LA SICUREZZA DELLE RETI

nelle infrastrutture critiche

Infrastrutture Critiche
Sicurezza tlc

Istituto Superiore delle Comunicazioni
e delle Tecnologie dell'Informazione
Ministero delle Comunicazioni

LA SICUREZZA DELLE RETI nelle infrastrutture critiche

Il presente documento è stato realizzato da:

Stefano AMICI	(Enav S.p.A.),
Riccardo BIANCONI	(SINCERT),
Danilo BRUSCHI	(Università degli Studi di Milano),
Bruno CARBONE	(Enav S.p.A),
Giancarlo CAROTI	(Terna S.p.A. - Rete Elettrica Nazionale)
Valentino DI TOMA	(Ancitel S.p.A.),
Silvio FANTIN	(GRTN S.p.A),
Giovanni FASSINA	(Poste Italiane S.p.A.)
Luisa FRANCHINA	(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione),
Vincenzo GESMUNDO	(Selenia Communications S.p.A.),
Carlo GUGLIELMINI	(Selenia Communications S.p.A.),
Maurizio MAYER	(AICT) ,
Giulio MICELI	(AICT),
Massimo PANICHELLI	(Ancitel S.p.A.),
Giovanni PATELLA	(Ministero delle Comunicazioni),
Daniele PERUCCHINI	(Fondazione Ugo Bordoni),
Armando PERUGINI	(C.V. AN (R) Consulente Amm.ne Difesa - TELEDIFE-SE.PRO TE.C. S.A.S),
Rodolfo PERUGINO	(Poste Italiane S.p.A.),
Gian Luca PETRILLO	(Consigliere del Ministro delle Comunicazioni),
Massimo PICCIRILLI	(Ministero delle Comunicazioni),
Francesco PIRRO	(CNIPA),
Gian Luigi PUGNI	(Enel Ape s.r.l),
Giovanna RICCI	(Rete Ferroviaria Italiana S.p.A.),
Giovanna SAMOGGIA	(Rete Ferroviaria Italiana S.p.A.),
Federico SANDRUCCI	(C. Amm. (Aus) Consulente Amm.ne Difesa - TELEDIFE-SE.PRO TE.C. S.A.S),
Alberto SARTI	(Finmeccanica S.p.A.),
Gianluigi SCAZZOLA	(Selenia Communications S.p.A.),
Stefano SCIASCIA	(Reparto Informazioni e Sicurezza - Stato Maggiore della Difesa-Ministero della Difesa),
Roberto SETOLA	(Presidenza del Consiglio dei Ministri - Dipartimento per l'Innovazione e le Tecnologie & Università Campus Bio-Medico di Roma),
Gigi TAGLIAPIETRA	(Siosistemi S.p.A),
Guido TRIPALDI	(I.NET S.p.A.),
Riccardo VALASTRO	(Poste Italiane S.p.A.).

Copertina e Progetto Grafico
Roberto Piraino (Graphics Lab - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)

Le opinioni e le considerazioni espresse in questo volume, nonchè le proposte avanzate, sono da considerarsi come personali dei singoli partecipanti e non riflettono necessariamente la posizione dei rispettivi Enti e Società d'appartenenza.
Il contenuto del presente volume è da considerarsi unicamente come studio tecnico/scientifico orientativo delle problematiche inerenti la sicurezza delle reti e la tutela delle comunicazioni.
Pertanto nessuna responsabilità potrà essere attribuita agli autori o all'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, che cura questa pubblicazione, per ogni eventuale conseguenza derivante da qualsivoglia utilizzo dei contenuti del presente testo.

Le citazioni di specifici marchi o nomi di prodotti presenti nel documento sono riportati a mero scopo esemplificativo, non esauriscono il novero di prodotti esistenti sul mercato e in nessun caso costituiscono elemento di valutazione o di raccomandazione per l'utilizzo dei prodotti stessi.

La presente pubblicazione è diffusa a titolo gratuito e gli autori hanno ceduto all'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione gratuitamente e a tempo indeterminato i diritti di autore.

LA SICUREZZA DELLE RETI NELLE INFRASTRUTTURE CRITICHE

Indice

Indice delle figure e delle tabelle

Indice delle figure

Indice delle tabelle

Introduzione

Questa pubblicazione nasce da una iniziativa dell'Istituto Superiore delle Comunicazioni e delle tecnologie dell'Informazione e dell'Osservatorio per la sicurezza e la tutela delle reti e delle comunicazioni, con la collaborazione di autori appartenenti a vari organismi pubblici e privati.

L'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, costituito nel 1907, opera nell'ambito del Ministero delle Comunicazioni in qualità di organo tecnico-scientifico. La sua attività, rivolta specificatamente verso le aziende operanti nel settore ICT, le Amministrazioni pubbliche e l'utenza, riguarda fondamentalmente la normazione, la sperimentazione e la ricerca di base e applicata, la formazione e l'istruzione specializzata nel campo delle telecomunicazioni.

La normazione tecnica nazionale ed internazionale in cui l'Istituto è attore attivo e propositivo, riveste un ruolo importante per garantire migliore trasparenza ed accessibilità ai servizi a favore degli utenti, dei manifatturieri e dei gestori delle reti di telecomunicazione.

In questo campo, l'azione dell'Istituto è duplice: tramite il CONCIT (Comitato di coordinamento formato da CEI-Comitato Elettrotecnico Italiano-, UNI-Ente Nazionale Italiano di Unificazione-

e dallo stesso Istituto e riconosciuto a livello europeo) effettua la trasposizione nell'ordinamento nazionale delle norme europee e, simultaneamente, rappresenta l'Amministrazione nelle funzioni di indirizzo e supporto nei gruppi nazionali presenti nelle varie commissioni e gruppi tecnici di studio dell'ITU (International Communication Union), della CEPT (Conference European des Poste et Telecommunication) e dell'ETSI (European Telecommunica-tion Standard Institute).

L'Istituto gestisce la Scuola Superiore di Specializzazione in Telecomunicazioni (attiva dal 1923), cui è affidata la specializzazione post-laurea nel settore delle comunicazioni elettroniche e delle tecnologie dell'informazione, con rilascio del relativo diploma . D'intesa con la facoltà di Ingegneria dell'Università "La Sapienza" di Roma, la Scuola organizza corsi annuali il cui piano di studi prevede anche attività di laboratorio, seminari e stage.

L'Istituto provvede anche alla formazione ed all'aggiornamento tecnico del personale appartenente al Ministero e ad altre pubbliche amministrazioni nei settori delle comunicazioni elettroniche e delle tecnologie delle informazioni, della sicurezza, della multimedialità e della qualità dei servizi, attraverso la pianificazione e realizzazione di percorsi formativi mirati all'acquisizione di competenze specialistiche. In tale ottica, l'Istituto si è dotato di un Test Center accreditato dall'AICA per il rilascio della Patente europea del Computer (European Computer Driving Licence - ECDL).

Inoltre attualmente è in fase di costituzione il Centro di formazione dei dipendenti della PA nel campo della sicurezza ICT .

Il Centro di formazione dovrà svolgere attività di formazione e di sensibilizzazione su larga scala dei dipendenti della PA in materia di sicurezza ICT, predisponendo in forma centralizzata e coordinata, un Piano di formazione e sensibilizzazione che diffonda in modo uniforme in tutta la Pubblica Amministrazione i principi e le metodologie della sicurezza.

L'Istituto, inoltre, promuove attività divulgativa tramite eventi di comunicazione esterna e pubblicizza le attività e le ricerche effettuate.

L'attività dell'Istituto nella ricerca è orientata allo sviluppo e al miglioramento dei servizi di telecomunicazione e di quelli legati alla tecnologia dell'informazione. Perseguendo queste finalità, le attività investono quasi tutte le aree del settore, dalla telefonia alla televisione, dall'elaborazione e trattamento del segnale, dall'architettura delle reti alla implementazione dei servizi.

Viste le competenze e le risorse strumentali di cui dispone, il ruolo dell'Istituto è rilevante nella partecipazione a progetti europei di sviluppo tecnologico per una più diffusa utilizzazione dei fondi europei. Tali attività sono svolte sia direttamente, sia d'intesa con altri Enti di Ricerca, con Università e con Centri di studi internazionali.

Nel contesto della Società dell'Informazione, sono di rilievo le azioni in svolgimento anche in collaborazione con la Fondazione Ugo Bordoni (FUB) nei settori del telelavoro, della sicurezza informatica, del teleinsegnamento e dell'accesso ai servizi di comunicazioni da parte di persone disabili ed anziani.

Grazie al supporto dell'Istituto poi, il Ministero ha potuto sostenere negli ultimi anni, una serie di iniziative per l'introduzione, sulle reti di comunicazione, di nuove tecnologie e nuovi sistemi. Tra queste, vanno sottolineati gli studi di fattibilità sull'applicazione di tecniche e di nuovi servizi televisivi e multimediali, lo studio di fattibilità per la fornitura di servizi macroregionali di televisione numerica via satellite, lo studio per la realizzazione di un sistema satellitare europeo per la fornitura di servizi a larga banda multimediali e interattivi, la partecipazione al progetto di ricerca e sviluppo tecnologico IST (Information Society Technologies) della Comunità Europea denominato ATLAS.

Considerando il suo ruolo di organismo pubblico e super partes, il valore aggiunto dell'Istituto, dato in termini di garanzia e competenza, è l'aspetto che contraddistingue i servizi di supporto tecnico e consulenziale forniti alle imprese e ai soggetti coinvolti nel settore delle telecomunicazioni. Tali servizi si sostanziano non solo nelle tradizionali attività di certificazione, realizzate grazie alle competenze e alle strumentazioni dei laboratori dell'Istituto che consentono di verificare la conformità di ogni apparato telematico alle varie norme e raccomandazioni di riferimento, ma anche in peculiari campagne di misura per la verifica della qualità del servizio (QoS), della sicurezza delle reti e per l'accertamento delle specifiche tecniche di interoperabilità dei servizi nell'ambito dell'interconnessione delle reti di vari operatori.

L'Istituto gestisce la banca dati relativa alle assegnazioni numeriche nella rete di telecomunicazione nazionale e alla portabilità dei numeri in tecnologia GSM e UMTS, gestisce inoltre il servizio di Orologio Nazionale di Riferimento (ONR) per la sincronizzazione della Rete Numerica di Telecomunicazione italiana e fornisce un supporto istituzionale ai proponenti che si sottopongono ai bandi di gara del programma comunitario E-TEN (Trans European Network per le TLC). L'Istituto collabora con Organismi di Certificazione per le attività di verifica e controllo sui Sistemi di Qualità Aziendale in osservanza delle norme UNI EN ISO 9000, è impegnato nell'attività di controllo dei Laboratori Accreditati a fronte della norma UNI CEI EN ISO/IEC 17025 ed è Organismo Notificato per le attività di cui al Decreto Legislativo 9 maggio 2001 n. 269. L'Istituto ricopre il ruolo di Organismo di Certificazione della sicurezza dei sistemi e prodotti informatici commerciali (OCSI), ed è Centro di Valutazione (Ce.Va.) di sistemi e prodotti ICT che trattano dati classificati. Inoltre è Organismo Notificato ai sensi della Direttiva riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione ed è Competent Body ed Organismo Notificato in materia di compatibilità elettromagnetica. Nel 2002 è diventato l'Ente di Certificazione internazionale per conto del TETRA MoU.

La presente pubblicazione è stata realizzata grazie anche al contributo di alcuni esperti dell'Osservatorio per la Sicurezza delle reti e la tutela delle comunicazioni.

L'Osservatorio per la sicurezza delle reti e la tutela delle comunicazioni è presieduto dal Segretario generale del Ministero delle comunicazioni ed è composto da rappresentanti dei ministeri delle Comunicazioni, della Giustizia, dell'Interno, della Difesa, delle Attività Produttive e della Presidenza del Consiglio dei ministri - Dipartimento per la Funzione Pubblica e Dipartimento per l'Innovazione e le Tecnologie, nominati con apposito decreto interministeriale dei Ministri delle comunicazioni, della giustizia e dell'interno.

Tra i compiti dell'osservatorio riportiamo:

a) monitoraggio dello sviluppo tecnologico del settore, con specifico riguardo alla sicurezza

b) collaborazione e consulenza, per gli aspetti tecnologici, alle amministrazioni pubbliche che manifestino l'esigenza di implementare la sicurezza dei propri "punti sensibili"

c) definizione di un "livello minimo" di sicurezza indispensabile per ottenere l'accesso alle reti pubbliche

d) formulazione di suggerimenti per la protezione delle infrastrutture civili relativamente ai temi degli attacchi e dei rischi di tipi elettronico ed elettromagnetico

e) indicazioni circa la certificazione ed elaborazione degli standard di sicurezza dei servizi e delle infrastrutture di telecomunicazioni

f) promozione di azioni di sensibilizzazione con apposite campagne informative.

La presente pubblicazione si inquadra in una serie di attività svolte dal Ministero delle Comunicazioni nel corso del 2004 e relative alla realizzazione di linee guida su:

- LA SICUREZZA DELLE RETI - DALL'ANALISI DEL RISCHIO ALLE STRATEGIE DI PROTEZIONE
- LA SICUREZZA DELLE RETI NELLE INFRASTRUTTURE CRITICHE
- LA QUALITA' DEL SERVIZIO NELLE RETI ICT

Si coglie volentieri l'occasione per ringraziare quanti hanno, con entusiasmo e professionalità, collaborato alla redazione del presente documento:

Stefano AMICI (Enav S.p.A.), Riccardo BIANCONI (SINCERT), Danilo BRUSCHI, Bruno CARBONE (Enav S.p.A), Giancarlo CAROTI (Terna S.p.A. - Rete Elettrica Nazionale), Valentino DI TOMA (Ancitel S.p.A.), Silvio FANTIN (GRTN S.p.A), Giovanni FASSINA (Poste Italiane S.p.A.), Vincenzo GESMUNDO (Selenia Communications S.p.A.), Carlo GUGLIELMINI (Marconi Selenia S.p.A.), Maurizio MAYER (AICT), Giulio MICELI (AICT), Massimo PANICHELLI (Ancitel S.p.A.), Giovanni PATELLA (Ministero delle Comunicazioni), Daniele PERUCCHINI (Fondazione Ugo Bordoni), Armando PERUGINI (C.V. AN (R) Consulente Amm.ne Difesa-TELEDIFE-SE.PRO TE.C. S.A.S), Rodolfo PERUGINO (Poste Italiane S.p.A.), Gian Luca PETRILLO (Consigliere del Ministro delle Comunicazioni), Massimo PICCIRILLI (Ministero delle Comunicazioni), Francesco PIRRO (CNIPA), Gian Luigi PUGNI (Enel Ape s.r.l), Giovanna RICCI (Rete Ferroviaria Italiana S.p.A.), Giovanna SAMOGGIA (Rete Ferroviaria Italiana S.p.A.), Federico

SANDRUCCI (C. Amm. (Aus) Consulente Amm.ne Difesa-TELEDIFE-SE.PRO TE.C. S.A.S), Alberto SARTI (Finmeccanica S.p.A.), Gianluigi SCAZZOLA (Selenia Communications S.p.A.), Stefano SCIASCIA (Reparto Informazioni e Sicurezza - Stato Maggiore della Difesa Ministero della Difesa), Roberto SETOLA (Presidenza del Consiglio dei Ministri-Dipartimento per l'innovazione e le tecnologie-Università CAMPUS Bio - Medico di Roma), Luigi TAGLIAPIETRA (Siosistemi S.p.A), Guido TRIPALDI (I.NET S.p.A.), Riccardo VALASTRO (Poste Italiane S.p.A.).

Si ringraziano ancora, per il loro apporto e i loro suggerimenti:

Pierpaolo ARGIOLAS (Rete Ferroviaria Italiana S.p.A.), Diego BISCI (Terna S.p.A. - Rete Elettrica Nazionale), Maurizio BONANNI (Ministero delle Comunicazioni), Davide BRACCINI (Consorzio ABI Lab), Giuseppe CAPORELLO (Agenzia delle Entrate - Dir. Centr. Audit e Sicurez.), Marco CARBONELLI (Fondazione "Ugo Bordoni"), Mario CICLOSI (Ministero dell'Interno), Mario Carlo DI GIORGIO (Ministero dell'Economia e delle Finanze), Antonio GRUPPINO (Rete Ferroviaria Italiana S.p.A.), Salvatore LEOTTA (Electronic Data Systems Italia S.p.A.), Alessandro LORENZINI (CommScope Solutions Italy S.r.l.), Stefano LUBERTI (Enel Holding S.p.A.), Mariano LUPO (Ministero Economia e Finanze-DPF/UTI Reparto V - Normativa Tecnica), Renato MAREGA (Nergal S.r.l.), Antonio MENGHINI (Electronic Data Systems Italia S.p.A.), Stefano Aurelio MOLINARI (Selenia Communications S.p.A.), Claudio PETRICCA (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione), Gianfranco PONTEVOLPE (CNIPA), Luciano PUCCI (Ministero dell'Interno), Michele RINALDI (Ministero dell'Economia e delle Finanze - Dipartimento per le Politiche Fiscali), Mauro SARTI (Anixter S.r.l.),

Romano STASI (Consorzio ABI Lab), Maurizio TALAMO (Università degli Studi di Roma "Tor Vergata"), Mario TERRANOVA (CNIPA), Paola TOGNETTI (Ministero dell'Economia e delle Finanze - Dipartimento per le Politiche Fiscali), Salvatore TURANO (Ancitel S.p.A.), Raffaele VISCIANO (Ministero dell'Economia e delle Finanze-Dipartimento per le Politiche Fiscali).

Roma, marzo 2005

Il Direttore
dell'Istituto Superiore delle Comunicazioni
e delle Tecnologie dell'Informazione

Ing. Luisa Franchina

Guida alla lettura

Questo documento rappresenta la sintesi del lavoro svolto dal gruppo "Infrastrutture Critiche" cui hanno partecipato esponenti delle diverse istituzioni pubbliche insieme con rappresentanti dei principali operatori di infrastrutture critiche operanti in Italia e di società impegnate nel settore della sicurezza delle reti di telecomunicazioni.

Il gruppo di lavoro nasceva dalla necessità di analizzare le implicazioni sulla continuità di esercizio e sulla sicurezza delle infrastrutture critiche rispetto al mutato contesto socio-economico e tecnologico che ha visto crescere l'importanza e la crucialità delle infrastrutture di telecomunicazione nei confronti di tutte le infrastrutture critiche nazionali. Questo si riflette in un crescente livello di interdipendenza fra le diverse infrastrutture, in gran parte dovuto alla diffusione delle tecnologie ICT. Inoltre occorre rilevare un aumento delle minacce che affliggono le infrastrutture sia legate a fenomeni naturali che ad azioni delittuose, ed in special modo terroristiche.

Queste motivazioni, come illustrato nel primo capitolo, hanno portato alla nascita di specifiche iniziative, sia a livello Nazionale che Europeo, tese ad innalzare il livello globale di sicurezza delle infrastrutture critiche e che genericamente sono indicate come strategie di Protezione delle Infrastrutture Critiche.

Il successivo capitolo delinea il nuovo scenario architetturale che caratterizza le infrastrutturale nazionali evidenziando gli elementi di interdipendenza e le minacce che affliggono gli elementi da considerare per una corretta gestione degli aspetti di sicurezza e continuità di servizio di tali infrastrutture.

Il capitolo terzo analizza in maggior dettaglio, in un ottica di Best Practice o Buone Regole, gli aspetti connessi con la necessità di proteggere le reti di comunicazione, non solo per la loro importanza intrinseca, ma perché il loro corretto funzionamento è indispensabile per garantire che le altre infrastrutture critiche eroghino i propri servizi.

In quest'ottica vengono analizzati gli aspetti peculiari che caratterizzano le reti di comunicazione che sono utilizzate per il supporto delle infrastrutture critiche nazionali evidenziando l'importanza delle diverse componenti che costituiscono queste infrastrutture di comunicazione. Un paragrafo specifico è dedicato agli aspetti di certificazione della sicurezza e alla sua importanza per aumentare la fiducia degli utenti sui livelli di sicurezza garantibili.

La sicurezza d queste infrastrutture non può ricondursi, ovviamente a meri aspetti tecnologici (che pure rivestono un ruolo non trascurabile), ma occorre prevedere un'opportuna organizzazione in grado di gestire efficacemente ed efficientemente le situazioni di crisi ed un'adeguata formazione di tutto il personale coinvolto a vario titolo nella gestione ed utilizzo di queste infrastrutture.

Esistono, inoltre, diverse attività di R&S tese ad individuare soluzioni tecnologiche che possono meglio adattarsi al mutato contesto infrastrutturale.

Il capitolo quattro riporta le principali conclusioni del lavoro svolto.

Completano il volume alcune appendici di cui una dedicata ai diversi standard di riferimento ed ai riferimenti normativi, una seconda nella quale sono descritte in dettaglio le linee guida che hanno portato alla stesura di un business continuity plan di un importante operatore di infrastrutture critiche ed, infine, un questionario di auto valutazione che può essere di ausilio ai responsabili delle diverse infrastrutture per effettuare una prima analisi del proprio livello di sicurezza rispetto a vulnerabilità connesse con l'utilizzo di infrastrutture di telecomunicazione.

LA SICUREZZA DELLE RETI NELLE INFRASTRUTTURE CRITICHE

1 - Generalità

1.1 INTRODUZIONE

Lo sviluppo e l'organizzazione dei Paesi industrializzati si fondano su un sistema di infrastrutture sempre più complesse e articolate: le **Infrastrutture Critiche Nazionali** (*Critical National Infrastructures, o CNI*) definite come quelle infrastrutture, pubbliche o private, la cui corretta operatività è vitale per il funzionamento e la sicurezza di un Paese.

Si tratta di infrastrutture che presidiano i fondamentali settori delle società moderne quali: la Sanità, l'Economia, l'Energia, i Trasporti, le Telecomunicazioni, l'Ordine Pubblico, la Difesa e in generale tutti i Settori della Pubblica Amministrazione.

Tali infrastrutture possono essere soggette ad eventi critici di varia natura in grado di comprometterne direttamente od indirettamente l'efficienza. Gli eventi critici sono, in prima approssimazione, riconducibili ad attacchi intenzionali o a disastri naturali.

Per il loro funzionamento, le CNI si basano sempre di più su infrastrutture di telecomunicazione (CII - *Critical Information Infrastructure*). Tali reti devono permettere l'operatività della CNI in normali condizioni di funzionamento, ma anche e soprattutto garantire un'adeguata capacità operativa in caso di eventi critici.

Si noti che gli eventi critici possono riguardare non solo la CNI, ma anche direttamente la relativa infrastruttura di telecomunica-

zione. Inoltre sia le CNI sia le CII possono essere soggette a guasti, anche in assenza di eventi esterni.

In questo contesto si parlerà di Infrastrutture Critiche Informatizzate (CII) come quelle Infrastrutture Critiche Nazionali che per il loro monitoraggio, controllo e gestione utilizzano, in tutto o in parte, una o più infrastrutture informatiche[1].

Tali infrastrutture informatiche devono non solo permettere l'operatività della CNI in normali condizioni di esercizio, ma anche e soprattutto garantire un'adeguata capacità operativa in caso di emergenza, ovvero all'occorrenza di eventi critici.

Non va neppure sottovalutato l'elevato grado di interdipendenza che molte Infrastrutture Critiche hanno tra loro. Infatti, ad un primissimo livello di dettaglio, è possibile raffigurare gerarchicamente l'interdipendenza tra i diversi settori come segue (*Fig. 1*):

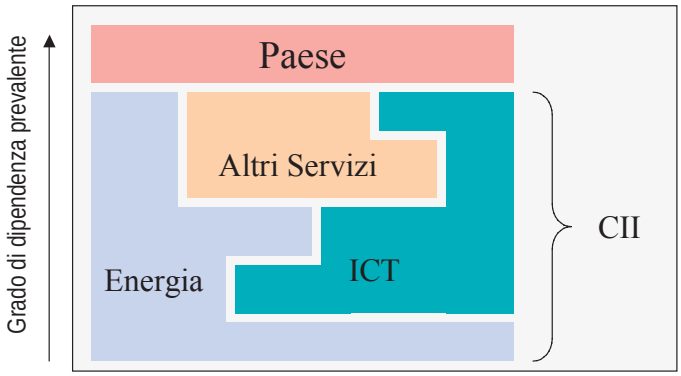


Figura 1: Interdipendenza tra i diversi settori delle CNI/CII

Si osservi che in testa alla gerarchia, vi è il "Paese": il corretto svolgersi e svilupparsi della vita sociale ed economica di una Nazione

[1] *In letteratura l'acronimo CII è utilizzato anche nell'accezione di "Infrastruttura Informatica Critica", dando una enfasi maggiore agli aspetti di protezione specifici del cyberspace e di Internet in particolare.*

dipenda fortemente dal grado di qualità di alcuni servizi essenziali sottostanti. Nella sua massima schematizzazione, i pilastri portanti sono l'Energia e le Telecomunicazioni (e l'Informatica correlata), nonché i servizi "a valore aggiunto" come la Sanità, la Protezione Civile, ecc. che comunque poggiano sui primi due.

L'Energia è, per definizione, l'elemento senza il quale nulla può svolgere un lavoro. Dalla corretta produzione, trasmissione e distribuzione dell'energia dipende quindi qualsiasi servizio avanzato.

Le Telecomunicazioni e l'Informatica sono l'elemento senza il quale non è possibile trasferire segnali, dati, informazioni, ovvero consentire il corretto coordinamento di risorse (umane o tecnologiche) locali e remote.

Energia e Telecomunicazioni sono però tra di loro fortemente interdipendenti: senza un'adeguata e costante alimentazione le apparecchiature che espletano i servizi telematici non possono operare, e le stesse strutture di produzione, trasmissione e distribuzione dell'energia possono operare solo in virtù dell'esistenza di sistemi di comunicazione correttamente funzionanti tra i diversi impianti.

In particolare, questo documento si occupa di fornire una prima serie di proposte riguardanti le criticità legate all'interdipendenza tra le CNI tradizionali con le infrastrutture di Telecomunicazione, comprendendo in queste le reti informatiche e di telecomunicazioni in senso stretto.

Il fine del documento è di fornire alle CNI le indicazioni basilari su come strutturare adeguatamente il proprio sistema di comunicazione, in modo da garantire la necessaria efficacia anche a fronte di situazioni d'emergenza.

1.2 CNI E CII: INTERDIPENDENZA E PROTEZIONE

Le CNI, nonostante le specificità derivanti dalle loro diverse funzioni, mostrano una serie di caratteristiche comuni:

- **Sono infrastrutture distribuite capillarmente su tutto il territorio**

- *Elevata visibilità*
- *Difficoltà di presidio di tutte le installazioni*
- *Potenziali problemi di coordinamento e intercomunicazione*

- **Hanno una missione di servizio pubblico**
  - *Requisiti stringenti di disponibilità e affidabilità*
  - *Caratteristiche di rapido intervento e ripristino a fronte di crisi*
  - *Infrastrutture con requisiti di massima robustezza e sicurezza*
  - *Potenziali ricadute sulla pubblica sicurezza della popolazione*
- **Devono avere interoperabilità con utenti/clienti esterni, pubblici e privati**
  - *Elevato rischio di intrusione*
  - *Necessità di punti d'accesso controllati e sicuri per comunicazioni multi-protocollo*
  - *Importanti conseguenze economiche di un guasto/sabotaggio*

Fra le infrastrutture identificate come critiche per una nazione si annoverano:

- Le reti per la trasmissione e la distribuzione dell'Energia (elettrica, gas, ecc.)
- Le reti di telecomunicazioni
- I trasporti (merci e passeggeri)
- I servizi di emergenza
- Le infrastrutture a servizio della Difesa
- I circuiti bancari e finanziari
- Il sistema sanitario nazionale
- I sistemi per il trasporto, distribuzione e trattamento delle acque
- I media ed il settore dell'informazione pubblica
- Le filiere agro-alimentari
- Le reti governative

Diversi sono gli eventi che possono condizionare in parte o globalmente l'efficienza delle infrastrutture del singolo Paese o di più Paesi: eventi naturali (alluvioni, terremoti, eruzioni vulcaniche), eventi causati da azioni umane volontarie (terrorismo, cyber-crime) o involontarie (errori, omissioni), eventi legati all'ambiente (inquinamento, agenti chimici, incendi), eventi legati al non corretto funzionamento di componenti infrastrutturali (rottura di un macchinario, bug nel software, ecc.).

