione al problema... Il restante 40% del campione indagato, conferma la preoccupante e diffusa tendenza a trattare operativamente le problematiche della sicurezza informatica con una poco chiara visione progettuale e, conseguentemente, si assemblano sistemi di sicurezza destrutturati ...”

² Nel campo della sicurezza informatica pubblica va ricordata la figura dell’Autorità Nazionale della Sicurezza, posta alle dipendenze della Presidenza del Consiglio dei Ministri, che si serve per la sua attività di controllo e di omologazione dell’Ufficio Centrale per la Sicurezza. Il suo campo di attività riguarda la protezione delle informazioni coperte dal segreto di stato, trattate in sistemi di elaborazione automatica e/o elettronica di dati e delle notizie di cui è vietata la divulgazione previste dall’art.12 della legge n.801 del 24 ottobre 1977. Nell’ambito delle sue competenze l’ANS ha emanato varie direttive con DPCM., l’ultima è stata quella dell’11 aprile 2002.

Vanno ricordati, tra gli altri, anche: il D.lgs. n.212 del 12/7/1991 relativo alle modalità di accesso delle amministrazioni pubbliche al sistema informativo dell'anagrafe tributaria, art.1; il DPR 27 /6/1992 n.352c, art.6; il c.d. Accordo Schengen (artt:114 e 118), ratificato dall'Italia con legge n.388 del 30 settembre 1993; il DPCM del 5/5/1994, relativo alle modalità tecniche e ripartizione delle spese connesse alla realizzazione di collegamenti, ecc., art.7 ed 8; il D.P.R. 23/12/1997 n.522, relativo ai compiti del Centro Tecnico per l'assistenza ai soggetti che utilizzano la RUPA, art. 2; il D.P.R. 10/11/1997 n.513, Regolamento recante criteri e modalità per l'archiviazione e la trasmissione di documenti con sistemi informatici e telematici, art.3, comma 3; il DPCM del 20/11/1997, Principi e modalità di attuazione della rete G-net, pr. 2; il D.P.R. n.428 del 20/10/1998, Regolamento per la tenuta del protocollo amministrativo con procedura informatica, ecc., art.3, comma 1 lett.a) e c); il DPCM 27/10/1999 n.437, Regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica, ecc., art 8; il DPCM del 31/10/2000, Regole tecniche per il protocollo informatico, ecc., art. 4.1 comma lett. c); il DPCM del 30/5/2002, Direttiva per la conoscenza e l'uso del domicilio internet "gov.it", ecc., pr. 26. Esistono infine vari decreti ministeriali relativi a specifici settori che qui non si elencano per brevità nonché varie circolari dell'AIPA in materia.

1.6.3 Sicurezza informatica e protezione dei dati personali

L'esame della normativa relativa alla sicurezza informatica fa emergere una particolare circostanza e cioè una prevalenza negli anni tra il 1996 ed il 2000 di prescrizioni dettagliate in tema di misure di sicurezza dirette alla protezione dei dati personali³.

Il trend normativo ha inizio con l'art.15 della legge n.675 del 23 dicembre 1996 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali) intitolato "Sicurezza dei dati" il cui comma 2 prevedeva la successiva emanazione di apposite "misure minime di sicurezza", poi effettivamente emanate con il DPR 28 luglio 1999 n.318 (successivamente, insieme ad altri provvedimenti citati in questo scritto -vedi, ad es, il D.lgs. 171/98, abrogato dal D.lgs. 30/6/2003 n.196, su cui amplius)⁴

Va osservato che con la legge n. 675/10 1996 venne introdotta la necessità del "documento programmatico per la sicurezza" (art.6) per quanto riguardava il trattamento dei dati di cui agli artt.22 e 24 della legge n.675/96.

Per inciso si rileva che il secondo comma del citato art.6 stabiliva che l'efficacia delle misure di sicurezza indicate nel documento programmatico avrebbe dovuto essere oggetto di controllo periodico da eseguirsi almeno annualmente.

Qualche innovazione in materia è stata introdotta con il D.lgs. n.196/2003 agli artt. da 31 a 36 e con il disciplinare tecnico di cui allegato B relativo alle misure minime di sicurezza,

³ Motivi socio politici inerenti anche ad un forte pressing effettuato da vari interessati sui "decision makers" dell'epoca, sembrano fornire una plausibile spiegazione in ordine alla indubbia prevalenza dell'azione politico-legislativa in tema di protezione della privacy rispetto alle esigenze, pur estremamente importanti, relative all'adozione, in modo coerente ed unitario, di iniziative decise in tema di sicurezza informatica nei sistemi pubblici. Con la creazione della figura del Ministro per l'innovazione e le tecnologie il problema della sicurezza informatica pubblica ha assunto carattere prioritario, rientrando tra gli obiettivi governativi.

⁴ Vari provvedimenti normativi emessi nel periodo 1996/2000, allorché accennano alla sicurezza informatica, richiamano espressamente l'art.15 della legge 675/1996. Vedi, ad es., l'art.2 del D.lgs. 13/5/1998 n.171, l'art.3, c.4 del DPR 10/11/1997 n.313, l'art.11 del D.M. 31/7/1998, ecc.

estendendosi -tra l'altro- la redazione del documento programmatico, prima previsto soltanto in relazione al trattamento dei dati sensibili e giudiziari, a tutti i trattamenti di dati personali⁵.

1.6.4 Le linee guida in tema di sicurezza informatica

Una decisa azione governativa diretta a sviluppare l'informatizzazione delle strutture della P.A. ed a regolamentare anche la sicurezza dei sistemi informatici pubblici si è verificata, come già detto, con la creazione della figura del Ministro per la Innovazione e le Tecnologie che già con il documento dal titolo "Linee Guida del Governo per lo sviluppo della società dell'informazione", al pr. 1/21 aveva annunciato la redazione del Piano Nazionale per la sicurezza ICT e la privacy, seguito poi dalla fondamentale Direttiva del 16/01/2002, relativa alla sicurezza informatica e delle telecomunicazioni nelle P.A., elaborata di concerto con il Ministro delle Comunicazioni alla quale erano allegati due documenti di orientamento (Valutazione del livello di sicurezza e Base Minima di sicurezza). L'azione è stata completata nella prima fase con la creazione, mediante il Decreto Interministeriale del 24/7/2002, del Comitato Tecnico Nazionale della sicurezza informatica e delle telecomunicazioni nelle P.A.⁶.

Per completezza di esposizione vanno qui ricordate le prescrizioni in tema di sicurezza informatica elaborate a cura dell'AIPA e cioè le "Linee Guida in tema di sicurezza informatica" pubblicate nel periodico Quaderni dell'AIPA, n.2, ottobre 1999, e soprattutto, la Raccomandazione n.1/2000 avente come titolo "Norme provvisorie in materia di sicurezza dei siti Internet delle Amministrazioni Centrali e degli Enti Pubblici"⁷.

1.6.5 Spunti per eventuali iniziative normative in materia di sicurezza informatica

Probabilmente, data la eterogeneità delle fonti normative e regolamentari relative alla materia, sarebbe opportuno, anche alla luce della legge 29/7/2003 n.229, (Interventi in materia di qualità della regolamentazione normativa e della codificazione-Legge di semplificazione 2001) e particolarmente dell'art.10 (Riassetto in materia di società dell'informazione) comma 1, e comma 2, lett.d) ricorrere allo strumento del decreto legislativo su iniziativa del Ministro per l'Innovazione e le Tecnologie, di concerto con quello delle Comunicazioni allo scopo di approntare un testo che coordini e regoli compiutamente la materia. L'opportunità di siffatta iniziativa appare chiara, ad avviso del Comitato, ove si consideri la necessità di coordinare l'attività di svariate entità pubbliche, stabilendo prescrizioni di natura cogente, in modo da assicurare coerenza ed uniformità di indirizzo, pur facendo salve le particolari esigenze di alcuni soggetti pubblici. Passando ad altro argomento e tenendo presenti anche le dichiarazioni del Ministro per

⁵ Qualche perplessità tuttavia suscita il confronto tra il testo dell'art.34 del D.lgs. n.196/2003 ed il par.19 dell'allegato B, intitolato "Documento programmatico sulla sicurezza" il quale, invece, prevede la redazione del citato documento soltanto nel caso dei dati sensibili e giudiziari, ripristinandosi in tal modo il testo dell'art.6 dell'abrogato DPR n.318/1999. Inoltre né l'art.34 né il pr.19 dell'allegato B contengono la prescrizione del secondo comma del citato art.6 del DPR n.318 circa l'obbligo del controllo periodico, *Quid iuris?*

⁶ Vedi in materia anche il paragrafo relativo alla sicurezza nella Direttiva del Ministro per l'innovazione, intitolata Linee Guida in materia di digitalizzazione dell'Amministrazione, del 20/12/2002. Dal canto suo il Ministro delle Comunicazioni con il Decreto del 14/1/2003, emesso di concerto con il Ministro della Giustizia, ha creato un Osservatorio per la sicurezza delle reti e la tutela delle telecomunicazioni.

⁷ Accenni alla materia sono contenuti in vari documenti dell'AIPA, vedi, ad es. "Lo Studio di fattibilità relativo alla RUPA" del gennaio 1996, la Relazione Annuale 2001, vol II, e il Piano Triennale 2002-2005 relativo alla informatica nella P.A.. Dal canto suo il Ministero della Giustizia ha commissionato al Politecnico di Torino uno studio dal titolo "Linee Guida per lo sviluppo di piani di sicurezza dei sistemi informatici del Ministero della Giustizia" consegnato il 12/11/2002. In argomento vedi anche i decreti dello stesso Ministro del 24/5/2001 e del 27/3/2002)

l'Innovazione e le Tecnologie relativamente allo sviluppo della posta elettronica, interna ed esterna, nell'ambito pubblico, appare opportuno disciplinare la materia, particolarmente per quanto riguarda la condotta degli operatori e degli utenti e le conseguenze legali di eventuali abusi, servendosi dello strumento regolamentare previsto dalla legge 10/1/2003 (Disposizioni ordinamentali in materia di Pubbliche Amministrazioni) con particolare riferimento all'art.27, comma 8, lett. E) che prevede appunto l'estensione della posta elettronica nell'ambito delle P.A. e dei rapporti tra P.A. e privati.

Altra area di intervento potrebbe essere quella dell'*outsourcing* nel campo pubblico, strumento che è previsto in generale per il settore pubblico da alcune disposizioni normative (vedi, tra l'altro, l'art.2 del D.lgs.12/2/1993 n.39, l'art.3, comma 2 del DPR 28/10/1994 n.478, e, da ultimo, i pr.25 e 26 –allegato B- del D.lgs. 30/6/2003 n.196.) e la cui estensione è stata sottolineata sia dalle indagini effettuate dall'AIPA (vedi il Piano Triennale 2003/2005) sia dalle audizioni svolte dallo stesso Comitato il quale, da tempo- sia detto per inciso-, ha manifestato le sue perplessità in ordine al ricorso a tale strumento per quanto riguarda particolarmente la sicurezza informatica. La necessità, in ogni caso, di un controllo penetrante da parte dell'Ente committente e di correlativi e particolari requisiti da parte del fornitore del servizio, in specie per quanto riguarda la serietà delle garanzie offerte –in particolare quanto all'affidabilità e professionalità del personale incaricato- postula che la “cabina di regia” in tema di sicurezza informatica resti saldamente nelle mani dell'Amministrazione. Ad avviso del Comitato, data la situazione di eterogeneità delle condotte da parte delle Amministrazioni pubbliche nella gestione della materia, sarebbe probabilmente opportuno un intervento normativo specifico.

Sempre nell'ambito di un auspicato intervento normativo in tema di sicurezza informatica andrebbe anche presa in considerazione la possibilità, peraltro largamente ammessa da alcune legislazioni estere (in particolare in USA) di ricorrere, almeno in relazione a particolari sistemi informatici c.d.critici, all'opera del *Tiger Teams o Red Teams* allo scopo di testare dall'esterno la validità delle misure adottate e la impenetrabilità del sistema informatico evidenziando le eventuali “falle” delle reti e suggerendo, al bisogno, gli eventuali rimedi. Va da sé che le aziende alle quali dovesse essere affidato tale delicato incarico dovrebbero rispondere a criteri assoluti di affidabilità e per i componenti delle équipes dovrebbe essere previsto uno speciale NOS⁸.

1.7 Cenni sulle iniziative internazionali in tema di sicurezza informatica.

In correlazione con il tema trattato e per offrire un succinto panorama delle iniziative recenti e attuali nel settore internazionale concernente le strategie dirette ad assicurare la protezione delle reti informatiche, verrà qui di seguito tracciato un breve panorama di tali iniziative. Come è noto, da tempo le maggiori organizzazioni internazionali si sono date carico del problema relativo alla sicurezza informatica e le azioni intraprese sono di recente divenute più incisive: ciò sia a seguito dell'attentato di New York dell'11 settembre 2001 e delle sue conseguenze, sia a causa dell'uso della rete per motivi di lotta politica e specificatamente di aggressione terroristica, sia infine a seguito dei gravi attacchi condotti verso le reti ed i sistemi di informazione mediante le tecniche cd. DoS e DdoS nei confronti della rete Internet a cui si sono aggiunte le diffusioni di Worms e Virus.

⁸ Particolare attenzione occorrerebbe dedicare, ad avviso del Comitato, ai problemi tecnici e giuridici delle reti Wireless.

La prima, e forse più importante iniziativa si deve all'OCSE che già nel 1992 emanò una Raccomandazione del Consiglio (16.11.1992) concernente le Linee Diretrici relative alla sicurezza dei sistemi di informazione, poi rivista e modificata recentissimamente in data 27 luglio 2002.

Nell'ambito dell'Unione Europea è da ricordare che il Consiglio approvò già nel 1992 una Decisione nel settore della sicurezza dei sistemi di informazione. Successivamente il 26 gennaio 2001 la Commissione inviò al Consiglio e al Parlamento una importante Comunicazione dal titolo "Creare una società dell'informazione sicura, migliorando la sicurezza delle infrastrutture dell'informazione mediante la lotta alla criminalità informatica".

A fronte di tale comunicazione il Parlamento emise il 6 settembre 2001 una "Raccomandazione relativa alla strategia per creare una società dell'informazione sicura".

Peraltro la stessa Commissione il 16 gennaio 2001 aveva inviato al Consiglio un'altra importante Comunicazione dal titolo "Sicurezza delle reti e sicurezza dell'informazione. Proposta per un approccio strategico europeo".

In essa richiamava tra l'altro il lavoro svolto dagli organismi pubblici e privati di intervento in caso di emergenza informatica (CERT) e da organismi simili, rilevando tuttavia che i CERT operavano in modo diverso a seconda degli Stati membri, per cui la cooperazione appariva difficile. In ogni caso – ricordava la Commissione – il coordinamento a livello internazionale avveniva tramite il CERT/CC, un organismo parzialmente finanziato dal Governo USA, per cui i CERT europei apparivano tributari della politica di divulgazione delle informazioni del CERT/CC e di altri organismi. Infine la Commissione suggeriva agli Stati membri l'opportunità di potenziare risorse e competenze dei CERT nazionali esistenti nell'ambito dell'UE e suggeriva, inoltre, di creare una rete dei CERT per lo scambio di informazioni, rete che avrebbe dovuto essere collegata ad organismi dello stesso tipo, attivi in tutto il mondo, come ad esempio il sistema di segnalazione degli incidenti proposto dal G8.

In esito a tale comunicazione il Parlamento europeo ha emanato il 22 ottobre 2002 una Risoluzione nella quale, dopo aver affermato che i CERT presenti nei vari Stati membri operavano in modo eterogeneo il che rendeva la cooperazione inutilmente complessa, e dopo aver citato il moltiplicarsi a livello internazionale di iniziative pubbliche e private per assicurare la affidabilità delle reti, quali ad esempio la rete per lo scambio di informazioni sulla sicurezza istituito nell'ambito del G8, nonché le reti di EUROPOL ed INTERPOL, in relazione agli aspetti istituzionali concordava con la Commissione sulla necessità di istituire quanto prima una "Task force" sulla sicurezza delle reti con determinati specifici obiettivi⁹.

⁹ Altri testi importanti in materia di sicurezza informatica sono la Risoluzione del Consiglio UE del 18/02/2003 avente come titolo "Per una cultura della sicurezza delle reti e dell'informazione", nella quale, tra l'altro, si invitano gli Stati membri a promuovere la sicurezza quale componente essenziale del governo pubblico e privato, in particolare incoraggiando l'assegnazione delle responsabilità, e la Posizione Comune n. 39-2003, definita dal Consiglio il 26/05/2003 in vista della Decisione del Parlamento Europeo e del Consiglio circa l'adozione di un piano pluriennale (2003-2005) per il monitoraggio del piano di azione eEurope, la diffusione delle buone prassi ed il miglioramento della sicurezza delle reti e dell'informazione (MODINIS).

Occorre ricordare anche il programma USA per la sicurezza, recentemente sottoscritto dal Presidente Bush e avente come titolo "National Strategy to Secure Cyberspace", il quale prevede – tra l'altro – la costituzione di una National Security Response System, una struttura pubblico/privata coordinata dal Department of Homeland Security di recente istituzione, sistema che, nel settore della sicurezza, ha i seguenti compiti, relativamente alle vulnerabilità, agli allarmi ed agli attacchi informatici, e cioè: Analysis, Warning, Incident Management, Response/Recovery.

A seguito di tali iniziative e decisioni, la Commissione UE nel febbraio di quest'anno elaborò uno schema di proposta relativa alla costituzione di una Rete europea e di una Agenzia avente per oggetto la "Information Security" che avrebbe dovuto operare come punto di riferimento e di affidabilità in vista della sua indipendenza, della qualità dei suoi pareri e dei risultati conseguiti, delle informazioni fornite, della trasparenza delle sue procedure e dei suoi moduli operativi nonché della sua diligenza nei compiti affidatigli. L'Agenzia avrebbe espletato i suoi compiti in stretto collegamento con gli Stati membri ed avrebbe dovuto essere aperta ai contatti con l'industria e con i gruppi interessati. Obiettivo principale dell'Agenzia, secondo il documento originario, sarebbe stato quello di facilitare l'applicazione delle iniziative e misure comunitarie relative alla sicurezza delle reti e dell'informazione ed aiutare ad ottenere la interoperabilità delle funzioni di sicurezza nella rete nei sistemi di informazione, contribuendo in tal modo al funzionamento del Mercato Interno e stimolando in ultima analisi le capacità della Commissione e degli Stati membri in tema di sicurezza delle reti e dell'informazione.

I compiti dell'Agenzia erano molteplici così come indicato nell'art. 2 della proposta originaria. Secondo gli intendimenti della Commissione, l'Agenzia avrebbe dovuto essere strutturata nel modo seguente:

- a) Management Board;
- b) Executive Director e relativo staff;
- c) Advisory Board;
- d) Working Groups (eventuali).