Il recente rapporto del governo Canadese sulla sicurezza delle proprie CNI [8] evidenzia che lo scenario previsto per i prossimi anni è caratterizzato da un forte incremento delle minacce associate ad eventi naturali (dovuti alla estremizzazione dei fenomeni climatici) e ad azioni delittuose (legate all'attuale scenario socio-politico ed in particolare alla minaccia terroristica).

Quest'ultimo elemento è legato ad una serie di cause indipendenti ma, purtroppo, concomitanti. Da un lato, infatti, la maggiore diffusione ed importanza delle tecnologie informatiche a tutti i livelli di gestione e controllo delle CNI induce su di esse la possibilità che eventi delittuosi possano configurarsi, oltre che nelle tradizionali forme, anche tramite i canali propri del cyberspace. Ciò comporta per le CNI la necessità di considerare, parallelamente alle minacce "tradizionali" di natura fisica, anche quelle che potrebbero essere indotte, in maniera diretta o indiretta, dall'utilizzo delle tecnologie proprie della società dell'Informazione.

Parimenti occorre considerare l'accresciuta minaccia terroristica, che potrebbe individuare in azioni contro le CNI il mezzo per creare panico e sfiducia nelle popolazioni dei diversi paesi. Azioni che potrebbero anche essere solo di "supporto" ad altre tipologie di misfatti al fine di amplificarne le conseguenze e/o rallentare le operazioni di soccorso e ripristino e, quindi, ingigantirne l'effetto mediatico.

Parallelamente alle minacce occorre considerare, come evidenziato nel documento "La Protezione delle Infrastrutture Critiche Informatizzate - La realtà italiana"[2], che lo scenario architetturale che

[2] *Elaborato nel marzo del 2004 dal gruppo di lavoro istituito presso il Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri*

caratterizza le CNI sta rapidamente e profondamente cambiando.

Infatti *"Fino ad un decennio fa, ognuna di queste infrastrutture poteva considerarsi come un sistema autonomo sostanzialmente indipendente, gestito da operatori verticalmente integrati. Per una serie di ragioni tale struttura si è profondamente modificata al punto che sempre di più le varie infrastrutture tendono a essere interdipendenti, soprattutto a causa della condivisione del cosiddetto cyberspace, ovvero lo spazio virtuale prodotto dall'interconnessione di calcolatori, sistemi di telecomunicazioni, applicazioni e dati. Ciò comporta che un guasto (di natura accidentale o dolosa) in una di tali infrastrutture può facilmente propagarsi, con un effetto domino, ad altre infrastrutture amplificando i suoi effetti e provocando disfunzioni e malfunzionamenti anche ad utenti remoti, sia dal punto di vista geografico che funzionale, rispetto al punto ove si è verificato il guasto iniziale"*. [1]

Il black-out che ha afflitto buona parte della costa nord-orientale degli Stati Uniti nell'agosto del 2003 è un evidente esempio di come un guasto ad alcuni moduli del sistema informatico di controllo di una società di distribuzione, unito ad altri eventi fortuiti, possa indurre la quasi totale paralisi di tutte le infrastrutture esistenti nell'area provocando danni dell'ordine di miliardi di dollari.

Questo anche in considerazione del fatto che, soprattutto in seguito alla diffusione delle tecnologie proprie della Società dell'Informazione, le Infrastrutture Critiche hanno sviluppato una crescente interdipendenza per cui azioni svolte in un settore possono avere immediate ripercussioni in tutti gli altri. In particolare eventi naturali o azioni delittuose che colpiscano una CNI comportano una moltiplicazione ed amplificazione degli effetti per cui anche eventi di limitata entità possono produrre un impatto notevole e geograficamente non circoscritto.

L'attuale scenario è caratterizzato, pertanto, sia da accresciute e differenziate minacce nei confronti delle CNI sia da un mutato contesto infrastrutturale che induce, a causa delle interdipendenze esistenti, nuove tipologie di vulnerabilità. Ciò impone una maggiore e diversa attenzione a tutti gli aspetti di protezione, sicurezza e robustezza sia specificatamente per ogni singola CNI, che complessivamente ed unitariamente per l'insieme delle CNI nazionali.

In tale scenario infrastrutturale sono inoltre in atto profondi cambiamenti che spingono le diverse infrastrutture ad erogare servizi

innovativi con livelli di qualità estremamente elevati ed al tempo stesso impongono stringenti vincoli sulle caratteristiche di efficienza ed economicità delle stesse. Ciò richiede uno sfruttamento ottimale delle diverse infrastrutture tecnologiche del paese che può essere ottenuto solo mediante una massiccia adozione di sofisticati sistemi automatici di controllo e, più in generale, un ricorso alle tecnologie proprie del ICT.

Per comprendere meglio il ruolo cruciale che rivestono gli aspetti connessi con la sicurezza informatica e delle comunicazioni nell'ambito della protezione delle infrastrutture critiche è utile rifarsi ad una schematizzazione quale quella riportata in *Fig. 2*. Ogni CNI può essere descritta come una struttura complessa articolata su più livelli: livello fisico, livello *cyber*, livello organizzativo e livello strategico. Esistono, all'interno di ciascuna CNI, legami funzionali fra i diversi livelli e parimenti esistono legami di dipendenza ed interdipendenza fra

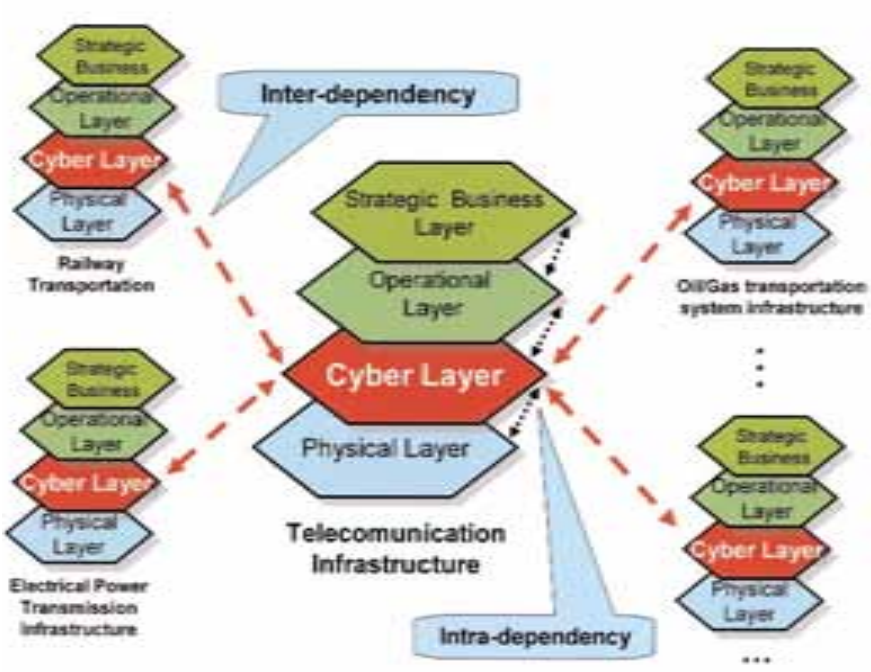


Figura 2: Modello infrastrutturale a più layer, sviluppato da ENEA nell'ambito del progetto europeo Safeguard

le componenti dei livelli omologhi appartenenti a CNI diverse.

La diffusione delle tecnologie ICT, ha fatto crescere in modo esponenziale l'importanza del cyber-layer all'interno delle singole infrastrutture e le interdipendenze fra le diverse infrastrutture a questo stesso livello.

Si precisa che in questo contesto, il termine cyber-layer non coincide con il sistema informatico aziendale, ma indica la parte di questo che è deputata alla gestione e al controllo del layer fisico dell'infrastruttura.

In quest'ottica, come evidenziato nella *Fig. 3*, nell'ambito del più ampio problema della protezione delle infrastrutture critiche (**Critical Infrastructure Protection** - **CIP**) la protezione di questo livello di "Controllo e Supervisione" è ciò che comunemente viene indicato come Protezione delle Infrastrutture Critiche Informatizzate (**Critical Information Infrastrucure Protection** - **CIIP**)

*Nell'ambito delle strategie di difesa delle Infrastrutture Critiche Nazionali (**CIP** – Critical Infrastructure Protection), le **CIIP** né rappresentano un elemento centrale e di crescente importanza*

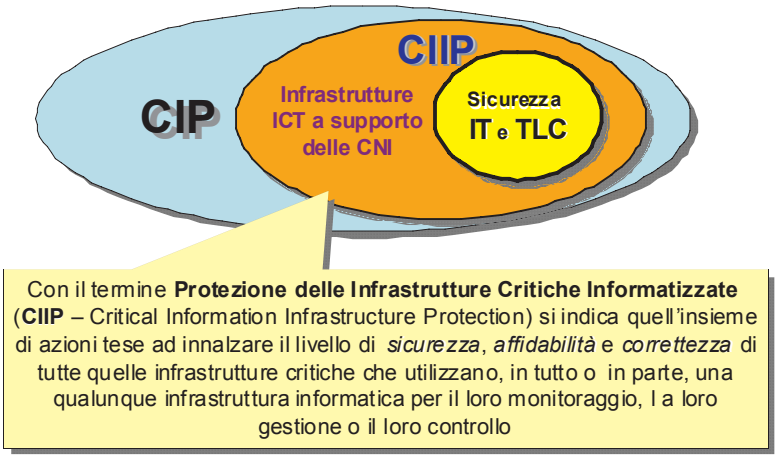


Figura 3: Ambito di definizione delle CIP e delle CIIP [CiSP]

Per cui, riprendendo la definizione formulata in [1] si ha che la **Protezione delle Infrastrutture Critiche Informatizzate** è l'insieme di azioni tese ad innalzare il livello di sicurezza, affidabilità e disponibilità di tutte quelle infrastrutture critiche che utilizzano, in tutto o in parte, una qualunque infrastruttura informatica per il loro monitoraggio, la loro gestione o il loro controllo.

Tali iniziative non sono circoscritte alla sola sicurezza informatica del cyber-layer, ma coprono tutti gli aspetti connessi con la continuità e correttezza di servizio.

1.3 SCOPO DEL DOCUMENTO E ATTIVITA' DEL GRUPPO DI LAVORO

Questo Rapporto nasce quale sintesi del lavoro svolto dal marzo 2004 da un Gruppo di Lavoro costituito in seno al Ministero delle Comunicazioni.

In particolare il Gruppo di Lavoro, composto da rappresentanti dei principali dicasteri coinvolti insieme con rappresentanti di alcuni dei principali operatori di CNI italiane e di società specializzate nel settore, ha focalizzato la propria attenzione sul ruolo che svolgono le infrastrutture di Telecomunicazione per quel che concerne la sicurezza e la continuità di servizio all'interno delle CNI.

Il Gruppo di Lavoro, mettendo a frutto le diverse esperienze dei componenti, ha cercato di coagulare le esigenze e le possibili soluzioni, al fine di fornire ai gestori di CNI quelle linee guida, o "best practice", che possano indirizzare verso un migliore e più consapevole uso dei sistemi di comunicazione necessari e disponibili.

Il Gruppo di Lavoro ha analizzato i seguenti aspetti:

- la Qualità del Servizio e la Sicurezza nelle Reti di Telecomunicazione tenendo anche in considerazione gli Standard e le Normative di Riferimento Nazionali ed Internazionali
- le problematiche indotte dalla presenza di interdipendenze fra le CNI e fra queste e le infrastrutture di telecomunicazioni

- l'individuazione delle principali minacce alle infrastrutture di telecomunicazione utilizzate dalle CNI
- l'individuazione di un insieme minimo di parametri per la sicurezza in grado di qualificare il livello di sicurezza di un infrastrutture di telecomunicazione che operi a supporto di una CNI
- l'individuazione di alcuni parametri tecnici minimi che garantiscano i livelli di Qualità del Servizio (QoS) adeguati a garantire la minima criticità
- l'individuazione di alcuni parametri tecnici, di elementi di trasparenza e di termini legali che è consigliabile adottare nelle relazioni contrattuali commerciali e nei Service Level Agreement (SLA) siglati con i Fornitori di servizi di telecomunicazioni
- la descrizione del ruolo potenziale che possono svolgere le Istituzioni nell'individuazione e realizzazione di strategie comuni di protezione
- alcune proposte di autoverifica sull'attuale livello di criticità ed organizzazione pertinente all'interno della propria CNI.

Non sono state invece contemplate:

- le problematiche inerenti le componenti critiche ma non informatizzate e non coinvolte nelle attività di telecomunicazione, peculiari per ciascuna CNI (come ad esempio le infrastrutture di distribuzione ed erogazione idrica, del gas) bloccanti in caso di guasto o attacco
- l'aspetto di sicurezza delle Piattaforme e degli Applicativi Gestionali utilizzati dalle Società proprietarie di CNI ma non direttamente legati alla gestione delle componenti critiche (es. ERP, paghe e stipendi, data base, ecc.).

1.4 INIZIATIVE IN ATTO A LIVELLO INTERNAZIONALE PER LA PROTEZIONE DELLE CII

I primi studi sulle problematiche di sicurezza e continuità di servizio per le infrastrutture critiche informatizzate furono avviati negli anni '90.

Gli Stati Uniti furono i primi a formalizzare azioni a livello governativo sul tema che si concretizzarono nel 1998 nella emanazione della Presidential Decision Directive 62 e 63.

Da allora molti altri paesi industrializzati hanno sviluppato azioni tese a:

- comprendere gli elementi di criticità e vulnerabilità delle diverse infrastrutture critiche presenti nel paese, evidenziandone le criticità
- definire strategie per mitigare tali vulnerabilità
- sensibilizzare i diversi operatori sul problema della protezione delle infrastrutture critiche
- predisporre piani di emergenza e di recupero da attivare in presenza di eventi negativi interessanti una o più infrastrutture critiche
- favorire lo sviluppo di tecnologie intrinsecamente sicure
- supportare la cooperazione internazionale.

Il tema della protezione delle Infrastrutture Critiche Informatizzate, vista la sua natura transnazionale, è stato di recente posto all'attenzione di diversi organismi internazionali.

Nel marzo 2003 si è svolta a Parigi la prima riunione degli esperti dei paesi del **G8** sul problema della CIIP nell'ambito della quale sono stati delineati i principi che dovrebbero ispirare le politiche dei diversi paesi al fine di accrescere il livello di protezione.

Il G8 al fine di favorire la cooperazione internazionale, anche a vantaggio di paesi non membri, ha predisposto un International CIIP Directory con l'indicazione delle strutture e dei punti di contatto esi-

stenti in ognuno dei paesi membri sulle diverse tematiche proprie delle CIIP.

La **Commissione Europea** attualmente si occupa delle problematiche attinenti alla ricerca nel campo della protezione delle Infrastrutture Critiche all'interno del Sesto Programma Quadro, nella priorità IST (Information Society Technologies) e nella *Preparatory Action on Security Research*.

Sesto Programma Quadro

Uno dei tre settori tecnologici principali evidenziati dalla Commissione Europea in ambito IST è *infrastrutture per le comunicazioni mobili, senza fili, ottiche e a larga banda nonché tecnologie software ed informatiche* che siano affidabili, capillari, interoperabili e adattabili alle nuove applicazioni e ai nuovi servizi.

Nella Priorità IST è stato indicato come uno degli obiettivi strategici quello di orientare la ricerca *"verso un quadro globale di affidabilità e sicurezza"*.

La Commissione si propone, tra l'altro, lo sviluppo di strumenti di ausilio al processo decisionale destinati a proteggere le infrastrutture critiche, a prevenire le minacce e a ridurre le vulnerabilità tenendo conto dell'interdipendenza dalle tecnologie dell'informazione e della comunicazione (ICT).

Già nel Quinto Programma Quadro, sempre all'interno della priorità IST, la Commissione Europea aveva trattato con attenzione le problematiche di ricerca legate alle infrastrutture critiche.

Il risultato dell'attività è stata la **European Dependability Iniziative** (**DEPPY** - http://deppy.jrc.it/default/). DEPPY ha lanciato una serie di progetti di ricerca e sviluppo sulla "dependability" dei sistemi e servizi per la Società dell'Informazione e, più recentemente, sull'analisi del rischio e delle vulnerabilità delle infrastrutture di comunicazione ed informazione nonché sulle loro interdipendenze con altre infrastrutture critiche; ha inoltre promosso la cooperazione internazionale con l'istituzione della **EU-US Joint Task Force on R&D on CIP**.

Ulteriori iniziative significative sono rappresentate dai proget-

ti DDSI (http://www.ddsi.org/DDSI-F/main-fs.htm) e ACIP (www.iabg.de/acip/index.html) che hanno contribuito a definire le priorità della ricerca sulla sicurezza e la dependability delle grandi infrastrutture informatiche.

Di particolare interesse le co-ordinated action SecurIST e CI2RCO che hanno quale obiettivo l'individuazione delle tematiche di ricerca nel campo della sicurezza dei sistemi informatici e delle infrastrutture.

Preparatory Action on Security Research

Nel 2004 la Commissione, incoraggiata dal Parlamento europeo, dal Consiglio e dall'industria ha varato un'azione preparatoria nel campo della ricerca in materia di sicurezza al fine di istituire un programma globale dopo il 2007.

L'azione preparatoria rappresenta un contributo della Commissione alla più ampia agenda dell'Unione su come affrontare le sfide e le minacce per l'Europa ed è illustrata tra l'altro nella Strategia Europea per la Sicurezza approvata nel dicembre 2003 dal Consiglio europeo.

La Commissione Europea ha individuato cinque "missioni" relative alla protezione nei confronti di attentati di stampo terroristico, una delle quali è incentrata sulla ricerca nel campo delle infrastrutture critiche.

Il nome della missione è **"Ottimizzare la sicurezza e la protezione dei sistemi collegati in rete"** ed il suo obiettivo è quello di analizzare, sotto il profilo della sicurezza d'uso, sistemi presenti e futuri collegati in rete, quali sistemi di comunicazione, sistemi di pubblica utilità, infrastrutture di trasporto, reti (anche elettroniche) per il commercio e gli affari, esaminandone i punti vulnerabili e le interdipendenze per evidenziare le modalità di realizzazione di misure di sicurezza contro le minacce sia elettroniche che fisiche.

Le priorità all'interno di questa missione sono le seguenti:

- Sviluppo di metodologie e strumenti di decisione standardizzati per valutare la natura delle minacce potenziali e determinare i punti vulnerabili

- Dimostrazione di misure per migliorare la protezione e la sicurezza di elementi critici per le infrastrutture pubbliche, private e governative nell'Europa allargata
- Sviluppo di capacità di rilevamento, prevenzione, risposta e allarme per rafforzare i sistemi d'informazione e di controllo, integrando l'uso di sistemi spaziali e di sistemi terrestri fissi e senza fili.

A livello politico e regolamentare, la Commissione ha iniziato, a partire dal 2001, a definire un approccio europeo alla sicurezza delle reti e dell'informazione che ha portato alla costituzione, nel novembre 2003, della **European Network & Information Security Agency** (**ENISA**).

ENISA

L'Agenzia ha l'obiettivo di contribuire ad assicurare un elevato livello di sicurezza delle reti dell'informazione della Comunità e a sviluppare una cultura in materia di sicurezza delle reti e dell'informazione responsabilizzando e coinvolgendo tutti gli attori - settori economici ed industriali, fornitori di servizi di connettività, pubblica amministrazione - nell'adottare tecnologie, standard e buone pratiche di sicurezza.

A livello operativo, la Commissione ha promosso il piano d'azione **eEurope 2005** *(*http://europa.eu.int/information_society/eeurope/2005/index_en.htm*)*; tale piano, che subentra al piano d'azione eEurope 2002, si articola in due categorie di interventi che si rafforzano a vicenda: da una parte, stimolare servizi, applicazioni e contenuti sia per i servizi pubblici online che per l'e-business; dall'altra, sostenere la creazione di un'infrastruttura di base a banda larga e considerare attentamente gli aspetti legati alla sicurezza.

NATO

La **NATO** fin dal 1997 ha analizzato il problema della

Protezione delle Infrastrutture Critiche nell'ambito di *Information Operation* (*IO*). Il tema è stato di recente esaminato anche in relazione agli aspetti di Protezione Civile da un lato e di terrorismo dall'altro ed è stata attivata una road-map il cui scopo è favorire una migliore comprensione del problema e l'attivazione di adeguate iniziative di formazione, cooperazione internazionale e attività di ricerca e sviluppo (R&S).

ONU

Le **Nazioni Unite** (**ONU**) hanno più volte sottolineato l'importanza di attuare politiche tese a migliorare la sicurezza delle infrastrutture informatiche.

Il tema specifico della protezione delle infrastrutture critiche è stato trattato dalla 78ma Assemblea Generale che nel dicembre 2003 ha adottato la risoluzione n.58 **Creation of global culture of cybersecurity and the protection of critical information infrastructures.**

La risoluzione, nel riconoscere che le infrastrutture critiche sono sempre più interdipendenti anche a causa del crescente ricorso alle infrastrutture informatiche, evidenzia come ciò si può tradurre in una maggiore vulnerabilità dell'intero sistema e, quindi, nella necessità di mettere in atto azioni tese a ridurre le vulnerabilità e le minacce, a minimizzare i possibili danni e a favorire le azioni di ripristino, anche intervenendo sulla formazione e preparazione del personale. In particolare, la risoluzione invita gli stati membri a tenere in conto, nella definizione delle proprie strategie, degli "Elements for protecting critical information infrastructures" riportati in allegato alla risoluzione stessa e che ricalcano, nella sostanza, i principi elaborati nel marzo 2003 dal G8.

Documenti dell'OCSE e delle Nazioni Unite

I documenti dell'Organizzazione per la cooperazione e lo Sviluppo Economico (OECD in inglese, OCDE in francese) costituiscono, anche per il credito di cui godono presso gli organi normativi

dell'UE, una fonte di riferimento di elevato valore sul piano sociale ed etico.

Rilevante è la Raccomandazione del Consiglio in data 25 luglio 2002, intitolata ***"Linee Guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione: verso una cultura della sicurezza"*** di cui si riassume di seguito il contenuto.

Sotto il comune denominatore della promozione della cultura della sicurezza si enunciano nove principi:

1. **Sensibilizzazione** - Le parti interessate devono essere consapevoli della necessità di tutelare la **sicurezza dei sistemi e delle reti d'informazione** e delle azioni che possono intraprendere per rafforzare la sicurezza.
2. **Responsabilità** - Le parti interessate sono responsabili della **sicurezza dei sistemi e delle reti d'informazione**.
3. **Risposta** - Le parti interessate devono operare tempestivamente e in uno spirito di cooperazione per prevenire, rilevare e rispondere agli incidenti di sicurezza.
4. **Etica** - Le parti interessate devono rispettare i legittimi interessi delle altre parti.
5. **Democrazia** - La **sicurezza dei sistemi e delle reti d'informazione** deve essere compatibile con i valori fondamentali di una società democratica.
6. **Valutazione dei rischi** - Le parti interessate devono procedere a valutazioni dei rischi.
7. **Concezione e applicazione della sicurezza** - Le parti interessate devono integrare la sicurezza quale elemento essenziale dei **sistemi e delle reti d'informazione**.
8. **Gestione della sicurezza** - Le parti interessate devono adottare un approccio globale della gestione della sicurezza.
9. **Rivalutazione della sicurezza** - Le parti interessate devono esaminare e rivalutare la sicurezza dei sistemi e delle reti d'informazione e introdurre adeguate modifiche nelle loro politiche, pratiche, azioni e procedure di sicurezza.

Sulla stessa linea del documento dell'OCSE è la risoluzione delle Nazioni Unite A/RES/58/199 del 23.12.2003 intitolata "Creation of a global culture of cyber-security and the protection of critical information infrastructures".

La risoluzione invita gli stati membri a considerare undici principi di sicurezza, ampiamente basati su quelli adottati dal G8 nel marzo del 2003.

La tabella 1, redatta dal NISCC (National Infrastructure Security Coordination Centre), indica i principi indicati dalla risoluzione N.U. con i riferimenti a quelli proposti nel documento OCSE in precedenza indicati. Come si può notare, rispetto al documento OCSE, ampiamente orientato alla società, agli operatori e agli utenti (principi 2, 4 e 5), la risoluzione delle Nazioni Unite appare più specificamente rivolta ai Governi e alle forze dell'ordine (principi 6, 7 e 9).

Direttive e altri documenti UE

Negli ultimi anni il Governo italiano non ha mancato di attuare con lodevole tempestività le direttive UE in materia di reti e sicurezza informatica. Notevole è la risoluzione del Consiglio (Trasporti/Telecomunicazioni) in data 11 dicembre 2001 *"Resolution on network and information security"*. Nel documento si richiede ai paesi membri, per la fine del 2002, di:

- promuovere la cultura della sicurezza con **campagne educative** presso amministrazioni, aziende private, ISP ecc.
- promuovere **best practice** di sicurezza basate su standard internazionali anche e soprattutto presso aziende medie e piccole
- promuovere la **sicurezza nei corsi di informatica**
- potenziare i **computer emergency response team**
- promuovere la conoscenza e l'adozione dello **standard di sicurezza Common Criteria** (CC) recepito nella norma ISO-15408
- promuovere lo studio e l'adozione di **dispositivi biometrici**

Argomenti	Principi della risoluzione UN 58/199	Riferimento ai principi OCSE
Avvisi e reazione agli incidenti	1. Disporre di strutture sulla rete per fornire avvisi circa le vulnerabilità informatiche, le minacce e gli incidenti.	3. Risposta
	5. Realizzare e mantenere reti di comunicazioni per situazioni di crisi, collaudandole periodicamente per assicurarne l'efficienza nei momenti d'emergenza.	
Promozione della consapevolezza e formazione	2. Promuovere la consapevolezza per agevolare la comprensione, da parte di tutte le parti coinvolte, dell'estensione e della natura delle proprie infrastrutture informatiche critiche e del ruolo che ciascuna parte ha nella protezione delle stesse.	1. Sensibilizzazione
	8. Condurre attività formativa ed esercitazioni per aumentare il grado di reattività e collaudare piani di continuità e di crisi in caso di attacchi alle infrastrutture informatiche, incoraggiando i corrispondenti ad effettuare analoghe attività.	
Analisi del rischio	3. Esaminare le infrastrutture e identificare le loro interdipendenze, in modo da incrementare il loro grado di protezione.	6. Valutazione dei rischi
		8. Gestione della sicurezza
		9. Rivalutazione della sicurezza
Tecnologia della sicurezza	11. Promuovere ricerche e sviluppi nazionali e internazionali e favorire l'applicazione di tecnologie di sicurezza coerenti con gli standard internazionali.	7. Concezione e applicazione della sicurezza
	4. Promuovere la collaborazione tra le diverse parti, sia pubbliche che private, per condividere e analizzare le informazioni relative alle infrastrutture critiche al fine di prevenire, investigare, reagire relativamente ad attacchi e danni concernenti tali infrastrutture.	
Condivisione delle informazioni e collaborazione internazionale	10. Impegnarsi in idonee collaborazioni internazionali al fine di porre in sicurezza sistemi informatici critici, anche tramite lo sviluppo e il coordinamento di sistemi di avviso e allarme, disseminazione e condivisione di informazioni riguardanti vulnerabilità, minacce e incidenti e coordinando attività investigative relative ad attacchi a tali sistemi informatici, in accordo con le leggi locali.	3. Risposta
Aspetti legali e di investigazione criminale	9. Avere leggi adeguate nella forma e nella sostanza e personale adeguatamente formato per consentire agli Stati di investigare e perseguire attacchi ai sistemi informatici critici e coordinare tali attività, quando del caso, con gli altri Stati.	
	6. Assicurare che le norme relative alla disponibilità dei dati tengano in considerazione l'esigenza di proteggere i sistemi informatici critici.	
	7. Facilitare il tracciamento degli attacchi ai sistemi informatici critici e, quando appropriato, la comunicazione delle informazioni relative a tali tracciamenti agli altri Stati.	
Considerazioni sociali e politiche		2. Responsabilità
		4. Etica
		5. Democrazia

Tabella 1: Confronto tra il documento OCSE e la Risoluzione delle Nazioni Unite

- promuovere lo scambio d'informazioni e **cooperazione tra paesi membri**.

Molto interessante anche la Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni del giugno 2001 intitolata ***"Sicurezza delle reti e sicurezza dell'informazione: proposte di un approccio strategico europeo"***.

In questo documento si passano in rassegna le diverse minacce e attacchi (conosciuti all'epoca, oggi occorrerebbe aggiungerne qualcuno) che possono riguardare le reti e i conseguenti rimedi. Si tratta di un utile documento di pianificazione della sicurezza, di cui si è tenuto conto anche nella stesura dei paragrafi successivi di questa sezione.

Il 12 luglio 2002 veniva emanata la ***"Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche"***. Questa norma, che sostituisce integralmente la precedente direttiva 97/66/CE, riflette le esigenze di aggiornamento intervenute a seguito dell'evoluzione, in un quinquennio, delle tecnologie e, di conseguenza, dei maggiori rischi di violazione della privacy a carico degli utenti. La norma introduce, tra l'altro, i termini di **rete e servizio di comunicazioni elettroniche** conseguenti alla convergenza tra i servizi di fonia e dati.

La direttiva in questione è stata ampiamente recepita, assumendo efficacia cogente per il territorio italiano, nel ***"Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali"***.

1.5 LA SITUAZIONE IN ITALIA

Nel Maggio 2002 la Commissione dei Ministri per la Società dell'Informazione ha realizzato il documento "Linee Guida del Governo per lo sviluppo della Società dell'Informazione" pubblicato dal Ministero per l'Innovazione e le Tecnologie.

Le Linee Guida descrivono e definiscono l'impegno del Governo a condurre l'Italia in una posizione di protagonista nell'era digitale, modernizzando il Paese attraverso un utilizzo diffuso delle nuove tecnologie ICT sia nel pubblico che nel privato.

Ma un aumento del traffico richiede altresì un parallelo aumento della sicurezza nell'uso della rete, nonché la realizzazione di un modello della sicurezza che sia in grado di avvicinare i cittadini e le imprese alla rete, soprattutto nelle interrelazioni con la Pubblica Amministrazione.

Nelle Linee Guida viene trattato anche il problema della sicurezza delle reti e viene introdotto un piano nazionale per la sicurezza ICT e la privacy.

Il documento individua cinque azioni principali su cui fondare la strategia nazionale globale per la sicurezza ICT:

- Recepimento della Direttiva sulla sicurezza ICT[3] : tale direttiva definisce una "Base minima di sicurezza" a cui tutte le Amministrazioni devono allinearsi dopo avere effettuato una autovalutazione sul proprio livello di sicurezza ICT
- Istituzione del Comitato Tecnico Nazionale sulla sicurezza ICT[4]: il comitato è composto da cinque esperti col compito di

[3] *DIRETTIVA DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI DEL 16 GENNAIO 2002 - DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE. Pubblicata sulla G.U. n.69 del 22 marzo 2002* - "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali"

[4] *DECRETO INTERMINISTERIALE IL MINISTRO DELLE COMUNICAZIONI E IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE - "Istituzione del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni".*

indirizzare e coordinare tutte le attività e gli sforzi relativi al fine di definire il Modello Nazionale di Sicurezza e quindi di predisporre gli interventi di natura organizzativa e tecnica. La composizione e l'attività del comitato si basa sulla piena collaborazione tra il Ministero delle Comunicazioni ed il Dipartimento per l'Innovazione e le Tecnologie

- Realizzazione di un'architettura nazionale in termini di strutture e responsabilità sulla sicurezza ICT, capace di sviluppare linee guida, raccomandazioni, standard e procedure di certificazione
- Predisposizione di un Piano Nazionale sulla Sicurezza Informatica che definisca attività, responsabilità, tempi per l'introduzione degli standard e delle metodologie necessarie per pervenire alla certificazione di sicurezza nella Pubblica Amministrazione.

Nel Marzo 2003, il Ministero per l'Innovazione e le Tecnologie ha istituito il *Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate*, nel quale hanno collaborato sia i rappresentanti dei diversi dicasteri interessati alla gestione di infrastrutture critiche (Ministero dell'Interno, delle Infrastrutture, delle Comunicazioni, ecc.), sia i principali operatori privati (ABI, ASI, CESI, GRTN, RFI, Snam Rete Gas, Telecom Italia, Wind e altri), oltre che esponenti del mondo della ricerca e dell'accademia.

Il principale obiettivo di tale Gruppo di Lavoro è stato quello di aiutare le istituzioni a meglio comprendere i problemi associati alle CIIP e di fornire una base per l'individuazione dei requisiti organizzativi per incrementare la robustezza delle infrastrutture critiche.

Il *Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate* ha rilasciato nel Marzo del 2004 il documento *Protezione delle Infrastrutture Critiche Informatizzate - La realtà Italiana* che rappresenta il risultato del lavoro svolto. Il documento analizza la situazione italiana relativa alle principali CNI evidenziando come la crescente complessità di ognuna di esse e la necessità di erogare servizi innovativi e qualitativamente elevati impone il massiccio ricorso alle tecnologie ICT e questo, unitamente all'eliminazione delle posizioni monopolistiche, contribuisce ad incrementare le interdipendenze esistenti fra le diverse infrastrutture.

Il Gruppo di Lavoro, fermo restando la competenza sugli aspetti di prevenzione, protezione e sicurezza che ogni operatore deve mettere in atto nel proprio settore sulla base delle indicazioni e direttive che pervengono dalle evoluzioni delle tecnologie e dal quadro normativo esistente, evidenzia la necessità di considerare nelle strategie di sicurezza anche quelle variabili che non sono sotto il diretto controllo di nessun operatore singolarmente ma per le quali occorre sviluppare delle politiche di co-partecipazione alla gestione dei rischi. L'adozione di tali strategie non può prescindere da una costante e fattiva collaborazione fra i diversi soggetti pubblici competenti e gli operatori privati.

Il Ministero dell'Interno, per il tramite della Polizia Postale e delle Comunicazioni, ha attivato specifiche iniziative tese a privilegiare la sicurezza delle infrastrutture informatiche a servizio delle CNI ed a facilitare l'azione di repressione degli atti criminosi nei confronti di questi soggetti. Tale attenzione scaturisce dalla constatazione di quelli che potrebbero essere gli effetti su larga scala di un'azione delittuosa perpetrata contro queste infrastrutture e da qui la necessità di attivare canali di comunicazione e scambi di informazioni fattivi con i diversi soggetti coinvolti. A tal fine la Polizia Postale e delle Comunicazioni sta stipulando delle convenzioni con i diversi operatori che definiscono opportuni protocolli per la comunicazione e per lo scambio delle informazioni.

1.5.1 Attività specifiche per la sicurezza delle reti

Su richiesta della Presidenza del Consiglio dei Ministri, l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione si è attivato per istituire l'Organismo di Certificazione della sicurezza dei sistemi e prodotti informatici commerciali (OCSI). Tale Organismo consente di certificare la sicurezza ICT dei prodotti/sistemi ICT in accordo con gli standard Common Criteria e ITSEC. L'OCSI sta predisponendo specifici programmi per la valutazione e la certificazione di sistemi critici e si impegnerà per la diffusione delle certificazioni e della cultura della sicurezza ICT in tutti gli ambiti (Pubblica Amministrazione, PMI, utenza residenziale, infrastrutture critiche, ecc.).

2 - La protezione delle Infrastrutture Critiche Nazionali Informatizzate

2.1 INTRODUZIONE

Il presente capitolo tratta gli aspetti che devono essere presi in considerazione quando si effettua una analisi delle infrastrutture critiche.

Si fa riferimento alle Infrastrutture Critiche Nazionali, ed in particolare alle Infrastrutture Critiche Nazionali Informatizzate (CNII o CII).

In relazione alle CNII o CII si illustrano le problematiche di sicurezza derivanti dalle interdipendenze tra le infrastrutture critiche e dalle particolari minacce che possono metterle a rischio, con l'indicazione di un approccio metodologico alla gestione della sicurezza.

2.2 LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE NAZIONALI INFORMATIZZATE

2.2.1 L'evoluzione tecnologica e la dipendenza dalle infrastrutture ICT

Le evoluzioni dei vari mercati stanno producendo un sostanziale mutamento nell'assetto infrastrutturale del Paese richiedendo servizi innovativi con caratteristiche di efficienza ed economicità.

Tale rinnovato contesto richiede uno sfruttamento ottimale

delle diverse infrastrutture tecnologiche e ciò può essere ottenuto mediante l'adozione di sofisticati sistemi automatici di controllo e mediante l'utilizzo di tutte le tecnologie proprie dell'ICT. Ciò comporta per le CNI la necessità di considerare, parallelamente alle minacce "tradizionali" di natura fisica, anche quelle che potrebbero essere indotte, in maniera diretta o indiretta, dall'utilizzo delle tecnologie proprie della società dell'Informazione.

Si assiste al passaggio da una situazione in cui erano individuabili alcune infrastrutture sostanzialmente isolate, autonome e gestite da operatori verticalmente integrati, ad una situazione caratterizzata da una nuova diffusa presenza di interdipendenze fra le varie infrastrutture per il ruolo prioritario che viene svolto dalle reti informatiche e di telecomunicazione.

L'instaurarsi di tali interdipendenze rappresenta un nuovo elemento di vulnerabilità per l'intero sistema Paese in quanto guasti tecnici, ma anche attacchi mirati a danno del sistema ICT di una CNI potrebbero ripercuotersi sulle altre Infrastrutture Critiche provocando disfunzioni e malfunzionamenti che possono essere amplificati arrivando ad affliggere anche utenti remoti (sia dal punto di vista geografico che funzionale) rispetto al punto di origine del guasto.

Al fine di proteggere i servizi erogati dalle CNI è necessario garantire che le infrastrutture ICT critiche (le CII) operino correttamente anche in situazioni di criticità, quando la fonte energetica principale o alcuni apparati o linee intermedie vengono meno, prevedendo nell'architettura complessiva elementi di ridondanza (di alimentazione, di apparecchiature, di percorso, di tecnologia, di impianti, ecc.) nonché elementi di prevenzione per eventuali guasti o malfunzionamenti, che possono essere determinati, come già accennato, da cause sia accidentali che intenzionali.

È utile a tal fine, interrogarsi sull'effettivo grado di consapevolezza propria, e del proprio fornitore, in merito alla resilienza dei sistemi Informatici e Telematici al sopraggiungere di un evento critico, e a quale possa essere l'impatto sull'esercizio del servizio che si è tenuti a garantire.

Detta consapevolezza implica innanzitutto la conoscenza del livello di degrado tollerabile (in termini temporali e prestazionali) di

uno o più degli elementi di servizio intermedio (interni o esterni).

La tollerabilità (vedi *Fig. 4*) dipende strettamente da due aspetti: l'efficacia della contromisura e il degrado prestazionale che subisce il servizio prima che l'evento diventi bloccante.

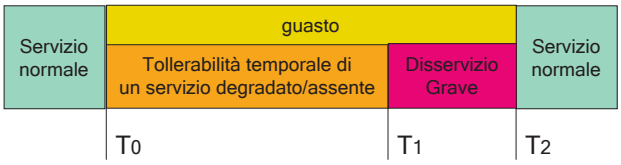


Figura 4: Tollerabilità del disservizio

Occorre predisporre contromisure temporanee adeguate a contenere entro gli estremi di tollerabilità (temporale e/o prestazionale) il disservizio, e scegliere elementi tecnologici o di servizio (esterni o interni) che garantiscano interruzione/degrado del servizio non superiori al livello di tollerabilità individuato.

Può essere utile a tal fine compilare una matrice dove si incrocino le tecnologie/servizi impiegati per specifiche operatività della CNI, con l'indicazione del loro livello di criticità per il buon funzionamento della CNI e il livello di tollerabilità del guasto.

Ovviamente ogni CNI compilerebbe una siffatta tabella in modo differente, e ne emergerebbe non solo l'articolata interdipendenza tra CNI e CII tra loro differenti, ma anche e soprattutto che non è possibile fornire uno stesso servizio e/o infrastruttura ICT adatti a soddisfare le criticità di tutte le differenti realtà. Quindi occorre effettuare innanzitutto un'attenta analisi interna, da estendere poi alle infrastrutture e ai servizi dei propri fornitori, onde costruire un'architettura resiliente rispetto alle specifiche criticità e minacce potenziali.

Ecco un esempio di tabella che prende in considerazione alcuni servizi TLC ed il loro ipotetico uso all'interno di una CNI: si evidenzia come per un medesimo servizio di TLC acquisito dal mercato si possa richiedere differenti livelli di affidabilità in funzione di quale sia la sua destinazione d'uso all'interno della CNI, cioè come si possa in certi casi considerare il servizio bloccante e conseguentemente richiedere una adeguata progettazione che minimizzi o annulli i disservizi in caso di malfunzionamento.

Funzione del servizio TLC nella CNI/Impatto			**Servizi TLC e affini con peso di criticità**				
Nome funzione	Impatto critico di questa funzione sulla missione della CNI:	Tollerabilità temporale in caso di blocco dello specifico servizio da parte del fornitore	IP WAN/ VPN	IP Internet	IP wireless cellulare (gprs/ umts)	Data Center	Altro
Comunicazione con l'esterno (non CNI)							
Comunicazioni con altre CNI							
Comunicazioni con altre sedi della medesima CNI							
Monitoraggio impianti remoti							
Altre funzioni specifiche della CNI							

Tabella 2: Esempio di tabella di correlazione tra funzioni e criticità dei servizi

DEFINIZIONI

Colonna "Impatto critico di questa funzione sulla missione della CNI": indicazione della criticità della funzione specifica rispetto alla missione della CNI
1=bassa criticità
2=criticità importante ma non bloccante
3=bloccante

Colonna "Tollerabilità temporale in caso di blocco continuativo dello specifico servizio da parte del fornitore": indicazione del numero di minuti/ore/giorni in cui è tollerabile (non genera criticità importanti) il blocco della funzione a causa di un disservizio grave del fornitore TLC

Per ogni colonna dei servizi TLC incrociata con la specifica funzione:
0=non utilizzata
1=bassa criticità
2=criticità importante ma non bloccante
3=bloccante

2.2.2 Problematiche di sicurezza nelle Infrastrutture Critiche Informatizzate

2.2.2.1 Generalità

Nella situazione descritta, è necessario applicare una metodologia che consenta una sistematica analisi e riduzione dei rischi, derivanti da nuovi e più estesi scenari di minacce e vulnerabilità, e che, tramite l'adozione di soluzioni tecnico-organizzative, consenta di elevare il grado di sopravvivenza e di protezione del Sistema Paese.

L'obiettivo è quello di avere a disposizione una metodologia di analisi, valida in generale per qualunque Sistema, corredata da una serie di soluzioni applicabili a largo spettro e specializzabili nei vari contesti, che consenta:

- la definizione della problematica e della situazione di rischio
- l'individuazione di azioni rivolte alla prevenzione di situazioni di crisi
- l'indicazione delle attività di Gestione di una Crisi una volta innescata.

Tale modello, proprio per la continua evoluzione dei fenomeni che mettono a rischio le CII, deve introdurre un processo continuo di sistematica verifica dei rischi.

2.2.2.2 Particolari criticità associate alle Infrastrutture Critiche Informatizzate

È opportuno segnalare alcune considerazioni sulle problematiche generali associate ai sistemi per le CII:

- Con l'estensione delle reti informatiche e la diffusione generalizzata della tecnologia risulta assai complessa l'identificazione dell'azione e la sua correlazione con gli effetti
- La minaccia ai sistemi CII non ha confini geografici o politici e l'estensione continua della rete mondiale rende complessi e

meno tempestivi i tracciamenti

- Il ciclo relativo all'individuazione di una vulnerabilità, alla predisposizione per sfruttarla ed alla messa in opera di una contromisura si sta abbreviando
- Le tecnologie per realizzare un attacco ai sistemi sono largamente disponibili ed a costi decrescenti e le informazioni sui metodi d'attacco sono sempre più facilmente accessibili
- I metodi di attacco si sono evoluti di pari passo con i sistemi attaccati, diventando sempre più automatizzati e sofisticati
- Ogni nuovo progetto dovrebbe essere sottoposto ad una analisi del rischio con conseguente definizione delle opportune risorse, sia organizzative che di budget, per garantirne la messa in sicurezza.

2.2.2.3 Le Interdipendenze fra le Infrastrutture Critiche Informatizzate

Nel caso delle reti di telecomunicazione, la convergenza dei media utilizzati, e in particolare l'utilizzo di Internet, sta portando alla creazione di un'infrastruttura globale a livello mondiale. Purtroppo questo fenomeno, contribuendo ad accoppiare le diverse infrastrutture, incrementa la vulnerabilità dell'intero sistema poiché ogni attacco o incidente, che si verifica in un'infrastruttura, può propagarsi ad altre infrastrutture, provocando inconvenienti e danni anche a soggetti remoti (sia dal punto di vista geografico che logico) rispetto alla causa del danno. In alcuni casi, l'interdipendenza tra CII può scavalcare i confini nazionali (si pensi ad esempio all'interconnessione tra le reti elettriche).

Capire in quale modo il corretto funzionamento di una CII dipende da quello delle altre è un passo importante in fase di programmazione degli interventi di sicurezza, in quanto permette di capire fino a quale punto una singola CII può in modo autonomo garantire la propria sicurezza e/o fronteggiare situazioni di emergenza. Sono identificabili almeno tre diverse tipologie di interdipendenze tra CII:

- Interdipendenze operative
- Interdipendenze logiche
- Interdipendenze geografiche.

Le interdipendenze esistenti tra le varie CII fanno sì che la condivisione delle informazioni fra le strutture (pubbliche e private) responsabili della loro gestione sia fondamentale ai fini della realizzazione di efficaci sistemi di protezione.

2.2.2.3.1 Interdipendenze operative

Questo tipo di interdipendenza si manifesta ogniqualvolta l'operatività di una CII dipende da quella di un'altra.

Ad esempio, l'operatività delle reti di telecomunicazioni dipende dalla disponibilità di energia elettrica e quindi dall'operatività della rete CII di erogazione della stessa. Si osservi che nell'esempio indicato l'interdipendenza operativa è mutua, in quanto l'operatività della rete elettrica dipende anche da quella delle reti di telecomunicazione.

2.2.2.3.2 Interdipendenze logiche

In alcuni casi un attacco o un incidente che comprometta l'operatività di una CII può avere ripercussioni su altre CNII senza che esista una dipendenza di tipo operativo tra di esse.

Si pensi ad esempio ad una epidemia localizzata che può provocare la crisi del sistema sanitario anche in aree lontane da quella colpita a causa dell'elevato numero di persone che potrebbero rivolgersi alle infrastrutture sanitarie pur non avendone motivo oppure alla possibile crisi del sistema dei trasporti dell'area colpita per mancanza di viaggiatori verso l'area interessata (si pensi alla crisi delle compagnie aeree negli USA dopo gli attentati dell'11 settembre).

2.2.2.3.3 Interdipendenze geografiche

Le dipendenze di tipo geografico tra CII sono dipendenze di natura completamente diversa rispetto alle precedenti. Esse si creano ogniqualvolta elementi critici per l'operatività di due o più CII, indipendentemente dalla loro natura, condividono una stessa locazione geografica.

Questo implica che determinati tipi di eventi accidentali o di attacchi deliberati possono compromettere contemporaneamente la capacità di più CII di offrire i propri servizi. Essere consci dell'esistenza di questo tipo di dipendenze è molto importante in fase di analisi del rischio in quanto permette di non fare assunzioni statistiche errate sulla probabilità di accadimento delle varie minacce.

2.2.2.4 Minacce

2.2.2.4.1 Definizione

Generalmente si associa la "minaccia" alla capacità, da parte di individui o di organizzazioni, di colpire un'infrastruttura critica nel deliberato intento di causare detrimento alla sua operatività.

Tuttavia nel contesto più esteso di sicurezza e protezione delle CNI che stiamo qui considerando dobbiamo tener conto che le minacce non sono necessariamente solo di origine umana ma possono essere anche di origine naturale o ambientale.

Si può quindi definire "minaccia" la potenziale capacità di un'azione o di un evento accidentale di provocare un danno sfruttando una particolare vulnerabilità dell'infrastruttura considerata.

2.2.2.4.2 Classificazione

Una prima classificazione delle sorgenti di minaccia suddivide le stesse in:

- *Sorgenti Naturali:* sono associate ad eventi catastrofici quali terremoti, inondazioni, eruzioni vulcaniche, fenomeni atmosferi-

ci, valanghe, ed altri eventi di questo tipo

- *Sorgenti Umane:* sono associate ad azioni umane dirette che a loro volta possono essere distinte in:
  - Azioni involontarie o accidentali (ad esempio l'introduzione di dati errati)
  - Azioni volontarie (deliberati attacchi ai sistemi, accessi non autorizzati ad informazioni, ecc.)
- *Sorgenti Ambientali:* sono associate ad un misto di azioni umane e di eventi naturali quali inquinamento, incendi, prolungate assenze di energia (black-out), dispersione di agenti chimici e di materiali nocivi, ecc.
- *Sorgenti Tecnologiche:* sono associate al cattivo funzionamento o errata configurazione di componenti Hardware o Software.

Alle varie sorgenti di minaccia devono essere associate le azioni attese all'attuarsi della minaccia.

Per le minacce derivanti da azioni umane volontarie, l'analisi dovrà anche considerare aspetti legati alla motivazione che sta alla base della minaccia.

Queste analisi rivestono particolare importanza nell'ambito delle CII dove motivazione e risorse possono potenziare significativamente il livello della minaccia. Ad esempio:

- Un "*hacker*" potrà agire per sfida e mirerà ad intromettersi nei sistemi protetti
- Un "*Computer criminal*"(o "*cracker*") sarà interessato all'acquisizione di informazioni protette o alla manipolazione di dati ed interverrà sulle applicazioni.
- Un terrorista avrà come scopo il massimo danno e potrà eseguire sia attacchi fisici che virtuali volti a rendere indisponibile il sistema
- Un insider (interno dell'organizzazione) agirà per curiosità, per procurarsi vantaggi, per rivalsa o anche chi per negligenza o semplicemente per errore, alterando le funzionalità del sistema.

Relativamente alle CII si possono ulteriormente classificare le minacce per tipo di obiettivo:

- **Fisico**: quale un apparato di comunicazione e o semplicemente un cavo di interconnessione
- **Virtuale**: quali i dati e le informazioni, o le applicazioni che risiedono in una CII

In modo analogo si identificano gli attacchi secondo il tipo di mezzo:

- **Fisico**: quale l'azione diretta sugli obiettivi fisici (sull'apparato o sul cavo), oppure un attacco fisico ad obiettivi virtuali (es. sistemi di disturbo elettronico)
- **Virtuale**: quale la compromissione o manipolazione dei dati oppure un fuori servizio delle apparecchiature causato intervenendo sul sistema di gestione.

2.2.3 La gestione della sicurezza

Il primo passo per la ricerca di una soluzione di Protezione delle Infrastrutture Critiche, è instaurare un processo sistematico e continuo di gestione dei rischi, per identificare, controllare e ridurre i rischi ed i potenziali impatti negativi ad essi collegati.

È essenziale che ogni CII identifichi correttamente la propria situazione anche in termini di utilizzo di infrastrutture comuni e interdipendenze con altre CII e crei un'infrastruttura organizzativa per attuare i processi necessari a definire, rendere operativo e mantenere un efficace programma di sicurezza.

Ciò significa definire strumenti metodologici, organizzativi (procedure, flussi operativi, modalità di intervento e comunicazione tra le entità preposte alla tutela della sicurezza dell'infrastruttura) ed informatici idonei ad affrontare in modo sistematico, consapevole e ragionato la protezione della CII ed a garantire un'ottimale gestione della crisi nei casi in cui questa non possa essere evitata.

Si tenga presente che, in considerazione della stretta interdipendenza tra le varie CNII, l'ottimizzazione delle risorse destinate alla

sicurezza richiede un approccio coordinato tra le varie CII e quindi un elevato livello di sensibilizzazione delle stesse in riferimento alle problematiche di protezione.

Dovrà essere quindi definita la metodologia di gestione della sicurezza (analisi e gestione del rischio). Questa dovrà disciplinare, in particolare, le fasi di:

1. identificazione e modellazione del contesto da proteggere
2. analisi delle minacce e delle vulnerabilità
3. valutazione del rischio
4. definizione delle strategie di trattamento del rischio
5. verifica della validità delle scelte effettuate
6. simulazioni e test delle procedure operative.

Il processo di gestione dei rischi è costituito da un insieme di attività sistematiche e ciclicamente ripetute, il cui fine è favorire un approccio alla sicurezza basato su elementi controllabili e misurabili, per quanto possibile non legati ad una percezione soggettiva del rischio o delle esigenze di sicurezza. Tale processo oltre a fornire garanzie sull'efficacia delle misure di protezione adottate, facilita l'efficiente allocazione delle risorse destinate alla tutela dell'Infrastruttura.

2.2.3.1 Identificazione e modellazione del contesto da proteggere

L'identificazione del contesto da proteggere è la fase iniziale e fondamentale dell'intero processo di "progettazione" della sicurezza. Da essa dipende infatti il livello a cui può successivamente essere sviluppata l'analisi del rischio e la qualità dei risultati ottenibili.

Durante questa fase occorre in particolare:

- identificare e censire gli elementi che costituiscono l'infrastruttura sotto esame
- identificare le interdipendenze tra tali elementi e tra questi e quelli di altre CII

- stabilire il livello di criticità dei vari elementi rispetto all'impatto che una loro eventuale compromissione avrebbe sulla capacità della CII di continuare a svolgere il proprio compito e rispetto agli effetti collaterali che tale compromissione potrebbe avere (in termini di perdite economiche dirette e/o indirette o addirittura di rischio per gli umani).

La metodologia di rappresentazione della realtà utilizzata dovrà permettere di rappresentare la CNII e le relative interazioni, mediante un modello che faciliti la successiva analisi del rischio. Di fondamentale importanza è, ad esempio, scegliere in modo opportuno il livello di dettaglio con cui descrivere e modellare la realtà in termini di cosiddette "Unità di rischio", ovvero di elementi atomici (impianti, persone o anche servizi, informazioni, ecc.), da considerare per la descrizione degli scenari di interesse rispetto ai quali sarà condotta l'analisi del rischio.

Tale metodologia ha un contesto di applicazione ampio, poiché l'identificazione di appropriate "Unità di Rischio" può essere effettuata a livello delle CNI stesse. Ad esempio, considerando la CNI "Rete trasporti ferroviari", le "unità di rischio" potrebbero essere: le stazioni o parti di esse; i passeggeri; il personale; i convogli; le tratte ferroviarie; le centrali di controllo; i depositi bagagli e merci; ecc.

Applicando questa metodologia allo specifico contesto delle CNII, potranno essere identificate, sempre a titolo di esempio, delle tipiche "unità di rischio" quali:

- i siti ove sono localizzati i centri di elaborazione dati e le infrastrutture di comunicazione
- gli ambienti ove sono installate le apparecchiature ICT
- il personale addetto
- i sistemi di controllo e gestione
- i sistemi di alimentazione
- le reti di comunicazione e le connessioni geografiche utilizzate dall'infrastruttura
- ecc.

Ad ogni "Unità di rischio" dovrà essere associato un insieme di attributi descrittivi della stessa ed altre informazioni utili (quali planimetrie, immagini, descrizioni, ecc.). Nel caso dell'"Unità di rischio" Centro di Elaborazione, ad esempio, questi attributi potrebbero includere (a titolo puramente indicativo):

- identificativo del sito
- nominativi dei funzionari responsabili
- dimensione e capacità del centro informatico
- collocazione geografica
- valore economico
- valore strategico
- valore in termini di immagine
- ecc.