In relazione alla istituzione dell'Agenzia in questione il Consiglio il 5/6/2003 convenne un orientamento generale che conteneva tre modifiche rispetto al testo proposto dalla Commissione¹⁰, e chiese al Comitato dei Rappresentanti permanenti di esaminare il parere del Parlamento Europeo (prima lettura) non appena disponibile per consentirgli di adottare una posizione comune in una delle successive sessioni. Il testo dell'Orientamento generale è stato approvato nell'ottobre scorso ma con due astensioni, una della delegazione tedesca ed una di quella inglese. A sua volta il Comitato economico e sociale emise il 18/06/2003 un parere favorevole ma con osservazioni in merito alla proposta della Commissione.

Il 20 novembre u.s. il Parlamento Europeo ha esaminato la proposta più volte citata approvandola ma con non trascurabili modifiche rispetto al documento originario della Commissione. Secondo la Risoluzione il compito dell'Agenzia deve essere quello di contribuire a mantenere un alto ed effettivo livello di "network and information security" nell'ambito della Comunità e di sviluppare una cultura della sicurezza informatica e delle reti a beneficio dei cittadini, dei consumatori e delle organizzazioni del settore pubblico e privato dell'Unione Europea, contribuendo in tal modo ad un corretto funzionamento del Mercato Interno.

¹⁰ Le modifiche principali erano: a) limitazione dell'attività dell'Agenzia ad un ruolo di consultazione e soppressione delle disposizioni riguardanti il comitato consultivo; b) modificazione della composizione del Consiglio d'amministrazione con l'inclusione di un rappresentante per ciascuno Stato, di tre rappresentanti nominati dalla Commissione e di altri tre rappresentanti, privi del diritto di voto, ciascuno dei quali in rappresentanza dell'industria, della tecnologia dell'informazione e della comunicazione, dei gruppi di consumatori e degli esperti universitari in materia di sicurezza delle reti e dell'informazione.

Non può tacersi, come già detto nel testo, che appare quantomeno strano che si sia trascurata del tutto la componente giuridica, giacché la funzione consultiva non può prescindere dalla conoscenza delle implicazioni giuridiche e normative della sicurezza informatica.

I molteplici compiti dell'Agenzia sono indicati dettagliatamente nell'art.3 della Risoluzione: il principale è quello di raccogliere le informazioni appropriate per analizzare i rischi correnti ed emergenti, in particolare a livello europeo, che potrebbero compromettere l'affidabilità delle reti di comunicazioni elettroniche ovvero l'autenticità, l'integrità e la riservatezza delle informazioni ricevute e trasmesse attraverso tali reti e fornire il risultato delle analisi agli Stati Membri della Comunità.

La struttura dell'Agenzia è così definita:

1) **Management Board**, composto da un rappresentante per ciascuno degli Stati Membri, tre rappresentanti nominati dalla Commissione, tre rappresentanti nominati dal Consiglio su nominativi proposti dalla Commissione, senza diritto di voto, ciascuno dei quali rappresenta uno dei seguenti gruppi: industria ITC, gruppi di consumatori, esperti accademici nel settore della sicurezza informatica e delle reti;

2) **Executive Director**, indipendente nelle sue funzioni, nominato dal Management Board per un periodo di cinque anni sulla base di una lista di candidati, meritevoli e dotati di documentate esperienze amministrative e manageriali proposti dalla Commissione a seguito di una "open competition" annunciata sulla GUCE;

3) **Permanent Group Stakeholders**, nominati dall'E.D. e che rappresentino importanti stakeholders, quali industrie ICT, gruppi di consumatori, esperti accademici nell'ambito della sicurezza delle reti e dell'informazione, avente funzione di consulenza per l'E.D. dal quale è presieduto.

È auspicabile che l'Agenzia dia risalto agli aspetti relativi alla componente giuridica, in quanto le funzioni da svolgere richiedono necessariamente il supporto di giuristi specializzati in materia di sicurezza informatica.

Per concludere, il problema relativo alla sicurezza informatica è certamente serio e non può essere risolto soltanto a livello nazionale, data la transnazionalità degli attacchi, per cui, superate le obiezioni di tipo giuridico e per evitare "situazioni di galleggiamento" della Agenzia in ambito comunitario, occorrono iniziative giuridiche e politico-legislative che diano vita ad organizzazioni corrispondenti nei Paesi membri, organizzazioni la cui esistenza appare il presupposto indispensabile per una azione comune e per un effettivo coordinamento operativo.



Proposte concernenti le strategie
in materia di sicurezza informatica
e delle telecomunicazioni (ITC)
per la pubblica amministrazione

Parte prima **proposte per un sistema di governo** **della sicurezza ict nella PA**

2. Parte prima - Proposte per un sistema di governo della sicurezza ICT nella PA

2.1 Modello organizzativo

La gestione della sicurezza nella P.A. deve essere eseguita attraverso un opportuno processo che preveda lo sviluppo di politiche di sicurezza sia a livello di Amministrazione (l'intera P.A. o, se necessario, specifiche Pubbliche Amministrazioni o parti di esse) sia a livello di sistemi ICT. Nell'ambito di tali politiche uno degli aspetti più rilevanti è costituito dalla individuazione dei ruoli ai quali assegnare la responsabilità di svolgere le principali funzioni che le politiche stesse considerano necessarie ai fini di una corretta gestione della sicurezza. Alcuni di tali ruoli sono di tipo centralizzato e prevedono l'istituzione di appositi organismi attraverso i quali assicurare la fornitura di servizi di sicurezza utili per tutte le Pubbliche Amministrazioni, servizi che sarebbe antieconomico realizzare in ciascuna di esse. Altri ruoli sono invece da collocare all'interno delle singole Amministrazioni e sono stati in gran parte già definiti nell'allegato 2 della direttiva [1]. Un primo ruolo centralizzato è evidentemente quello attribuito con il decreto 24/7/2002 del Ministro delle Comunicazioni e del Ministro per l'Innovazione e le Tecnologie al Comitato Tecnico Nazionale per la sicurezza informatica e delle telecomunicazioni nelle Pubbliche Amministrazioni. Si tratta di un ruolo di coordinamento, indirizzamento e monitoraggio nella gestione della sicurezza ICT da parte delle Pubbliche Amministrazioni, come risulta dall'elenco dei compiti, riportato nell'introduzione, assegnato al Comitato.

Attualmente il Comitato non dispone tuttavia di risorse: pertanto non può offrire alla P.A. una serie di servizi operativi dei quali si percepisce invece una forte necessità. Per tale motivo si ritiene che sia da considerare la sua confluenza in un apposito organismo dotato di mezzi atti a consentirne piena operatività, cui è stato assegnato il nome di Centro Nazionale per la Sicurezza Informatica (CNSI), e le cui funzioni verranno descritte nel paragrafo che segue.

Successivamente verranno trattati ulteriori organismi preposti alla fornitura centralizzata di servizi operativi e, a seguire, i ruoli da prevedere nell'ambito delle singole Amministrazioni al fine di completare la definizione del modello organizzativo.

2.1.1 Il Centro Nazionale per la Sicurezza Informatica (CNSI)

Nell'ambito di questa sezione si definisce quale potrebbe essere la struttura organizzativa del CNSI e le funzionalità che dovrebbe svolgere. Tale organismo, nelle intenzioni del Comitato, deve possedere autonomia organizzativa e contabile nelle forme di una agenzia o alto commissario.

Il CNSI è realizzato sulla base dei seguenti presupposti:

- Molte organizzazioni o loro responsabili che decidono di adottare soluzioni ICT spesso trascurano il problema sicurezza. Quindi non si preoccupano di proteggere i propri sistemi, che divengono così facili obiettivi di attacchi informatici. D'altro lato le tecnologie per la sicurezza sono difficili da comprendere e gestire correttamente.

- Questo significa che vi è la necessità di incentivare azioni mirate a promuovere la sicurezza informatica nonché programmi di formazione per il corretto uso delle tecnologie.
- Laddove esistano contromisure efficaci per far fronte a problemi di sicurezza, la situazione può cambiare drasticamente nel caso di forme di attacco innovative o mutanti. In questi casi per individuare la soluzione ad un attacco informatico può essere necessaria la consultazione di esperti in diversi settori e la disponibilità di sofisticati laboratori di ricerca. Sono poche le organizzazioni che possono disporre di queste risorse.
 - La soluzione di problemi derivanti dall'insicurezza dei sistemi può richiedere la collaborazione di più entità non necessariamente residenti nella stessa nazione; è quindi indispensabile per poter far fronte ad ogni problema di questo tipo contattare ed interallacciare rapporti con diverse organizzazioni di diversi paesi. Questa azione può essere svolta solo da opportuni organismi che abbiano ricevuto un riconoscimento nazionale ed internazionale che consenta loro lo svolgimento delle suddette "indagini". Tutto ciò significa che il CNSI deve predisporre efficaci piani di consapevolezza, deve poter disporre di risorse e competenze per far fronte ad attacchi informatici sviluppando "intelligence" e soprattutto deve essere inserito in un contesto internazionale. Tale organismo, per poter svolgere efficacemente i propri compiti deve inoltre godere di particolari prerogative.

Il Centro Nazionale per la Sicurezza Informatica deve infatti essere autonomo ed indipendente da ogni fornitore di prodotti e servizi di sicurezza informatica; deve possedere, direttamente o indirettamente, le competenze necessarie per generare le informazioni di cui necessita e saper valutare criticamente quelle ottenute da altre fonti; deve inoltre essere messo in grado di emanare, nell'ambito delle proprie competenze, direttive a tutte le Pubbliche Amministrazioni. Accanto a queste prerogative il CNSI ha degli obblighi verso i propri utenti: a fronte di una richiesta d'intervento da parte di un utente deve essere in grado di garantire, in ogni situazione, tempi di risposta estremamente contenuti, e deve essere in grado di generare e distribuire informazioni di qualità molto elevata.

2.1.2 Le funzionalità del Centro Nazionale per la Sicurezza Informatica

Gli obiettivi principali del Centro Nazionale per la Sicurezza Informatica devono essere:

- accrescere il livello medio di protezione dei sistemi informatici degli utenti Internet Italiani con particolare riferimento agli utenti della Pubblica Amministrazione;
- predisporre le misure adeguate per far fronte ad eventuali attacchi informatici a sistemi della PA;
- predisporre le misure adeguate per ripristinare in tempi brevi i sistemi compromessi.

Si riporta di seguito un elenco dettagliato delle attività che devono essere intraprese dal CNSI. Per una migliore chiarezza espositiva si suddividono in tre categorie in base al loro principale scopo: prevenzione, rilevamento e risposta.

Prevenzione

Promuovere programmi per accrescere la consapevolezza del problema sicurezza informatica tra gli utenti della rete Internet. Come già accennato precedentemente diversi prodotti e metodologie sono disponibili per far fronte al problema della sicurezza informatica; la grande maggioranza degli utenti della rete ne ignorano, però, i fondamenti essenziali o addirittura ignorano il problema.

Studiare, valutare e promuovere l'uso di "best practice" nel settore della sicurezza informatica. La maggior parte delle tecnologie e metodologie di sicurezza sono relativamente moderne e tra gli utenti non esiste sufficiente esperienza nell'uso di questi strumenti. È necessario quindi un piano per la diffusione di informazioni sull'uso e l'applicazione degli stessi. Tale informazione deve coprire diversi settori che vanno dai processi aziendali legati alla sicurezza, agli schemi per la classificazione delle informazioni, ai meccanismi di identificazione/autenticazione, PKI, firewall, intrusion detection system, sand-box, ecc. ecc..

Promuovere attività di ricerca e la cooperazione tra i centri di ricerca. La ricerca è l'unico strumento che può essere utilizzato per aumentare il livello di sicurezza degli attuali prodotti ICT e per creare e diffondere il livello di conoscenza necessario per far fronte o prevenire nuove forme di intrusione informatica. È quindi necessario promuovere la creazione di centri di ricerca nel settore della sicurezza informatica e costituire uno stretto legame tra il CNSI e questi centri.

Raccogliere e distribuire informazioni aggiornate sulle intrusioni e relative contromisure. È necessario rendere disponibili tutte le informazioni legate a nuove forme di intrusione al fine di consentire agli utenti di poterle riconoscere. A tal fine è indispensabile costruire un data base pubblico contenente questo tipo di informazioni. Nella diffusione di tali informazioni è inoltre da privilegiare un approccio "push", essere cioè propositivi e tempestivi nella diffusione di informazioni aggiornate.

Promuovere corsi di formazione per i dipendenti della Pubblica Amministrazione. La formazione è il primo passo da compiere per far crescere negli utilizzatori delle tecnologie la consapevolezza del problema sicurezza. Nell'ambito della Pubblica Amministrazione il problema è particolarmente sentito ed è quindi necessario predisporre un massiccio programma di formazione per tutti gli utilizzatori.

Promuovere il ricorso agli standard di sicurezza. La certificazione dell'IT security in accordo agli standard riconosciuti a livello internazionale rappresenta un mezzo importante per costruire la fiducia e la confidenza sia nei confronti di un'organizzazione che tra le varie parti coinvolte. In sostanza, due standard ISO/IEC sono applicabili per la certificazione. Lo standard ISO 15408, noto anche come Common Criteria for Information Technology Security, che fornisce le principali direttive per la valutazione e certificazione di prodotti e sistemi informatici. Lo standard ISO 17799, che invece fornisce importanti indicazioni sulle misure organizzative da intraprendere, in un'azienda, per poter far fronte al problema della sicurezza informatica.

Rilevamento

Controllare le attività svolte sulla rete. Al fine di individuare situazioni anomale correlate ad attacchi in corso è necessario controllare costantemente la rete. Esistono tecnologie che potrebbero essere utilizzate per supportare questo tipo di attività, che denominiamo monitoraggio attivo. Il monitoraggio attivo è molto importante poiché consente di "catturare" sul nascere un tentativo di intrusione o un attacco in corso. Questo tipo di monitoraggio consente inoltre di raccogliere dati attendibili sulle intrusioni informatiche che possono essere proficuamente utilizzati per previsioni e trend nel settore.

Collezionare ed analizzare tutte le segnalazioni provenienti dagli utenti finali. Un altro modo per monitorare la rete, che possiamo chiamare monitoraggio passivo, è quello di raccogliere le segnalazioni di intrusioni inoltrate da utenti finali e, dopo averle analizzate, utilizzarle per gli scopi di cui al punto precedente. Questo approccio richiede però che l'utente finale possieda una notevole padronanza delle tecnologie, requisito soddisfatto solo in minima parte dagli utenti della rete.

Risposta

Fornire supporto agli utenti vittime di un'intrusione. Individuata o ricevuta la segnalazione di un'intrusione è necessario fornire il necessario supporto, in termini di competenze tecniche, alla vittima. Gli obiettivi di questa fase devono essere: ridurre l'impatto dell'attacco sul sistema vittima, tentare di risalire all'intrusore e consentire il ripristino dei sistemi compromessi nel minor tempo possibile.

Contattare uno o più centri di ricerca. Al fine di individuare la tecnica utilizzata e le contromisure da adottare, i dati relativi all'intrusione devono essere inviati ad esperti del settore che dalla loro analisi potranno risalire alle cause ed alle origini. Una volta individuate le cause sarà estremamente facile individuare le contromisure per evitare l'attacco. Questa fase si rende ovviamente necessaria solo per intrusioni di cui non si conoscono gli effetti e le contromisure.

Allertare tutti i responsabili di sistemi che possono essere oggetto di un attacco simile. Un altro modo per ridurre gli effetti di un attacco informatico è quello di limitare il numero di sistemi compromessi. Questo effetto può essere ottenuto allertando in tempo debito tutte le potenziali vittime di un attacco e fornendo loro le istruzioni per come far fronte allo stesso.

Diffondere l'informazione a livello internazionale. Nel caso in cui ci si trovi di fronte ad una nova forma di attacco informatico è necessario allertare l'intera comunità Internet; è quindi necessario che il CNSI sia in collegamento con organismi equivalenti in tutto il mondo.

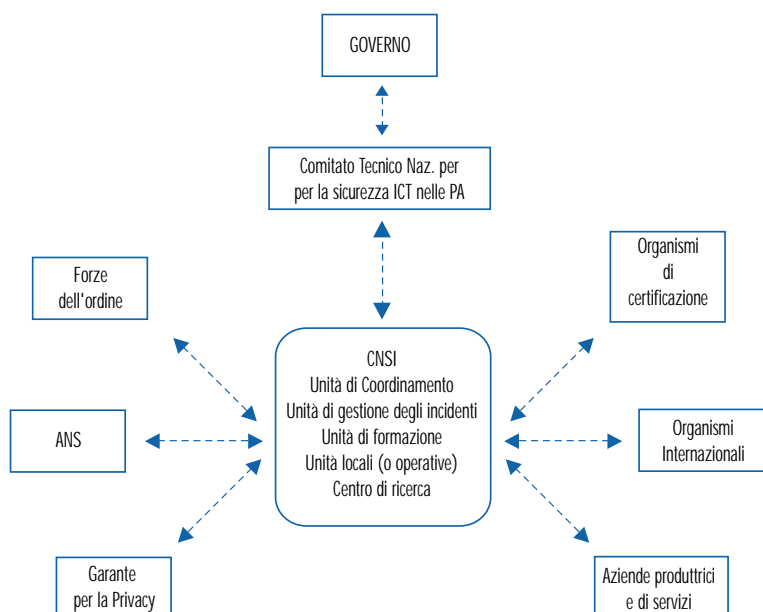
2.1.3 La struttura del Centro Nazionale per la Sicurezza Informatica

Al fine di assicurare la massima tempestività nella diffusione delle informazioni, di garantire un assoluto livello di qualità e omogeneità della stessa e di poter aver una visione unica e complessiva sulla situazione di sistemi della P.A. è importante che il CNSI sia, logicamente parlando, un'unica entità che opera su scala nazionale. Fisicamente si può ipotizzare che lo stesso sia composto da diverse unità dislocate sul territorio nazionale; è però importante che le stesse facciano riferimento ad un unico centro di raccordo. Inoltre si ritiene che debba trattarsi di un organismo civile che non mancherà però di avere i necessari rapporti con le forze dell'ordine, l'Autorità Giudiziarica, l'Autorità Nazionale per la Sicurezza ed ogni altra istituzione che a livello nazionale si occupa del problema. Il modello proposto individua nell'ambito del CNSI cinque componenti fondamentali che devono cooperare affinché il CNSI possa raggiungere i propri obiettivi.

Riportiamo una breve descrizione di queste componenti e rinviamo ai paragrafi successivi una descrizione più dettagliata degli stessi. Talune componenti potrebbero essere realizzate presso singole P.A., ove esistano già le necessarie competenze. In altri casi il CNSI potrà attivare convenzioni con Enti esterni pubblici o privati per la fornitura parziale o totale dei servizi di una componente.