Le "Unità di rischio" dovranno essere valutate con riferimento ai requisiti di Riservatezza, Integrità, Disponibilità (triade R.I.D.) sulla base di metodi qualitativi o quantitativi, definendone il livello di criticità.

Alle "Unità di rischio" dovrà poi essere possibile associare, anche in considerazione delle dipendenze esistenti con altri elementi della CNI e con altre CNI:

- le minacce pertinenti
- le misure di protezione in atto
- le vulnerabilità riscontrate.

2.2.3.2 Analisi di minacce, impatti e vulnerabilità

Obiettivi primari di questa fase sono:

- identificare le possibili minacce contro la Infrastruttura Critica e più precisamente contro le "Unità di rischio" che la costituiscono

- caratterizzare le varie minacce in termini di:
  - frequenza attesa dell'attuarsi della minaccia
  - impatto massimo dell'eventuale attuarsi della minaccia (in assenza di misure di protezione) in termini di:
    - capacità della CII di continuare a svolgere il proprio compito
    - perdite economiche dirette e/o indirette

  anche in relazione alle individuate interdipendenze con altre infrastrutture critiche
- stimare il livello di vulnerabilità della CNI rispetto alla minaccia considerata, ovvero stimare l'efficacia delle misure in atto di prevenzione (capacità di diminuire la frequenza attesa della minaccia) e di protezione (capacità di ridurre l'impatto delle minacce). Si noti che il livello di vulnerabilità è strettamente correlato alle capacità distruttive dell'evento naturale o dell'azione di attacco.

Da un punto vista metodologico la fase di analisi richiede:

- la definizione di una metrica per la misura qualitativa e/o quantitativa dell'impatto delle minacce
- la definizione di una metrica per la misura del livello di vulnerabilità rispetto alle varie minacce
- l'instaurazione di un processo ciclico nell'ambito del quale l'analisi delle minacce e delle vulnerabilità viene continuamente ripercorsa in modo da tener conto del mutare delle condizioni (graduale o legato al manifestarsi di specifici fattori amplificatori del rischio come, ad esempio, momenti di crisi internazionale, previsione di condizioni climatiche estreme, ecc.).

Da un punto di vista operativo l'analisi richiede:

- la creazione e il mantenimento di archivi storici relativi agli incidenti/attacchi subiti e alle loro conseguenze
- la disponibilità di banche dati di minacce standard di riferimen-

to messe in relazione con le tipologie di unità di rischio per le quali sono pertinenti

- la disponibilità di banche dati relative a minacce rare che possono però avere un impatto importante sull'infrastruttura
- il costante adeguamento delle competenze professionali nell'ambito delle nuove tecnologie
- la disponibilità di canali di comunicazione per scambiare con gli organismi di sicurezza delle altre infrastrutture le informazioni critiche per la sopravvivenza.

2.2.3.2.1 Le minacce per le CII e per i relativi sistemi di comunicazione

In generale, la minaccia alle CII ed in particolare ai sistemi di comunicazione associati è definibile in termini di sorgente, risorse interessate, motivazione, attuabilità, obiettivo e risultato.

Nel nostro contesto possono costituire sorgenti possibili di minaccia:

- Nazioni straniere
- Terroristi
- Hacker/Hacktivist
- Criminali
- Cracker
- Insider
- Ambiente
- Script kiddy (sorgenti involontarie).

Ai fini dell'analisi può essere utile far riferimento alla Tabella 3 nella quale sono illustrate alcune minacce, aventi per oggetto le CII e i relativi sistemi di comunicazione, con l'indicazione della eventuale natura accidentale o intenzionale.

Tipo di minaccia	Minaccia	Accidentale	Intenzionale
Fisica	Fuoco	●	●
	Danni da acqua	●	●
	Inquinamento	●	●
	Incidenti maggiori	●	●
	Clima	●	
	Sismi	●	
	Vulcani	●	
	Fulmini	●	
	Inondazioni	●	
	Avaria al sistema di condizionamento	●	●
	Interruzione alimentazione	●	●
	Distruzione hardware		●
	Sottrazione hardware		●
	Spionaggio		●
	Sabotaggio, vandalismo, abuso, frode od intrusione/sostituzione fisica		●
	Radiazioni termiche		●
	Impulsi elettromagnetici di elevata intensità		●
	Interruzioni delle comunicazioni	●	●
Elettronica	Interferenze elettromagnetiche	●	●
	Intercettazione delle comunicazioni	●	●
Telecomunicazioni	Mancata/Alterata autenticazione dell'originatore		●
	Alterazione dei dati sulla rete		●
	Estrazione dei dati sulla rete		●
	Blocco del funzionamento		●
Fattore umano	Divulgazioni di informazioni all'interno	●	●
	Divulgazioni di informazioni all'esterno	●	●
	Indisponibilità del personale preposto	●	●
	Errori o carenze del personale preposto	●	
	Furto dei documenti		●
	Furto di materiali		●
	Assunzione non autorizzata del controllo dei sistemi		●
	Uso non autorizzato di materiali		●
	Atti terroristici		●
	Scioperi/disordini civili		●
	Omissioni od errori intenzionali		●
Infrastrutture ICT	Danni o avaria all'hardware	●	
	Saturazione dell'hardware	●	
	Errore o avaria al software	●	
	Errore di data entry	●	
	Uso improprio del sistema	●	
	Manutenzione non corretta	●	
	Modifiche non autorizzate al data base od ai sistemi		●
	Mascheramento		●
	Negazione del servizio (Dos)		●
	Impiego di sistemi di monitoraggio analisi ed infiltrazione		●
	Impiego di codici o sistemi di inganno (Malware)		●

Tabella 3: Suddivisione delle minacce

2.2.3.2.2 Vulnerabilità specifiche dei sistemi di comunicazione delle CII

I sistemi di comunicazione per le CII hanno subito un forte impatto dal punto di vista della loro vulnerabilità per effetto di una serie di fattori tecnico-organizzativi che hanno caratterizzato scelte ed innovazioni, sia dal lato Clienti che dal lato Fornitori/Provider, tra cui:

1. La progressiva adozione all'interno delle reti per le CII di architetture e protocolli standard sviluppati in ambito Internet (TCP/IP), anche per applicazioni strategiche di controllo di processi geograficamente distribuiti (es. applicazioni SCADA) in passato caratterizzate da protocolli proprietari e reti strettamente private
2. La proliferazione di reti per le CII realizzate con soluzioni tipo "reti private virtuali" (VPN o IP-VPN), con traffico "mission-critical" che attraversa reti pubbliche multiservizi
3. L'esigenza di realizzare interconnessioni tra una rete per CII ed altre reti (interne o esterne all'organizzazione) per motivi funzionali e di consentire accessi distribuiti da remoto per attività correnti o attività straordinarie di supervisione e gestione (sulle 24 ore)
4. I problemi per la gestione delle congestioni e per le implementazioni di sicurezza, che possono presentare reti formate dall'unione di sub reti indipendenti
5. I processi di terziarizzazione delle attività O&M messi in atto in misura sempre più estesa dagli operatori di tlc per le proprie tecnologie, che hanno fatto proliferare il numero degli operatori abilitati e di conseguenza l'esigenza di regole e controlli sulle autorizzazioni
6. Le frequenti cause di avaria alle reti dovute a danni provocati da terzi sui circuiti di accesso (local loop) che forniscono risorse di connettività, ad es. sui cavi interrati. L'introduzione di nuovi collegamenti conseguenza della liberalizzazione non ha comportato variazioni rilevanti per questa specifica minaccia, essendo spesso utilizzato il criterio di utilizzo promiscuo dei cavidotti per ottimizzarne i costi. L'impatto di questi danni è

correlato alla ridondanza prevista, a quella effettivamente garantita dal Provider (diversificazione fisica) nonché alla quantità dei dati trasferiti dal link fisico. Come esempio di specifiche minacce su tali Linee di Comunicazione si riporta la Tabella 4

7. Gli errori umani, possibile sorgente di danno o di avaria
8. La maggiore dipendenza delle piattaforme di reti pubbliche, che spesso fanno da supporto alle reti di comunicazione per le CII, da software e data base complessi e talvolta da Internet
9. Sistemi operativi di supporto (OSS) delle reti pubbliche sempre più standard e informazioni sul controllo di questi sistemi (COTS) largamente diffuse e pertanto accessibili da un largo numero di "potenziali nemici"
10. Il permanere di vulnerabilità da ottimizzare a livello degli Host, nonostante Internet stia divenendo sempre più sicura, implementando protocolli di sicurezza che interessano gli alti livelli OSI
11. La dipendenza critica, nelle reti IP, dai servizi di routing e dalle traduzioni degli indirizzi. La lista dei connessi servizi critici si espande regolarmente includendo i servizi di directory ed i certificati a chiave pubblica, che a loro volta generano altri servizi critici
12. La crescita della capacità di routing dei protocolli di rete, che provoca una crescita dei rischi connessi
13. L'inadeguatezza degli algoritmi di routing, che non scalano in modo ottimale, necessitano potenza di calcolo e non hanno politiche flessibili: occorre risolvere i problemi tra la stabilità degli algoritmi ed il cambio di routing in risposta ad una avaria su componenti di rete.

Minaccia	Sorgente della minaccia
Vibrazione	Treno, metro e traffico veicolare, attività sismica, attività edile o di manutenzione in atto
Liquido penetrante nei cavi	Acqua ed altri liquidi
Radiazioni	Nucleare, Campi elettrici a banda stretta, Campi a banda larga
Temperatura	Fuoco, accidentale o doloso, alta temperatura confinata in ambiente ristretto
Esposizione a fuoco	Incendio di foreste, di carburante, incidenti di veicoli, fuoriuscita di gas incendiato
Vento e ghiaccio	Uragani, tornadi, simultanea esposizione a ghiaccio e vento forte
Attività di costruzione	Errori umani, attività di scavo
Corrosione	Ambiente industriale chimico, ambiente costiero, traffico di automobili e camion pesanti
Fulmini e sovratensione	Fulmini, alta tensione
Mancanza di alimentazione elettrica agli apparati di telecomunicazioni	Blackout prolungato

Tabella 4: Esempio di minacce per le linee di comunicazione

2.2.3.2.3 Correlazione minacce - Servizi

Un esempio di correlazione minacce/servizi è riportato in Tabella 5, dove si considerano soltanto alcune delle minacce possibili in relazione alle principali categorie di servizi, avendo verificato che le altre statisticamente non incidono in modo significativo (tipico è l'evento terremoto in zone non sismiche o eventuali inondazioni in zone lontane da mari, fiumi o laghi).

I servizi suscettibili di degrado in caso di disservizio da parte della infrastruttura di rete da cui sono supportati sono elencati sotto forma di macro categorie:

- *e-mail:* le differenti categorie di posta elettronica e più in generale i sistemi di messaging

		Servizi								
		Servizi gestionali			*Infrastrutture*				*Infrastrutture critiche*	
Categoria	**Tipo di minaccia**	email	web based	Enterprise IP services	Contact center	Telefonia Fissa	Telefonia Mobile	Controllo di processo	Controllo di processi critici	Sicurezza
Eventi dannosi esterni	**Eventi naturali**				X	X	X	X	Y	X
	Interruzione di servizi essenziali	Y	Y	Y				X	Y	Y
	Atti terroristici				X	X		X	X	X
	Epidemie				X			X	X	X
	Attacchi da parte di hacker	Y	Y	Y	Y	Y				
Eventi interni all'azienda	**Guasti HW**	X	X	X			X	Y	Y	Y
	Manutenzione HW e SW dei sitemi									
	Sabotaggi e altri attacchi interni	X	X	X	X			X	Y	Y
	Inter-dipendenza con terze parti				X		X	X	Y	Y

X Il servizio è vulnerabile alla minaccia

Y Il servizio è vulnerabile alla minaccia ma sono in atto contromisure a livello applicativo (non network)

Tabella 5: Servizi/Minacce

- *Web Based:* i servizi interni o esterni all'azienda basati in generale sull'interfaccia WEB/Browser
- *Enterprise IP Service:* comprende uno spettro, peraltro molto ampio, di applicazioni aziendali di natura gestionale, basate sul protocollo IP. In realtà a questa categoria appartiene un insieme articolato di applicazioni (integration framework) di criticità molto differenziata
- *Contact Center:* I servizi infrastrutturali e applicativi che consentono all'azienda di essere contattata dai propri clienti/utenti mediante differenti canali. In questa categoria sono quindi compresi i servizi CRM, IVR, CTI ed anche i servizi di gestione documentale
- *Telefonia fissa:* i servizi di comunicazione interni ed esterni all'azienda
- *Telefonia Mobile:* i servizi per la comunicazione mobile aziendale
- *Controllo di processo:* i servizi per il controllo locale o remoto di impianti e sistemi finalizzato al monitoraggio, controllo ed accounting
- *Controllo di processi critici:* i servizi per il controllo locale o remoto di impianti e sistemi, la cui corretta e continua disponibilità è essenziale per l'erogazione dei servizi core-business
- *Sicurezza:* in generale i servizi necessari a garantire la sicurezza delle infrastrutture mediante adeguati sistemi di protezione. In questo ambito si collocano ad esempio i sistemi di sorveglianza, le applicazioni informatiche per la sicurezza (PKI, SSO System ecc). Si tratta di una categoria che naturalmente si articola a sua volta in diverse sottocategorie.

2.2.3.3 Valutazione e analisi del rischio

Per questa valutazione i dati raccolti vengono elaborati per giungere ad una stima del livello di rischio globale cui è esposta la CII.

In generale, il livello di rischio relativo ad una minaccia viene

normalmente considerato pari all'entità del danno che ci si aspetta (statisticamente) di subire durante un prefissato intervallo di tempo a causa dell'attuarsi della minaccia stessa.

Utilizzando i parametri stimati durante la fase di analisi delle minacce e delle vulnerabilità, il livello di rischio connesso ad una minaccia può essere espresso in funzione della frequenza della minaccia, del suo impatto massimo (nelle sue componenti dirette ed indirette, dovute ad effetti collaterali) e del livello di vulnerabilità.

L'adozione di contromisure ha l'effetto di ridurre il livello di vulnerabilità della CII rispetto alla minaccia considerata e conseguentemente la frequenza e l'impatto effettivo della minaccia stessa. Nel caso di minacce riconducibili ad azioni volontarie, l'adozione di misure di sicurezza può anche avere l'effetto di ridurre la frequenza con cui le minacce vengono attuate.

L'adozione di misure di sicurezza a contrasto delle varie minacce ha quindi l'effetto di ridurre il livello di rischio globale cui la CII è esposta.

Durante la fase di analisi del rischio specifico per le reti di comunicazione vengono svolte le seguenti attività:

- Classificare tutti i dati in modo da individuare le informazioni più critiche
- Analizzare la criticità dei sistemi che compongono la rete e per ciascun sistema determinare un coefficiente di rischio di intrusione informatica
- Definire le contromisure tecnologiche, organizzative e logistiche da intraprendere per ridurre il livello di rischio delle suddette componenti. È possibile adottare diverse strategie di riduzione del rischio, adattabili alle diverse politiche di gestione del rischio che si decide di intraprendere.

Le operazioni da eseguire sono:

- **FASE 1 - Identificazione e Valutazione dei seguenti beni:**
  - *Dati* (Informazioni contenute nei sistemi IT)
  - *Software* (sistema/applicazione)
  - *Beni Fisici* (Hardware)

  tenendo conto delle perdite in cui si incorrerebbe qualora i suddetti beni fossero scoperti (perdita di riservatezza) o modificati (perdita di integrità) o resi indisponibili (perdita di disponibilità).

- **FASE 2 - Analisi delle Minacce e delle Vulnerabilità:**
  - *Identificazione* delle minacce ai beni (o a gruppi di beni)
  - *Valutazione* dei livelli di quelle minacce (alto, medio, basso), cioè della probabilità di manifestarsi delle minacce
  - *Identificazione* delle vulnerabilità dei beni (o gruppi di beni)
  - *Valutazione* dei livelli delle vulnerabilità (alto, medio, basso), intesi come probabilità che una minaccia possa essere portata a termine con successo sfruttando una data vulnerabilità
  - *Valutazione* del livello del rischio globale calcolato in base al valore dei beni ed in base ai livelli stimati delle minacce e delle vulnerabilità. In tale valutazione deve essere incluso anche il fattore "Immagine" che può avere un notevole impatto economico.

- **FASE 3 - Identificazione delle Contromisure:**
  - *Evitare il rischio:* evitare il rischio significa non intraprendere alcuna attività specifica che comporti rischio (ad es. per evitare il rischio della rivelazione di dati informatici particolarmente sensibili si può togliere questi dati dal sistema)
  - *Ridurre il rischio:* ridurre il rischio ad un livello accettabile implica l'adozione di contromisure appropriate
  - *Accettare il rischio* identificato: alla fine bisogna accettare che

il sistema è comunque sottoposto ad un rischio che è stato ridotto fin quanto possibile. Bisogna considerare il fatto che non è possibile costruire un sistema completamente esente da rischio sia perché sarebbe di difficile utilizzo (per l'esistenza di procedure troppo restrittive) sia perché non è possibile prevedere tutti i tipi di attacchi perpetrabili sia dall'esterno che dall'interno.

In conclusione, quindi, l'esito di questa analisi conduce a delle scelte (Gestione del rischio): censiti i beni, viste le minacce e le vulnerabilità, analizzate le ragioni che potrebbero motivare degli attaccanti, esaminati costi e benefici delle possibili contromisure, si scelgono quelle contromisure che si reputano idonee ad evitare e/o ridurre il rischio. Quindi non tutte le contromisure identificate devono essere adottate. Esse possono essere rilassate per ragioni di costo o di fattibilità. Il rischio aumenterà ma nell'ottica costo/beneficio sarà un rischio accettabile. Il punto fondamentale è quello di prevedere almeno una contromisura per ogni attacco sferrato su un bene considerato "di valore" per il sistema.

Vale la pena ricordare il principio secondo cui non esiste la sicurezza totale. Saranno sempre possibili attacchi che superano le

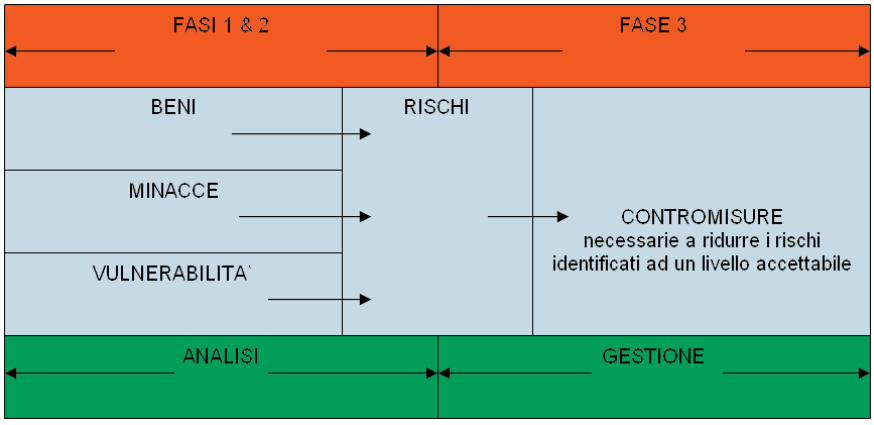


Figura. 5: Fasi dell'Analisi del Rischio

contromisure adottate, ma anche quegli attacchi hanno un costo. Per disincentivarli è normalmente sufficiente che costino di più del beneficio che si ottiene perpetrandoli con successo.

2.2.3.4 Definizione delle strategie di trattazione del rischio

Durante questa fase, strettamente connessa a quella di valutazione del rischio, vengono definiti i livelli massimi di rischio accettabili e vengono scelte le strategie da adottare per ridurre il rischio al di sotto di tali livelli.

Il livello di rischio può essere ridotto adottando misure di protezione che abbassano il livello di vulnerabilità, ma in alcuni casi è possibile agire anche su altri fattori come la frequenza della minaccia.

Il processo di analisi dovrà fornire:

- la selezione della strategia e delle misure di protezione più adatte
- l'ottimizzazione dell'uso delle risorse (umane, economiche, tecnologiche, ecc.) allocate alla sicurezza
- la documentazione delle decisioni prese e il trasferimento delle stesse ai responsabili dell'attuazione.

Di fondamentale importanza in questa fase è la disponibilità di una banca dati di misure di sicurezza attiva, passiva e organizzativa messe in relazione con le minacce che queste sono in grado di contrastare.

2.2.3.5 Verifica della validità delle scelte effettuate

Il processo di verifica ha come obiettivo il costante monitoraggio della CII, con il fine di comprendere se le misure di sicurezza adottate sono effettivamente in grado di ridurre il rischio fino ai livelli desiderati. Qualora ciò non avvenga, il processo dovrà fornire le informazioni necessarie affinché possano essere avviate idonee azioni correttive.

Le azioni correttive possono riguardare il modo in cui le misure di protezione sono state attuate, i criteri di stima degli impatti delle minacce e/o dei livelli di vulnerabilità, i parametri di taratura degli algoritmi per il calcolo del livello di rischio, ecc.

Il processo di verifica è pertanto un processo di apprendimento (incident learning) che dovrà avvalersi di efficaci strumenti di segnalazione degli incidenti e che richiede la creazione di una banca dati nella quale tali segnalazioni sono raccolte, insieme ad ogni altra informazione ritenuta utile ai fini di una completa comprensione delle cause degli incidenti stessi.

All'arricchirsi della banca dati degli incidenti, le informazioni raccolte permetteranno di affinare la conoscenza statistica dei fenomeni di interesse e, sulla base del confronto tra i valori attesi del danno e l'entità del danno effettivamente subito, permetteranno il costante monitoraggio della validità delle soluzioni adottate al variare nel tempo delle condizioni.

2.2.3.6 Simulazione e test delle procedure operative

Anche se l'analisi del rischio viene aggiornata costantemente e le procedure operative adeguate ai nuovi dati rilevati dalle analisi, è comunque di fondamentale importanza istituire un processo che consenta di simulare, prima in modo teorico e poi in termini pratici, incidenti o attacchi al fine di verificare le reazioni della struttura e dell'organizzazione a tali eventi.

Durante questa fase occorre:

- effettuare test periodici per verificare l'effettiva messa in sicurezza delle infrastrutture
- effettuare simulazioni periodiche di incidenti per verificare l'effettiva efficacia delle strutture ed i relativi tempi di risposta.

Per l'esecuzione del processo è di fondamentale importanza definire uno specifico team dedicato, in una struttura che non si occupi d'esercizio e che abbia l'obiettivo di effettuare le simulazioni ed i test periodici.

A regime, questo team deve ricevere i risultati delle analisi del rischio aggiornate unitamente alla "mappatura" dei processi aziendali per poter produrre un documento che illustri in dettaglio i singoli impatti sul core business e le aree nelle quali poter operare dei miglioramenti.

2.2.3.6.1 Test delle procedure operative

La simulazione deve essere il punto di partenza per l'analisi delle reazioni in caso d'incidente. Le simulazioni devo essere effettuate considerando i più svariati casi d'incidente rilevati dalla analisi del rischio.

Non appena terminata questa fase è importante effettuare i cosiddetti "test sul campo". Spesso anche le migliori procedure e simulazioni si infrangono sul classico "interruttore non considerato". L'esecuzione dei test può mostrare quale sia il livello di impatto sul business, in quanto la creazione volontaria di un incidente potrebbe dimostrare effetti che non erano stati previsti nella fase di simulazione.

Un buon sistema per limitare l'impatto è quello di utilizzare ambienti di collaudo dedicati: è importante considerare come un assioma il fatto che più l'ambiente di collaudo è diverso dall'ambiente di produzione, più i test perdono di efficacia. In condizioni normali si suggerisce di effettuare i test sistematici sugli ambienti di collaudo in modo da incrementare il processo di apprendimento (incident learning), e di effettuare un numero ridotto di test sull'ambiente di produzione.

Fondamentale è l'analisi da effettuare durante i test, prevedendo diversi livelli di osservazione sul business, sui servizi informatici e sulle infrastrutture tecnologiche. Tutte le informazioni rilevate dovranno confluire nella analisi del rischio e dovranno essere di supporto al management per poter individuare gli interventi da compiere.

2.2.3.6.2 Simulazione d'incidenti

La tecnica di simulazione degli incidenti presuppone di utilizzare i risultati dell'analisi del rischio e di avere proceduralizzato le atti-

vità di business. L'ideale è quello di realizzare un flessibile tool informatico basato su di un modello matematico che sia in grado di rispondere alle variazioni dei predetti risultati.

Il modello deve prevedere una opportuna contro reazione in quanto la modifica di uno dei possibili stati iniziali può comportare plurime variazioni di stato in cascata. Dopo aver realizzato il modello si potrà passare alla fase di simulazione: verrà analizzato cioè cosa comporta la modifica del generico stato iniziale del sistema. Questa fase di studio è necessaria per effettuare dei test mirati negli ambienti di collaudo, con l'obiettivo di minimizzare costi e sforzi attuativi. I test negli ambienti di collaudo devono essere più fedeli possibile all'ambiente d'esercizio dove si svolge il business aziendale.

Punti fondamentali sono: l'individuazione dei livelli di osservazione (informatico, tecnologico, ecc.), e la definizione delle metriche con cui si valuteranno le simulazioni.

Solo un'attenta definizione delle metriche ci permetterà di confrontare i risultati delle varie simulazioni e individuare univocamente il livello di criticità di un evento.

2.2.4 Dalla protezione delle CII alla protezione del loro sistema di comunicazione

È opportuno sottolineare che nel presente documento il concetto di *Sistema di Comunicazioni* è inteso nella sua compiuta definizione comprendente anche quella parte di Sistema Informativo necessario al suo funzionamento.

In quest'ottica al fine di affrontare in modo strutturato la sicurezza del Sistema Informativo delle CII, è opportuno sottolineare che la soluzione va ricercata, oltre che per gli aspetti più prettamente tecnologici, anche per gli aspetti organizzativi, formativi e procedurali.

Dal punto di vista tecnologico/organizzativo, la protezione di una CII può essere suddivisa nelle seguenti aree:

- **Protezione Fisica** - Ovvero tutte quelle azioni che si rendono necessarie per evitare che eventi accidentali o dolosi possa-

no perpetrarsi nei confronti delle strutture fisiche di supporto. In quest'ambito si annoverano:

- Sistemi di sorveglianza
- Sistemi di protezione fisica
- Sensori per il monitoraggio
- Meccanismi di controllo accessi

Ovviamente in tale area rientrano anche i dispositivi cosiddetti "intelligenti", sensori e attuatori:

- Sensori ed attuatori disseminati
- Sistemi di gestione, comando e controllo con alta automazione
- Sistemi di rivelazione allarmi intelligenti
- Apparati e sistemi telegestibili.

- **Protezione Logico-strutturale** - Questa tipologia di azioni si estrinseca in:
  - Irrobustimento architetturale (sistemi in classe HA)
  - Ridondanze
  - Separazione del traffico
  - Creazione di canali di comunicazione alternativi per back-up
  - Sistemi di disaster recovery
  - Alimentazioni elettriche secondarie (UPS e gruppi elettrogeni)
  - Addestramento del personale
  - Certificazioni.

- **Protezione delle Comunicazioni** - intesa come quell'insieme di azioni tese a garantire la continuità e correttezza del flusso informativo e in particolare:
  - il livello di qualità del servizio
  - la gestione dei livelli di priorità assegnabili al traffico critico per l'operatività o per la sopravvivenza

- la cifratura delle informazioni
- i sistemi per la sicurezza informatica (firewall, anti-virus)
- il sistema per la gestione della sicurezza del sistema informatico (IDS).

Al problema della protezione del *Sistema Informativo* nelle tre aree descritte precedentemente, cioè nella sua accezione fisica, logica e di comunicazione, è dedicato il prossimo capitolo.

3 - La protezione delle reti di comunicazione

3.1 INTRODUZIONE

Nel presente capitolo analizzeremo le prestazioni richieste alle "Reti di Comunicazioni" associate alle suddette CII ed al relativo Sistema Informativo delegato al funzionamento di tali reti. In particolare nel seguito verranno analizzate in maggior dettaglio le caratteristiche peculiari delle CII che utilizzano sistemi di comunicazione basati sulla famiglia di protocolli IP in quanto esse rappresentano la quasi totalità delle implementazioni attualmente in uso.