1. **Unità di coordinamento:** il compito principale del centro di coordinamento è quello di raccordare tutte le attività intraprese dalle varie unità che operano all'interno della struttura, di raccogliere, elaborare e distribuire informazioni, di coordinare le attività delle varie unità operative e fornire alle stesse il necessario supporto.
2. **Unità di gestione degli incidenti informatici:** si tratta di un'unità preposta al rilevamento delle intrusioni informatiche sui sistemi della Pubblica Amministrazione ed alla loro gestione. Questa unità svolge anche il ruolo di centro early warning e information sharing, come sarà chiarito nella sezione successiva.
3. **Unità di formazione:** compito di questa Unità è la predisposizione e l'erogazione di corsi di formazione per i dipendenti della P.A. in tema di sicurezza ICT.
4. **Unità Locali (o Operative):** si tratta di organismi tecnici preposti alla gestione operativa della sicurezza informatica, che svolgono il loro operato presso le Pubbliche Amministrazioni dove operano di concerto con il CNSI e quindi svolgono anche una funzione di raccordo tra il CNSI e le varie sedi della Pubblica Amministrazione. Ogni istituzione di rilievo della P.A. deve prevedere una di queste unità operativa.
5. **Centro di ricerca** Il principale scopo di questo centro di ricerca è quello di creare il corpo di conoscenze e di esperienze necessarie per risolvere casi di minacce o attacchi informatici particolarmente complessi, prevedere nuove forme di attacco informatico e virus. Un ulteriore compito svolto da questo centro è la formazione del personale del CNSI con alti contenuti scientifici e tecnologici nel settore della sicurezza informatica.
6. **Una rete di rapporti e collaborazioni** con istituzioni ed Enti che a livello nazionale ed internazionale si occupano della problematica. Riportiamo brevemente in Figura 1 un possibile schema di interrelazioni che il CNSI dovrà sviluppare. Queste relazioni si dovranno concretizzare attraverso la definizione e la realizzazione di tavoli di lavoro comuni, osservatori su tematiche di comune interesse, studi e ricerche comuni, ecc. ecc.

Figura 1: Schema delle interrelazioni del CNSI



2.1.3.1 L'Unità di Coordinamento

È la componente del CNSI incaricata di attivare e dirigere tutte le attività del Centro, promuovere specifiche attività di ricerca nel settore, svolgere le funzioni di raccolta e smistamento delle informazioni e fornire supporto consulenziale a tutte le Pubbliche Amministrazioni, specie quando vengono richieste rapide implementazioni di progetti o misure preventive urgenti. Questa componente del CNSI deve anche farsi carico di intrattenere rapporti con equivalenti organismi che operano a livello internazionale nello stesso settore.

I principali obiettivi che l'unità di coordinamento dovrebbe perseguire sono:

- aumentare il livello di consapevolezza del problema "sicurezza informatica" in tutta la PA;
- predisporre azioni al fine di migliorare le capacità di prevenzione degli incidenti informatici nella PA;
- adoperarsi affinché il CNSI diventi, nel panorama nazionale, un punto di riferimento nonché un centro di eccellenza nelle diverse tematiche che caratterizzano la sicurezza informatica (Metodologiche, Legali, Tecniche);
- costruire rapporti tra il CNSI e tutte le istituzioni, che nel panorama nazionale si interessano al problema;
- fungere da unità di crisi in caso di gravi problemi riguardanti il mondo dell'IT;
- adoperarsi affinché, attraverso il CNSI, il livello di esposizione al rischio informatico delle singole amministrazioni, diminuisca sensibilmente.

Accanto alle necessarie competenze di management l'Unità di coordinamento dovrà anche possedere quelle di ordine tecnologico per i seguenti motivi:

- accrescere la credibilità dell'istituzione verso il mondo esterno;
- consentire all'unità di coordinamento di disporre di una fonte di informazioni garantita in situazioni critiche.
- svolgere al meglio le funzioni di rappresentanza nei rapporti internazionali.

Il team di supporto tecnico deve sempre mantenere un alto livello di competenze tecnologiche, in particolar modo riguardo ai prodotti commerciali, specialmente quelli diffusamente utilizzati nei settori pubblici e deve essere in grado di operare negli ambiti qui sotto riportati.

- selezione dei prodotti ICT in base alle proprietà di sicurezza;
- formazione, informazione e consiglio sulle tecnologie dell'IT security;
- assistenza attiva durante gli incidenti informatici più critici;
- penetration testing;
- analisi di software;
- altri tipi di supporto tecnico nel campo dell'IT security.

2.1.3.2 Le Unità di gestione degli incidenti e di formazione

Queste unità vengono diffusamente descritte nel seguito del documento.

2.1.3.3 Le Unità Locali (o Operative)

Ogni pubblica amministrazione, sia centrale che locale, è direttamente responsabile per la realizzazione di un livello sufficiente di sicurezza nei confronti dei propri sistemi informatici. Ciò significa che ogni Amministrazione deve essere in grado di identificare e di valutare le conseguenze della sua dipendenza dall'IT e di occuparsi dei rischi implicati da tale dipendenza. Più precisamente ogni amministrazione deve provvedere alla elaborazione di

una propria politica di sicurezza che includa, tra l'altro, un piano di Business Continuity. La struttura organizzativa delle unità locali è definita successivamente, nell'ambito del paragrafo che tratta i ruoli nelle singole Amministrazioni.

In questo quadro al CNSI è attribuita la responsabilità di fornire a tutte le Amministrazioni, attraverso le unità locali, le competenze necessarie per svolgere le attività sopra descritte e fornire un supporto operativo nella fase di monitoraggio dei sistemi e gestione degli incidenti. Sarà quindi indispensabile garantire lo scambio reciproco di informazioni tra il CNSI e queste Amministrazioni ai fini di consentire ad entrambi di mantenere adeguatamente aggiornato il proprio livello di informazione.

2.1.3.4 Centro di ricerca

Nell'organigramma del CNSI il centro di ricerca svolge il ruolo di fonte di notizie e competenze per il centro di coordinamento del CNSI e per l'Unità di Gestione degli Incidenti. Il centro di ricerca potrà assistere le altre entità espletando studi o ricerche, per acquisire informazioni esaustive e per assicurare la formazione del personale specialistico. Come già anticipato il Centro di Ricerca non è necessariamente un organo del CNSI ma può essere costituito da una o più entità esterne con il quale il centro di coordinamento decide di stabilire dei rapporti di collaborazione. Anche in questo caso visto il ruolo di indipendenza che il CNSI deve mantenere rispetto al mercato, è auspicabile che i centri individuati non siano Enti appartenenti ad organizzazioni commerciali.

2.1.4 Rapporti con le altre istituzioni

Di fondamentale importanza per il CNSI è possedere la massima visibilità su ciò che accade sia in ambito nazionale che internazionale nel settore della sicurezza informatica: a tal scopo è necessario che il CNSI intrattenga regolari rapporti con Enti nazionali ed internazionali che perseguano obiettivi equivalenti, come di seguito riportati.

2.1.4.1 Forze dell'ordine

Nel nostro paese tutte le forze dell'ordine (Polizia, Finanza e Carabinieri) posseggono unità specializzate per la lotta contro il crimine informatico nelle diverse forme in cui si presenta. È indispensabile per il CNSI stabilire dei rapporti di collaborazione e di reciproco scambio di informazioni con ciascuna di queste unità.

2.1.4.2 Autorità Nazionale per la Sicurezza

È estremamente importante che il CNSI sia raccordato con l'Autorità Nazionale per la Sicurezza e che tra i due Enti si instauri un rapporto di reciprocità improntato allo scambio di informazioni e alla produzione di documenti e linee guida comuni.

2.1.4.3 Organismi di Certificazione

Come descritto nel seguito del documento, le certificazioni di sicurezza possono essere eseguite sia a livello dell'organizzazione sia a livello dei sistemi ICT. In quest'ultimo caso la struttura nell'ambito della quale le certificazioni vengono eseguite viene denominata Schema Nazionale di Certificazione ed è coordinata da un Organismo di Certificazione governativo. Nel quadro della sicurezza informatica del paese lo Schema Nazionale svolge quindi un ruolo molto critico. È quindi estremamente importante che lo stesso, tramite l'Organismo di Certificazione, stabilisca con il CNSI un rapporto di stretta collaborazione per un reciproco travaso di competenze e di informazione.

2.1.4.4 Altri Enti privati

Nella lotta all'insicurezza informatica è estremamente importante che i settori pubblici e privati che operano nel settore siano in grado di condividere le conoscenze e fornire supporto reciproco per far fronte alle "emergenze informatiche". È quindi auspicabile che nell'ambito del settore privato nascano delle iniziative analoghe al CNSI con le quali interallacciare stretti rapporti di collaborazione. A tale riguardo vale forse la pena rifarsi all'esperienza USA dove il 22 maggio 1998 attraverso la direttiva presidenziale USA PDD-63, è stata data la spinta decisiva per la nascita di Information Sharing and Analysis Center (ISAC), all'interno di ognuno dei settori ritenuti critici per la sicurezza della nazione. Brevemente ricordiamo che gli ISAC sono associazioni di aziende private preposte alla diffusione di dati relativi agli attacchi ed alle vulnerabilità informatiche. Il sistema ISAC raccoglie questi dati dai propri membri e da altre fonti esterne e li diffonde ai propri membri dopo averli opportunamente analizzati ed integrati in un'immagine coerente che rispecchi lo stato attuale della minaccia informatica.

2.1.4.5 Cooperazione internazionale

La società dell'informazione non conosce confine; proprio per questo motivo e per proteggerla da attacchi di diverso tipo, deve essere prevista una struttura di difesa che operi e che si basi sulla cooperazione internazionale. È quindi importante che il CNSI instauri contatti stabili con la nascente Agenzia Europea per la Sicurezza Informatica (ENISA), l'Agenzia statunitense per la Sicurezza Informatica, il NISCC inglese (National Infrastructure Security Coordination Centre), il SEMA (Swedish Emergency Management Agency) svedese, il BSI (Bundesamt für Sicherheit in der Informationstechnik) tedesco, il "Secrétariat Général de la Défense Nazionale", francese.

Il nostro Paese inoltre dovrebbe assumere un ruolo attivo nei processi che si occupano della definizione di standard comuni per la sicurezza, nei processi che si occupano di trattamento delle informazioni e nella definizione delle infrastrutture IT.

L'Italia dovrebbe anche sostenere attivamente gli accordi e le regole internazionali riguardo la rilevazione di attività non autorizzate all'interno di sistemi informativi e nel settore informatico in generale. Tali rilevazioni possono, sotto ben definiti vincoli di privacy e di segretezza, avvenire anche all'interno dei confini nazionali.

2.1.5 L'Unità di gestione degli attacchi informatici

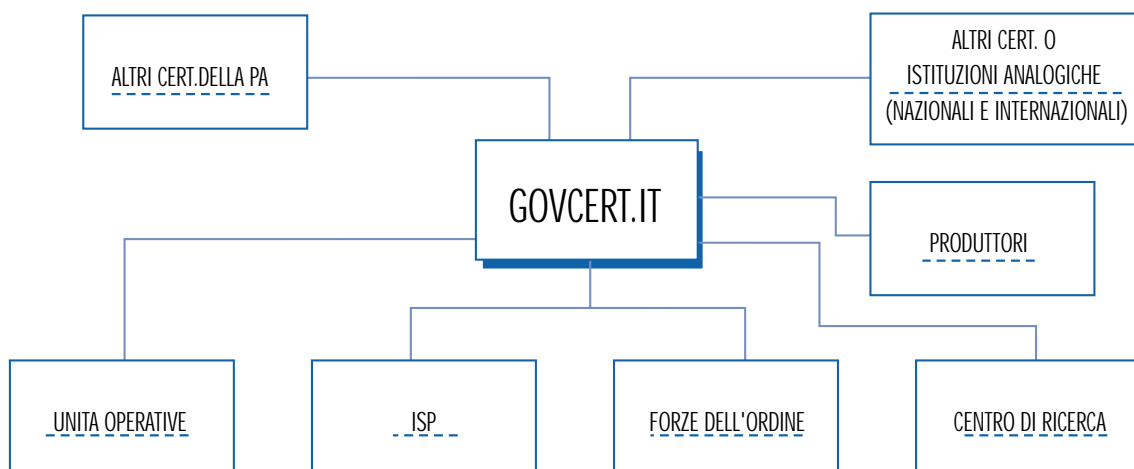
Nell'ambito della sicurezza informatica una particolare attenzione è sicuramente rivolta agli attacchi informatici, definiti come una serie di attività svolte intenzionalmente da un "avversario" per ottenere un accesso non autorizzato ad un sistema informatico. Nell'ambito del CNSI si è quindi pensato di predisporre un'apposita unità preposta a gestire i diversi aspetti legati alla prevenzione, al rilevamento ed alla gestione degli attacchi informatici. Vista la complessità sia in termini di articolazione che di funzionalità che questa unità deve possedere si riportano qui di seguito, seppur sommariamente le funzionalità che devono essere svolte da questa unità:

- Information sharing: inteso come la possibilità di condividere informazioni ed esperienze relative ad attacchi o più in generale vulnerabilità informatiche con entità equivalenti che operano sul territorio nazionale o in ambito internazionale;
- Early Warning: inteso come capacità di avvisare tempestivamente i responsabili delle infrastrutture informatiche, sulla presenza di nuove vulnerabilità e nuovi pericoli;

- Rilevamento e gestione delle intrusioni: l'unità deve intervenire direttamente a risolvere situazioni di incidente informatico in tutte quelle pubbliche amministrazioni che non dispongono di una propria struttura per lo svolgimento di questa funzione, o può operare in supporto ad altre strutture equivalenti nella soluzione di intrusioni informatiche;
- Distribuzione di informazioni per la prevenzione degli incidenti informatici;
- Raccolta ed elaborazione delle informazioni relative agli incidenti informatici.

Per svolgere queste funzioni l'unità si avvale di un Computer Emergency Response Team che opera a livello di pubblica amministrazione e che al fine di evitare equivoci potrà denominarsi GOVCERT.IT. Al fine di acquisire una reale efficacia è importante che il GOVCERT.IT operi in stretta collaborazione con le entità che si indicano in Figura 2.

Figura 2: Struttura dell'Unità per la gestione degli attacchi informatici



Di seguito si descrivono queste entità ed il ruolo che le stesse svolgono nell'ambito dell'unità di gestione degli attacchi informatici.

2.1.5.1 GOVCERT.IT

Si tratta dell'organismo su cui è impernata l'intera Unità. Lo scopo principale di GOVCERT.IT deve essere quello di gestire gli attacchi IT non solo a livello dell'Amministrazione centrale, ma, eventualmente e in conformità con adeguati accordi, anche a livello di Amministrazioni locali. Non solo attraverso il monitoraggio attivo il GOVCERT.IT sarà in grado di intercettare preventivamente i tentativi di intrusione e quindi ridurre drasticamente l'impatto degli stessi. Il GOVCERT.IT deve diventare, per tutta la P.A., il punto di riferimento per quanto riguarda le informazioni che riguardano gli attacchi informatici: tecniche di intrusione, vulnerabilità, minacce e patch. Il team deve svolgere i seguenti compiti:

- ricevere i reports degli attacchi;
- distribuire alarms e warnings in relazione ad attacchi informatici;

- mantenere le statistiche sugli attacchi informatici;
- dare supporto e informazioni riguardo a contromisure per prevenire gli attacchi informatici;
- fornire informazioni su rischi, vulnerabilità e minacce;
- svolgere su richiesta e previo nulla osta del Centro di coordinamento, attività di penetration testing sui sistemi dell'Amministrazione;
- fornire supporto alle P.A. qualora le stesse siano oggetto di un attacco informatico ovvero un virus. Tale supporto si esplica nel fornire indicazioni alle persone che presidiano i sistemi informatici delle suddette P.A. sulle azioni più appropriate da eseguire per ridurre gli effetti dell'intrusione e quelle da intraprendere per ripristinare i sistemi compromessi dall'attacco;
- diffondere le informazioni di sicurezza preventiva inerenti i sistemi in possesso delle P.A.;
- cooperare con organi nazionali e internazionali nella prevenzione delle intrusioni informatiche;
- cooperare con le forze dell'ordine nella prevenzione e gestione delle intrusioni informatiche;
- stimolare la nascita di organismi equivalenti in ambito pubblico e privato;
- monitorare la rete della P.A. centrale al fine di intercettare eventuali attacchi informatici (7 x24);
- promuovere l'effettuazione di esercitazioni.

È estremamente importante che GOVCERT.IT sia formato da personale altamente qualificato che gli consenta di guadagnare credibilità e reputazione nell'ambito della comunità Internet e di conseguenza quella visibilità che è necessaria per poter consentire ad un CERT di operare con il massimo rendimento.

Nel nostro continente in particolare i Governi di Francia, Germania, Inghilterra, Olanda, Svezia e Finlandia hanno già provveduto a costituire un CERT per la Pubblica Amministrazione centrale.

La collocazione operativa dell'Unità è presso il CNIPA, al fine di avvalersi delle capacità tecniche ivi residenti. È prevedibile un impegno di circa 15 persone. Sono anche da prevedere eventuali servizi erogati da fornitori esterni opportunamente selezionati. Si può stimare come previsione dei costi per un biennio di attività la cifra di 2,5 mln di euro.

2.1.5.2 Altri CERT della PA

Come già anticipato è necessario prevedere che alcune Pubbliche Amministrazioni decidano di costituire in propria autonomia l'Unità di risposta alle intrusioni informatiche. Ad oggi, ad esempio risulta che il Ministero della Difesa abbia già da tempo attivato, nell'ambito dello Stato Maggiore della Difesa, un CERT denominato CERT.DIFESA.IT, che opera su tutti gli Enti di competenza del Ministero della Difesa. Sicuramente altre amministrazioni vorranno seguire l'esempio del Ministero della Difesa mentre altre decideranno di affidarsi al GOVCERT.IT.

Nell'ambito del Piano Nazionale della sicurezza informatica è però fondamentale che siano stabiliti degli stretti contatti tra questi organismi e che sia creato uno spirito di collaborazione e scambio di informazione. In particolare sarà necessario prevedere momenti di incontro periodici per lo scambio di informazioni, iniziative comuni quali la

predisposizione di alert, linee guida ecc. ecc. È importante che tutti gli altri CERT della P.A. possano avvalersi delle risorse messe a disposizione da GOVCERT.IT per la soluzione dei problemi più incombenti.

2.1.5.3 Altri CERT o organi equivalenti

Attualmente esistono più di 120 CERT al mondo, di cui 79 in Europa. Questi CERT si sono federati al fine di facilitare lo scambio di informazioni e l'aiuto reciproco, in due grosse organizzazioni il FIRST (Forum of Incident Response and Security Teams), che opera a livello mondiale e il TF-CSIRT (Task Force- Computer Security Incident Response Team) una task force costituita presso la Trans-European Academic Network (TERENA), che accorpa la stragrande maggioranza dei CERT Europei. È estremamente importante che GOVCERT.IT aderisca e partecipi attivamente a queste istituzioni al fine di allargare sempre più il proprio bagaglio di conoscenze ed esperienze. Ovviamente stretti rapporti dovranno anche essere allacciati con i due CERT che attualmente operano a livello nazionale: il CERT-IT e il GARR-CERT.

2.1.5.4 Unità Locali (o Operative)

Si è già parlato delle unità locali nel paragrafo 2.1.3.3. e si è sottolineato che queste unità devono possedere anche competenze tecniche. Le unità locali con l'ausilio del GOVCERT.IT forniscono supporto alle proprie amministrazioni e le aiutano a risolvere situazioni critiche, provvedendo anche a mantenerle aggiornate sui problemi di sicurezza informatica. Le unità locali possono essere coinvolte nella preparazione e diffusione di programmi di formazione per il personale tecnico delle amministrazioni e di sessioni di divulgazione per gli utenti finali. Nel caso in cui un'unità locale non riuscisse a risolvere un problema posto da un'amministrazione farà riferimento al GOVCERT.IT o al CNSI.