3.2 LE RETI DI COMUNICAZIONE PER LE STRUTTURE CII

3.2.1 Le prestazioni funzionali per le reti di comunicazione sensibili al fine della garanzia del servizio

La Tabella 6 definisce, in termini di Requisiti Funzionali, le principali prestazioni richieste ad una generica Rete di Comunicazione che supporta le operazioni di una CII e introduce il concetto di SLA (Service Level Agreement) come strumento fondamentale per regolare i rapporti tra il cliente (CII) ed i fornitori di servizi di TLC.

Requisiti Funzionali	Descrizione
Trattamento avanzato di priorità	Il servizio di emergenza dovrà avere priorità su tutto il resto del traffico
Rete sicura	La rete deve essere protetta dagli accessi non autorizzati, includendo tecniche di criptazione e autenticazione dell'utente
Non tracciabilità	Utenti selezionati potranno usare la rete, senza il rischio di essere tracciati
Ripristinabilità	Quando un'interruzione avviene, il servizio deve essere ripristinato al livello previsto, su una base di priorità
Connessione internazionale (*)	Il servizio deve garantire l'accesso ai carrier internazionali
Interoperabilità	Il servizio deve garantire l'interconnessione con altre reti selezionate
Mobilità (*)	L'infrastruttura di comunicazione deve poter essere trasportabile, reimpiegabile o pienamente mobile (es. GSM, Satellitare, HF...)
Copertura (*)	Il servizio deve essere accessibile da ogni postazione, considerata primaria
Sopravvivenza - Resilienza	Il servizio deve essere robusto, in grado di garantire continuità, in presenza di qualsiasi minaccia, sia intenzionale che accidentale
Voce	Il servizio deve garantire il trasporto della voce
Banda Larga (*)	Il servizio deve garantire il trasporto di video, immagini, multimedia
Scalabilità di banda	Deve essere prevista la possibilità di variare la larghezza di banda senza sostituzione del HW entro un range prefissato
Capacità di crescita	Il servizio deve essere in grado di moltiplicare la capacità della rete
Disponibilità	Il servizio deve essere conforme ai requisiti di progetto e deve essere utilizzabile nel momento in cui si ha necessità

Tabella 6: Requisiti delle reti CNI. Le voci contrassegnate da (*) sono da intendersi come requisiti funzionali da rispettare ove necessario e previsto.

3.2.2 Le soluzioni adottabili per le reti di comunicazione

3.2.2.1 Le attuali reti per le infrastrutture CII

Possiamo in linea generale rappresentare le Reti di Comunicazione delle Infrastrutture Critiche attualmente utilizzate secondo le seguenti caratteristiche comuni:

- raramente di proprietà della Infrastruttura critica, si appoggiano tipicamente su operatori di mercato
- il servizio acquistato è assai variegato, spaziando da intranet a soluzioni di VPN sino a reti completamente open world quali Internet
- alcune delle suddette realizzazioni gestiscono l'aspetto di Sicurezza della Informazione attraverso le seguenti soluzioni:
  - Firewall
  - Antivirus
  - Cifratura (end to end, bulk encription)
  - Autenticazione (PKI)
- sono ampiamente usate, data la copertura globale, le Reti Wireless che in genere risultano altamente critiche dal punto di vista della connettività e della protezione dell'informazione
- la garanzia della QoS (Quality of Service) risulta spesso carente e sovente viene identificata come la capacità di fornire normalmente il servizio senza dettaglio delle prestazioni in termini di:
  - assenza di "single point of failure"
  - sufficiente o definita connettività
  - garanzia di "graceful degradation"
- Risulta assente in genere la capacità di gestione differenziata dei dati in termini di "**Dati Normali, Sicuri e Strategici**"
- Altrettanto assente risulta spesso l'applicazione del concetto di "Rete Isolata" ovvero di rete che non prevede il collegamento con altre reti che potrebbero essere sorgente di attacchi informatici

- Inoltre non risulta che siano impiegate/previste Federazioni di Reti o reti utilizzanti differenti mezzi trasmissivi (se si escludono le applicazioni di tipo "down hill" in ponte radio quali accesso a reti terrestri).

Alcune Infrastrutture Critiche hanno iniziato ultimamente a considerare molto seriamente gli aspetti legati alla Security delle Comunicazioni.

Tipico esempio è rappresentato da Terna che, recentemente, ha scelto di riprendere la strada dello sviluppo di soluzioni di "rete privata", rese possibili dalle evoluzioni tecnologiche e dalle caratteristiche delle proprie infrastrutture elettriche ad alta tensione.

In particolare, Terna sta sviluppando per la trasmissione dei dati di controllo (funzionali cioè all'esercizio ed al monitoraggio remoto della Rete Elettrica di Trasmissione Nazionale), una propria architettura ATM. La nuova infrastruttura sfrutta quali portanti trasmissive onde convogliate digitali su elettrodotti in alta tensione, risultando isolata e gestita in totale autonomia, e quindi è in grado di offrire elevate garanzie di qualità e sicurezza. Il progetto nasce come integrazione e potenziamento della piattaforma di networking in esercizio basata su risorse acquisite dal mercato, ma offre interessanti prospettive di *insourcing*.

3.2.2.2 Il modello delle reti (e la loro interazione) per raggiungere le prestazioni richieste

3.2.2.2.1 Premessa

Il presente paragrafo presenta alcune soluzioni relative alla implementazione nelle Reti di Comunicazione dei requisiti di sicurezza; tali soluzioni ed indicazioni sono in linea con la **Good Practice** e quindi con l'esperienza maturata a livello nazionale ed internazionale e con i trend dello stato dell'arte.

Le soluzioni che vengono di seguito descritte si sviluppano secondo il seguente percorso:

- dai requisiti essenziali per la sicurezza delle reti di comunica-

zione si definiscono i servizi essenziali e l'approccio metodologico per la caratterizzazione di reti sicure

- si identificano quindi le caratteristiche delle reti di comunicazione a secondo del livello di sicurezza che si intende raggiungere definendo le caratteristiche globali (principalmente QoS, connettività e sicurezza delle informazioni) a livello di rete "stand alone"
- si sviluppando i vari aspetti di dettaglio legati:
  - alla "connettività" di una singola rete
  - alle possibilità di incrementare la connettività tramite la "federazione di reti"
  - agli aspetti legati alla sicurezza delle informazioni in termini di accessi (Porta di Rete) e di applicazione (Middleware)
  - ai Data Center ed alle Strutture di Utilizzazione dei Dati
  - alle problematiche legate alle alimentazioni
- si termina con una breve descrizione relativamente alle possibili Reti di Emergenza.

Ovviamente quanto sopra deve sempre essere supportato da una rigorosa analisi del rischio e delle conseguenze, effettuata con le metodologie che sono state descritte nel capitolo precedente.

3.2.2.2.2 Requisiti essenziali per la sicurezza delle reti

Di seguito saranno fornite indicazioni sulle soluzioni adottabili per affrontare con successo le problematiche della sicurezza nell'ambito delle reti informatiche.

Nell'attuale contesto è complesso fornire precise indicazioni tecniche da seguire per applicazioni di massima sicurezza; tuttavia è possibile illustrare i requisiti minimi essenziali per la sicurezza delle Reti di Comunicazione.

Utilizzando quanto già definito nell'ambito del Capitolo 2, si elencano di seguito i requisiti fondamentali per la sicurezza delle reti (*Fig. 6*):

Fig. 6: Servizi fondamentali per la sicurezza delle reti (ISO)

- *La disponibilità:* la capacità di accedere ai dati critici per la sopravvivenza dell'infrastruttura in ogni momento anche se la rete sta operando in condizioni estreme
- *L'autenticazione dell'origine dei dati:* la capacità di identificare un utente adeguata alla tipologia di informazione e servizio trattato
- *Il controllo degli accessi:* assicura che solo gli utenti autorizzati abbiano accesso alle risorse in rete
- *La riservatezza dei dati:* assicura che solo gli utenti autorizzati possano accedere ai dati protetti
- *L'integrità dei dati:* assicura che i dati non vengono alterati da utenti non autorizzati o da software od hardware non garantiti
- *Il non-ripudio:* serve per fornire la prova incontestabile di una avvenuta spedizione o di una avvenuta ricezione di dati in rete.

Inoltre occorre garantire, nel caso delle reti per CII, che i sistemi di autenticazione possano essere condivisi su base di necessità mediante il possibile utilizzo di:

- un sistema coordinato di generazione, distribuzione e gestione delle chiavi crittografiche basato su architetture PKI o proprietarie, ma comunque gerarchico e distribuito
- sistemi di controllo degli accessi che dovranno tenere conto della necessità di un sistema distribuito di validità dei certificati per poter servire alle necessità di centinaia di migliaia di utenti con grande affidabilità, alte prestazioni, sicurezza assicurata e minimi costi di messa in opera.

Allo scopo di evitare interferenze provenienti da reti estranee alle reti CII, sia pubbliche che private, sono possibili due soluzioni alternative:

- completa separazione delle reti CII dalle altre reti
- applicazione di particolari sistemi di sicurezza per la connessione delle reti esterne alle reti CNI.

La completa separazione delle reti CII dalle altre reti assicura un elevato grado di sicurezza contro le intromissioni od i disservizi creati dall'esterno. La rete USA "Govnet" è un esempio di rete amministrativa indipendente la quale è stata progettata come rete privata voce e dati basata sul protocollo Internet (IP) ma senza interconnessione alle reti commerciali e pubbliche. Lo stesso avviene per le reti delle FF.AA. Italiane (per esempio, MARINTRANET e DIFENET) le quali soddisfano il requisito di un funzionamento senza rischio di penetrazioni o di interferenze dall'esterno, per garantire la sicurezza di dati riservati o sensibili.

Tuttavia, specie in condizioni di normalità, è virtualmente impossibile separare le reti CII da quelle esterne in quanto esse hanno la necessità o la convenienza di interconnettersi con altre reti per lo scambio di dati essenziali e per motivi commerciali o finanziari. Da ciò l'importanza che in tali condizioni sia assicurata la massima sicurezza nell'interconnessione delle reti, utilizzando adeguate politiche di protezione e soluzioni tecniche che garantiscano la piena sicurezza degli accessi e dello scambio di dati sia a livello di porta di rete che a livello di utenti.

I passi principali dell'approccio metodologico, applicabili sia al caso di progettazione di una nuova rete sicura, sia nel caso della messa in sicurezza di una rete esistente, sono i seguenti:

- caratterizzare la tipologia di rete o di servizio
- condurre un'accurata analisi del rischio
- verificare gli elementi distintivi dell'architettura della rete per renderla conforme agli standard di sicurezza CII
- definire la porta di rete per l'accesso in sicurezza alle reti delle altre infrastrutture CII e alle reti esterne
- dotare il sistema, anche a livello di middleware, di applicazioni e di procedure, di opportune misure di sicurezza.

L'adozione dei seguenti cinque principi consente la realizzazione di una rete sicura con il necessario rapporto costo-efficacia:

- valutazione del rischio e delle esigenze
- attivazione di un gruppo centrale per la sicurezza della rete
- attivazione delle misure di sicurezza ritenute più appropriate e dei relativi controlli di sicurezza
- diffusione della consapevolezza dei rischi connessi con il mancato rispetto delle norme di sicurezza
- controllo e valutazione dell'efficacia delle misure e dei controlli di sicurezza.

3.2.2.2.3 Caratterizzazione della tipologia di reti

Dal punto di vista di chi propone, progetta e realizza una rete e i servizi che su di essa si appoggiano, è essenziale ricondurre a un numero limitato di categorie le tante realtà differenti di reti CII.

I vari casi in cui suddividere le reti corrispondono ai seguenti criteri di base:

- copertura territoriale
- confinamento della rete
- disponibilità di strutture di comunicazione.

Dal punto di vista della copertura territoriale, una rete CII può avere una copertura locale oppure essere estesa a livello nazionale e in tale caso la distribuzione delle sedi può essere capillare, con sedi di importanza molto diversa, oppure limitata a pochi centri, tutti di importanza paragonabile.

La Tabella 7 mostra alcuni esempi di CII, riferiti allo scenario italiano, a illustrazione del concetto.

	Copertura territoriale locale	**Copertura territoriale estesa a livello nazionale**
Distribuzione limitata delle sedi	- Una Azienda Sanitaria Locale - Gli impianti di un sistema di trasporto locale (es.di una metropolitana) - Gli attracchi, le zone di movimentazione e stoccaggio merci e i varchi in ambito di porto	- Le basi o gli arsenali della Marina Militare - I Centri di Elaborazione Dati dei Servizi Interbancari
Distribuzione capillare delle sedi	- Una Cassa di Risparmio presente sul territorio di una Provincia - Gli impianti di una Utilità locale	- Le stazioni dell'Arma dei Carabinieri - Gli impianti di commutazione di Telecom Italia - Le stazioni ferroviarie - Le stazioni di trasformazione dell'ENEL

Tabella 7: Esempi di reti CII nello scenario italiano

Quanto ciò possa influire sulla struttura di rete risulta immediatamente:

- La copertura territoriale locale rende economicamente competitiva la realizzazione di reti con l'utilizzo di portanti trasmissive private, come ad esempio una rete wireless o realizzata in fibra ottica a copertura di un'area portuale o ospedaliera.

Poche organizzazioni (in Italia Ferrovie, RAI, Ministero della Difesa, le varie Telecom) possono infatti permettersi di costituire (o già dispongono di) reti estese a livello nazionale che utilizzino portanti trasmissive private

- La distribuzione capillare delle sedi pone importanti problemi nella realizzazione di reti sicure; infatti la vulnerabilità delle reti aumenta al crescere del numero dei punti d'accesso. Per motivi di ordine economico e geografico, le reti di questo tipo si prestano a essere realizzate su più livelli, introducendo punti di concentrazione. La presenza di punti di concentrazione aumenta la vulnerabilità di una rete. Una distribuzione capillare di sedi rende inoltre necessario adottare sistemi di protezione degli accessi a costi contenuti, a copertura di reti di accesso spesso molto articolate.

La Tabella 7 può quindi essere "riletta" in termini di caratteristiche architetturali, come riportato in Tabella 8.

	Copertura territoriale locale	**Copertura territoriale estesa a livello nazionale**
Distribuzione limitata delle sedi	-Reti di tipo LAN o MAN che collegano un numero limitato di "isole" -Reti di accesso spesso assenti -Portanti trasmissive private disponibili a costo contenuto o medio	-Reti WAN che collegano grosse LAN -Reti di accesso generalmente poco articolate -Portanti trasmissive private disponibili a costo alto
Distribuzione capillare delle sedi	-Reti che in scala ridotta presentano già le caratteristiche delle WAN -Reti di accesso articolate e con presenza di punti di concentrazione- -Portanti trasmissive private disponibili a costo medio o alto (se riferito alla totalità delle sedi)	-Reti WAN spesso strutturate su più livelli -Reti di accesso molto articolate e con presenza di punti di concentrazione -Portanti trasmissive private disponibili a costo alto e spesso proibitivo (se riferito alla totalità delle sedi)

Tabella 8: Caratteristiche Architetturali di Reti CII

Un secondo criterio è quello del confinamento della rete. Una rete confinata è una rete chiusa e separata dal "mondo esterno", ossia da ogni altra rete, pubblica o appartenente ad altre organizzazioni. Una intranet è un buon esempio di rete confinata.

Alcune organizzazioni non vogliono o non possono adottare un modello di rete confinata: si pensi per esempio alle opportunità date al cittadino di ottenere certificati anagrafici dal Comune di residenza attraverso procedure di e-government.

Il confinamento di una rete può avvenire sia a livello fisico, sia a livello logico. Le reti di massima sicurezza sono evidentemente reti confinate sia fisicamente, che logicamente. Una rete che non sia confinata né fisicamente, né logicamente è detta "aperta". Internet è un buon esempio di rete aperta. Generalmente, per una rete l'essere confinata fisicamente implica esserlo anche logicamente. Non vale il viceversa; infatti molte reti che logicamente sono confinate, in realtà insistono su portanti fisiche fornite ed esercite da organizzazioni esterne (Service Provider).

In una rete confinata gli utenti sono tutti noti o almeno appartengono a categorie note. Ciò semplifica la gestione degli accessi rispetto al caso di rete non confinata che debba poter accettare anche l'utente anonimo in possesso di credenziali sufficienti, spesso conferite da una "terza parte accreditata" (o Certification Authority).

Un terzo criterio è quello della disponibilità di strutture di comunicazione presso una determinata organizzazione, cioè di siti o di infrastrutture che supportino o che possano supportare una rete di telecomunicazioni.

Dipendendo dalla propria copertura territoriale, un'organizzazione può disporre di siti tra loro in visibilità ottica che possono supportare la creazione di una rete di telecomunicazioni, scelta una data portante trasmissiva, ad un dato costo. In mancanza di ciò e specie quando la copertura territoriale sia estesa e la distribuzione delle sedi capillare, l'organizzazione in questione può dotarsi di una rete sicura appoggiandosi a portanti trasmissive altrui. La scelta della soluzione più conveniente dipende dalla valutazione effettuata nel progetto della rete e, in particolare, dalle considerazioni riguardo all'affidabilità ed alla disponibilità della rete fisica.

Il progetto di una rete sicura deve partire dalla definizione di due elementi fondamentali e precisamente:

- la definizione del livello di sicurezza che il Cliente richiede
- la definizione del requisito operativo della rete.

La definizione del livello di sicurezza che l'organizzazione deve coprire tocca vari aspetti quali:

- la definizione del/dei livello/i di sicurezza dell'informazione
- la definizione dei parametri di QoS richiesti
- la definizione della/delle integrità dei dati richiesti
- la definizione della minaccia in presenza della quale la rete deve operare al 100% o in modo ridotto gestendo solamente i dati "essenziali"
- la definizione di quale porzione della rete si vuole che operi in sicurezza massima, quale in sicurezza media e quale a bassa sicurezza (open world)
- ogni altro aspetto legato alla definizione della sicurezza richiesta.

La definizione del requisito operativo della rete dovrà comprendere, tra l'altro, i seguenti aspetti:

- numero di utenti
- tipologia di ogni singolo utente o di ogni singola LAN
- traffico massimo
- priorità assegnate
- livelli di sicurezza
- importanza
- dislocazione degli utenti
- connettività richiesta ed eventuale utilizzo di portanti trasmissive in diversità (cavo, ponte radio, satellite, ecc.).

3.2.2.2.4 Mantenimento ciclico del sistema di produzione

Il Sistema di Protezione impostato risente delle variazioni logistiche e dello scenario tecnologico ed è quindi necessario garantire che tali variazioni vengano in esso recepite.

Di seguito si riporta un elenco (ancorché non esaustivo) degli eventi che richiedono un aggiornamento del Sistema di Protezione:

- variazione del quadro legislativo nazionale
- variazioni organizzative
- variazione degli obiettivi di sicurezza
- individuazione di nuove tipologie di minacce
- individuazione di nuove tipologie di vulnerabilità
- evoluzione della tecnologia
- variazione del perimetro d'intervento.

Queste variazioni impongono una revisione di tutto il ciclo di Analisi del Rischio sopra descritto, a partire dai suoi requisiti e presupposti di base. L'adeguamento tempestivo del Sistema di Protezione e della relativa documentazione sono importanti dal punto di vista dell'efficacia del livello di protezione fornito; diventano indispensabili nel caso in cui si voglia procedere a Certificazione del Sistema di Protezione.

3.2.2.2.4.1 La valutazione e la certificazione di sicurezza

Con il termine "certificazione di sicurezza" si intende la verifica e l'attestazione, condotta da enti terzi indipendenti, qualificati e ufficialmente riconosciuti, della conformità di un sistema, di un prodotto, di un processo o di un servizio rispetto ai requisiti di sicurezza previsti da uno standard o da una norma di riferimento.

Il processo di valutazione e certificazione della sicurezza ICT deve avere le seguenti caratteristiche:

- · *Ripetibilità*: a parità di obiettivi e requisiti di sicurezza inizialmente imposti, il processo di valutazione deve portare allo

stesso verdetto finale se rieseguito da parte dello stesso Ente di valutazione

- *Riproducibilità*: a parità di obiettivi e requisiti di sicurezza inizialmente imposti, il processo di valutazione deve portare allo stesso verdetto finale se rieseguito da parte di un altro Ente di valutazione
- *Imparzialità*: il processo di valutazione e certificazione non deve essere influenzato da fattori esterni
- *Oggettività*: il risultato della valutazione di sicurezza deve essere basato su fatti il più possibile immuni da opinioni o esperienze soggettive.

Gli aspetti fondamentali che nel mondo reale rendono utile ed efficace un processo di valutazione e certificazione della sicurezza sono, quindi, la dimostrata efficacia degli standard di riferimento e l'effettiva terzietà degli enti certificatori e valutatori rispetto agli utenti finali, agli sviluppatori del sistema, del processo o del prodotto e ai finanziatori del processo di certificazione.

Nel caso specifico della certificazione di sicurezza, il primo aspetto può essere considerato soddisfatto, in particolare, quando vengono applicati standard collaudati nel tempo da una pluralità di soggetti e siano state individuate modalità di attuazione che, da un lato, risultino efficaci per migliorare la sicurezza ICT e, dall'altro, che consentano una effettiva integrazione delle misure di sicurezza nei processi produttivi delle Organizzazioni che li adottino.

Per quanto riguarda il secondo aspetto, una valida garanzia riguardo alla terzietà del processo di certificazione può essere rappresentata dalla circostanza che almeno gli Enti certificatori, se non addirittura anche gli Enti che svolgono le valutazioni di sicurezza, abbiano una investitura ufficiale da parte dello Stato in cui operano e/o siano riconosciuti da parte di organizzazioni internazionali indipendenti.

Nel caso specifico delle infrastrutture critiche, il Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni si riserva di raccomandare che almeno i sistemi/prodotti ICT che gestiscono le informazioni e le applicazioni che necessitano di una elevata protezione siano sottoposti a cer-

tificazione secondo i Common Criteria o i criteri ITSEC. Questa indicazione è in linea con quanto previsto dal DPCM "Approvazione dello Schema Nazionale per la valutazione di certificazione e Sicurezza nel settore della Tecnologia dell'Informazione, ai sensi del'art. 10 comma 1 del D.Lgs. 10/2002". Ad esempio il documento "National Security Telecommunications and Information Systems" edito dal "National Security Telecommunications and Information Systems Security Committee (NSTISSC) consiglia l'uso della certificazione di sicurezza sia per i sistemi che trattano informazioni che, sebbene non classificate ai fini della sicurezza nazionale, possono essere considerate critiche o essenziali per lo svolgimento delle funzioni primarie dell'Amministrazione, sia per i sistemi da cui dipendono l'operatività e/o la manutenzione delle infrastrutture critiche.

Inoltre, nel documento "The National Strategy to Secure Cyberspace" - Documento governativo USA - Febbraio 2003, 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. I due principali tipi di certificazione della sicurezza ICT oggi utilizzati sono stati standardizzati dall'ISO/IEC, sebbene per uno dei due il relativo processo non si può considerare completo. Più precisamente, nel 1999 è stata adottata dall'ISO/IEC la raccolta completa di criteri conosciuta come "Common Criteria", che consente la valutazione e la certificazione della sicurezza di prodotti e sistemi ICT. Tale adozione si è formalmente realizzata attraverso l'emanazione dello standard ISO/IEC IS 15408.

Per quanto riguarda il secondo tipo di certificazione, nel 2000 l'ISO ha adottato la sola prima parte dello standard BS7799 sviluppato in Gran Bretagna. Nella versione ISO/IEC ha assunto la denominazione IS 17799-1. La seconda parte dello standard, quella che contiene 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 hanno lo scopo di certificare cose ben diverse: nel caso dei Common Criteria (CC) oggetto della certificazione è un *sistema* o un *prodotto* ICT[5], nel caso 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 viene indicato nello standard con l'acronimo ISMS che sta per "Information Security Management System". La certificazione BS7799 può essere considerata una certificazione aziendale, del tipo, quindi, della ben nota certificazione ISO 9000, ma specializzata nel campo della sicurezza ICT.

La precisazione circa l'oggetto della certificazione è opportuna poichè, 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. 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.

---

[5] 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.

3.2.2.2.4.1.1 I Common Criteria

La filosofia che è alla base dei Common Criteria (CC) è stata ripresa dai precedenti criteri europei ITSEC[6] (Information Technology Security Evaluation Criteria) che per primi l'hanno introdotta. In base a tale filosofia non ha senso verificare se un sistema/prodotto è sicuro se non si specifica:

- "sicuro" per fare cosa (*obiettivi di sicurezza*)
- "sicuro" in quale contesto (*ambiente di sicurezza*)
- "sicuro" a fronte di quali verifiche (requisiti di *garanzia*).

Un *obiettivo di sicurezza* viene definito, secondo i *CC*, come l'intenzione di contrastare una minaccia o quella di rispettare leggi, regolamenti o politiche di sicurezza preesistenti. Il conseguimento degli obiettivi avviene attraverso l'adozione di *misure di sicurezza* tecniche (*funzioni di sicurezza*) e non tecniche (fisiche, procedurali e relative al personale).

L'*ambiente di sicurezza* viene descritto in termini di:

- uso ipotizzato del sistema/prodotto (applicazioni, utenti, informazioni trattate ed altri beni con specifica del relativo valore)
- ambiente di utilizzo (misure di sicurezza non tecniche, collegamento con altri apparati ICT)
- minacce da contrastare, specificando caratteristiche dell'attaccante (conoscenze, risorse disponibili e motivazione), metodi di attacco (citando, tra l'altro, lo sfruttamento di eventuali vulnerabilità note del sistema/prodotto ICT), beni colpiti
- politiche di sicurezza dell'Organizzazione.

---

[6] In questo contesto, si ritiene opportuno non entrare nei dettagli dello standard ITSEC, limitandosi alla descrizione dei soli Common Criteria. Tale scelta è motivata dal fatto che, nonostante sia ancora possibile, anche in Italia, certificare la sicurezza ICT applicando i criteri ITSEC, la comunità europea consiglia l'uso dei Common Criteria (vedi risoluzione del Consiglio dell'Unione Europea del 28 gennaio 2002 (2002/C 43/02).

Le verifiche previste durante il processo di valutazione mirano ad accertare che siano stati soddisfatti, da parte del sistema/prodotto, del suo sviluppatore e del valutatore, opportuni requisiti di *garanzia* che diventano sempre più severi al crescere del livello di valutazione. I CC definiscono una scala di 7 livelli di valutazione (EAL1, EAL2,..., EAL7) o livelli di *garanzia*, precisando, per ogni livello di tale scala uno specifico insieme di r*equisiti di garanzia*.

Le verifiche, eseguite in base ai requisiti di *garanzia* del livello di valutazione considerato, hanno lo scopo di fornire garanzie circa:

- l'idoneità delle funzioni di sicurezza a soddisfare gli obiettivi di sicurezza del sistema/prodotto
- l'assenza di errori nel processo che dalle specifiche iniziali di sicurezza (ambiente e obiettivi di sicurezza) porta alla pratica realizzazione delle funzioni di sicurezza (errori di interpretazione delle specifiche tecniche, errori di programmazione, ecc.)
- l'adeguatezza delle procedure di sicurezza previste per la consegna e per l'installazione del sistema/prodotto (per evitare che il sistema/prodotto che perviene all'utente finale possa differire, magari anche di poco, da quello sottoposto a valutazione/certificazione), la chiarezza dei manuali d'uso e d'amministrazione (questi ultimi potrebbero infatti indurre gli utilizzatori a comportamenti che introducono vulnerabilità nell'utilizzo di un prodotto/sistema dotato di funzioni di sicurezza del tutto idonee e realizzate senza errori), il supporto che lo sviluppatore si impegna a fornire a chi usa il sistema o prodotto per rimediare ad eventuali vulnerabilità emerse dopo la valutazione.

Le garanzie circa l'assenza di errori nel processo di realizzazione delle funzioni di sicurezza non vengono ottenute solamente ricercando direttamente gli errori stessi (analizzando la documentazione presentata dal richiedente della valutazione e sottoponendo il sistema/prodotto a *test* funzionali e ad attacchi), bensì anche verificando che nel processo di realizzazione sia stato previsto l'impiego di strumenti, metodologie e procedure finalizzati alla riduzione della probabilità di errori.