2.1.5.5 Internet Service Provider

Gli ISP sono una componente importante dell'intera organizzazione e sono attualmente gli unici organismi in grado di raggiungere ogni utente Internet, in particolare ogni Pubblica Amministrazione, e consentire attività di monitoraggio attivo. Essi possono facilmente raggiungere ogni utente ad essi connesso per inviargli messaggi informativi o di allerta, oppure possono ricevere segnalazioni dagli stessi da trasmettere agli organi competenti della struttura. Gli ISP sono anche i punti dove è possibile inserire sistemi di monitoraggio di una serie di parametri quantitativi del traffico di rete che consentono di intercettare sul nascere eventi anomali. Un ISP che riceve la notifica di un'intrusione o un tentativo di intrusione può risolvere il caso, se possiede le necessarie competenze, oppure rivolgersi all'unità operativa del CNSI.

2.1.5.6 Produttori

Con il termine "Produttori" ci si riferisce a tutti gli operatori che realizzano prodotti software, in particolare sistemi operativi e prodotti di sicurezza, con particolare riferimento ai produttori di antivirus. È estremamente importante avere dei contatti diretti con queste aziende poiché tipicamente sono proprio i sistemi operativi o più in generale i prodotti software che contengono dei buchi di sicurezza, e quindi quando queste debolezze sono rilevate è necessario rifarsi immediatamente al relativo costruttore perché lo stesso individui le patch correttive da applicare. Nel caso di virus è invece molto importante potersi rifare ai costruttori di antivirus perché preparino nel minor tempo possibile il relativo antidoto.

2.1.5.7 Centri di Ricerca

Per la soluzione di particolari problemi o casi di intrusione il centro di coordinamento deve potersi avvalere dell'apporto di uno o più centri di ricerca specializzati nei diversi settori della sicurezza informatica. Il principale scopo di questi centri di ricerca è quello di creare, attraverso attività di ricerca, il corpo di conoscenze e di skill necessari per risolvere casi particolarmente complessi, prevedere nuove forme di attacco informatico e virus.

2.1.5.8 La gestione degli Incidenti

Dopo aver descritto le principali componenti e le relative attività degli organismi che compongono l'unità di gestione degli attacchi informatici del CNSI se ne delineano qui le modalità operative nella gestione di un incidente, ferme restando le altre funzionalità.

La gestione di un incidente avviene solitamente attraverso le seguenti fasi:

- l'unità operativa dell'Amministrazione che subisce l'intrusione contatta il GOVCERT.IT via email o web server segnalando l'intrusione e gli effetti da questa provocati; nel caso in cui per l'Amministrazione in questione sia stato attivato un servizio di monitoraggio attivo sarà il GOVCERT.IT che attiverà automaticamente la procedura di gestione degli incidenti avvertendo l'unità operativa di riferimento;
- ricevuta la segnalazione il CERT provvede a registrare l'incidente e a studiare le caratteristiche dell'attacco; individuate le quali si può risalire alle cause che hanno consentito l'attacco e quindi alla loro rimozione; in questa fase il GOVCERT.IT può avvalersi della sua rete di collaborazioni; in prima istanza può interpellare la comunità dei CERT ed il proprio centro di ricerca;
- se ci si trova di fronte ad una nuova forma di virus o di attacco informatico si allerta attraverso i propri canali di comunicazione (in particolare gli ISP) l'intera comunità Internazionale e si attivano i costruttori di antivirus o i produttori del prodotto compromesso per individuare delle patch risolutive o l'antivirus;
- si contatta poi il provider dal cui dominio proveniva l'intrusione per tentare di raccogliere informazioni sul possibile intrusore e contemporaneamente si coinvolgono le forze dell'ordine; nel caso in cui l'intrusione provenga dall'estero si contatta il CERT di riferimento;
- individuate le contromisure, si ricontatta l'unità operativa del sito colpito e gli si forniscono le informazioni necessarie per ripristinare la situazione rimuovendo le cause che hanno consentito l'intrusione;
- l'incidente viene chiuso.

Per molte delle suddette comunicazioni è ovviamente opportuno disporre di un canale di comunicazione cifrato, ma questi dettagli sono al di fuori della portata di questo documento.

Con questo modo di procedere si raggiungono almeno tre scopi:

- chi riporta l'incidente riceve l'assistenza necessaria per risolvere i propri problemi;
- in caso di nuove forme di attacco è possibile allertare in tempo debito la comunità internazionale;
- i dati raccolti possono essere utilizzati per scopi statistici e fornire informazioni essenziali per l'identificazione di attacchi contro il paese e i suoi interessi nazionali.

2.1.5.9 Early Warning e Information Sharing

Per sistema di Early Warning si intende una struttura che sia in grado di diffondere capillarmente e in tempo utile informazioni il più possibile accurate su nuove minacce o precauzioni da prendere per proteggere i propri sistemi informatici da nuove forme di attacco. Tutta la comunità internazionale è protesa alla realizzazione di sistemi di early warning che sono ritenuti uno strumento estremamente importante per ridurre drasticamente gli effetti di un'intrusione informatica. Le informazioni che devono essere distribuite sono disponibili da diverse fonti ma generalmente in forma non direttamente accessibile ad un utente medio.

Queste informazioni sono:

- Warning e Alert: sono documenti che descrivono imminenti minacce o vulnerabilità di sistemi informatici; sono rilasciati dalle più svariate fonti e nelle più svariate modalità.
- Servizi di helpdesk: necessari per supportare gli utenti nella comprensione dei documenti sopra menzionati o per ripristinare il sistema in caso di incidente informatico.

Come già detto queste informazioni sono in gran parte disponibili sulla rete; non tutti gli attori però ne vengono in possesso nello stesso istante. Per rendere il processo di diffusione di queste informazioni il più rapido possibile è quindi necessario prevedere delle forme di condivisione delle informazioni (Information Sharing) tra tutti gli Enti che possono accedere ad esse. In una prima fase è necessario definire delle iniziative di Information Sharing a livello nazionale e in un secondo tempo estendere le stesse a livello internazionale. Per la realizzazione di tali iniziative è consigliabile ispirarsi alle diverse iniziative in vari stati.

Le più significative sono:

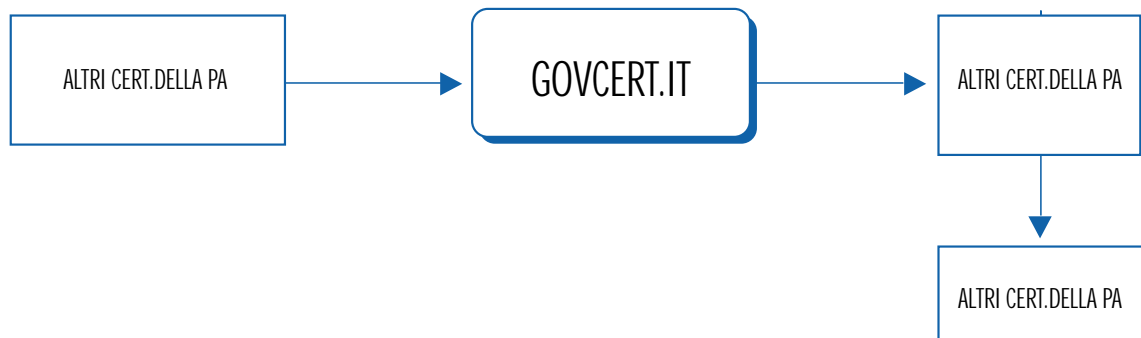
- la comunità dei CERT/CSIRT svolge questa attività da lungo tempo, le informazioni diffuse in questo caso però oltre a non essere sufficientemente tempestive, sono molto specialistiche e quindi dirette solo agli addetti ai lavori;
- negli USA sotto la spinta governativa sono stati avviati gli ISAC, già precedentemente descritti. Attualmente sono in corso negli USA iniziative per consentire lo scambio di informazioni tra i diversi ISAC ed è allo studio la realizzazione di una rete per collegare tra loro CERT, ISAC e centri di studio e ricerca, questa rete è stata per ora denominata Cyber Warning & Information Network (CWIN);
- in UK l'istituzione governativa NISCC (National Infrastructure Security Coordination Centre) fornisce informazioni sulla sicurezza informatica a tutti le istituzioni governative e attraverso il sito web a tutti i cittadini;
- simili attività sono svolte in Francia dal CERT-A, nei Paesi Bassi dal CERRT-RO, in Germania dal CERT-BUND e in Finlandia dal CERT-FI.

Tutte queste iniziative sottolineano l'importanza dell'argomento e riteniamo che lo stesso debba essere affrontato anche nel nostro paese. In particolare il CNSI dovrebbe farsi promotore per la costruzione di una simile struttura che dovrebbe essere costruita intorno al GOVCERT.IT. Come già anticipato una simile struttura deve essere basata su una fitta rete di comunicazione con tutti gli attori che operano su Internet al fine di consentire:

- un'intercettazione immediata delle informazioni dal momento del loro rilascio;
- una diffusione capillare della stessa.

È quindi fondamentale che nell'ambito di questa struttura il CNSI stringa accordi di partnership con tutte le entità che sono in grado di fornire informazioni utili allo scopo. È inoltre auspicabile che anche in ambito privato si provveda alla costituzione di strutture che facilitino lo scambio di informazioni tra le varie realtà e con le quali sarebbe più facile stipulare accordi. In prospettiva la struttura di early warning del CNSI potrebbe essere la seguente:

Figura 3: Struttura del sistema di Early Warning del CNSI



2.1.6 L'Unità di formazione

Un'adeguata gestione della sicurezza ICT all'interno della P.A. non può prescindere dalla necessità che tutti i soggetti coinvolti in tale gestione siano in grado di svolgere con la sensibilità e la competenza richieste i compiti associati al ruolo che ricoprono (per quanto riguarda l'affidabilità, che è ovviamente altrettanto importante, sono state svolte varie considerazioni nel paragrafo relativo alla gestione del personale).

Ciò vale ad esempio per i dirigenti, che devono possedere un'adeguata sensibilità per le problematiche di sicurezza ed essere consapevoli dei danni, spesso cospicui, che possono derivare dalla mancata protezione del patrimonio informativo trattato dai sistemi ICT dell'Amministrazione. In assenza di tale sensibilità e consapevolezza, infatti, con l'attuale crescita dei fenomeni di cybercrime, si dovrebbero più attentamente rilasciare le autorizzazioni, da parte delle Direzioni, per gli investimenti nel campo della sicurezza.

Discorso analogo può farsi per i soggetti che ricoprono ruoli di responsabilità nella gestione tecnica della sicurezza ICT (ad esempio il Responsabile della sicurezza ICT, il Responsabile dei sistemi informativi automatizzati ed i suoi assistenti, l'Addetto alle verifiche di sicurezza ICT ed i suoi assistenti): tali soggetti, infatti, devono mantenere costantemente aggiornate conoscenze tecniche altamente specialistiche al fine di consentire la prevenzione degli incidenti di sicurezza o almeno la minimizzazione dei relativi danni. La carrellata sui soggetti per i quali è richiesta un'adeguata sensibilizzazione e formazione non sarebbe completa se non si considerassero gli utenti finali dei sistemi ICT dell'Amministrazione, per i quali è estremamente importante il possesso di conoscenze che garantiscano la corretta utilizzazione dei servizi di sicurezza disponibili sui sistemi ICT utilizzati (ad esempio scelta idonea delle password e oculata gestione delle stesse, collaborazione nell'aggiornamento del sw, nella misura stabilita dal Responsabile dei sistemi informativi automatizzati, ecc.) e la padronanza delle norme e procedure di sicurezza.

za riferibili agli utenti (ad esempio sollecita segnalazione di anomalie ai responsabili della gestione tecnica della sicurezza ICT, esecuzione periodica di back-up ove tale servizio non sia disponibile in forma centralizzata, eventuali divieti di stabilire connessioni della rete dell'Amministrazione con l'esterno utilizzando collegamenti modem, ecc.).

Inevitabilmente, nei casi in cui tra il personale di un'Amministrazione non siano presenti soggetti in possesso delle competenze necessarie per qualcuno dei ruoli sopra descritti, non rimane altra scelta che affidarsi inizialmente a risorse esterne (outsourcing). È però del tutto evidente che la P.A. dovrebbe tendere a non delegare ad altri una materia così delicata come la sicurezza ICT e dovrebbe conseguentemente arrivare a disporre di professionalità tali da consentirle di ricoprire con risorse interne i vari ruoli sopra descritti. Ciò potrà realizzarsi solo se la P.A. si doterà permanentemente di un'Unità di formazione nel campo della sicurezza ICT che riesca a raggiungere con corsi, diversificati in base al ruolo ricoperto, il maggior numero possibile di dipendenti della P.A. Sarà anche importante che dopo la prima erogazione dei corsi vengano previsti frequenti aggiornamenti per evitare che le conoscenze trasferite con la prima erogazione diventino rapidamente superate.

Per tale motivo si è deciso di inserire nell'ambito del CNSI un'unità appositamente dedicata alla formazione. I principali obiettivi che questa unità si propone sono:

- creare la necessaria consapevolezza in ordine alle minacce, vulnerabilità e rischi che potenzialmente possono gravare sul patrimonio informativo della P.A.;
- generare la conoscenza di base per comprendere i fabbisogni di sicurezza e relativi accorgimenti di prevenzione/protezione in termini organizzativi, operativi, tecnologici e giuridico-normativi;
- promuovere l'utilizzo di adeguate metodologie e strumenti relativamente alla gestione dei processi fondamentali della sicurezza;
- monitorare e valutare il grado di fruizione dei corsi ed il livello di apprendimento dei partecipanti individuando le azioni di miglioramento;
- istituire l'eventuale attività di "tutoraggio" on-line per supportare approfondimenti su temi specifici.

I compiti e le competenze di questa unità sono:

- predisporre i contenuti dei programmi di formazione;
- predisporre i tempi ed i modi per l'erogazione dei suddetti corsi;
- indirizzare e coordinare i docenti e le attività formative;
- promuovere i contatti con i media al fine di pubblicizzare adeguatamente l'iniziativa formativa sulla sicurezza del patrimonio informativo della P.A.;
- partecipare alle sessioni dei corsi sia come osservatore sia come portatore di competenze e know how;
- valutare l'andamento dei corsi evidenziando eventuali disallineamenti con gli obiettivi definiti, provvedendo ad un pronto reindirizzamento delle attività ed eventualmente dei contenuti dei corsi.

La collocazione operativa dell'Unità è presso l'Istituto Superiore di Comunicazioni (Ministero delle Comunicazioni).

Si può stimare come previsione dei costi per un biennio di attività la cifra di 2,5 mln di euro.

2.2 Ruoli delle singole amministrazioni: le unità locali.

Le unità locali sono di fatto il front-end del CNSI. È attraverso queste unità che le informazioni e le iniziative elaborate dal CNSI sono trasmesse alle singole amministrazioni, e che i problemi di queste ultime, in materia di sicurezza informatica, possono essere portati all'attenzione del CNSI. Per lo svolgimento di queste funzionalità è fondamentale che le singole amministrazioni si dotino di un'adeguata infrastruttura, sinora genericamente indicata come unità locale. Nell'ambito di un'unità locale accanto ai ruoli già definiti nell'allegato 2 della direttiva¹¹ [1] ne vanno aggiunti altri che rendano possibile una capillare attuazione della politica di sicurezza ed un'altrettanto capillare verifica circa l'attuazione stessa.

Prima di descrivere tali ruoli è opportuno precisare che, sebbene sia auspicabile la loro ricopertura da parte di personale della PA, può ritenersi ammissibile il coinvolgimento di risorse esterne (outsourcing) ove non esistano o sia troppo costoso formare le competenze necessarie. Tale giudizio potrebbe però mutare una volta che fosse diventato pienamente operativo l'organismo responsabile della formazione e sensibilizzazione dei dipendenti della P.A. nell'area della sicurezza ICT, che in effetti trova come importante motivazione per la sua costituzione anche il risparmio economico per la P.A. relativamente alle voci di spesa connesse con le esternalizzazioni dei servizi di sicurezza. In ogni caso è comunque estremamente importante che nei casi di outsourcing siano ben definite contrattualmente le responsabilità e gli impegni che il fornitore del servizio deve assumersi, in sintonia con quanto previsto in [4].

Di seguito vengono riportati per comodità alcuni dei ruoli già definiti nell'allegato 2 della direttiva [1] per ogni singola Amministrazione. Più precisamente vengono presi in considerazione quei ruoli per i quali si ritiene necessario integrare i compiti già associati ad essi nella direttiva [1] con ulteriori compiti che tengono conto di quanto previsto nel presente documento. Successivamente verranno invece descritti i ruoli aggiuntivi che si ritiene opportuno introdurre.

Comitato per la Sicurezza ICT

È l'organo cui viene demandata, in base alla direttiva [1] la politica della sicurezza delle infrastrutture tecnologiche e del patrimonio informativo gestito prevalentemente con soluzioni automatizzate. Ne fanno parte a titolo di esempio:

- il responsabile/coordinatore generale per la legge 626
- il responsabile/coordinatore generale per la legge 675
- il responsabile della segreteria NATO/UEO o di analogo articolazione per il segreto di Stato
- il responsabile dei sistemi informativi ex d.lgs. 39/93
- il responsabile della sicurezza ICT (da nominare ove non previsto)
- il responsabile della sicurezza delle infrastrutture e del controllo degli accessi
- il responsabile dell'ufficio legislativo
- il responsabile della programmazione e pianificazione finanziaria

Alla luce di quanto esposto nei precedenti paragrafi, al Comitato per la Sicurezza ICT dovrebbero in particolare essere assegnati i seguenti compiti principali:

¹¹ Per i riferimenti tra parentesi quadre ved. paragrafo 2.3.8

- definire, ove necessario, una politica di sicurezza ICT dell'Amministrazione per gestire in modo specifico la protezione di particolari informazioni/servizi dell'Amministrazione, fornendo indicazioni di maggior dettaglio rispetto a quelle generali contenute nella politica di sicurezza della P.A.; a tal fine dovrà essere applicata una opportuna metodologia di analisi e gestione dei rischi;
- richiedere, se necessario, assistenza al Comitato Tecnico Nazionale per la sicurezza informatica e delle telecomunicazioni nelle Pubbliche Amministrazioni relativamente alla definizione della politica di sicurezza ICT dell'Amministrazione;
- trasmettere al responsabile della sicurezza ICT le indicazioni della politica di sicurezza ICT della P.A. e della eventuale politica di sicurezza ICT dell'Amministrazione ai fini del loro recepimento all'interno dell'Amministrazione;
- nominare l'Addetto alle verifiche di sicurezza ICT, ruolo più avanti definito;
- gestire l'aggiornamento della politica di sicurezza ICT dell'Amministrazione tenendo anche conto delle indicazioni del Responsabile della sicurezza ICT, dell'Addetto alle verifiche di sicurezza ICT, del Responsabile dei sistemi informativi automatizzati e dei Proprietari dei dati e delle applicazioni.