Al crescere del livello di valutazione:

- vengono richieste specifiche realizzative più dettagliate (ad esempio progetto ad alto livello, progetto a basso livello, codice sorgente)
- il livello di rigore con il quale le specifiche devono essere descritte aumenta (descrizione informale, semiformale, formale).

Nella *Fig. 7* sono riportati, per ogni livello di valutazione, il rigore di descrizione delle specifiche richiesto (area di colore giallo) e le principali verifiche effettuate in sede di valutazione (area di colore verde).

Il rigore della valutazione non viene individuato solo dal livello di valutazione bensì anche da un altro parametro. Infatti per le funzioni che devono essere realizzate con meccanismi probabilistici o di

	Specifiche Funzion.	Disegno Architettur.	Disegno Dettaglio	Implementazione	Test Funzionali	Test Intrusione	Configur. Manag.	Consegna e Instal.	Sic. Ambiente Svil.	Tools sviluppo
EAL0	-	-	-	-	-	-	-	-	-	-
EAL1	inform	-	-	-	√	-	√	√	-	-
EAL2	inform	inform	-	-	√	√	√	√	-	-
EAL3	inform	inform	-	-	√	√	√	√	√	-
EAL4	inform	inform	inform	parz	√	√	√	√	√	√
EAL5	s.form	s.form	inform	compl	√	√	√	√	√	√
EAL6	s.form	s.form	s.form	strutt	√	√	√	√	√	√
EAL7	form	form	s.form	strutt	√	√	√	√	√	√

inform: descrizione informale
s.form: descrizione semi-formale
form: descrizione formale

parz: documentazione parziale
compl: documentazione completa
strutt: documentazione strutturata

Fig. 7: Specifiche e test in funzione del livello di valutazione

permutazione (*password*, funzioni *hash*, ecc.), i CC richiedono (a partire da EAL2) che venga specificato un livello minimo di robustezza (SOF - *Strength Of Functionality*) su una scala a tre valori (*basic*, *medium*, *high*).

Le funzioni di sicurezza del sistema/prodotto vengono descritte in base ai requisiti cui devono soddisfare. Tali requisiti, denominati *requisiti funzionali*, così come i già citati *requisiti di garanzia*, devono essere espressi (a meno di possibili eccezioni che occorre comunque giustificare) utilizzando un catalogo di componenti fornito nei CC. Più precisamente il catalogo delle componenti funzionali costituisce la parte 2 dei CC, mentre quello delle componenti di *garanzia* la parte 3. I cataloghi sono strutturati su più livelli gerarchici in modo da raccogliere componenti di tipo omogeneo. A titolo di esempio, per quanto riguarda le componenti funzionali, al livello gerarchico più elevato è previsto un raggruppamento secondo le undici classi: *Audit, Communication, Cryptographic Support, User Data Protection, Identification and Authentication, Security management, Privacy, Protection of the TOE Security Function, Resource Utilization, TOE Access, Trusted Path/Channels* (l'acronimo TOE ricorrente in alcuni nomi di classi funzionali indica il sistema/prodotto ICT da valutare).

Tra i vari documenti che il richiedente della valutazione deve/può consegnare ai valutatori, unitamente al sistema/prodotto ICT da valutare, due meritano un particolare cenno. Il primo, denominato *Security Target*, deve essere obbligatoriamente fornito e rappresenta il documento principale della valutazione. Nel *Security Target* devono essere descritti l'ambiente di sicurezza, gli obiettivi di sicurezza, i requisiti funzionali e di *garanzia* (e quindi il livello di valutazione), la robustezza minima delle funzioni di sicurezza ed una prima descrizione ad alto livello delle funzioni di sicurezza. Quest'ultima sezione non è invece contenuta nel secondo documento, il *Protection Profile*, che per il resto ha una struttura del tutto simile a quella del *Security Target*. Il *Protection Profile* può essere opzionalmente sviluppato con riferimento ad un'intera classe di prodotti (per la quale si lascia la libertà di realizzare le funzioni di sicurezza in un qualsiasi modo che soddisfi i requisiti funzionali) piuttosto che con riferimento ad uno specifico sistema/prodotto ICT (come è il caso, invece, del *Security Target*). Il *Protection Profile* può essere registrato e anche valutato per verificarne la coerenza interna.

I principali vantaggi ottenibili da una valutazione e certificazio-

ne in accordo con i CC sono:

- la verifica, eseguita da una terza parte per la quale viene riconosciuto il possesso di conoscenze specialistiche, che le funzionalità di sicurezza del sistema/prodotto ICT, affiancate alle contromisure non tecniche previste, siano adeguate al soddisfacimento degli obiettivi di sicurezza
- lo svolgimento di un'azione di contrasto preventivo degli incidenti di sicurezza ICT
- le maggiori garanzie che i CC offrono rispetto ad altri strumenti di contrasto di tipo preventivo
- la disponibilità di vasti cataloghi relativamente alle funzionalità di sicurezza ICT e ai requisiti di *garanzia* adottabili
- la possibilità di esprimere in forma standardizzata requisiti di sicurezza per sistemi e prodotti ICT.

3.2.2.2.4.1.2 Gli standard ISO/IEC IS 17799-1 e BS7799-2

L'evoluzione storica degli standard del tipo BS7799 può essere così sintetizzata:

- 1995: il British Standard Institution (BSI) pubblica lo standard BS7799-1 "Code of Practice for Information Security Management" derivato da una raccolta di "best practices" prodotta dal Department of Trade and Industry
- 1998: il BSI viene aggiunta la seconda parte intitolata BS7799-2 "Part 2: Specification for Information Security Management Systems"
- 1999: il BSI pubblica una nuova versione delle due parti dello standard identificate come BS7799 - 1 e BS7799 - 2
- 2000: la parte 1 dello standard BS7799 diviene lo standard internazionale ISO/IEC 17799-1
- 2002: viene pubblicata una nuova versione della parte 2, lo standard in relazione al quale vengono attualmente rilasciate le certificazioni

Gli standard BS7799 sono nati con lo scopo principale di costituire un riferimento universalmente riconosciuto e accettato per la certificazione della capacità di un'organizzazione di tutelare il proprio patrimonio informativo e di mantenere tale capacità nel tempo. Essi costituiscono, inoltre, una raccolta di best practice in materia di sicurezza delle informazioni e forniscono un riferimento metodologico per la gestione della sicurezza del patrimonio informativo aziendale.

Ogni organizzazione dovrebbe proteggere le informazioni che tratta mediante la corretta individuazione e gestione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o, in inglese, ISMS: Information Security Management System) composto di componenti logiche, fisiche e organizzative. La metodologia di approccio al problema suggerita dagli standard BS7799 e conosciuta con l'acronimo PDCA (Plan Do Check Act), prevede l'esecuzione di quattro fasi:

- Plan: in cui si definiscono le politiche di sicurezza, gli obiettivi, i processi e le procedure rilevanti per gestire e minimizzare il rischio e per migliorare la sicurezza delle informazioni, in modo da produrre risultati in accordo con le politiche e gli obiettivi dell'intera organizzazione
- Do: in cui si realizzano e si rendono operative le politiche, le contromisure, i processi e le procedure di sicurezza
- Check: in cui si valutano e, ove possibile, si misurano, le prestazioni del processo (rispetto alle politiche di sicurezza), gli obiettivi, le esperienze pratiche e si segnalano i risultati al management per la revisione
- Act: in cui si adottano azioni preventive e correttive, basate sui risultati del Management Review, al fine di realizzare il miglioramento continuo del SGSI.

La *Fig. 8* tratta dalla BS7799-2, schematizza le fasi fondamentali della metodologia PDCA.

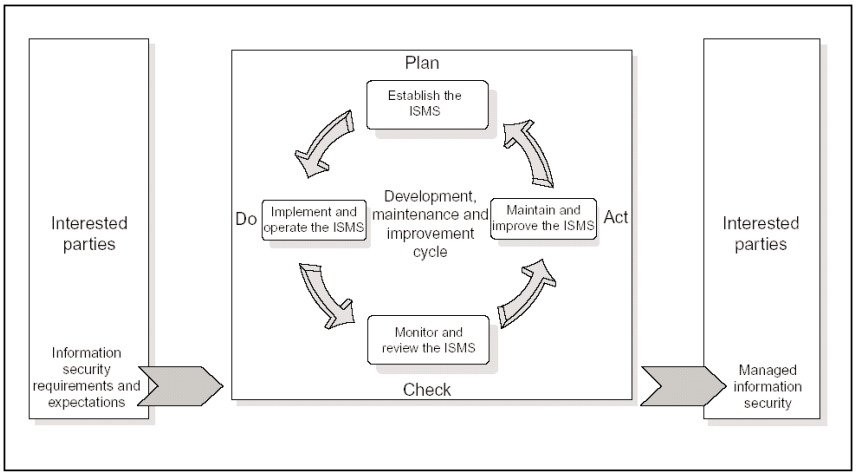


Fig. 8 Modello PDCA applicato ai processi ISMS

Un aspetto fondamentale nella corretta applicazione della BS7799 è rappresentato dalla effettuazione di una corretta attività di analisi dei rischi. Le basi fondamentali di attività sono descritte nello standard ISO/IEC 13335 "Guidelines for the management of IT security", a cui si rimanda per un utile approfondimento.

Nella BS7799-2, infine, sono riportati in dettaglio i controlli di sicurezza che devono essere realizzati, in base all'analisi dei rischi effettuata, dall'Organizzazione al fine di verificare se l'SGSI adottata è stata individuata applicando correttamente l'approccio previsto dallo standard. I controlli di sicurezza sono suddivisi nelle seguenti aree:

- *Politiche di sicurezza:* corretta individuazione e gestione nel tempo delle politiche di sicurezza
- *Organizzazione della sicurezza:* organizzazione e le responsabilità aziendali in materia di sicurezza ICT, che disciplinano l'accesso di terze parti ai sistemi informativi aziendali e che regolamentano i rapporti nei contratti di outsourcing
- *Controllo e classificazione dei beni da proteggere:* classificazione dei beni aziendali e la loro assegnazione a soggetti ben individuati
- *Sicurezza del personale:* comportamenti di sicurezza degli utenti dei beni aziendali, includendo anche la formazione sul corret-

to uso e i comportamenti che devono essere tenuti in caso di incidente informatico

- *Sicurezza ambientale e fisica:* sicurezza fisica degli ambienti di lavoro e degli strumenti hardware e software
- *Gestione delle comunicazioni:* gestione delle comunicazioni interaziendali, gestione degli aspetti di rete, protezione contro software maliziosi e gestione dei guasti
- *Controllo d'accesso:* autorizzazioni all'accesso alle informazioni, all'accesso alla rete e alla identificazione e autenticazione degli utenti
- *Manutenzione e sviluppo dei sistemi:* uso della cifratura, aspetti di preservazione dell'integrità delle informazioni e norme per l'aggiornamento e gestione di sistemi hardware e software.
- *Gestione della "business continuity":* migliorare e assicurare la continuità delle funzionalità critiche
- *Adeguamento alle leggi vigenti:* assicurare il rispetto delle normative vigenti e delle politiche di sicurezza aziendali, sia da parte dell'organizzazione, sia da parte dei singoli utenti.

3.2.2.2.4.2 La certificazione di sicurezza in Italia secondo i Common Criteria (e ITSEC)

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 uti-

lizzata 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 cinque Ce.Va., due dei quali appartenente alla P.A., ossia quello gestito dall'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero delle Comunicazioni e quello della Difesa, dipendente dallo Stato Maggiore della Difesa, Reparto Informazioni e Sicurezza, dislocato a S. Piero a Grado (PISA)[7].

Per la gestione delle valutazioni e certificazioni di sicurezza in ambito commerciale secondo gli standard ITSEC e CC, con DPCM del 30 ottobre 2003 (G.U. n. 98 del 27 aprile 2004) è stato istituito lo Schema Nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione. Lo Schema Nazionale definisce l'insieme delle procedure e delle regole nazionali necessarie per la valutazione e la certificazione di sistemi e prodotti ICT, in conformità ai criteri europei ITSEC e alla relativa metodologia applicativa ITSEM o agli standard internazionali ISO/IEC IS-15408 (Common Criteria).

Nell'ambito dello Schema Nazionale di valutazione e certificazione è stato istituito l'Organismo di certificazione della sicurezza informatica (O.C.S.I.). L'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione è l'Organismo di certificazione della sicurezza informatica nel settore della tecnologia dell'informazione[8].

Le principali motivazioni che hanno portato alla istituzione dello Schema nazionale in ambito commerciale derivano dalle seguenti considerazioni:

- l'informazione, nell'attuale società, costituisce un bene essenziale e si rende necessario garantirne l'integrità, la disponibilità

[7] Per completezza si riportano anche gli altri CE.VA.: Consorzio RES, INFORSUD, IMQ.

[8] Anche ai sensi dell'articolo 10 del decreto legislativo 23 gennaio 2002, n. 10 e dell'articolo 3, paragrafo 4 della direttiva 1999/93/CE.

e la riservatezza con misure di sicurezza che costituiscano parte integrante di un sistema informatico

- da tempo i produttori offrono sistemi e prodotti dotati di funzionalità di sicurezza, per le quali dichiarano caratteristiche e prestazioni al fine di orientare gli utenti nella scelta delle soluzioni più idonee a soddisfare le proprie esigenze
- in molte applicazioni caratterizzate da un elevato grado di criticità, le predette dichiarazioni potrebbero risultare non sufficienti, rendendo necessaria una loro valutazione e certificazione della sicurezza, condotte da soggetti indipendenti e qualificati, sulla base di standard riconosciuti a livello nazionale ed internazionale
- le garanzie concernenti l'adeguatezza, la qualità e l'efficacia dei dispositivi di sicurezza di un sistema informatico possono essere fornite solo da certificatori e valutatori indipendenti ed imparziali
- la necessità di favorire, a livello comunitario e internazionale, la cooperazione tra gli Organismi di Certificazione e il mutuo riconoscimento dei certificati di valutazione della sicurezza nel settore della tecnologia dell'informazione.

Nello Schema commerciale, l'OCSI svolge i seguenti compiti principali:

- predispone le regole tecniche in materia di certificazione sulla base delle norme e direttive nazionali, comunitarie ed internazionali di riferimento
- gestisce i rapporti internazionali con enti esteri omologhi al fine di favorire il mutuo riconoscimento dei rispettivi Schemi e delle Certificazioni rilasciate
- coordina le attività nell'ambito dello Schema nazionale in armonia con i criteri ed i metodi di valutazione
- predispone le Linee Guida per la valutazione di prodotti, traguardi di sicurezza (*security target*), profili di protezione e sistemi (*protection profile*), ai fini del funzionamento dello Schema

- gestisce l'accreditamento, la sospensione e la revoca dell'accreditamento dei Laboratori di valutazione della sicurezza (LVS)
- verifica il mantenimento dell'indipendenza, imparzialità, affidabilità, competenze tecniche e capacità operative da parte dei LVS accreditati
- approva i Piani di Valutazione
- approva i Rapporti Finali di Valutazione
- emette i Rapporti di Certificazione sulla base delle valutazioni eseguite dai LVS
- gestisce l'emissione e la revoca dei Certificati
- gestisce la predisposizione, la tenuta e l'aggiornamento dell'elenco degli LVS accreditati
- gestisce la formazione, abilitazione e addestramento dei Certificatori, personale dipendente dell'Organismo di Certificazione, nonché dei Valutatori, dipendenti dei LVS e Assistenti, ai fini dello svolgimento delle attività di valutazione
- gestisce la predisposizione, tenuta e aggiornamento dell'elenco dei Certificatori, Valutatori e Assistenti.

Il processo di valutazione e certificazione secondo lo Schema nazionale può, quindi, essere rappresentato come in *Fig. 9*

L'OCSI, dopo aver accreditato l'LVS, interviene controllando e gestendo l'intero processo di valutazione della sicurezza effettuato dall'LVS stesso, rendendosi garante della corretta applicazione delle regole dello Schema Nazionale. L'emissione del Certificato viene effettuata dall'Organismo di Certificazione.

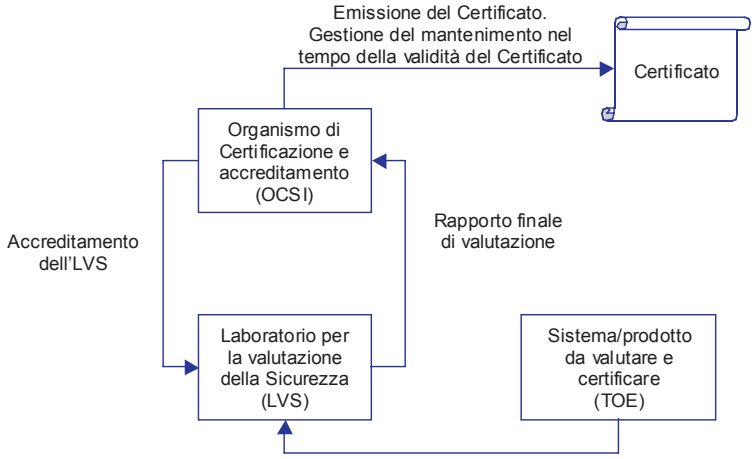


Fig. 9: Schematizzazione del processo di valutazione e certificazione secondo i CC

3.2.2.2.4.2.1 L'accreditamento per la certificazione volontaria secondo la Norma BS 7799-2:2002

Il processo di certificazione secondo gli standard volontari, quali le Norme ISO 9001, ISO 14001, BS 7799-2 e la Specifica Tecnica OHSAS 18001, per come integrata dalle Linea Guida UNI INAIL, avviene sulla base delle attività di Audit e di valutazione svolte dagli Organismi di Certificazione che operano sotto l'Accreditamento. Nel nostro Paese, l'Ente riconosciuto per svolgere le attività di Accreditamento è il SINCERT. Ciò nonostante, sono pienamente valide e riconosciute anche le Certificazioni emesse sotto Accreditamento rilasciato dagli Enti stranieri, firmatari dei cosiddetti MLA - Multilateral Agreement - riconosciuti nell'ambito dell'Unione Europea dall'EA [European Cooperation for Accreditation] ed in ambito internazionale dall'IAF [International Accreditation Forum] ed attraverso i quali, oltretutto, si tende a ridurre le barriere presenti nel commercio internazionale.

Tale mutuo riconoscimento garantisce il rispetto di regole precise di comportamento degli Organismi di Certificazione che, volontariamente, si sottopongono a verifiche molto approfondite, da parte

delle rispettive "Authority" di controllo e degli stessi Enti di Accreditamento, a loro volta soggetti a rigorosi controlli nell'ambito degli accordi multilaterali di cui sopra.

Quali sono dunque i principi di base che regolano l'accreditamento di un Organismo di Certificazione? In primis, ovviamente, la competenza delle risorse umane addette alle attività di valutazione delle diverse Organizzazioni clienti. Quindi il comportamento non sperequativo nei confronti delle stesse Organizzazioni, se appartenenti a gruppi di interesse diversi, ma, significativamente, anche l'assenza di qualunque conflitto di interessi tra il chi certifica e le Organizzazioni certificande. L'Ente di Accreditamento, così come gli Organismi di Certificazione, deve dare evidenza di avere una forte rappresentatività delle diverse parti interessate al processo di certificazione, clienti, consumatori, produttori ed Autorità Pubbliche deputate al controllo ovvero alla disciplina del mercato.

L'accreditamento, quindi, è un processo che fornisce una garanzia al mercato, attraverso la valutazione e la successiva sorveglianza, affinché si possa avere fiducia nei certificati rilasciati dagli organismi accreditati.

Purtroppo, accade che nel mercato nazionale operino anche soggetti che non hanno alcuna legittimazione, creando confusione sull'applicazione delle regole e rilasciando delle pseudo-certificazioni, che non possono avere alcun valore nell'ambito della negoziazione con la Pubblica Amministrazione, che risultano autoreferenziate e, come tali, non possono avere il valore di riconoscibilità offerto, per contro, sul mercato nazionale ed internazionale dalle Certificazioni emesse sotto Accreditamento degli Enti che si riconoscono nell'EA e nell'IAF.

Specificatamente per le certificazioni secondo la BS 7799-2, il SINCERT sta emettendo un Regolamento Tecnico. Tale documento individua delle prescrizioni aggiuntive per gli Organismi di Certificazione [non per le Organizzazioni certificande], mirate alla definizione di una cornice di comportamenti il più possibile omogenei, con l'obiettivo di individuare delle caratteristiche degli Auditor e delle regole di valutazione, atte a garantire un elevato valore aggiunto non solo per le Organizzazioni che richiedono la Certificazione, ma anche per il mercato. Infatti, quest'ultimo, sulla base di tale riconoscimento,

può attribuire alle Organizzazioni certificate, nel loro complesso, un livello di fiducia che può e deve essere garantito nel migliore dei modi.

Lo schema generale di certificazione secondo la norma BS7799-2 è riportato nella *Fig. 10* e differisce da quello presentato in precedenza per i CC essenzialmente nel fatto che il certificato viene emesso dagli Organismi di Certificazione (che potrebbero essere assimilati agli LVS nello Schema CC) e non dal SINCERT (che potrebbe essere assimilato all'OCSI nello Schema CC).

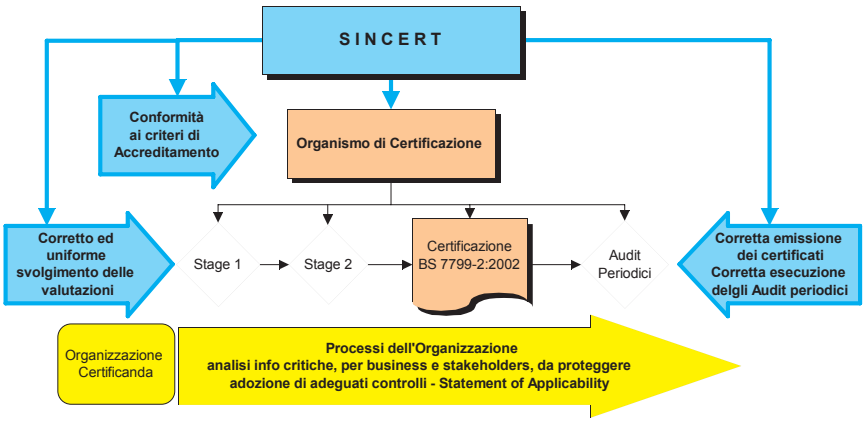


Fig. 10: Schema di certificazione secondo la BS7799-2:2002

3.2.2.2.5 Le architetture delle reti di supporto alle infrastrutture critiche

3.2.2.2.5.1 Le tipologie di reti sicure

La Buona Pratica "raccomanda" che le problematiche legate alle Reti di Comunicazioni a supporto delle Infrastrutture Critiche siano affrontate con tre diverse tipologie e precisamente:

- **Reti a Massima Sicurezza** per operare con ***dati strategici*** (**critici**)
- **Reti Sicure** per operare con **dati sicuri**

- **Reti Robuste** per operare con **dati normali.**

I paragrafi che seguono forniscono le caratteristiche consigliate per Reti di Comunicazione che debbano operare rispettivamente con le suddette tre tipologie di dati.

3.2.2.2.5.1.1 Reti a Massima Sicurezza

Le **Reti a Massima Sicurezza** rappresentano una soluzione altamente affidabile alle problematiche di operare con dati strategici e critici la cui presenza, trasmissione e integrità, debba di fatto essere garantita "sempre" ovvero anche in presenza di condizioni anomale quali disastri naturali o azioni terroristiche.

Alcune raccomandazioni tipiche di alto livello relative a tale tipo di rete possono essere sintetizzate come segue.

La **Rete a Massima Sicurezza** deve:

- essere "isolata"[9] ovvero separata da altre reti non a massima sicurezza che operano su dati sicuri o normali (open world)
- essere altamente ridondata (nelle sue componenti HW e SW)
- avere alta connettività K (cfr. par. 3.2.2.2.5.2)
- essere differenziata (si veda *Fig. 11*) nelle sue componenti tipiche:
  - rete di accesso ridondata: tipicamente in tecnica mista (fibra e/o ponte radio "downhill" e/o wireless oppure in fibra con collegamenti ridondati differenziati a livello di percorso fisico)
  - rete di backbone di terra ad alta connettività realizzato tipicamente in fibra
  - rete in ponte radio a incremento della connettività e, in parte, della capacità globale

[9] Con il termine "Isolata" si intende una Rete che non ha alcuna connessione fisica con utenti che non appartengono alla rete o con altre reti a minore livello di sicurezza (ad esempio Internet).

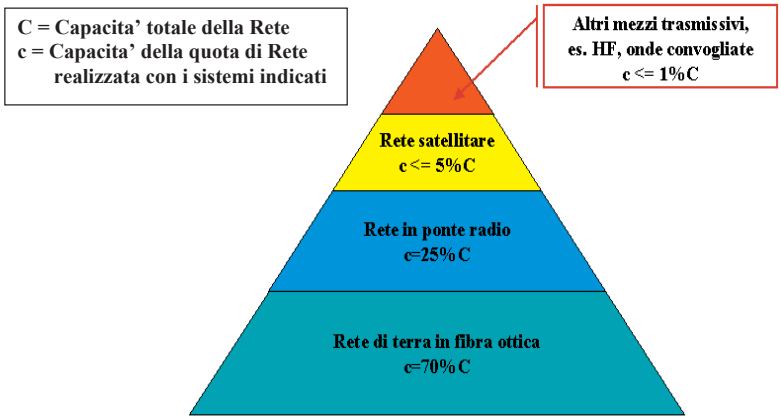


Fig. 11: Componenti tipiche di una Rete a Massima Sicurezza

  - rete satellitare a incremento della connettività
  - altri mezzi trasmissivi quali, ad esempio, le Onde Convogliate
- garantire elevati livelli di servizio per classi di utenza e gestione delle priorità
- garantire elevata integrità dei dati anche prevedendo trasmissione degli stessi tramite diverse componenti della rete (ad esempio fibra più satellite)
- essere dimensionata per il traffico che dovrà trasportare (tenendo conto delle capacità differenti dei mezzi portanti in fibra, in ponte radio e satellitari e quindi coerentemente caratterizzata nelle classi di utenza e nelle priorità)
- essere confinata nell'ambito dell'organizzazione che la usa e si occupa di esercirla e manutenerla, escludendo, di principio, l'outsourcing
- supportare funzionalità di cifratura adeguate a garantire la protezione dell'informazione in funzione della classificazione dei dati trattati; tali funzionalità devono essere rese disponibili a livello di singola componente di accesso e di transito.

In maggiore dettaglio le principali caratteristiche di un esempio di **Rete a Massima Sicurezza** sono elencate nella Tabella 9.