Responsabile della sicurezza ICT

In base alla direttiva [1] è il soggetto cui compete la definizione delle soluzioni tecniche, in attuazione delle direttive impartite direttamente 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'Amministrazione. Tale sviluppo deve essere eseguito partendo dalle indicazioni contenute nella politica di sicurezza della P.A. e nella eventuale politica di sicurezza dell'Amministrazione e si deve avvalere di una metodologia di analisi e gestione dei rischi, come descritto nel seguito. Il Responsabile della sicurezza ICT ha il compito di fornire al Responsabile dei sistemi informativi automatizzati le definizioni relative alle soluzioni tecniche al fine della loro realizzazione e del monitoraggio del loro corretto funzionamento.

Responsabile dei sistemi informativi automatizzati

È il referente istituito dal decreto legislativo 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 automatizzati può nominare suoi Assistenti in numero proporzionato alla complessità dei servizi informatici gestiti dall'amministrazione.

Gestore esterno

È il fornitore di servizi che opera sotto il controllo del responsabile dei sistemi informativi. Fintanto che non sarà completata l'attuazione di un adeguato piano di formazione e sensibilizzazione del personale della P.A. in tema di sicurezza ICT attraverso l'istituzione dell'apposito organismo i soggetti che ricopriranno questo ruolo potranno anche svolgere servizi critici dal punto di vista della sicurezza (ad esempio quelli connessi con i ruoli, successivamente descritti, di Assistente del Responsabile dei sistemi informativi automatizzati nel campo della sicurezza ICT). In tali casi è estremamente importante che l'Amministrazione 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.

Proprietario dei dati e delle applicazioni

È ciascun direttore generale per la sfera di informazioni di diretta competenza o trattamento. Ai fini di una corretta gestione della sicurezza ICT è necessario che i Proprietari dei dati e delle applicazioni interagiscano strettamente con il Comitato per la Sicurezza ICT sia in una fase iniziale, ai fini dell'eventuale predisposizione di una politica di sicurezza ICT dell'Amministrazione, sia successivamente, per garantire un tempestivo aggiornamento della politica stessa reso necessario da significative variazioni relative ai dati e alle applicazioni gestite.

Gli ulteriori ruoli, non esplicitamente definiti nella direttiva [1], che si ritiene necessario considerare sono descritti nel seguito.

Assistente del Responsabile dei sistemi informativi automatizzati nel campo della sicurezza ICT

A tale importante ruolo compete principalmente il compito di provvedere alla prima installazione e configurazione delle misure di sicurezza sui sistemi ICT dell'amministrazione e al costante aggiornamento hw/sw di tali sistemi al fine di eliminare o ridurre tempestivamente le vulnerabilità note che per tali sistemi vengono scoperte. I soggetti che ricoprono questo ruolo potranno ricevere indicazioni circa l'aggiornamento dei sistemi ICT dal Responsabile della sicurezza ICT, dal Responsabile dei sistemi informativi automatizzati e direttamente dall'organismo GOVCERT.IT, una volta che sia stato istituito e che risulti operativo.

Addetto alle verifiche di sicurezza ICT

Secondo quanto specificato nella direttiva [1], 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'Amministrazione 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'Amministrazione ad eventuali attacchi. In base al principio della separazione dei compiti enunciato nella direttiva [1], 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 (Assistente del Responsabile dei sistemi informativi automatizzati nel campo 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'amministrazione.

Assistente dell'Addetto alle verifiche di sicurezza ICT

A tale importante ruolo compete principalmente il compito di eseguire sui sistemi ICT dell'Amministrazione il piano di auditing sviluppato dall'Addetto alle verifiche di sicurezza ICT.

2.3 Il “processo della sicurezza ICT” nella PA

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 in un documento noto come politica di sicurezza¹². 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 (nel caso in esame la P.A.), 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 desidera siano soddisfatte da tutti i sistemi ICT dell'organizzazione;
- a livello di singole componenti, nel caso di un'organizzazione molto complessa (come la PA), può essere conveniente sviluppare ulteriori politiche di sicurezza valide per una singola Amministrazione o per parti di essa. 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 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.

Di seguito sono riportate alcune indicazioni in merito ai processi, che nell'ambito della P.A. devono essere coinvolti dal processo di sicurezza, e un primo insieme di prescrizioni, le più rilevanti ad un elevato livello di generalità, che si ritiene debbano essere inserite nella politica di sicurezza di una Amministrazione al fine di garantire una efficace protezione del patrimonio informativo da essa gestito. Ovviamente tale elenco non è da ritenersi esaustivo ma vuole semplicemente essere una base comune di riferimento per tutte le amministrazioni. In particolare si ritiene che la maggior parte delle indicazioni contenute in questa sezione debba essere considerata nella stesura di un documento di politica di primo livello cioè il cui dominio di applicazione è l'intera Pubblica Amministrazione. A tale proposito si rammenta che per P.A. si intendono i destinatari della direttiva [1] e quindi:

¹² Per politica di sicurezza si intende l'insieme delle leggi, regole e pratiche (di tipo tecnico, o di tipo procedurale o attinenti alla sicurezza fisica e del personale) che regolano la gestione e protezione dei beni (principalmente le informazioni) all'interno del dominio di validità della politica stessa.

- le Amministrazioni dello Stato
- le aziende ed Amministrazioni autonome dello Stato
- gli Enti pubblici non economici nazionali.

Nel seguito del presente documento, per semplicità espositiva si è scelto di indicare con il termine generico “Amministrazione” un’organizzazione pubblica che sia di uno dei tipi sopra elencati.

2.3.1 Adozione di una metodologia di analisi del rischio

Ogni Amministrazione che intenda provvedere allo sviluppo di adeguate politiche di sicurezza dovrà necessariamente rifarsi ad una metodologia di analisi del rischio inteso come quel processo necessario per identificare i rischi di sicurezza e determinarne la loro portata. In altri termini l’analisi del rischio è quel processo che definisce le esigenze di sicurezza ICT di un’organizzazione e concorda su quali siano le più appropriate misure di controllo.

A tal fine ogni Amministrazione potrà avvalersi di una metodologia di analisi e gestione dei rischi che segua l’approccio descritto in [1]. Tale approccio si basa sulla considerazione che un’analisi accurata di tutti i sistemi ICT richiederebbe tempi e costi molto elevati che spesso non risulterebbero giustificati dall’entità dei rischi associati ai sistemi stessi. Conseguentemente l’approccio prevede che su tutti i sistemi ICT (o classi di essi) venga preliminarmente eseguita un’analisi dei rischi ad alto livello che consenta di stimare approssimativamente il livello di rischio. Successivamente si procede nel modo seguente:

- 1) per tutti i sistemi ICT che l’analisi preliminare ha riconosciuto “a basso rischio” viene adottata una protezione di base tra quelle comunemente riconosciute valide per la tipologia dei sistemi stessi (si veda a tal proposito il paragrafo denominato “Adozione di standard per la sicurezza”)
- 2) per tutti i sistemi ICT ad elevata criticità viene eseguita un’analisi dei rischi accurata basata su metodologie strutturate (un esempio di tale metodologia è fornito in [3], e nella seconda parte di questo documento sono riportate delle linee guida per l’individuazione di una corretta metodologia di analisi dei rischi).

2.3.2 Adozione di un piano di Business Continuity

Naturalmente tutti gli sforzi devono essere compiuti affinché gli incidenti informatici non abbiano a verificarsi, adottando le opportune contromisure sia 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 sviluppato per l’intera P.A. un piano di Business Continuity. 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. Nella seconda parte di questo documento sono riportate delle linee guida su come debba essere affrontato questo problema nell’ambito della Pubblica Amministrazione.

2.3.3 Stesura di capitolati per l'acquisizione di sistemi/prodotti ICT dotati di funzionalità di sicurezza

Una volta selezionate, con l'ausilio di una metodologia di analisi e gestione dei rischi, le funzionalità di sicurezza di cui deve essere dotato un sistema/prodotto ICT di cui necessita la P.A. diventa molto importante formularne le specifiche in modo accurato e non soggetto a molteplici interpretazioni da parte dei fornitori. A tal fine il riferimento a precise specifiche tecniche quali gli standard effettivi o de facto costituisce la soluzione più consigliabile. A tal proposito ricordiamo che per quanto riguarda l'individuazione di funzionalità di sicurezza idonee a contrastare le minacce ipotizzabili per il sistema valide indicazioni possono essere trovate in [8] e, soprattutto, in [12]. A tal riguardo si può fare ad esempio riferimento al paragrafo 2.5 che riporta i meccanismi di sicurezza che sono stati oggetto di standardizzazione da parte di ISO/IEC/JTC1/SC27. Qualora si sia interessati a contrastare minacce tipiche per una prefissata tipologia di prodotto, un ausilio particolarmente valido è costituito dai cosiddetti Protection Profile, sviluppati utilizzando lo standard ISO/IEC IS 15408 (Common Criteria) per la valutazione della sicurezza di sistemi e prodotti ICT.

2.3.4 Gestione del personale

Il personale addetto all'utilizzo dei sistemi ICT che tratta informazioni e applicazioni rilevanti dal punto di vista della sicurezza ICT e, soprattutto, il personale che ricopre i ruoli di gestione della sicurezza ICT sopra descritti deve essere attentamente selezionato sulla base di criteri di affidabilità e competenza, in modo da rendere il più possibile basso il rischio che tale personale possa compiere, intenzionalmente o accidentalmente, azioni che compromettano la protezione delle informazioni e applicazioni dell'Amministrazione. È anche necessario che il personale suddetto sia messo in condizione di svolgere al meglio i suoi compiti, dotandolo delle risorse e del supporto necessari e consentendogli la fruizione di un adeguato piano di formazione e sensibilizzazione nell'area della sicurezza ICT. Inoltre dovrà essere garantita un'alta motivazione del personale, preferibilmente istituendo ruoli specifici per la sicurezza ICT che prevedano un trattamento adeguato alle responsabilità assunte. Queste ultime, d'altro canto, dovranno essere ben esplicitate e formalizzate negli incarichi conferiti, così come previsto in [3], [4], [5] e [6].

2.3.5 Sicurezza nell'accesso di terze parti ai sistemi ICT della P.A.

È evidente che non avrebbe senso gestire adeguatamente il personale della P.A. che utilizza i sistemi ICT se non ci si preoccupasse anche dell'accesso ai sistemi stessi che la P.A. deve consentire a soggetti esterni per offrire alcuni servizi. In parte il tema è stato già trattato nell'ambito delle considerazioni svolte relativamente al ruolo "Gestore esterno" previsto nella direttiva [1]. Considerazioni del tutto analoghe possono essere qui ripetute, conformemente a quanto previsto in [3] e [4], per qualsiasi accesso di terze parti ai sistemi ICT della P.A.. Ad esempio per gli accessi che, diversamente da quelli del Gestore esterno, sono necessari per la fornitura di un servizio da parte della P.A. piuttosto che da parte del soggetto esterno. Occorrerà infatti, soprattutto nei casi in cui sia inevitabile concedere privilegi di accesso particolarmente elevati, far assumere formalmente alla terza parte impegni e responsabilità che la obblighino a comportamenti corretti sotto il profilo della sicurezza ICT. In tali casi, inoltre, la massima attenzione dovrà essere posta nell'equipaggiare i sistemi ICT della P.A. con funzionalità di sicurezza (controllo d'accesso, monitoraggio delle azioni degli utenti, ecc.) che offrano le più ampie garanzie.

2.3.6 Outsourcing

Come già evidenziato precedentemente è facile che nel settore della sicurezza ICT, a causa di carenza di competenze interne, un'Amministrazione sia costretta ad affidare la gestione della propria sicurezza ICT a risorse esterne (outsourcing). In questi casi va ribadita la necessità di un controllo molto rigoroso da parte dell'Ente committente e l'esplicita richiesta di particolari requisiti da parte del fornitore del servizio, in specie per quanto riguarda la serietà delle garanzie offerte, con particolare riguardo all'affidabilità e professionalità del personale incaricato.

Va comunque fatto salvo il principio che la "cabina di regia" in tema di sicurezza informatica resti saldamente nelle mani dell'Amministrazione.

2.3.7 Il ricorso alle certificazioni di sicurezza nella PA

Definiamo in questa sezione una serie di indicazioni che è opportuno seguire relativamente all'uso delle certificazioni di sicurezza nell'ambito di una Pubblica Amministrazione.

2.3.7.1 Le certificazioni della sicurezza ICT

I due principali tipi di certificazione della sicurezza ICT oggi utilizzati sono stati entrambi oggetto di standardizzazione ISO/IEC, sebbene per uno dei due, come vedremo, il relativo processo non si può considerare completo. Più precisamente nel 1999 è stata adottata in tutte le sue tre parti dall'ISO/IEC la raccolta di criteri denominata Common Criteria che consente la valutazione e certificazione della sicurezza di prodotti e sistemi ICT. Tale adozione si è formalmente realizzata attraverso l'emanazione dello standard ISO/IEC IS 15408. L'anno successivo, questo stesso organismo internazionale ha fatto propria solo la prima parte di un altro standard di certificazione della sicurezza ICT che è stato sviluppato in Gran Bretagna, il ben noto BS7799 che nella versione ISO/IEC ha assunto la denominazione IS 17799-1.

La seconda parte dello standard, quella che contiene le indicazioni più precise ai fini della certificazione, è invece al momento disponibile solo come standard della British Standards Institution. Lo standard ISO/IEC IS 15408 (Common Criteria) e la coppia di standard ISO/IEC IS 17799-1 e BS7799-2, sebbene abbiano in comune la sicurezza ICT, hanno lo scopo di certificare cose ben diverse. Nel caso dei Common Criteria (in seguito denominati brevemente CC), infatti, oggetto della certificazione è, come già anticipato, un sistema o un prodotto ICT¹³, nel caso invece del BS7799 ciò che viene certificato è il processo utilizzato da un'organizzazione, sia essa una società privata o una struttura pubblica, per gestire al suo interno la sicurezza ICT (tale processo, come è noto, viene indicato nello standard con l'acronimo ISMS che sta per "Information Security Management System"). In altri termini, la certificazione BS7799 può essere considerata una certificazione aziendale, del tipo quindi della ben nota certificazione ISO 9000, ma specializzata nel campo della sicurezza ICT¹⁴.

¹³ Un sistema ICT, secondo la terminologia utilizzata nei CC, è un'installazione informatica utilizzata per scopi ben specificati e in un ambiente operativo completamente definito. Un prodotto ICT, invece, è un dispositivo hardware o un pacchetto software progettato per l'uso e l'installazione in una grande varietà di sistemi.

¹⁴ La precisazione circa l'oggetto della certificazione è opportuna poiché, alcune caratteristiche dello standard britannico BS7799-2 potrebbero generare confusione e far ritenere che la relativa certificazione possa rendere quasi superflua la certificazione Common Criteria. Infatti, tra i requisiti che un'organizzazione deve soddisfare per poter ottenere una certificazione BS7799, ve ne sono anche alcuni che rappresentano requisiti funzionali per i sistemi/prodotti ICT dell'organizzazione. Ai fini della certificazione BS7799, tuttavia, è sufficiente verificare che i suddetti requisiti funzionali siano stati selezionati sulla base di una corretta analisi e gestione dei rischi e verificare a campionamento che le corrispondenti funzioni di sicurezza siano presenti sui sistemi ICT ove risultano necessarie. (Segue)

2.3.7.2 I servizi di certificazione in Italia

Le valutazioni e certificazioni della sicurezza di sistemi/prodotti ICT sono state effettuate in Italia a partire dal 1995 limitatamente al settore della sicurezza nazionale. Più precisamente, fino alla primavera del 2002 sono stati obbligatoriamente sottoposti a certificazione secondo i criteri europei ITSEC tutti i sistemi/prodotti ICT utilizzati in ambito militare per trattare informazioni classificate concernenti la sicurezza interna ed esterna dello stato. Con il DPCM dell'11 aprile 2002, pubblicato sulla Gazzetta Ufficiale n. 131 del 6 giugno 2002, è stata resa obbligatoria la certificazione anche per i sistemi/prodotti ICT che trattano informazioni classificate al di fuori del contesto militare e si è prevista la possibilità di utilizzare i CC in alternativa ai criteri ITSEC. La struttura utilizzata per le suddette valutazioni e certificazioni include un Organismo di certificazione, le cui funzioni sono svolte dall'Autorità Nazionale per la Sicurezza – Ufficio Centrale per la Sicurezza (ANS-UCSi), e da un certo numero di Centri di Valutazione (Ce.Va.). Attualmente sono accreditati quattro Ce.Va., uno solo dei quali appartenente alla P.A., ossia quello gestito dall'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero delle Comunicazioni (ISCTI).

Recentemente è stato istituito un nuovo Schema Nazionale utilizzabile per valutare e certificare, secondo i CC o i criteri ITSEC, i sistemi/prodotti ICT che non trattino informazioni classificate. In tale Schema è previsto che il ruolo di Organismo di certificazione sia svolto dall'ISCTI.

Per quanto riguarda invece le certificazioni di sicurezza relative allo standard BS7799 due organismi sono stati accreditati in Italia dal Sincert per operare in accordo alla parte due dello standard britannico, la quale come già detto, non è stata fino ad oggi recepita dall'organismo internazionale ISO/IEC.

2.3.7.3 Indicazioni relative all'utilizzo delle certificazioni nell'ambito della P.A.

Per quanto riguarda la coppia di standard ISO/IEC IS 17799-1 e BS7799-2, i principi ispiratori sono stati già recepiti negli allegati 1 e 2 della direttiva [1]. Tuttavia alcune delle verifiche previste negli standard sono state affidate alle singole Amministrazioni, mentre ovviamente in una certificazione sono svolte da un organismo accreditato. Tale scelta iniziale ha evidentemente il limite di non garantire che chi esegue le verifiche abbia tutte le competenze allo scopo necessarie e che il principio di separazione dei compiti di realizzazione e di verifica della sicurezza indicato nella direttiva [1] sia soddisfatto. Sulla base delle informazioni derivabili dal questionario di autovalutazione descritto nell'allegato 1 della direttiva [1], nonché di ulteriori informazioni disponibili sulle singole Amministrazioni, il Comitato potrà raccomandare, nei casi in cui risultino situazioni di elevata criticità per le quali si debbano richiedere elevate garanzie circa il processo di gestione della sicurezza ICT, che vengano eseguite vere e proprie certificazioni BS7799-2 in singole Amministrazioni o in parti di esse.

In questi stessi casi potrà essere raccomandato dal Comitato che almeno i sistemi/prodotti ICT che gestiscono le informazioni e le applicazioni che necessitano di una elevata protezione siano sottoposti a certificazione secondo i Common Criteria o i criteri ITSEC.