Caratteristica	Valori o Termini di Riferimento	Note
Connettività	k≥2 per accesso, k≥3 per backbone	Realizzata utilizzando percorsi fisici differenziati (criterio prioritario) e/o portanti trasmissive di natura diversa (criterio secondario)
Disponibilità (Availability)	≥ 99.999% da nodo a nodo (per ogni coppia di nodi) per il backbone; ≥ 99.99% end-to-end (per ogni coppia di end-point)	Calcolata su base MTBF, MTTR e connettività in condizioni di normale funzionamento
Indisponibilità operativa	0,1 h	nel periodo di un anno
Dimensionamento a traffico	Rendimento di progetto pari all' 80% sul picco di traffico stimato	Il massimo stimato del traffico impegna l'80% delle risorse in termini di occupazione di banda; il restante 20% delle risorse rimane a disposizione per assorbire eventuali ulteriori sovraccarichi
Differenziazione livelli di QoS	Supportata	Per connessione
Priorità e appropriazione (pre-emption)	Supportate	Priorità definibile a più livelli (MLPP)
Instradamento dipendente dal livello di sicurezza dell'informazione e della risorsa trasmissiva	Supportato	Adattivo automatico su base connessione. Di derivazione militare
Integrità	Garantita	Trasmissione dei dati critici tramite diverse componenti della rete
Graceful Degradation	Garanzia del 90% di espletamento del servizio con rete funzionante all'80%; garanzia dell'80% del servizio con rete funzionante sino al 50%; nessuna garanzia, se non il best effort per i servizi essenziali e per quelli solo oltre il 50% di degrado della rete (es. NATO MINIMIZE, situazione in cui la rete instrada solo il traffico da un certo livello di priorità in su e blocca all'origine il traffico meno prioritario)	La percentuale di funzionamento è in genere misurata in termini di banda residua/banda nominale sulla sommatoria di tutti i collegamenti della rete di backbone. In caso di fuori servizio di un nodo di commutazione si considerano fuori servizio tutti i link ad esso afferenti. La percentuale di degrado è il complemento al 100% della percentuale di funzionamento

Tabella 9: Principali caratteristiche di una Rete a Massima Sicurezza

Caratteristica	Valori o Termini di Riferimento	Note
Possibilità di traffico multiprotocollo (ATM, IP, MPLS, altri)	Supportata	Ritenuta essenziale in caso di alta probabilità di cyber attack
Federabilità con altre reti allo stesso livello di sicurezza.	Ammessa	Deve essere prevista e pianificata a priori
Gateways verso Internet e altre reti non allo stesso livello di sicurezza	Assenti	Non sono ammesse deroghe
Componente di accesso in ponte radio o wireless sicuro	Normalmente presente	Fortemente consigliata, eventualmente come back-up di linea "wired"
Componente di transito in ponte radio	Normalmente presente	Fortemente consigliata
Componente satellitare di accesso	Normalmente presente	Fortemente consigliata
Componente satellitare di transito	Normalmente presente	Fortemente consigliata
Componente deployable (dispiegabile/trasportabile sul territorio)	Normalmente presente	Irrinunciabile in caso di un'Organizzazione che debba supportare lo svolgimento di pubblici servizi in caso di calamità. Può comprendere una componente satellitare di accesso di tipo dispiegabile
Cifratura dei dati in transito	Presente	È garantita la riservatezza e l'autenticazione dei dati in transito con tecniche di "bulk encryption" (cifratura punto-punto a livello link) o "network encryption" (cifratura end-to-end, tipicamente tramite meccanismi di tunnel a livello rete tipo IPSec)
Sicurezza perimetrale (firewalling)	Supportata	È possibile definire policy di rete a livello di accesso
Ownership dell'infrastruttura di trasmissione e di linea	Interna all'organizzazione	Leased line ammesse se di provider diversi con reti diverse e comunque nel minor numero possibile
Ownership dell'infrastruttura di commutazione	Interna all'organizzazione	Non sono ammesse deroghe
Ownership dell'infrastruttura di gestione	Interna all'organizzazione	Non sono ammesse deroghe
Ownership dell'infrastruttura di sicurezza	Interna all'organizzazione	Non sono ammesse deroghe

Tabella 9: Principali caratteristiche di una Rete a Massima Sicurezza (cont.)

3.2.2.2.5.1.2 Reti Sicure

Le **Reti Sicure** si differenziano dalla Reti a Massima Sicurezza principalmente per il fatto di ammettere il collegamento, seppure "protetto", con reti a livello di sicurezza inferiore.

Un altro elemento distintivo e significativo è rappresentato dall'uso di infrastrutture di trasmissione, di commutazione e di gestione non necessariamente proprietarie.

Le principali caratteristiche di un esempio di rete sicura sono riportate in Tabella 10.

3.2.2.2.5.1.3 Reti Robuste

Rappresentano il più basso livello di Rete Sicura in quanto accettano che la Rete operi nell'ambiente "Open World".

Le principali caratteristiche di un esempio di rete robusta sono riportate in Tabella 11.

3.2.2.2.5.2 Topologia di rete - Connettività

Riferendosi alla topologia di una rete, il concetto di "sicurezza" è da interpretarsi come "affidabilità".

Parametro determinante per l'affidabilità di una rete è il suo grado di **Connettività** definito come il parametro **K** così calcolato:

$$\mathbf{K = \min_N \{k(n)\}}$$

dove

- N l'insieme dei nodi di una rete
- n il nodo generico
- k(n) il numero di nodi a cui il nodo n è direttamente connesso.

Caratteristica	Valori o Termini di Riferimento	Note
Connettività	k=2 per accesso dalle postazioni considerate principali, k≥2 per backbone	Realizzata utilizzando percorsi fisici differenziati (criterio prioritario) e/o portanti trasmissive di natura diversa (criterio secondario)
Disponibilità (Availability)	≥ 99.99% da nodo a nodo (per ogni coppia di nodi) per il backbone; ≥ 99.9% end-to-end (per ogni coppia di end-point)	Calcolata su base MTBF, MTTR e connettività in condizioni di normale funzionamento
Indisponibilità operativa	1 h	Nel periodo di un anno
Dimensionamento a traffico	Rendimento di progetto pari all' 80% sul picco di traffico stimato	Il massimo stimato del traffico impegna l'80% delle risorse in termini di occupazione di banda; il restante 20% delle risorse rimane a disposizione per assorbire eventuali ulteriori sovraccarichi
Differenziazione livelli di QoS	Supportata	Per connessione
Priorità e appropriazione (pre-emption)	Supportate	Priorità definibile a più livelli (MLPP)
Instradamento dipendente dal livello di sicurezza dell'informazione e della risorsa trasmissiva	Supportato	Adattivo automatico su base connessione. Di derivazione militare
Integrità	Opzionale	Consigliata
Graceful Degradation	Garanzia del 70% di espletamento del servizio con rete funzionante all'80%; garanzia del 60% del servizio con rete funzionante sino al 50%; nessuna garanzia, se non il best effort per i servizi essenziali e per quelli solo oltre il 50% di degrado della rete (es. NATO MINIMIZE, situazione in cui la rete instrada solo il traffico da un certo livello di priorità in su e blocca all'origine il traffico meno prioritario)	La percentuale di funzionamento è in genere misurata in termini di banda residua/banda nominale sulla sommatoria di tutti i collegamenti della rete di backbone. In caso di fuori servizio di un nodo di commutazione si considerano fuori servizio tutti i link ad esso afferenti. La percentuale di degrado è il complemento al 100% della percentuale di funzionamento

Tabella 10: principali caratteristiche di una Rete Sicura

Caratteristica	Valori o Termini di Riferimento	Note
Possibilità di traffico multiprotocollo (ATM, IP, MPLS, altri)	Fortemente consigliata	Ritenuta essenziale in caso di alta probabilità di cyber attack
Federabilità con altre reti allo stesso livello di sicurezza.	Ammessa	Deve essere prevista e pianificata a priori
Gateways verso Internet e altre reti non allo stesso livello di sicurezza	Protetti da Firewall	Non sono ammesse deroghe all'uso di firewall e strumenti di protezione
Componente di accesso in ponte radio o wireless sicuro	Supportata	Fortemente consigliata, eventualmente come back-up di linea "wired"
Componente di transito in ponte radio	Opzionale	Consigliata
Componente satellitare di accesso	Opzionale	Consigliata
Componente satellitare di transito	Opzionale	Fortemente consigliata
Componente deployable (dispiegabile/trasportabile sul territorio)	Normalmente presente	Irrinunciabile in caso di Organizzazione che debba supportare lo svolgimento di pubblici servizi in caso di calamità. Può comprendere una componente satellitare di accesso di tipo dispiegabile
Cifratura dei dati in transito	Presente	È garantita la riservatezza e l'autenticazione dei dati in transito con tecniche di "bulk encryption" (cifratura punto-punto a livello link) o "network encryption" (cifratura end-to-end, tipicamente tramite meccanismi di tunnel a livello rete tipo IPSec)
Sicurezza perimetrale (firewalling)	Supportata	È possibile definire policy di rete a livello di accesso
Ownership dell'infrastruttura di trasmissione e di linea	Non necessariamente interna all'organizzazione	Leased line ammesse se di provider diversi con reti diverse e comunque nel minor numero possibile
Ownership dell'infrastruttura di commutazione	Meglio se interna all'organizzazione	
Ownership dell'infrastruttura di gestione	Meglio se interna all'organizzazione	
Ownership dell'infrastruttura di sicurezza	Interna all'organizzazione	Non sono ammesse deroghe

Tabella 10: principali caratteristiche di una Rete Sicura (cont.)

Caratteristica	Valori o Termini di Riferimento	Note
Connettività	k≥2 per backbone	Realizzata utilizzando percorsi fisici differenziati (criterio prioritario) e/o portanti trasmissive di natura diversa (criterio secondario)
Disponibilità (Availability)	≥ 99.9% end-to-end (per ogni coppia di end-point)	Calcolata su base MTBF, MTTR e connettività in condizioni di normale funzionamento
Indisponibilità operativa	10 h	Nel periodo di un anno
Dimensionamento a traffico	Rendimento di progetto pari al 90% sul picco di traffico stimato	Il massimo stimato del traffico impegna il 90% delle risorse in termini di occupazione di banda; il restante 10% delle risorse rimane a disposizione per assorbire eventuali ulteriori sovraccarichi
Differenziazione livelli di QoS	Supportata, almeno sui tipi di traffico	Meglio se per connessione
Priorità e appropriazione (preemption)	Fortemente consigliate	Priorità definibile a più livelli (MLPP)
Instradamento dipendente dal livello di sicurezza dell'informazione e della risorsa trasmissiva	Fortemente consigliate	Adattivo automatico su base connessione. Di derivazione militare
Integrità	Opzionale	Consigliata
Graceful Degradation	Garanzia del 70% di espletamento del servizio con rete funzionante all'80%; garanzia del 60% del servizio con rete funzionante sino al 50%; nessuna garanzia, se non il best effort per i servizi essenziali (quando differenziabili) e per quelli solo oltre il 50% di degrado della rete (es. NATO MINIMIZE, situazione in cui la rete instrada solo il traffico da un certo livello di priorità in su e blocca all'origine il traffico meno prioritario)	La percentuale di funzionamento è in genere misurata in termini di banda residua/banda nominale sulla sommatoria di tutti i collegamenti della rete di backbone. In caso di fuori servizio di un nodo di commutazione si considerano fuori servizio tutti i link ad esso afferenti. La percentuale di degrado è il complemento al 100% della percentuale di funzionamento

Tabella 11: principali caratteristiche di una Rete Robusta

Caratteristica	Valori o Termini di Riferimento	Note
Possibilità di traffico multiprotocollo (ATM, IP, MPLS, altri)	Opzionale	Fortemente consigliata, eventualmente come back-up di linea "wired"
Federabilità con altre reti	Ammessa	
Gateways verso Internet e altre reti non allo stesso livello di sicurezza	Protetti da Firewall	Non sono ammesse deroghe all'uso di firewall e strumenti di protezione; può essere costituita una "zona demilitarizzata" (DMZ)
Componente di accesso in ponte radio o wireless sicuro	Normalmente presente	Fortemente consigliata, eventualmente come back-up di linea "wired"
Componente di transito in ponte radio	Opzionale	Fortemente consigliata
Componente satellitare di accesso	Opzionale	Fortemente consigliata
Componente satellitare di transito	Opzionale	Fortemente consigliata
Componente deployable (dispiegabile/trasportabile sul territorio)	Opzionale	Irrinunciabile in caso di un'Organizzazione che debba supportare lo svolgimento di pubblici servizi in caso di calamità. Può comprendere una componente satellitare di accesso di tipo dispiegabile
Cifratura dei dati in transito	Supportata	È garantita la riservatezza e l'autenticazione dei dati in transito con tecniche di "bulk encryption" (cifratura punto-punto a livello link) o "network encryption" (cifratura end-to-end, tipicamente tramite meccanismi di tunnel a livello rete tipo IPSec)
Sicurezza perimetrale (firewalling)	Supportata	È possibile definire policy di rete a livello di accesso
Ownership dell'infrastruttura di trasmissione e di linea	Non necessariamente interna all'organizzazione	Leased lines ammesse se di provider diversi con reti diverse e comunque nel minor numero possibile
Ownership dell'infrastruttura di commutazione	Non necessariamente interna all'organizzazione	
Ownership dell'infrastruttura di gestione	Non necessariamente interna all'organizzazione	
Ownership dell'infrastruttura di sicurezza	Meglio se interna all'organizzazione	

Tabella 11: principali caratteristiche di una Rete Robusta (cont.)

Tanto più una rete sarà connessa, tanto più risulterà affidabile, a parità degli altri fattori che concorrono all'affidabilità di un sistema.

La misura del grado di connettività di una rete è data dal numero di nodi a cui un generico nodo è connesso ed è buona norma che, in una qualsiasi rete, **K** sia scelto sufficientemente grande, e comunque sia almeno $\mathbf{K} \geq 2$.

Un valore ritenuto sufficiente per la componente di backbone di una rete sicura è **K**=3, corrispondente a una rete in grado di mantenere la propria connettività globale anche nel caso di due guasti, concomitanti e comunque dislocati, su altrettanti collegamenti.

Per quanto riguarda la periferia della rete, ossia la sua componente di accesso, è buona norma che i più importanti nodi di accesso siano collegati a due nodi appartenenti al backbone di transito. È questa la tecnica cosiddetta del "double homing", diffusa anche nelle reti di telecomunicazioni pubbliche. Un valore ritenuto sufficiente per la componente di accesso di una rete sicura è quindi **K**=2.

La *Fig. 12* mostra una rete dove i nodi di transito, indicati con N_i, sono **K** connessi con **K** = 2 e i nodi di accesso, indicati con M_j, sono connessi con il backbone di transito in double homing.

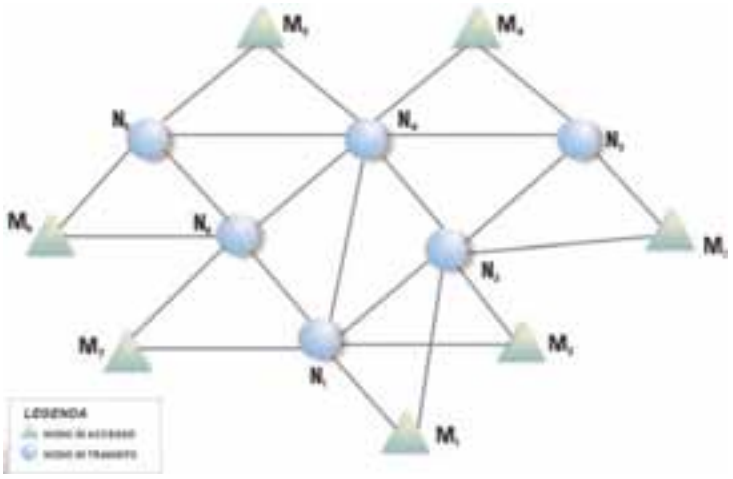


Fig. 12: Esempio di connettività di rete

Si noti che **K** è pari a 2, anche se

$k(N_4) = 5$ e $k(N_1) = k(N_2) = k(N_6) = 3$.

I concetti sopra esposti si applicano tanto alle reti fisiche, quanto alle reti logiche dei "livelli superiori": è per questo che la sicurezza derivante dalla topologia è considerata una caratteristica "trasversale" rispetto ai criteri di sicurezza della rete fisica e della rete logica.

È evidente che alta connettività, double homing e ogni altra caratteristica topologica e strutturale che aumenti il grado di sopravvivenza di una rete devono essere caratteristiche proprie di ogni livello di rete, a partire dal livello fisico.

Per tale motivo, una differenziazione fisica dei percorsi operata a livello geografico o con mezzi portanti fisici diversi è sicuramente raccomandabile.

3.2.2.2.5.3 La federazione di reti

3.2.2.2.5.3.1 Premessa

Il presente paragrafo fornisce una distinzione tra i concetti di Interoperabilità di Reti e Federazione di Reti.

La **Interoperabilità tra due Reti** (**A** e **B)** crea un'integrazione tra le due reti con una situazione nella quale:

- gli utenti della Rete A possono connettersi con quelli delle Rete B e viceversa
- gli utenti della Rete A possono accedere ai Data Base della Rete B e viceversa creando di fatto una fusione delle due reti in un'unica struttura.

La **Federazione di Reti** ha lo scopo di incrementare la connettività e capacità di trasmissione in presenza di una emergenza tramite opportuni collegamenti tra reti che normalmente operano in modo separato.

Nessuna connessione tra utenti e data base delle due reti viene instaurata.

In altre parole la **Federazione di Reti** consiste nel collegare tra loro due o più reti normalmente indipendenti in modo che una rete (la rete A nella *Fig. 13*) possa utilizzare parte dell'altra rete per operare correttamente il proprio servizio.

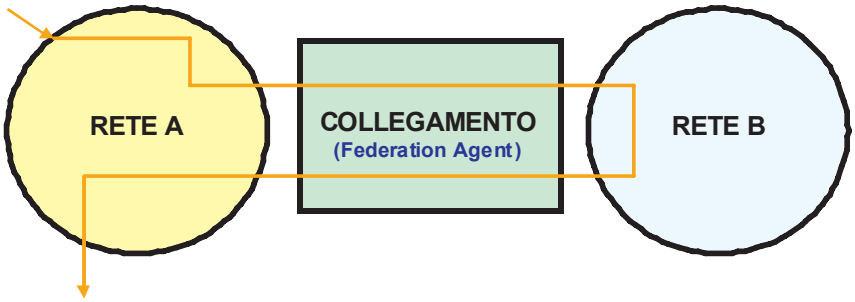


Fig. 13: Federazione di Reti

In tale modo in una situazione di emergenza le Infrastrutture Critiche possono basarsi su una ampia connettività incentrata, teoricamente, su tutte le reti "legacy" nazionali.

Potenzialmente tali Reti Legacy possono essere teoricamente rappresentate da:

- reti che supportano le Infrastrutture Critiche
- reti di comunicazione di tipo PSTN
- reti di comunicazioni wireless
- reti militari e paramilitari
- reti di strutture pubbliche e private distribuite a livello nazionale (broadcaster, TV satellitare, Reti Governative, ecc.).

La **Federazione di Reti** quindi si limita agli aspetti di connettività e non affronta né garantisce la Interoperabilità delle Reti.

La Federazione di Reti risulta possibile solamente se le reti da federare sono dotate di capacità di "supervisione della rete" e risultano in grado di "gestire" le priorità del routing della informazione.

3.2.2.2.5.3.2 Federation agent

L'entità principale coinvolta nella **Federazione delle Reti** risulta il **"Federation Agent"** il quale deve:

a) Collegare le Reti (da A a B)

Il collegamento risulta sempre predisposto ma viene **utilizzato** solamente in presenza di una emergenza che sia riconosciuta come potenzialmente in grado di pregiudicare la funzionalità di una o più Infrastrutture Critiche.

Per rendere possibile tale modo di operare, i proprietari delle reti interessate devono aver raggiunto un accordo che preveda tale supporto reciproco e quindi che, a seguito di una situazione di emergenza, una rete accetti di ridurre il proprio servizio non essenziale per supportare il servizio essenziale richiesto dall'altra rete.

Si suggerisce la presenza di un opportuno numero di **Federation Agent** in modo da garantire una connettività tra reti almeno pari a **K**=3.

b) Interfacciare le Reti

Il **Federation Agent** opererà come interfaccia (HW, Trasporto e Standard) tra le due reti accettando i dati della Rete A e rendendoli compatibili con l'"ambiente" della Rete B.

Di fatto il Federation Agent è visto dalla Rete B come un utente che genera dati che devono essere trasferiti ad altri utenti della Rete B (rappresentati da altri Federation Agent) che riportano tali dati alla Rete A.

c) Gestire le Priorità

La rete A soggetta ad emergenza, tramite il proprio sistema di supervisione e la propria capacità di gestione delle priorità, identifica la situazione anomala, la quantizza e identifi-

ca il supporto che necessita dalle reti federate.

Organizza quindi i dati strategici (critici) e li fornisce ai Federation Agent che li indirizzano verso la rete B che li gestisce come dati ad elevata priorità (o comunque come dati a livello di priorità preconcordato).

Ciò non esclude che, se possibile e se accettato dalla Rete B, il Federation Agent indirizzi anche altri dati quali i dati sicuri.

d) Gestire la Sicurezza

È altamente auspicabile che il **Federation Agent** risulti in grado di operare cifratura di tipo "end-to-end" tra i nodi rappresentati dai **Federation Agent**.

Altre caratteristiche delle reti da federare:

- Le reti devono essere in grado di gestire le priorità dei dati
- È auspicabile che le reti risultino omogenee in termini di livelli di sicurezza garantiti.

Riguardo a questo ultimo aspetto si ritiene che limitatamente alle Reti Sicure ed alle Reti Robuste l'emergenza abbia priorità rispetto alla garanzia della sicurezza.

Conseguentemente per tali reti è opportuno che la predisposizione di federazione avvenga anche con reti non ad omogenei livelli di sicurezza pur se si ritiene che l'attivazione dei **Federation Agent** debba essere operata, ove possibile, prioritariamente tra Reti con livelli di sicurezza omogenea.

Si esclude comunque, in tale ottica, che le **Reti a Massima Sicurezza** possano essere "federate" con reti a minore livello di sicurezza.

3.2.2.2.5.4 Accesso alle reti - Porta di Rete

La regolamentazione dei servizi di acceso alle reti è uno degli aspetti importanti di un valido sistema di sicurezza di cui tenere conto nella progettazione di reti CII che devono essere interconnesse con reti esterne o con altre reti CII.

Si definisce **Porta di Rete CII** (**PdR**) la componente logica di accesso tra il dominio o sito di un singolo utente e l'infrastruttura CII: la definizione si applica anche al caso di accesso all'infrastruttura di interconnessione di più CII.

La PdR assicura:

- Il servizio di connettività interfacciando i componenti di accesso specifici (wired, satellitare, ponte radio)
- Appropriati servizi di sicurezza.

Il concetto di PdR è valido per nodi di tipo:

- *Fisso*: in cui le infrastrutture di comunicazione del nodo sono installate in un edificio in configurazione fissa, l'ambiente è condizionato e protetto
- *Trasportabile*: nel quale le strutture di comunicazione del nodo sono installate in un sito in configurazione semi-fissa, nel senso che è possibile, con mezzi e tempi a disposizione, disinstallare gli apparati, trasportarli e installarli in un sito diverso
- *Mobile:* nel quale le infrastrutture di comunicazione del nodo sono installate in shelter/container e sono alimentate e condizionate da apparati dedicati. Per le antenne è prevista un'installazione da campo o sugli shelter stessi
- *Veicolare:* nel quale gli apparati radio di trasmissione/ricezione sono installati su veicoli per trasporto persone o cose (automobili, fuoristrada, autocarri,…).

Il numero dei servizi da offrire sulla PdR può essere variato in funzione dei requisiti e delle caratteristiche del singolo sito/utente.

La PdR è quindi realizzata da una o più componenti fisiche, a seconda del numero di servizi e del loro livello di integrazione sullo stesso dispositivo.

La *Fig. 14* schematizza la collocazione della PdR.

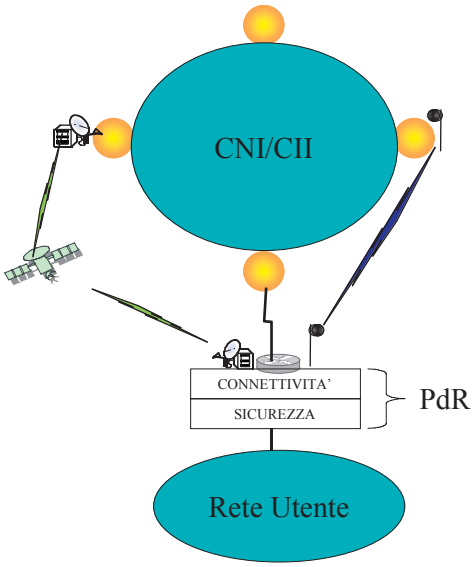


Fig. 14: Porta di Rete

I servizi di sicurezza che vengono forniti a livello di PdR, facendo principalmente riferimento ad una infrastruttura di comunicazione basata su protocollo IP, sono tipicamente:

- Protezione del flusso di traffico e controllo degli accessi
- Sicurezza perimetrale
- Sistemi di rilevamento delle intrusioni nella rete
- Sistemi di rilevamento delle intrusioni negli host
- Sistemi antivirus e di controllo dei contenuti.

Gli obiettivi del servizio ***Protezione del flusso di traffico e controllo degli accessi*** sono:

- *Data Origin Authentication:* verifica l'autenticità del nodo mittente di ciascun datagramma IP
- *Data integrity:* verifica che il contenuto di ciascun datagramma non sia stato modificato (deliberatamente o a causa di errori di linea) durante il transito tra sorgente e destinazione
- *Data confidentiality:* nasconde il testo in chiaro contenuto in un messaggio, mediante l'impiego della crittografia
- *Replay protection:* assicura che un hacker, intercettato un datagramma IP, non sia in grado, a posteriori, di rispedirlo a destinazione per qualche scopo illecito.

Per la ***Protezione del flusso di traffico*** ad esempio il protocollo IPSec, parte integrante della nuova versione del protocollo IP (IPv6) ma utilizzabile anche con IPv4, rappresenta un'architettura aperta, definita dall'IPSec Working Group dell'IETF (RFC 2401), e costituisce la soluzione più generale per la protezione (cifratura/integrità/autenticazione) dei dati in transito su una rete. Il protocollo IPsec può essere utilizzato come soluzione end-to-end, proteggendo cioè lo scambio di informazioni direttamente tra il mittente e il destinatario della comunicazione, oppure può intervenire tra due sistemi intermedi che hanno la funzione di security gateway, come accade nella realizzazione di reti private virtuali. Trovandosi a livello di rete, IPsec è una soluzione molto generale (può proteggere tutto il traffico IP) ed è trasparente rispetto alle applicazioni.

La PdR può utilizzare sia algoritmi crittografici standard (DES, 3-DES, RSA, ...) che proprietari.

Vengono utilizzate Chiavi di cifratura di lunghezza adeguata a garantire la "robustezza" sia per la Riservatezza (*Strong Encryption*) che per la Autenticazione (*Strong Authentication*).

Il meccanismo di autenticazione normalmente utilizza Chiavi Asimmetriche e Certificati Digitali X.509, consentendo l'integrazione del servizio in una struttura PKI.

Per il ***controllo degli accessi***, poiché la convalida di un certificato digitale è una funzione che ha un impatto significativo sulle prestazioni complessive di un'infrastruttura PKI, lo standard dell'IETF

OCSP (On Line Certificate Status Protocol) consente l'utilizzo di certificati digitali per l'autenticazione dell'origine dei dati, in particolare del tipo in tempo reale (RTC = Real Time Certification), e l'attivazione del servizio di controllo accessi fra:

- PdR del sito "a" e PdR del sito "b"
- Postazioni stand-alone e PdR di un sito.

Gli obiettivi del servizio ***Sicurezza perimetrale logica*** sono quelli di garantire:

- *Firewalling:* il servizio implementa le classiche funzionalità di filtraggio di traffico, Gestione delle politiche di permesso (per esempio "Nega qualsiasi servizio eccetto quelli esplicitamente permessi"), ecc. mantenendo Auditing e logging del traffico che attraversa il firewall

  Questo tipo di servizio può essere fornito anche separatamente per:
  - Il traffico dalla CII alla PdR (e viceversa)
  - Il traffico fra la Rete Utente e l'ambiente dove è installata la PdR, come nel caso in cui siano previsti dei Server specifici (per esempio di Management, di Middleware, ...) su una "DMZ" a valle della PdR
- *Protezione da attacchi di tipo Denial of Service* (*DOS*): il servizio contribuisce ad aumentare la sicurezza del sistema di comunicazione, in termini di Disponibilità e Continuità del servizio, prevenendo attacchi di tipo informatico (*Cyber Attack*) tesi a provocare la impossibilità di utilizzare le risorse informatiche.

Il servizio di ***rilevamento delle intrusioni nella rete*** consiste nell'attivazione e gestione di sistemi di rilevamento delle intrusioni (detti *Network Intrusion Detection System* - NIDS), il cui funzionamento si basa sulla capacità di osservare il traffico in rete. Un NIDS è una configurazione hardware/software, con uno o più sistemi (sensori) installati su reti con lo scopo di:

- identificare tutte le situazione di attacco alla rete che si intende proteggere

- identificare tutte le situazioni in cui non vi è un attacco alla rete che si intende proteggere.