¹⁴ (Segue da pag. 38) Ai fini di una eventuale certificazione Common Criteria di un sistema/prodotto ICT dell'organizzazione, occorrerebbe invece verificare che le suddette funzionalità non contengano difetti realizzativi e siano in grado di resistere, fino ad una soglia fissata dal grado di severità della valutazione, ad un insieme di minacce specificate in un ambiente ben definito

Questa indicazione può considerarsi in linea con quanto previsto nel documento [14] che presenta come consigliabile l'uso della certificazione di sicurezza:

- 1) per i sistemi che trattano informazioni le quali, sebbene non classificate ai fini della sicurezza nazionale, possono essere considerate critiche o essenziali per lo svolgimento delle funzioni primarie dell'Amministrazione,
 - 2) per i sistemi da cui dipendono l'operatività e/o la manutenzione delle infrastrutture critiche.
- Inoltre nel documento [10] viene affermato che il governo statunitense si propone di verificare, dal punto di vista della fattibilità economica, l'estensione dell'obbligo di certificazione ai sistemi/prodotti ICT utilizzati da tutte le agenzie federali, anche nei casi in cui non trattino informazioni classificate. Il governo statunitense prevede peraltro che, qualora tale estensione possa essere effettuata, essa influenzerebbe molto positivamente il mercato dei prodotti ICT consentendo di godere dei relativi benefici anche al di fuori del contesto governativo.

2.4 Documenti di riferimento

- [1] Direttiva 16 gennaio 2002 del Presidente del Consiglio dei Ministri "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali" (pubblicata sulla G.U. n.69 del 22 marzo 2002).
- [2] Decreto 24 luglio 2002 del Ministro delle comunicazioni e del Ministro per l'innovazione e le tecnologie "Istituzione del Comitato Tecnico Nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni".
- [3] ISO/IEC IS 17799-1 - Information security management - Part 1: Code of practice for information security management - Standard.
- [4] BS7799-2 - Information security management systems - Specification with guidance for use.
- [5] ISO/IEC TR 13335-1, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 1: Concepts and models of IT security
- [6] ISO/IEC TR 13335-2, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 2: Managing and planning IT security
- [7] ISO/IEC TR 13335-3, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 3: Techniques for the management of IT security
- [8] ISO/IEC TR 13335-4, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 4: Selection of safeguards
- [9] ISO/IEC TR 13335-5, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 5: Management guidance on network security
- [10] The National Strategy to Secure Cyberspace - Documento governativo USA - Febbraio 2003.
- [11] ISO/IEC IS 15408-1 Evaluation Criteria for Information Technology Security - Part 1: Introduction and general model.
- [12] ISO/IEC IS 15408-2 Evaluation Criteria for Information Technology Security - Part 2: Security functional requirements.
- [13] ISO/IEC IS 15408-3 Evaluation Criteria for Information Technology Security - Part 3: Security assurance requirements.
- [14] National Security Telecommunications and Information Systems Security Committee (NSTISSC) - "National Security Telecommunications and Information Systems

Security Policy (NSTISSP) No. 11, Subject: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products” – Documento governativo USA - Gennaio 2000

2.5 Elenco meccanismi di sicurezza standardizzati da ISO/IEC/JTC1/SC27

ISO/IEC FDIS 7064:	(2002), Data processing - Check character systems (2nd edition, revision of ISO 7064: 1983)
ISO 8372: 1987,	Modes of operation for a 64- bit block cipher algorithm
ISO/IEC 9796-2:	(2002), Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms
ISO/IEC 9796-3:	1999, Digital signatures schemes giving message recovery - Part 3: Discrete logarithm based mechanisms
ISO/IEC 9797-1:	1999, Message authentication codes (MACs) - Part 1: Mechanisms using a block cipher
ISO/IEC 9797-2:	(2002), Message authentication codes (MACs) - Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 9798-1:	1997, Entity authentication - Part 1: General (2nd edition)
ISO/IEC 9798-2:	1999, Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms (2nd edition)
ISO/IEC 9798-3:	1998, Entity authentication - Part 3: Mechanisms using digital signature techniques (2nd edition)
ISO/IEC 9798-4:	1999, Entity authentication - Part 4: Mechanisms using a cryptographic check function (2nd edition)
ISO/IEC 9798-5:	1999, Entity authentication - Part 5: Mechanisms using zero knowledge techniques
ISO/IEC 9979:	1999, Procedures for the registration of cryptographic algorithms (2nd edition)
ISO/IEC 10116:	1997, Modes of operation for an n-bit block cipher algorithm (2nd edition, in fase di revisione)
ISO/IEC 10118-1:	2000, Hash-functions - Part 1: General (2nd edition)
ISO/IEC 10118-2:	2000, Hash-functions - Part 2: Hash-functions using an n-bit block cipher algorithm (2nd edition)
ISO/IEC 10118-3:	1998, Hash-functions - Part 3: Dedicated hash-functions
ISO/IEC 10118-4:	1998, Hash-functions - Part 4: Hash-functions using modular arithmetic
ISO/IEC 11770-1:	1996, Key management - Part 1: Framework
ISO/IEC 11770-2:	1996, Key management - Part 2: Mechanisms using symmetric techniques
ISO/IEC 11770-3:	1999, Key management - Part 3: Mechanisms using asymmetric techniques
ISO/IEC 13888-1:	1997, Non-repudiation - Part 1: General (in fase di revisione)
ISO/IEC 13888-2:	1998, Non-repudiation - Part 2: Using symmetric techniques
ISO/IEC 13888-3:	1997, Non-repudiation - Part 3: Using asymmetric techniques
ISO/IEC TR 14516:	2002 (ITU-T X.842), Guidelines on the use and management of Trusted Third Party services (in attesa di pubblicazione)

ISO/IEC 14888-1:	1999, Digital signatures with appendix - Part 1: General
ISO/IEC 14888-2:	1999, Digital signatures with appendix - Part 2: Identity-based mechanisms
ISO/IEC 14888-3:	1999, Digital signatures with appendix - Part 3: Certificate-based mechanisms
ISO/IEC 15816:	2002 (ITU-T X.841), Security information objects for access control
ISO/IEC 15945:	2002 (ITU-T X.843), Specification of TTP services to support the application of digital signatures
ISO/IEC 15946-1:	(2002), Cryptographic techniques based on elliptic curves - Part 1: General (in attesa di pubblicazione)
ISO/IEC 15946-2:	(2002), Cryptographic techniques based on elliptic curves - Part 2: Digital signatures (in attesa di pubblicazione)
ISO/IEC 15946-3:	(2002), Cryptographic techniques based on elliptic curves - Part 3: Key establishment (in attesa di pubblicazione)
ISO/IEC FCD 15946-4:	2002, Cryptographic techniques based on elliptic curves - Part 4: Digital signatures giving message recovery
ISO/IEC TR 15947:	(2002), IT intrusion detection framework (in attesa di pubblicazione)
ISO/IEC 17799:	2000, Code of practice for information security management (in fase di revisione)
ISO/IEC 18014-1:	(2002), Time stamping services - Part 1: Framework (in attesa di pubblicazione);
ISO/IEC FDIS 18014-2:	2002, Time stamping services - Part 2: Mechanisms producing independent tokens
ISO/IEC CD 18014-3:	2002, Time stamping services - Part 3: Mechanisms producing linked tokens
ISO/IEC WD 18028:	2001, Information technology - Security techniques - IT network security
ISO/IEC CD 18031:	2002, Random bit generation
ISO/IEC CD 18032:	2002, Prime number generation
ISO/IEC CD 18033-1:	2002, Encryption algorithms - Part 1: General
ISO/IEC WD 18033-2:	2002, Encryption algorithms - Part 2: Asymmetric ciphers
ISO/IEC CD 18033-3:	2002, Encryption algorithms - Part 3: Block ciphers
ISO/IEC WD 18033-4:	2002, Encryption algorithms - Part 4: Stream ciphers
ISO/IEC WD 18043:	2002, Guidelines for the implementation, operation and management of Intrusion Detection Systems (IDS)
ISO/IEC WD 18044:	2002, Information security incident management
ISO/IEC WD 18045:	2002, Methodology for IT security evaluation



Proposte concernenti le strategie
in materia di sicurezza informatica
e delle telecomunicazioni
per la pubblica amministrazione

Parte seconda

Linee guida per l'attuazione della sicurezza ICT nella PA

3.1 Parte seconda - Linee guida per l'analisi dei rischi

3.1.1 Considerazioni generali

L'analisi 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 e sul posizionamento dell'Amministrazione, risulta impossibile definire un sistema di sicurezza veramente equilibrato e bilanciato rispetto ai rischi ed ai danni/perdite che potrebbero verificarsi.

Nel nuovo sistema di Governo delle P.A. sempre più aperto, cooperante, digitale ed interconnesso, anche a livello internazionale, i confini del rischio non hanno più barriere e le minacce diventano tutte possibili e, in qualche misura, sempre più probabili.

Ciascuna Amministrazione si deve pertanto dotare di un processo continuo di analisi e gestione del rischio conforme agli standard internazionali di sicurezza

L'obiettivo dell'analisi e gestione del rischio è cogliere quali siano i rischi associati agli asset aziendali (individuati, classificati e valorizzati) e concordare quali siano le misure più idonee a ridurre il livello di vulnerabilità a fronte di minacce o a minimizzare l'impatto su violazioni della sicurezza e quindi sul servizio. In sintesi l'Analisi del Rischio è quel processo necessario per identificare i rischi di sicurezza e determinarne la loro ampiezza (compliant BS7799 che è il "Codice professionale per la gestione della sicurezza delle informazioni"). In altri termini l'analisi del rischio è quel processo che definisce le esigenze di sicurezza e concorda su quali siano le più appropriate misure di controllo. 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. L'analisi del rischio è un'attività considerata parte essenziale e propedeutica all'adozione di efficienti sistemi per una sicurezza globale nell'Amministrazione e comprende essenzialmente i seguenti argomenti:

- Identificazione e Valutazione degli Asset (beni) informativi;
- Assessment delle Minacce e delle vulnerabilità;
- Identificazione dell'esistente e Pianificazione dei Controlli di Sicurezza;
- Risk Assessment;
- Identificazione e Selezione dei Controlli di Sicurezza e Riduzione dei Rischi;
- Accettazione del Rischio.

I risultati di un'analisi del rischio possono contribuire in modo determinante ad aumentare la consapevolezza della Direzione (e di conseguenza di tutta la struttura della PA), verso la sicurezza ma soprattutto verso l'adozione di una forma mentale volta al trattamento degli asset in modo "protettivo". Fornisce altresì un meccanismo pratico per comprendere i pericoli della mancanza o utilizzo incompleto o anomalo dei sistemi di protezione e supporta, con dati qualitativi e quantitativi, la valutazione e selezione delle adeguate misure di sicurezza.

L'analisi del rischio è comunque prevista dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali". Si presenta di seguito uno schema di riferimento per indirizzare la stesura, da parte delle Amministrazioni, dei requisiti atti ad identificare e selezionare una metodologia per l'analisi dei rischi adeguata alle esigenze di sicurezza espresse dalla direttiva.

3.1.2 Requisiti di conformità della metodologia

Nella identificazione e selezione di una metodologia di analisi del rischio si dovranno tenere conto delle seguenti caratteristiche di base:

- deve poter valutare oltre al rischio tecnologico, anche il rischio organizzativo, operativo e amministrativo;
- deve poter valutare il rischio di un singolo bene informativo o di un'intera applicazione intesa come unità distinta a supporto di un processo;
- deve essere progettata per essere usata sia per nuove applicazioni in via di sviluppo che per applicazioni esistenti o applicazioni acquisite dal mercato;
- deve essere progettata con l'ottica di supportare l'analisi dei rischi per applicazioni di tutti i tipi e basate su tutte le tecnologie;
- deve supportare coloro che si occupano sia di sicurezza Organizzativa che di sicurezza ICT;
- deve supportare in particolare coloro che hanno la responsabilità di valutare il rischio per l'Amministrazione, della mancanza della fornitura (o di una fornitura alterata), del servizio alla clientela;
- deve essere progettata anche per fornire una guida alla progettazione o selezione di specifiche tecniche di controllo;
- deve essere progettata in conformità degli standard BS7799;
- deve prevedere l'impiego di strumenti automatici e tool per l'analisi generale e per l'analisi specifica del rischio.

3.1.3 Logiche per sviluppare la richiesta di offerta

Sia nel caso che l'Amministrazione decida di svilupparla in casa, sia che scelga di acquisire una metodologia per l'analisi del rischio dall'esterno, occorre che vengano rispettati alcuni requisiti di tipo strutturale e funzionale:

1. un'articolazione in fasi operative, ciascuna finalizzata ad uno o più obiettivi specifici;
2. una serie di attività, per ogni fase, mirate a svolgere le funzioni basilari dell'analisi del rischio.

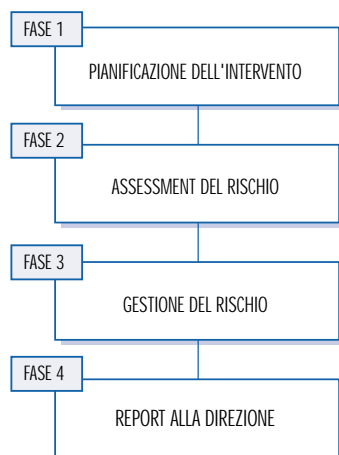
Per guidare l'individuazione di tali requisiti viene fornito uno schema di riferimento (framework) articolato in fasi ed attività.

Framework di riferimento

Qualsiasi metodologia di analisi del rischio dovrebbe prevedere almeno 4 fasi consequenziali e interrelate:

- pianificazione dell'intervento;
- valutazione (assessment) del Rischio;
- gestione del Rischio;
- report alla Direzione.

Ciascuna di queste fasi dovrà poi prevedere lo svolgimento di tutte le attività necessarie per conseguire l'obiettivo di fase. Nelle pagine seguenti vengono quindi evidenziati i requisiti di ciascuna fase in termini di passi e di attività che la metodologia prescelta dovrà contenere.

Requisito di articolazione di una metodologia di analisi del rischio**3.1.3.1 Fase 1 - Pianificazione dell'intervento***Descrizione della Fase*

Deve essere stabilito, all'inizio del processo di pianificazione del singolo intervento di analisi del rischio da parte del responsabile/delegato della sicurezza, il piano di intervento di analisi e le persone coinvolte.

Ciascun piano di intervento dovrà identificare:

- gli asset da analizzare;
- l'unità organizzativa coinvolta;
- i tempi di intervento;
- il responsabile del prodotto/processo/applicazione;
- le risorse da coinvolgere cioè il project leader, e il gruppo di lavoro nell'analisi.

Inoltre il responsabile/delegato alla sicurezza dovrà predisporre e inviare una lettera di incarico a tutti gli attori coinvolti nell'analisi, in cui sono specificati tempi e responsabilità.

Attività specifiche della Fase

Deve essere definito l'obiettivo di questa fase di pianificazione dell'intervento descrivendo:

- lo scopo della fase di pianificazione;
- le finalità degli interventi di valutazione della situazione di rischio;
- la pianificazione dei passi operativi;
- l'identificazione degli "Attori" coinvolti;
- i compiti di ogni risorsa o entità coinvolta;
- la predisposizione del piano vero e proprio.

3.1.3.2 Fase 2 - Assessment del Rischio*Descrizione della Fase*

La fase deve prevedere di identificare il rischio e la sua misura attraverso una valutazione delle minacce e vulnerabilità dell'asset/servizio ed il conseguente impatto sul business.

Dovrà essere previsto di assegnare delle specifiche competenze in termini di “chi fa-che cosa” relativamente a:

- chi decide la tempistica di intervento (pianificata o richiesta specifica);
- chi è responsabile del processo di analisi del rischio;
- chi identifica e definisce l'utilizzo di eventuali strumenti di supporto all'analisi;
- chi effettua l'analisi del rischio “globale” e chi quella settoriale.

Nello sviluppo di questa fase devono venire individuate (e valutate) le contromisure specifiche in essere a protezione del patrimonio informativo e quindi del business.

Attività specifiche della Fase

La fase deve prevedere dei passi procedurali che sviluppino la sequenza dell'assessment e che comunque prevedano almeno la seguente suddivisione:

- un passo che realizzi un assessment circa le minacce esistenti percepite;
- un passo che realizzi un assessment circa le vulnerabilità (incluse le contromisure esistenti);
- un passo che preveda di “individuare” le contromisure già pianificate a protezione del business e di ricalcolare un nuovo indice di vulnerabilità;
- un passo che fornisca il calcolo del rischio relativamente alla situazione esistente ed a quella pianificata, (col calcolo del gap tra i due indici).

In particolare per quanto attiene all'assessment delle minacce dovrà essere possibile:

- individuare e descrivere l'associazione Asset/Minacce;
- valutare le minacce, in particolare riguardo:
 - alla verosimiglianza;
 - alla frequenza;
 - alla probabilità;
 - alla gravità;
- fare in modo che venga calcolato l'indice di minaccia come media ponderata delle perdite per minaccia.

In particolare per quanto attiene all'assessment delle vulnerabilità dovrà essere possibile redigere le regole per:

- identificare le vulnerabilità (mancanza o carenza delle contromisure);
- identificare e descrivere l'associazione scoperto/minacce;
- valutare le vulnerabilità (per ciascuna minaccia) come quota di perdita dell'asset in caso di vulnerabilità attuata;
- prevedere le diverse tipologie di calcolo nel caso venissero utilizzati strumenti automatici di analisi.

In particolare per quanto attiene all'identificazione delle contromisure già pianificate, dovrà essere possibile:

- identificare le contromisure pianificate;
- rielaborare l'assessment di vulnerabilità dopo aver considerato e valutato la presenza delle contromisure in essere (pianificate).

In particolare per quanto attiene al calcolo del rischio, dovrà essere possibile:

- fare in modo che venga calcolato il valore di rischio a contromisure attuali;
- fare in modo che venga calcolato il valore di rischio a contromisure pianificate.

3.1.3.3 Fase 3 - Gestione del Rischio

Descrizione della Fase

Questa fase deve esplicitare il modo per definire il rischio residuo accettabile dalla Direzione, derivante dall'applicazione di contromisure, ciascuna delle quali contribuisce, in modo cost-effective, a ridurre marginalmente il rischio iniziale.

Oltre all'individuazione e attribuzione delle specifiche responsabilità, in questa fase devono venire definite le simulazioni sui margini di riduzione del rischio conseguenti all'applicazione delle contromisure e che devono portare all'individuazione del massimo rischio tollerabile per ciascun asset informativo.

Attività specifiche della Fase

La metodologia deve prevedere dei passi procedurali che sviluppino la sequenza della fase di gestione del rischio e che comunque prevedano almeno la seguente suddivisione:

- l'individuazione e la selezione delle contromisure a fronte delle vulnerabilità identificate;
- l'individuazione e calcolo del rischio residuo, in funzione del portafoglio delle contromisure stabilite dopo la valutazione dell'investimento a copertura del rischio netto e dopo aver classificato le contromisure in relazione al margine di riduzione dei rischi;
- la definizione delle regole utili a determinare l'accettazione del rischio residuo dopo l'applicazione delle contromisure.

In particolare per quanto attiene all'individuazione e selezione delle contromisure, dovrà essere possibile:

- individuare i principi di associazione contromisure a vulnerabilità/minacce;
- definire i modelli e gli algoritmi di simulazione dell'andamento dell'indice di rischio secondo le contromisure implementabili;
- definire i metodi di assegnazione a ciascuna contromisura selezionata, della relativa riduzione del margine di rischio conseguibile e delle caratteristiche di costo/efficacia.

In particolare per quanto attiene al calcolo del rischio residuo dovrà essere possibile :

- definire il calcolo dell'investimento a copertura del rischio netto (rischio calcolato meno MRT);
- identificare il portafoglio di contromisure;
- definire il calcolo del rischio residuo.

In particolare per quanto attiene alla definizione del livello di accettazione del rischio si dovrà poter:

- formalizzare i termini dell'accettazione del rischio residuo;
- individuare e sviluppare le specifiche di fattibilità tecnico/organizzativa delle contromisure.

3.1.3.4 Fase 4 - Report alla Direzione

Descrizione della Fase

Questa fase deve prevedere l'analisi delle informazioni scoperte nella fase precedente, 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.

Attività specifiche della Fase

Questa fase deve prevedere almeno due passi procedurali:

- un primo passo che descriva la preparazione, strutturazione e stesura di un report per la Direzione descrivendo specificatamente la (o le) situazione riscontrata/e e gli obiettivi di rischio/sicurezza definiti;
- il secondo che consista nella formalizzazione degli obiettivi negoziati tra le parti coinvolte.

In particolare per quanto attiene la stesura di un report, la metodologia deve prevedere di:

- descrivere le minacce/vulnerabilità all'asset;
- descrivere il valore della potenziale perdita misurata a fronte dei rischi dell'investimento a protezione;
- descrivere il portafoglio di contromisure;
- descrivere le modalità di accettazione del rischio residuo.

In particolare per quanto attiene alla formalizzazione degli obiettivi condivisi sarà necessario prevedere di:

- programmare gli incontri con la Direzione per illustrare/dibattere la relazione;
- programmare gli atti formali (Firma) per presa di visione della relazione.

3.2 Linee guida per lo sviluppo di un piano di Business Continuity

3.2.1 Premessa

Vengono di seguito fornite le linee guida per l'impostazione di un sistema di Business Continuity Management atte ad integrare gli aspetti di organizzazione (ruoli e responsabilità), processi/procedure e le soluzioni tecnologiche di supporto.

3.2.2 Lo scopo del Business Continuity Management

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 impreveduti 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, ecc...)
- Atti dolosi miranti a ridurre la disponibilità delle informazioni (Sabotaggi e frodi; diffusione di virus; bombardamento di messaggi; interruzione di collegamenti; ecc....).

Le minacce di tipo doloso possono provenire da operatori/ambienti sia interni sia esterni al Gruppo ed in particolare da utenti connessi alla rete internet.

A fronte di questi possibili eventi, il BCM deve essere focalizzato sulla garanzia di continuità del supporto delle tecnologie ICT ai processi che consentono all'Ente/Organizzazione l'erogazione del/dei servizio/servizi.

3.2.3 Le componenti del Business Continuity Management

Lo sviluppo di un sistema di Business Continuity Management deve tener in considerazione le seguenti componenti:

- Crisis and Incident Management: assicura la gestione dello stato di crisi e la risposta ad incidenti nel caso in cui si verifichi un evento in grado di compromettere la continuità dell'operatività
- Continuity Management: assicura la continuità dei processi durante e dopo un'emergenza attraverso la predisposizione di processi/procedure alternative (spesso manuali) a quelle normalmente supportate dall'infrastruttura di ICT
- Disaster Recovery Management: assicura il recovery delle infrastrutture tecnologiche a supporto dei processi di business
- Business Recovery Management: assicura il recovery dei processi di business dopo un'emergenza e il ritorno alla normalità.

La pianificazione di un Sistema di Business Continuity Management è una misura preventiva nell'ambito della gestione dei rischi, con particolare riferimento ai rischi di disponibilità delle informazioni.

L'esecuzione dei piani e delle procedure previste in caso di eventi in grado di compromettere la continuità operativa deve essere rivolta a ridurre al minimo gli impatti derivanti dal verificarsi di tali eventi.

3.2.4 Il ciclo del Business Continuity Management

Il ciclo di realizzazione del Sistema di Business Continuity Management deve prevedere le seguenti fasi:

- Progettazione del BCM: prevede il disegno e la pianificazione dell'intero sistema sia negli aspetti organizzativi che tecnologici
- Implementazione del BCM: prevede l'implementazione del sistema progettato con particolare attenzione agli aspetti di comunicazione/ sensibilizzazione diffusa e di formazione specifica sulle procedure e sui piani
- Monitoraggio del BCM: prevede il monitoraggio dell'efficacia del sistema implementato attraverso test e simulazioni dei piani e audit periodici specifici
- Mantenimento ed ottimizzazione: prevede l'evoluzione del sistema in relazione ai feedback derivanti dal monitoraggio e ad eventuali ulteriori requisiti interni ed esterni sopraggiunti nel frattempo ed avvia un nuovo ciclo progettuale.

3.2.5 Le strategie per il Business Continuity Management

Gli indirizzi strategici da seguire nella progettazione e realizzazione del Sistema di Business Continuity Management sono le seguenti:

- Considerare le logiche di gestione della continuità come parte integrante e non aggiuntiva della gestione dell'attività di cui ciascun Ente è titolare
- Sviluppare una gestione della continuità in relazione agli impatti che i processi e le infrastrutture di supporto hanno sulle attività dell'organizzazione
- Garantire un mix di interventi di tipo organizzativo e tecnologico adeguato, con una costante attenzione al rapporto costi/benefici
- Assicurare il coordinamento e l'integrazione delle attività di gestione dell'emergenza con le attività di analisi e gestione dei rischi operativi
- Disegnare una struttura di responsabilità chiara e coerente e attribuire esplicitamente le responsabilità aggiuntive ai ruoli già esistenti o nuovi

- Garantire che le nuove logiche di gestione della continuità siano un patrimonio dell'intera Organizzazione e che ciascun dipendente contribuisca affinché queste diventino parte integrante della cultura organizzativa
- Per garantire l'affidabilità e la continuità di erogazione dell'infrastruttura tecnologica valutare l'opzione strategica di delega in outsourcing attraverso una approfondita e corretta definizione e gestione dei livelli di servizio.

Il ciclo deve essere attivato dalla valutazione degli impatti derivanti da una possibile interruzione dei processi sull'erogazione dei prodotti/servizi, anche ricorrendo, ove possibile, alle esperienze e a situazioni già verificate.

A valle della valutazione degli impatti specifica per ogni Ente, si sceglierà di adottare la soluzione che verrà ritenuta più equilibrata, valutando le alternative, in particolare quelle correlate ai tempi di ripartenza e ripristino.

3.2.6 Le linee guida all'elaborazione dei piani del Business Continuity Management

Il Business Continuity Plan (BCP)

Al fine di ottenere un piano di continuity che possa essere effettivamente adoperato in caso di disastro e, quindi, riesca ad assicurare la continuità, almeno quella minimale e il ripristino dei processi con priorità rispetto a quelli ritenuti chiave, si devono prevedere le seguenti fasi:

1. definizione di obiettivi e ipotesi;
2. definizione della Business Impact analysis;
3. progetto e sviluppo del piano;
4. realizzazione del piano;
5. test del piano di BCP;
6. manutenzione del piano;
7. esecuzione in caso di disastro.

Nel caso specifico il Business Recovery Plan, volto ad assicurare il ripristino dei processi di business dopo l'emergenza, deve essere considerato come un'appendice del BCP, mirato ad assicurare il sostegno ai processi vitali dell'Ente durante e dopo l'emergenza.

1. Definizione di obiettivi e ipotesi

Questa fase si compone di:

- Definizione degli obiettivi;
- Individuazione di uno sponsor;
- Definizione di un Comitato guida (nella fattispecie il Comitato della sicurezza);
- Sviluppo di un piano di progetto;
- Preparazione del budget;
- Definizione di un sistema di reporting.

2. Definizione del Business Impact Analysis

Questa fase consiste nell'identificazione di tutti i processi critici, delle relative dipendenze reciproche, delle tecnologie impattate, dei partners strategici del business, delle principali risorse umane da coinvolgere, delle informazioni vitali da registrare, e degli impatti quantificati che un disastro può avere sull'organizzazione.

Le attività di questa fase dovrebbero essere:

- Identificazione dei rischi organizzativi
- Identificazione dei processi critici
- Definizione dei Tempi di non funzionamento ed impatti finanziari dei processi critici
- Definizione delle interdipendenze dei processi critici allo scopo di determinare l'ordine in cui devono essere riattivati
- Definizione del massimo tempo tollerabile di indisponibilità per ogni processo
- Identificazione del tipo e della quantità di risorse necessarie al ripristino cioè dei dispositivi fisici quali, tavoli, sedie, fax, fotocopie, files, personal computers, stampanti, telefonini per ciascuna attività
- Determinare l'impatto sia finanziario che di reputazione in caso di disastro.

In questa fase i rischi dovrebbero essere definiti in termini qualitativi, di verosimiglianza e di conseguenza sul business. Si noti che le attività di questa fase sono tipicamente identificate nella Metodologia di Classificazione e Valorizzazione degli asset.

3. Progetto e sviluppo del piano

L'obiettivo di questa fase deve essere di definire le strategie operative alternative appropriate per ciascun disastro al fine di fornire un recupero operativo tempestivo per tutti i processi critici e per i processi da questi dipendenti.

Se venisse scelta un'errata strategia di azione per rispondere ad un disastro, le conseguenze del disastro stesso potrebbero essere esacerbate.

Ogni strategia di azione dovrebbe sempre affrontare sia gli aspetti organizzativi che quelli tecnici.

Una strategia di azione di ripristino deve essere sviluppata per il ripristino dei processi del "Core Business" in ottica di sopravvivenza.

Inoltre la singola strategia deve essere scelta in funzione della necessità di tempo di ripristino, inteso come tempo di tolleranza dell'organizzazione senza soffrire perdite significative finanziarie o di immagine (Tempo di Recovery).

4. Realizzazione del piano

Scopo di questa fase è di sviluppare e documentare i processi di ripristino che assicurano la Business Continuity, nel caso si verifichi un disastro, in una formulazione appropriata all'esecuzione in condizioni di emergenza.

Le attività che devono essere incluse in questa fase sono:

- Scelta dei tools per la creazione ed esecuzione del piano di BCP;
- Definizione delle attività di ripristino (sequenze, tempi e responsabilità);
- Definizione dei processi di "escalation" e di ridefinizione delle priorità in funzione della successione degli eventi e della gestione della crisi;
- Identificazione degli individui, dei reparti e delle interdipendenze necessari a effettuare attività specifiche;
- Identificazione e differenziazione dei team di ripristino;
- Identificazione e lista dei contatti chiave, dei fornitori e delle risorse;
- Documentazione del piano ai fini della futura manutenibilità.

5. Test del piano di BCP

L'obiettivo di questa fase è quello di strutturare complete ed efficaci esercitazioni e test per assicurare che il piano funzioni come è stato progettato.

Se il piano non viene testato su basi di regolarità non c'è assicurazione che, nel caso il piano venisse attivato, l'organizzazione sopravviverebbe al disastro.

Gli obiettivi specifici di effettuare i BCP test sono di assicurare che:

- Le procedure di ripristino siano complete ed attuabili;
- La competenza del personale nelle procedure di ripristino possa essere valutata come efficiente;
- Le risorse necessarie a effettuare i processi di ripristino, quali processi, sistemi ICT, personale, risorse fisiche e dati, siano ottenibili ed operative;
- Le procedure manuali di ripristino ed i sistemi ICT di backup siano aggiornati e possano essere o operativi o ripristinabili;
- Il programma di addestramento sia monitorato.

Ci sono tre livelli di test di BCP:

1. verifica del grado di conoscenza del personale coinvolto, per i processi scelti e identificati nella Business Impact Analysis, usando le procedure di BCP nei vari scenari di disastro, tramite sessioni di gruppo;
2. prova di ripristino di alcuni processi scelti, usando le procedure di BCP, comprendendo nelle prove i sistemi IT coinvolti ed il raduno di personale di ripristino in un luogo alternativo a quello usuale;
3. prova di ripristino di tutti i processi critici, con le procedure di BCP, includendo i sistemi critici ed il coordinamento con tutti i gruppi dell'Organizzazione.

Le attività da eseguire sono:

1. Definizione delle strategie di test;
2. Scelta dei metodi di test;
3. Definizione degli obiettivi di test e dei piani di test;
4. Esecuzione dei test;
5. Documentazione delle deviazioni rispetto ai processi critici;
6. Redazione di un report;
7. Ridefinizione del BCP in base ai risultati del test.

6. Manutenzione del piano

L'obiettivo di questa fase è di mantenere il piano aggiornato e pronto al supporto delle attività in caso di emergenza.

Le attività da intraprendere sono:

1. determinare le responsabilità di aggiornamento del piano;
2. identificare i meccanismi organizzativi per innescare i cambiamenti del piano, assicurando che ogni modifica organizzativa, operativa e infrastrutturale, sia comunicata al personale responsabile dell'aggiornamento del piano;
3. determinare delle regole procedurali di manutenzione per assicurare che il piano rimanga aggiornato;
4. determinare i processi per modificare il piano;
5. determinare le regole di controllo dei cambi di versione del piano.

7. Esecuzione in caso di disastro

L'obiettivo di questa fase è la risposta in caso di disastro, ovvero la Gestione della Crisi.

3.2.7 Disaster Recovery Plan

Per Disaster Recovery Plan (DRP) si intendono gli aspetti tecnologici del 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. In particolare non si riferisce quindi a interruzioni minori che non richiedono ri-locazione di sito.”

Affinchè 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.

Di seguito viene sintetizzata un'ipotesi di scenari di disastro:

1. Un disastro di primo livello su una locazione può causare, in alcuni casi, la parziale ma non completa distruzione delle operazioni svolte giornalmente. La situazione può essere risolta usando personale nel sito ed effettuando localmente sforzi di ripristino, pur con la riallocazione di alcune persone o funzioni.
2. Un disastro di livello 2 coinvolge diverse locazioni o piani. Le operazioni di routine possono essere distrutte ed i processi critici possono dover essere eseguiti off-site. Personale locale può dover cercare assistenza all'esterno. Il coordinamento delle persone avviene attraverso un centro di operazioni di emergenza.
3. Un disastro di livello 3 può coprire una vastissima zona, ad esempio una regione; tipici esempi di questi disastri sono: inondazioni, terremoti o uragani. In questo caso sono richieste risorse esterne ed assistenza, ma il ripristino completo può comportare settimane o mesi. Generalmente un disastro di questo livello comporta la paralisi delle normali funzioni di business.

I sistemi dovrebbero essere classificati secondo le definizioni seguenti:

Critici

Le relative funzioni non possono essere eseguite senza essere sostituite da strumenti (mezzi) di caratteristiche identiche. Le applicazioni critiche non possono essere sostituite con metodi manuali. La tolleranza in caso di interruzione è molto bassa, di conseguenza il costo di una interruzione è molto alto.

Vitali

Le relative funzioni possono essere svolte manualmente, ma solo per un breve periodo di tempo. Vi è una maggiore tolleranza all'interruzione rispetto a quella prevista per i sistemi critici, conseguentemente il costo di una interruzione è inferiore, anche perchè queste funzioni possono essere riattivate entro un breve intervallo di tempo (generalmente entro cinque giorni).

Delicati

Queste funzioni possono essere svolte manualmente, a costi tollerabili, per un lungo periodo di tempo. Benchè queste funzioni possano essere eseguite manualmente, il loro svolgimento risulta comunque difficoltoso e richiede l'impiego di un numero di persone superiore a quello normalmente previsto in condizioni normali.

Non-critici

Le relative funzioni possono rimanere interrotte per un lungo periodo di tempo, con un modesto, o nullo, costo per l'azienda, e si richiede un limitato (o nullo) sforzo di ripartenza quando il sistema viene ripristinato.

Le procedure applicative, il software di sistema ed i file che sono stati classificati e documentati come critici, devono essere ripristinati prioritariamente.

Applicazioni, software e file classificati come critici hanno una tolleranza molto bassa alle interruzioni. La criticità di applicazioni, software di sistema e dati, deve essere valutata in funzione del periodo dell'anno in cui il disastro può accadere.

Un piano d'emergenza deve prevedere il ripristino di tutte le funzioni aziendali e non solo il servizio ICT centrale.

Per la definizione del DRP devono essere valutate le strategie di ripristino più opportune su: siti alternativi, metodi di back up, sostituzione degli equipaggiamenti e ruoli e responsabilità dei team.

La prolungata indisponibilità del servizio elaborativo derivante in particolare situazione di disastro, e quindi dei servizi primari, rende necessario l'utilizzo di una strategia di ripristino in sito alternativo.

Le più comuni strategie di ripristino in sito alternativo includono i seguenti approcci:

Offsite storage

Tutti i sistemi informativi dovrebbero prevedere un regolare back up ed un sistema di archiviazione delle informazioni in un ambiente protetto in base alla criticità dei sistemi e dei dati, insieme alle licenze Software, le system configurations, e le altre informazioni vitali.

Interoperabilità

Utilizzo di piattaforme e configurazioni standard riducono le spese di recovery e sostituzione delle apparecchiature da sostituire.

Ridondanza

Una ridondanza di data storage, communications paths, alimentazioni e componenti di sistema riducono la probabilità di blocco dei sistemi. Inoltre devono essere valutate le seguenti opzioni in base a criticità dei processi/applicazioni/sistemi e a considerazioni di costo/benefici:

Hot sites (siti "caldi")

Questi centri prevedono una completa configurazione in grado di funzionare entro poche ore. L'apparecchiatura e il software di base devono essere compatibili con l'installazione primaria per la quale si svolge funzione di servizio IT alternativo. Le uniche esigenze aggiuntive sono il personale, i programmi, i file dati e la documentazione.

Il sito "caldo" è destinato alle operazioni d'emergenza per un periodo di tempo limitato e non ad un esteso utilizzo a lungo termine.

Perciò il sito "caldo" dovrebbe essere considerato come un mezzo per ottenere la continuità delle operazioni essenziali per un periodo di alcune settimane subito dopo un disastro o una grossa emergenza.

Il piano di ripristino per la connettività della rete a un sito caldo che utilizza una rete pub-

blica commutata dovrebbe prevedere la ridondanza e la disponibilità di una sufficiente capacità su diversi percorsi per reinstradare il traffico in caso di necessità. Dovrebbe essere inoltre previsto un instradamento notturno mediante centrali differenti in modo che un problema in un singolo punto non possa rendere inoperante l'intera rete.

Warm sites (siti "tiepidi")

Questi sono siti parzialmente configurati, generalmente con connessioni alle reti e ad unità periferiche specifiche, come unità disco, unità nastro, unità di controllo ma senza l'unità centrale. A volte è presente una CPU di minore potenza.

L'unità centrale può essere ottenuta rapidamente per una installazione di emergenza (fornendo uno dei modelli più comuni).

Dopo l'installazione dei componenti necessari, il centro può essere pronto per il funzionamento in poche ore, anche se l'installazione e l'avviamento dell'unità centrale e delle altre unità mancanti potrebbe richiedere alcuni giorni o settimane.

Questa soluzione è meno dispendiosa rispetto alla soluzione "hot".

Cold sites (siti "freddi")

Questi sono ambienti nei quali sono predisposti gli impianti base (ad esempio cavi elettrici, aria condizionata, pavimenti rialzati) per contenere una sala macchine. Il "cold site" è predisposto per ricevere le apparecchiature ma non dispone di alcun componente prima che questo sia necessario. L'attivazione di simile realtà può richiedere diverse settimane.

Mobile Sites

sono siti trasportabili, personalizzati con equipaggiamenti IT e di telecomunicazioni necessari a soddisfare i fabbisogni di sistema. Il sito è trasferibile e può essere installato al sito alternativo.

Mirrored Sites

sono siti completamente ridondati con mirroring completo. I dati sono elaborati e memorizzati contemporaneamente nei siti primario e alternativo consentendo un'elevata disponibilità del sistema.

Un'opzione strategica da tenere in considerazione è la possibilità di impostare un accordo di reciprocità tra due centri differenti.

Per garantire la fattibilità di una simile soluzione si dovrebbe verificare che:

- Esista una compatibilità di base degli impianti per realizzare una comune infrastruttura
- Esista la disponibilità delle risorse addizionali disponibili
- Siano effettuate regolarmente delle prove di verifica.

Gli accordi reciproci sono accordi tra due o più società con apparecchiature o applicazioni simili.

Le caratteristiche tipiche di questa soluzione prevedono che i partecipanti forniscano tempo macchina agli altri in caso di emergenza.

I vantaggi sono:

- Bassi costi
- Potrebbe essere l'unica alternativa praticabile se non esistessero servizi alternativi con hardware compatibile.

Gli svantaggi sono:

- Di norma non può essere imposto;
- Possibili differenze nella configurazione hardware, spesso impongono delle modifiche ai programmi per renderli funzionanti;
- Cambiamenti non segnalati nel carico di lavoro o nella configurazione delle apparecchiature rendono l'accordo limitato o impraticabile.

Nel piano di Disaster Recovery dovrebbero essere specificate le caratteristiche contrattuali, nel caso di servizi alternativi forniti da terze parti.

Queste dovrebbero coprire i seguenti aspetti:

- Configurazioni
- Definizione di disastro
- Tempestività, cioè in quanto tempo i servizi alternativi saranno disponibili dopo un disastro
- Numero di Utenze per centro per edificio o per area
- Priorità di servizio in caso di disastro comune a più utenti
- Copertura assicurativa per il personale della società operante nei locali del centro alternativo
- Periodo di utilizzo e di disponibilità per l'uso e tipo di supporto tecnico fornito dalle persone del servizio alternativo
- Sistema di comunicazione
- Garanzie che offre il fornitore relativamente alla disponibilità del sito e alla adeguatezza delle strutture
- Diritti di prova
- Affidabilità del centro.

Nell'ambito del Disaster Recovery Plan devono essere previste le procedure di back up e recovery. Le principali sono le seguenti:

Salvataggio dei supporti e della documentazione

La disponibilità di archivi dati adeguati è di cruciale importanza per ripristinare le elaborazioni (internamente o esternamente) in caso di emergenza. La duplicazione dei dati più importanti e della corrispondente documentazione, nonché la relativa conservazione in adeguati ambienti esterni all'azienda, sono un prerequisito fondamentale per ogni tipo di piano d'emergenza.

Procedure di salvataggio periodiche

Sia gli archivi dati, sia i programmi dovrebbero essere periodicamente copiati. La periodicità di queste operazioni può essere diversa per programmi applicativi e per il software di sistema.

L'utilizzo di sistemi software specifici per la gestione dei nastri (tape management system) e per la schedulazione automatica dei lavori (automated job scheduling), può facilitare la pianificazione periodica di queste operazioni.

Le copie dei dati e dei programmi consentono la gestione continua delle modifiche.

Una copia del file o del record effettuata con periodicità viene conservata per le operazioni di ripristino.

Tutte le modifiche o le transazioni avvenute dall'ultimo salvataggio degli archivi devono essere salvate.

Analogamente, ogni documentazione necessaria alla operatività corrente dell'Amministrazione dovrebbe essere conservata in opportune località esterne.

Analoga considerazione vale per i documenti necessari per ripristinare il database di produzione. Come per i file di dati, anche le copie conservate all'esterno devono essere mantenute aggiornate per assicurarne l'utilizzabilità.

La documentazione da archiviare e conservare esternamente comprende:

- Documentazione sistemistica e dei programmi
- Procedure speciali
- Documenti di INPUT / OUTPUT
- Piano di continuità aziendale.

I dati riservati/critici, posti nell'archivio remoto dovrebbero essere archiviati in appositi armadi ignifughi.

Si dovrebbe mantenere un inventario contenente informazioni quali:

- Il nome del file, il numero di serie del volume, la data di creazione, il periodo contabile di riferimento, il numero di locazione fisica del back-up, per tutti i nastri di back-up.
- Il nome del documento, la sua posizione, il sistema interessato, la data dell'ultimo aggiornamento, per tutta la documentazione critica.

Ripristino delle Reti di telecomunicazioni

Le reti delle telecomunicazioni sono soggette agli stessi disastri naturali dei centri elaborazione dati, ma sono anche esposte ad alcuni eventi disastrosi peculiari delle telecomunicazioni.

Questi potrebbero includere un disastro alla centrale di smistamento, il taglio dei cavi, errori e malfunzionamenti del software per le telecomunicazioni, vulnerabilità nella sicurezza dovute a pirateria informatica (gli hacker delle linee telefoniche sono noti come ph-racker), e molti altri malfunzionamenti causati dall'uomo.

L'Amministrazione dovrebbe prendere provvedimenti per effettuare il back-up delle proprie infrastrutture di telecomunicazione.

Il piano di Disaster Recovery dovrebbe considerare e fornire adeguate risorse di telecomunicazioni per la continuità delle attività aziendali critiche.

Le infrastrutture di telecomunicazione da prendere in considerazione includono i circuiti di fonia, le reti geografiche (ad esempio per connettersi a centri dati distribuiti), le reti locali (per connettere gruppi di PC) e gli ISV.

La capacità critica dovrebbe essere classificata in varie soglie, cioè 2, 8, 24 ore di fuori servizio, per le diverse risorse di comunicazione.

Le apparecchiature UPS dovrebbero essere sufficienti per fornire un adeguato back-up sia alle apparecchiature trasmissive sia alle apparecchiature elaborative.

I metodi più comuni per fornire continuità di comunicazione sono:

- Ridondanza
- Instradamento alternativo
- Instradamento del traffico tramite il frazionamento dei mezzi infrastrutturali fisici trasmissivi o la loro duplicazione.

- Diversificazione delle reti geografiche grazie al reinstradamento automatico e linee ridondanti per offrire un ripristino istantaneo in caso di caduta
- Ridondanza dei circuiti "all'ultimo miglio".

Il piano deve definire i modi di approvvigionamento delle apparecchiature alternative. Ad esempio si possono valutare le seguenti alternative:

Accordo di fornitura di hardware con un fornitore o terzi

Gli accordi con il venditore dovrebbero pianificare il passaggio da un sito "caldo" a un sito "tiepido" o "freddo"

Disponibilità presso il fornitore

I componenti sono facilmente disponibili presso il fornitore in poco tempo e con una minima necessità di speciali predisposizioni.

Immagazzinamento degli equipaggiamenti

Gli equipaggiamenti dovrebbero essere acquistati in anticipo e immagazzinati in un sito alternativo.

Nel piano di Disaster Recovery dovrebbe essere prevista la descrizione della sicurezza del sito alternativo.

Il centro di elaborazione alternativo, deve disporre dello stesso livello di sicurezza e controllo del centro originale.

Questo implica adeguati controlli per l'accesso fisico quali porte chiuse, assenza di finestre, servizio di sorveglianza. Il centro alternativo dovrebbe essere sottoposto a costanti verifiche e controlli ambientali come il centro originale.

Questo comporta il continuo controllo di temperatura, umidità e aria condizionata per raggiungere le condizioni ottimali previste per la conservazione dei supporti magnetici ed, eventualmente, per l'unità centrale e per le diverse unità periferiche.

I controlli ambientali devono prevedere inoltre il pavimento sopraelevato, rilevatori di fumo e di acqua, il gruppo elettrogeno di continuità ed il sistema di spegnimento automatico di incendio adeguatamente provato e funzionante.

L'archiviazione in luoghi esterni di quelle applicazioni che non sono direttamente collegate al mainframe diventa di importanza vitale per sopravvivere in caso di disastro.

Le attività di conservazione per le attività elaborative di supporto all'utente comprenderanno normalmente l'archiviazione in luoghi diversi dei floppy disk e la duplicazione dei file del server.

Al fine di poter riattivare completamente le elaborazioni critiche dell'utente, il centro alternativo dovrebbe comprendere le apparecchiature PC considerate necessarie, le connessioni di telecomunicazione (incluse le connessioni per la fonia) e le apparecchiature ed il software per le LAN.

Il piano dovrebbe prevedere una schedulazione formalizzata delle elaborazioni di tutto il sistema.

Questa schedulazione andrebbe definita per tutti i giorni dell'anno al fine di facilitare l'identificazione di quei sistemi che sono critici al momento in cui avviene il disastro.

La schedulazione andrebbe dettagliata fino al punto da indicare l'ordine da seguire per l'esecuzione di tutti i lavori da elaborare. Il mantenere aggiornata questa sezione del piano di Disaster Recovery è fattore critico se avvengono variazioni all'ambiente elaborativo.

Gestione della crisi

Per Gestione della Crisi si intende il coordinamento complessivo della risposta organizzativa ad una possibile crisi in modo efficace e tempestivo, con lo scopo di evitare o minimizzare i danni al profitto, alla reputazione ed alla capacità di operare dell'Amministrazione.

Le fasi di gestione della crisi dovrebbero essere:

1. Notificazione ed attivazione della crisi
 - Procedure di notifica al personale coinvolto e sequenza delle chiamate
 - Assessment dei danni
 - Piano di attivazione della crisi
2. Recovery dell'emergenza
 - Definizione della sequenza delle attività di recovery
 - Procedure di recovery
3. Ricostituzione dell'operatività
 - Ricostituzione del sito originale
 - Test dell'operatività
 - Termine delle operazioni di emergenza e ripresa dell'operatività normale
4. Attività di gestione post crisi.

La gestione della crisi necessita del coinvolgimento e del coordinamento di team specifici comprendenti le persone incaricate di realizzare i piani di azione.

Queste persone sono generalmente a capo di gruppi creati in corrispondenza di una funzione o compito critico definito nel piano.

A seconda delle dimensioni della struttura organizzativa, questi gruppi si possono anche definire come posizioni di una persona singola.

Ogni team dovrebbe essere addestrato affinché capisca la funzione del team durante il ripristino, ogni passo da eseguire e come i team si relazionano agli altri team; Il team dovrebbe essere pronto ad operare in ogni momento in caso di necessità di attivazione del piano.

I possibili team identificabili sono i seguenti:

Senior Management Official Team (Gruppo di management)

Questo gruppo è responsabile del coordinamento delle attività di contenimento e contrasto del disastro, supervisiona tutti gli altri gruppi e prende le decisioni chiave per le emergenze interne ed esterne. Il team è responsabile l'attivazione del piano d'emergenza. Il team è guidato da un esponente del Senior Management con l'autorità di prendere decisioni su livelli di spesa, rischio accettabile e coordinamento tra funzioni aziendali e con gli organi esterni di Polizia e Protezione civile.

Management Team (Gruppo per la gestione dell'emergenza)

Questo gruppo funziona come supporto tecnico operativo all'unità di crisi ed opera come "supervisore del disastro". Da esso dipende il coordinamento di tutte le attività degli altri team ed in particolare:

- Recuperare i dati critici e essenziali dal deposito
- Installare e provare il software di sistema e le varie applicazioni presso il sito di recovery del sistema (sito "caldo", sito "freddo", service bureau)
- Identificare, comprare e installare l'hardware opportuno presso il sito di recovery del sistema
- Operare dal sito di recovery del sistema

- Reinstradare il traffico sulle reti di comunicazione
- Reinstallare la rete utente/sistema
- Trasportare gli utenti alla installazione di recovery
- Ricostruire i data base
- Fornire i necessari materiali di ufficio (per es. moduli speciali, scorte di controllo, carta, etc.)
- Coordinare l'uso dei sistemi e i piani di lavoro degli addetti.

Emergency team (Gruppo per le attività di emergenza)

È il gruppo di primo intervento. Sono i componenti delle squadre pompieri e delle cosiddette squadre di emergenza e la loro funzione è il trattamento degli incendi o di altre situazioni d'emergenza. Una delle loro funzioni primarie sarà l'evacuazione ordinata del personale e la salvaguardia di vite umane.

Damage assessment team (Gruppo per la valutazione dei danni)

La funzione di questo gruppo è di valutare le dimensioni dei danni causati dal disastro. Il gruppo dovrebbe comprendere persone in grado di valutare il danno e stimare il tempo richiesto per ripartire con le attività usuali nel sito interessato.

Questo gruppo dovrebbe includere personale esperto nell'uso di apparecchi di collaudo, con conoscenza di sistemi e reti ed addestrato sui regolamenti e procedure di sicurezza da applicare. Inoltre, queste persone avranno la responsabilità di identificare le possibili cause del disastro e il suo impatto in termini di danni e di prevedibile tempo di fermo del sistema.

Altri team si occupano della gestione degli aspetti finanziari del ripristino, del trattamento delle questioni legali derivanti dal disastro, nonché delle pubbliche relazioni e delle informazioni ai media.

Per queste funzioni sono identificabili anche i seguenti gruppi operativi:

Media Relations Team (Gruppo delle pubbliche relazioni)

Questo gruppo si occupa delle relazioni pubbliche per ridurre i rischi di immagine.

Legal Affairs Team (Gruppo affari legali)

Questo gruppo si occupa di tutti gli aspetti inerenti le implicazioni legali e normative, comprese quelle sulla Privacy e quelle di Responsabilità degli amministratori previste dal DPR. 31/2001.

Physical/Personal Security Team (Gruppo di sicurezza)

Questo gruppo si occupa di tutte le condizioni che impattano i rischi legati alla sicurezza, ambientale fisica e del personale coinvolto nel disastro.

In particolare controlla in modo continuativo durante l'emergenza la sicurezza del sistema e delle comunicazioni; inoltre risolve ogni conflitto di sicurezza che impedisca un rapido recovery del sistema. Assicura l'appropriata installazione ed il funzionamento del pacchetto software di sicurezza.

Procurement (equipment and supplies) Team (Gruppo fornitori)

Questo gruppo ha l'obiettivo di gestire l'approvvigionamento dei materiali e degli equipaggiamenti necessari all'emergenza.

Supporta il lavoro del gruppo hardware utente contattando i fornitori e coordinando la logistica per la fornitura giornaliera del necessario materiale di supporto per il computer e gli uffici.

Altri gruppi di supporto tecnico al Disaster Recovery possono essere i seguenti:

Systems Software Team (Gruppo software di sistema)

È responsabile di effettuare il "restore" dei dischi di sistema, di caricare e provare il software del sistema operativo, e di risolvere i problemi a livello sistemistico.

Server Recovery Team (e.g., client server, web server) (Gruppo di ripristino dei server)

È responsabile di tutte le attività sistemistiche ed operative per il ripristino dei server e delle server farm.

Application Recovery Team(s) (Gruppo applicativo)

Si reca al sito di recovery del sistema e effettua il restore dei dischi utente e dei programmi applicativi sul sistema. A mano a mano che procede il recovery, questo gruppo può assumere la responsabilità di controllare le prestazioni applicative e l'integrità dei data base.

Operating System Administration Team (Gruppo operativo d'emergenza)

Consiste di operatori e supervisori che, a turno, rimarranno presso il sito di recovery del sistema e gestiranno le operazioni di sistema durante tutta la durata dei progetti di disaster recovery. Un'altra responsabilità potrebbe essere quella di coordinare l'installazione dell'hardware qualora non sia stato scelto come centro di recovery un sito "caldo" o altra installazione con macchine già disponibili.

LAN/WAN Recovery Team (Gruppo di ripristino delle reti)

È responsabile per il reinstradamento delle comunicazioni in voce e dati su larga scala e il ristabilimento dei controlli e degli accessi alla rete su host presso il sito di recovery del sistema.

Network Operations Recovery Team (Gruppo operativo delle reti)

Fornisce un supporto continuativo per la trasmissione dati e supervisiona l'integrità delle comunicazioni.

Telecommunications Team (Gruppo delle telecomunicazioni)

Si reca al sito di recovery utente dove lavora insieme con il gruppo di recovery delle reti remote per ristabilire una rete utente/sistema. È anche responsabile per sollecitare e installare hardware per le comunicazioni presso il sito di recovery utente e di lavorare con gli uffici della società dei telefoni locali ed i fornitori gateway nel reinstradamento del servizio locale e accesso ai gateway.

Database Recovery Team (Gruppo della preparazione e registrazione dei dati)

Aggiorna i database applicativi lavorando da terminali installati presso il sito di recovery utente. Supervisiona il personale temporaneo addetto alla immissione dati e assiste ai tentativi di salvataggio dei record acquisendo i documenti originali e altre fonti d'informazione di input.

È responsabile anche di ottenere, imballare e spedire i supporti e altre registrazioni all'installazione di recovery come pure di stabilire e supervisionare un piano per la conservazione delle informazioni create durante l'attività del sito di recovery

Transportation and Relocation Team (Gruppo di trasporto)

Serve come un gruppo di supporto per localizzare un sito di recovery utente se non ce n'è già uno prefissato ed è responsabile per coordinare il trasporto dei dipendenti dell'azienda a un sito distante di recovery utente. Possono anche aiutare a contattare i dipendenti per informarli sui nuovi luoghi di lavoro e a pianificare e prendere accordi per la sistemazione logistica dei dipendenti stessi.

Hardware Salvage Team (Gruppo dell'hardware utente)

Localizza e coordina la consegna e installazione di terminali utente, stampanti, macchine da scrivere, fotocopiatrici, e altre apparecchiature necessarie. Offre supporto al gruppo delle comunicazioni e a qualsiasi tentativo per il salvataggio di hardware e apparecchiature.

Administrative Support Team (Gruppo di supporto amministrativo)

Fornisce un supporto d'ufficio agli altri gruppi e serve come centro di raccolta/smistamento messaggi per il sito di recovery utente. Può controllare le funzioni di contabilità e stipendi come pure la supervisione giornaliera dell'installazione.

Alternate Site Recovery Coordination Team (Gruppo di rilocalizzazione al sito alternativo)

Dirige il progetto di rilocalizzazione. Fa una valutazione più dettagliata, rispetto a quella fatta inizialmente, dei danni subiti dall'installazione e dalle apparecchiature. Fornisce al gruppo per la gestione dell'emergenza le informazioni necessarie per determinare se i piani devono orientarsi verso la ricostruzione oppure la rilocalizzazione. Fornisce le informazioni necessarie per avanzare richieste di rimborso alle assicurazioni (un'assicurazione è la prima fonte di fondi per il lavoro di ripristino).

Coordina gli sforzi necessari per il salvataggio immediato delle registrazioni (per es. recuperare documenti cartacei, supporti elettronici, etc.).

Original Site Restoration/Salvage Coordination Team (Gruppo di ripristino del sito originale o di salvataggio)

Coordina il trasferimento dal sito caldo ad una nuova locazione o alla locazione originaria ripristinata.

Ciò comporta la rilocalizzazione delle attività elaborative, le comunicazioni e le attività utente. Questo gruppo controlla anche il ritorno verso i normali livelli di servizio.