Il servizio consente di:

- proteggere i beni informatici
- identificare e correggere eventuali vulnerabilità della rete in tempi brevi
- raccogliere e conservare tracce accurate degli avvenuti attacchi allo scopo di favorire l'individuazione degli autori dell'attacco e come deterrente per scoraggiare ulteriori azioni ostili.

Il servizio è completato da una componente di NIDS Management che consente di:

- ottenere informazioni sugli eventi di attacco dalle sorgenti di informazione ("sensori") posti sulla rete
- effettuare un'analisi predeterminata degli eventi rilevati
- generare una notifica specifica a fronte della identificazione di un evento di attacco.

Il servizio ***rilevamento delle intrusioni negli host*** consiste nell'attivazione e gestione di sistemi di rilevamento delle intrusioni su host (detti Host Intrusion Detection System - HIDS), il cui funzionamento si basa sulla capacità di osservare informazioni prelevate dagli host che si intende proteggere.

Un HIDS è un software installato su host con lo scopo di:

- identificare tutte le situazione di attacco all'host che si intende proteggere
- identificare tutte le situazioni in cui non vi è un attacco all'host che si intende proteggere.

Il servizio, completo della componente di Management, consente di:

- proteggere le postazioni di lavoro e i sistemi server
- identificare e correggere eventuali vulnerabilità di tali host in tempi brevi
- raccogliere e conservare tracce accurate degli avvenuti attacchi allo scopo di favorire l'individuazione degli autori dell'attacco e come deterrente per scoraggiare ulteriori azioni ostili
- attivare reazioni specifiche a fronte della identificazione di un evento di attacco.

Il servizio ***antivirus e controllo dei contenuti*** consiste nella implementazione e gestione di un sistema di protezione di eventuali server applicativi (installati presso la PdR) da codici dannosi. Con il termine "codice dannoso" si intende qualsiasi tipologia di codice software eseguibile (Virus, Worm, Cavallo di Troia, ecc.) che può provocare danni all'ambiente IT in modo intenzionale o non intenzionale.

Anche questo servizio consente la gestione centralizzata del software antivirus installato su una porzione o sull'intero parco macchine del sistema informativo che si intende rendere sicuro.

3.2.2.2.5.5 Struttura di sicurezza a livello Middleware - Applicativo - Procedurale

La sicurezza delle reti CII non può prescindere da un'infrastruttura di sicurezza a livello di middleware, di software per la gestione dei dati, di applicazioni e a livello organizzativo che preveda anche delle apposite procedure cui deve attenersi tutto il personale che accede e utilizza il sistema.

Innanzi tutto, è necessario accertarsi che sistemi operativi e software utilizzati nelle reti CII siano rispondenti ai requisiti standard di certificazione sulla sicurezza, siano utilizzati nelle più recenti versioni e siano costantemente aggiornati.

Una delle funzionalità più importanti a tutti i livelli (client, middleware e server dati) è l'*autenticazione*, cioè la possibilità di individuare univocamente i soggetti che operano sul sistema.

Così facendo, si possono definire differenti livelli di accesso al sistema ed alle sue risorse in base alle caratteristiche ed al profilo del singolo utente; ogni servizio del sistema controlla le credenziali fornite e, in base alle Access Control List (ACL), fornisce i corretti accessi alle risorse (ad es. read only, read and write, no permission, ecc). Per i sistemi i cui dati risultino particolarmente sensibili, l'impiego di tali criteri di accesso dovrebbe essere realizzato direttamente dal *kernel* del gestore della base dati anziché a livello applicativo. Solo in tale modo, infatti, è possibile scongiurare il pericolo di accessi non voluti in grado di aggirare i controlli effettuati dalle applicazioni.

La funzionalità di autenticazione dell'utente può essere per esempio realizzata tramite una architettura di Public Key Infrastructure (PKI) con una Certification Authority (di tipo tecnologico) in grado di generare i Certificati Digitali in formato X.509 per ogni utente, applicazione e servizio che deve essere autenticato nel sistema (anche per gli apparati di Rete).

La *Fig. 15* mostra una architettura di PKI molto generica con differenti attori e che interagisce con altre PKI.

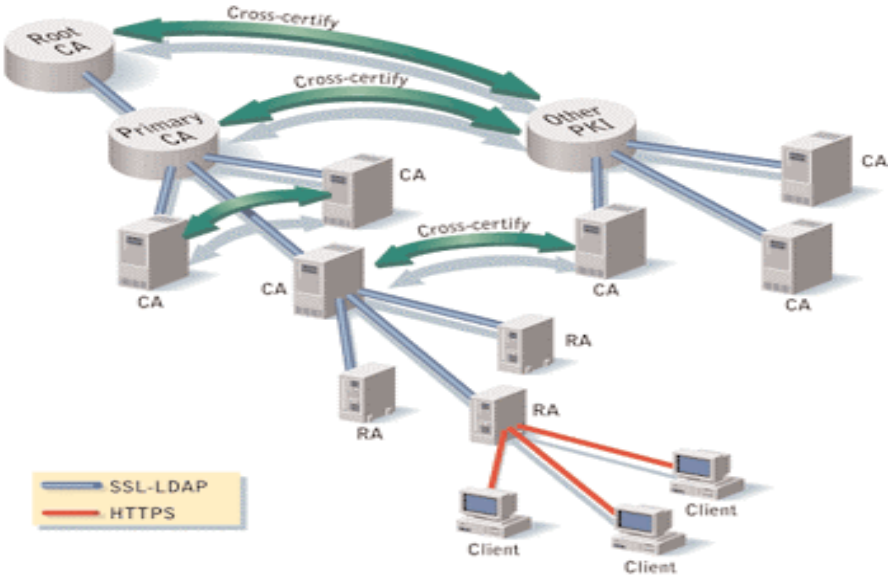


Fig. 15: Esempio di Architettura di PKI

Le componenti principali di una PKI sono:

- Certification Authority (CA): responsabile della emissione e della revoca dei Certificati Digitali
- Registration Authority (RA): responsabile della verifica delle informazioni che associano una chiave pubblica all'entità che ne farà utilizzo (che può essere distinta da quella che richiede il Certificato Digitale)
- Possessore del Certificato Digitale: persona, dispositivo hardware, agent software che rappresenta l'entità che farà utilizzo della chiave pubblica (ovvero del Certificato Digitale) per attestare la propria identità
- Utilizzatore del Certificato Digitale: persona, dispositivo hardware, agent software che valida una autenticazione a partire da una chiave pubblica (Certificato Digitale) di una CA.

I Certificati e le liste di quelli revocati sono memorizzati e pubblicati in appositi archivi. Il modello di funzionamento e di interazione dei vari attori della PKI è riassunto nella *Fig. 16*:

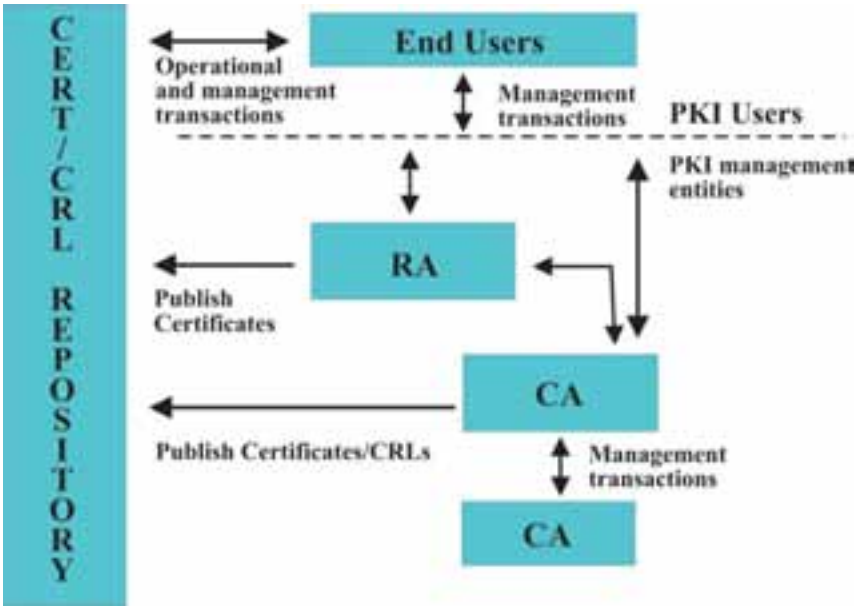


Fig. 16: Modello di Funzionamento di PKI

L'utente della PKI richiede alla RA di poter avere un Certificato Digitale. La RA, dopo aver verificato tutti i dati ed eseguito i passi previsti dal protocollo di gestione della PKI, richiede alla CA l'emissione del Certificato Digitale. La CA fornisce il Certificato Digitale all'utente e lo pubblica nel Repository pubblico.

Gli utenti finali della PKI possono utilizzare tutte le funzioni di cifratura, Firma Digitale, Hash, messe a disposizione dalla PKI, utilizzando il proprio Certificato Digitale e quelli degli altri utenti con cui vogliono interagire andandoli a reperire dal Repository dei Certificati.

Tale repository deve essere realizzato seguendo opportune precauzioni di sicurezza.

Durante le operazioni di Gestione ed Amministrazione della PKI possono essere richieste dalle varie RA delle revoche di Certificati Digitali per utenti non più *trusted* dalla PKI. La CA provvede alla revoca invalidando i Certificati Digitali ed emettendo una Certification Revocation List (CRL) che viene pubblicata nel Repository. Ogni utente finale, prima di autenticare un Certificato Digitale pervenutogli, dovrebbe controllare che quest'ultimo non sia presente nelle CRL pubblicate.

Per gestire le Policy della CA vengono utilizzati una o più Certification Authority Operator (CAO), mentre per gestire le richieste di certificati digitali da parte degli utenti vengono realizzate una o più Registration Authority (RA) che possono essere anche via Web per consentire di generare le richieste dal Web Browser della postazione dell'utente.

Per risolvere il problema delle dimensioni delle certificazioni presenti nel sistema delle CRLs può essere utilizzato il protocollo OCSP che è in grado di:

- inviare solo l'informazione sullo stato del certificato in questione (e non l'intera lista)
- interagire con l'Autorità di Certificazione (CA) che rilascia le CRLs
- consentire una gestione centralizzata dello stato di certificato.

Più in particolare, per il conseguimento di elevate prestazioni ed alta affidabilità, è possibile l'impiego di un sistema OCSP distribuito (D-OCSP) il quale fornisce una buona protezione contro gli attacchi tipo DoS e non è vulnerabile agli attacchi di intrusione. Il sistema D-OCSP consente, inoltre, di ottenere:

- *Scalabilità effettiva* grazie alla separazione del processo di convalida dalle operazioni di sicurezza associate con il processo di validazione del certificato
- *Affidabilità elevata* ottenuta perché le applicazioni degli utenti finali si collegano ad un server LDAP locale
- *Prestazioni elevate* ottenute con la diminuzione della distanza tra l'applicazione dell'utente ed i Repository
- *Disponibilità elevata* perché eventuali attacchi multipli volti ad impedire il servizio sono virtualmente eliminati dall'impiego di molteplici Repository dispersi geograficamente
- *Ottimizzazione dei costi* poiché i Repository non richiedono comunicazioni, collocazioni o modalità operative sicure e il costo associato al loro impiego in forma distribuita su vasta scala è minimo
- *Flessibilità e adattabilità:* ciascun Repository può supportare più di una CA con la conseguente possibilità di mantenere il controllo completo sul proprio dominio
- *Capacità di dislocazione elevate:* i risponditori possono essere dislocati ovunque senza che ciò comporti per l'utente un decadimento delle prestazioni dovute a rallentamenti nella rete
- *Fattori ambientali migliori:* poiché i Repository non contengono alcun dato sensibile ai fini della sicurezza, essi possono essere dislocati anche in ambienti dove la minaccia di attacco è reale
- *Architettura ideale per scenari suscettibili di varianti repentine:* dato che è facile ed immediato aggiungere od eliminare Repository
- *Sicurezza elevata:* in quanto sono stati significativamente migliorati due importanti fattori di sicurezza rispetto ai sistemi OCSP tradizionali:

- le richieste di validità dei certificati vanno solo ai risponditori, non all'autorità di validazione. Poiché l'autorità di validazione non consente alcuna comunicazione in entrata dal mondo esterno, la minaccia di un attacco proveniente dall'esterno è virtualmente eliminata
- un incremento della struttura di validità per adattarla a bacini di utenza di dimensioni sempre crescenti non richiede una corrispondente ulteriore distribuzione di dati sensibili e di applicazioni sicure. Pertanto ne consegue che la capacità di gestire in sicurezza tali operazioni è fortemente migliorata.

Il sistema necessita inoltre di uno o più Time Stamp Server in modo da realizzare il servizio di Time Stamping necessario per la funzionalità di Firma Digitale e Non-Repudiation.

La Certification Authority può anche non essere connessa alla rete della CNI (in modo da non subire attacchi dall'esterno).

Il sistema di PKI fornisce a tutti gli utenti del sistema una libreria di funzioni interfacciabile con le applicazioni (che possono essere applicazioni Web Oriented, Client di Posta, e applicazioni sviluppate ad-hoc) che permette tutte le funzioni di hash dei documenti, cifratura, firma digitale, reperimento delle informazioni dal server LDAP di riferimento (ad es. CRL, Certificati Digitali e chiavi pubbliche di altri utenti, servizi, ...).

Ogni utente della PKI deve avere un supporto dove memorizzare la propria Chiave Privata ed il proprio Certificato Digitale. Questo supporto deve inoltre fornire delle caratteristiche di sicurezza tali da non permettere la perdita (o il cloning) della chiave privata che permetta tutte le operazioni della PKI (cifratura, firma digitale, ...).

Per quanto riguarda i servizi software (come ad esempio la Certification Authority stessa) vengono memorizzate le chiavi private su supporti detti Hardware Security Module (HSM) che permettono anche il back-up della chiave privata in maniera sicura (se si perdesse la chiave privata della CA verrebbe inficiata l'intera PKI).

Ad ogni utente finale della PKI viene fornita una Smart Card (ad esempio la Carta Multiservizi della Difesa CMD) tramite la quale

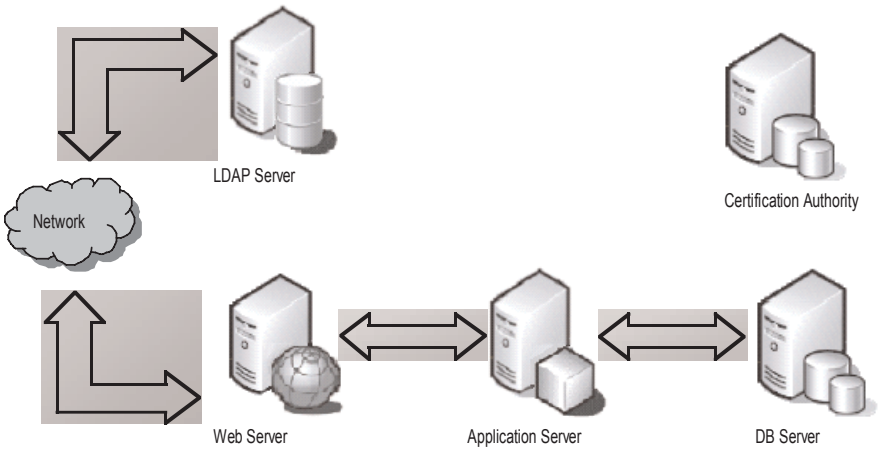


Fig. 17: Architettura di PKI

l'utente può autenticarsi al sistema (anche con funzionalità biometriche: impronta digitale) e interagire con la PKI (sulla Smart Card viene generata e memorizzata la chiave privata del Certificato Digitale dell'utente).

È necessario solo un lettore di Smart Card sulla postazione di lavoro dell'utente.

Sul Server LDAP, oltre ai Certificati Digitali ed alle chiavi pubbliche, vengono anche memorizzati i profili degli utenti in modo tale da catalogarli all'interno di diverse Organizational Unit (OU) e concedere diversi privilegi di accesso alla rete, ai servizi ed alle applicazioni.

Tutti i servizi e le applicazioni, una volta autenticata la controparte di comunicazione con i servizi offerti dalla PKI, controllano il profilo dell'utente e applicano le Access Control List (ACL) delle proprie risorse nei confronti dell'utente.

Una funzionalità importante che si può ottenere con una PKI è quella del Single-Sign-On che permette all'utente di autenticarsi al sistema con solo una credenziale (quella fornita dal certificato digitale) e poter accedere a tutte le risorse con i corretti profili e permessi.

L'utente così non deve più avere differenti meccanismi di log-on alle risorse (ad esempio differenti username e password per ogni sistema).

Altra importante funzionalità è, quindi, quella del controllo degli accessi che presenta maggiori caratteristiche di sicurezza se vengono utilizzate soluzioni in tempo reale (RTC) e sistemi distribuiti di validità dei certificati (D-OCSP) i quali possono servire centinaia di migliaia di utenti con grande affidabilità, alte prestazioni, sicurezza e minimi costi di messa in opera.

Il sistema RTC impiega l'architettura di validazione distribuita descritta nella *Fig. 18* e supporta sia verifiche di validità a firma digitale che verifiche auto-convalidanti del tipo V-Token, CRL o Mini-CRL.

3.2.3 Impianti di alimentazione delle Reti

L'alimentazione da rete elettrica rappresenta la fonte di energia primaria per gli apparati di telecomunicazione delle CII e dalla sua continua disponibilità dipende direttamente il loro corretto funzionamento.

Dando per scontato che l'erogazione primaria derivi da uno o più gestori specifici è indispensabile una corretta definizione dei livelli di servizio garantiti in condizioni normali e delle condizioni di intervento e di collaborazione in caso di emergenza.

Nel corso del normale esercizio le condizioni di fornitura sono

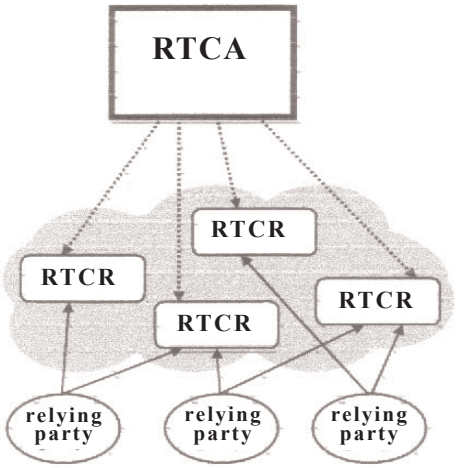


Fig. 18: Architettura RTC distribuita

regolate da appositi accordi di servizio, in caso di emergenza si deve perseguire la totale autonomia energetica del gestore della rete o dell'infrastruttura, valutando in termini di criticità la capacità e la durata di funzionamento in autonomia.

Ovviamente la disponibilità di un servizio *end-to-end* anche in caso di evento catastrofico dipende dalla effettiva disponibilità di soluzioni autonome per tutti gli elementi interessati al transito delle informazioni.

La disponibilità effettiva va misurata tenendo conto dell'elemento più debole della catena: ad esempio, se è possibile ipotizzare che un data centre disponga di un gruppo elettrogeno in grado di garantire qualche giorno di autonomia in caso di emergenza, non è pensabile estendere tale soluzione a tutti i restanti componenti nodali dell'infrastruttura di rete. Per questi ultimi dovranno essere comunque messe in atto soluzioni di minor costo che garantiscano un'adeguata autonomia.

Tutti gli apparati di rete e di nodo, essendo sensibili alle variazioni delle componenti dell'energia elettrica, devono essere dotati di opportuni sistemi di filtraggio e stabilizzazione dell'energia in ingresso. Inoltre devono essere predisposte idonee protezioni dalle micro-interruzioni di erogazione o dagli abbassamenti momentanei di tensione.

3.2.3.1 Sistemi di continuità

In caso di interruzione dell'erogazione di energia da parte del fornitore primario, i sistemi di alimentazione d'emergenza devono entrare in funzione senza soluzione di continuità e al ripristino delle condizioni di normalità devono escludersi in modo totalmente trasparente.

Tutti i sistemi devono disporre di procedure di avvio manuale in caso di mancata attivazione automatica.

Riferendosi in particolare ai gruppi elettrogeni, la disponibilità di produzione autonoma di energia elettrica è funzione della capacità dei serbatoi di carburante, della efficienza dei gruppi e della quantità di energia necessaria al funzionamento dei sistemi.

Il grado di autonomia sarà ovviamente superiore nel caso in cui le condizioni climatiche, ad esempio, non richiedano il pieno utilizzo dei sistemi di condizionamento, e inferiore nel caso opposto.

I sistemi di produzione autonoma devono essere ridondati e opportunamente dimensionati rispetto al fabbisogno d'esercizio.

Tutti gli apparati non indispensabili devono poter essere esclusi dal sistema ad erogazione autonoma per non ridurre il tempo di autonomia.

È opportuno definire le politiche di approvvigionamento dei combustibili durante l'emergenza facendo ricorso anche alla disponibilità di fornitori alternativi.

Deve esistere un piano di distacco progressivo dei carichi non indispensabili al fine di garantire la continuità di alimentazione ai sistemi considerati vitali.

3.2.4 Aspetti di sicurezza dei Data Centre

I Data Centre, ovvero gli ambienti fisici in cui sono installati gli apparati e le infrastrutture informatiche, rappresentano un elemento particolarmente delicato nella continuità di esercizio di una Infrastruttura Critica.

In moltissimi casi si tratta di locali non specificatamente progettati allo scopo, ma frutto di adeguamenti tecnologici di edifici costruiti con diversa destinazione con le ovvie lacune e limitazioni per gli aspetti strutturali e logistici.

Gli eventi seguiti agli attentati del settembre 2001 hanno inoltre evidenziato come nuovi fattori di rischio richiedano adeguate infrastrutture fisiche.

3.2.4.1 Ambiente e confini

La localizzazione specifica di un Data Centre nel territorio deve tenere conto dei fattori di rischio legati:

- all'ambiente naturale (sismicità del territorio, rischi di inondazioni o maremoti)
- alle realtà confinanti che possono rappresentare una minaccia diretta o un possibile amplificatore di eventi dannosi (depositi di carburanti, lavorazioni pericolose, industrie chimiche, ecc.)
- a possibili obiettivi di specifici attacchi (installazioni militari)
- a possibili fattori critici in caso di emergenze (impianti sportivi o di spettacolo ad alta densità di pubblico).

La localizzazione può influenzare inoltre la disponibilità/continuità di erogazione di fattori primari di produzione (es. la vicinanza di grandi complessi industriali può avere forti ripercussioni sulla fornitura di energia elettrica) oppure la accessibilità da parte degli operatori o delle squadre di emergenza.

3.2.4.2 Struttura dell'edificio

L'edificio ideale deve essere progettato specificamente per consentire l'idonea distribuzione degli impianti tecnologici e strutturali e per realizzare l'ambiente più facilmente difendibile o gestibile in caso di emergenza.

Nel riadattamento e/o adeguamento di infrastrutture esistenti devono essere riprogettati e correttamente dimensionati tutti gli impianti e la distribuzione fisica degli spazi.

La struttura deve essere divisibile in "zone stagne" per circoscrivere e confinare il danno a perimetri definiti.

La struttura esterna deve essere difendibile da attacchi armati, cintata e sorvegliata e non deve ospitare altre entità o servizi.

I palazzi fuori terra non devono ospitare garage, automezzi o depositi di materiale se non strettamente necessario al funzionamento del Data Centre.

La struttura deve limitare allo stretto indispensabile i punti di accesso (persone e merci) ed evitare viali di accesso diretti che possano facilitare tentativi di sfondamento.

Deve essere garantita la rapida e facile raggiungibilità da parte di squadre di soccorso in caso di incidente e deve disporre di ampi spazi di manovra delle stesse.

In caso di indisponibilità della via d'accesso primaria deve esistere un percorso alternativo di accesso e di evacuazione.

3.2.4.3 Impianti tecnologici

3.2.4.3.1 Local Loop

L'accesso alle reti TLC deve avvenire tramite percorsi fisici distinti e ridondati in modo da garantire la continuità del servizio in caso di eventi tali rendere inutilizzabile accidentalmente o per motivi di sicurezza una via d'accesso.

3.2.4.3.2 Impianto elettrico

Una particolare cura deve essere dedicata al disegno, al dimensionamento e alla continuità della distribuzione dell'energia elettrica.

L'intero sistema produttivo e distributivo deve essere ridondato, possibilmente in punti opposti dell'edificio.

Il Data Centre deve disporre di adeguati gruppi elettrogeni in grado di garantire il funzionamento anche in caso di prolungata assenza di erogazione energetica principale.

Devono essere previste e regolamentate attività periodiche di simulazione incidenti e test di tutti i sistemi ausiliari e di ridondanza.

I gruppi di continuità, le batterie e altri elementi strutturali di un impianto elettrico di tipo industriale rappresentano specifici fattori di rischio incendio che vanno accuratamente valutati e neutralizzati.

3.2.4.3.3 Impianto di condizionamento

Analoga cura deve essere dedicata al progetto, al dimensionamento e alla continuità del sistema di condizionamento degli ambien-

ti: il mantenimento della corretta temperatura è infatti indispensabile al funzionamento dei sistemi.

La miniaturizzazione e concentrazione delle componenti informatiche, nel ridurre lo spazio fisico occupato, aumenta la concentrazione e la quantità di calore sviluppata dai sistemi il che richiede una gestione del raffreddamento con fattori di distribuzione flessibili e con carichi diversi da zona a zona del Data Centre, tanto per l'apporto dell'aria condizionata che per l'estrazione dell'aria calda.

Devono essere valutati e neutralizzati gli effetti collaterali del condizionamento (vibrazioni, polveri, fuoriuscite d'acqua).

3.2.4.3.4 Impianto antincendio

Le stesse accortezze devono essere dedicate al progetto, al dimensionamento e alla continuità del sistema di rilevazione e neutralizzazione degli incendi.

Devono essere possibili azioni di spegnimento a ondate successive per neutralizzare le riattivazioni dei focolai.

La protezione dal fuoco deriva anche da specifiche scelte strutturali (da cui il vantaggio di spazi specificamente progettati) quali l'assenza di finestre, la possibilità di contenimento del fuoco nelle diverse sezioni, l'assenza di materiali infiammabili nelle strutture e la presenza di isolanti e di contro soffittature.

Tutti i locali con possibili fattori di rischio (centrali elettriche, depositi di materiale, ecc.) devono essere separati e distanti dalle aree operative destinate ad ospitare i sistemi di elaborazione.

Devono essere previste e regolamentate attività periodiche di simulazione antincendio per tutto il personale addetto.

3.2.4.3.5 Controllo accessi

L'accesso delle persone ai locali deve essere rigorosamente controllato mediante identificazione personale, sorveglianza remota continua e nel caso scorta diretta per il personale esterno.

Di tutti gli accessi deve essere tenuta traccia.

In caso di emergenza occorrono specifiche procedure di rapido sblocco degli accessi per gli operatori di soccorso.

3.2.4.3.6 Sistemi di monitoraggio e d'allarme

Tutti i sistemi infrastrutturali devono disporre di idonei sistemi di monitoraggio e di allarme con procedure automatiche di escalation a seconda dei fattori di pericolosità rilevata.

3.2.4.4 Formazione del personale sulle procedure d'emergenza

Tutto il personale deve ricevere specifica formazione sulle modalità di accesso e fruizione della struttura nonché su tutte le procedure di emergenza anche se non di propria specifica competenza.

In tutte le zone operative deve esistere documentazione delle procedure di emergenza e quadri di sintesi che consentano l'intervento anche da parte di personale non specificamente addetto.

3.2.5 Reti di emergenza

Normalmente si definiscono reti di emergenza le reti che non risultano in grado di supportare la trasmissione dei dati (siano essi Normali, Sicuri o Strategici) necessari per il corretto funzionamento della Infrastruttura Critica ma permettono di riportare ad un Centro di Controllo (a livello di Infrastruttura Critica o a livello nazionale) le condizioni della Infrastruttura critica in oggetto (dati e/o voce).

Sono di fatto strutture considerate l'ultima risorsa per informare un ente superiore dello stato della infrastruttura (tipicamente delle cause e dei danni che hanno portato alla situazione di crisi che sta comportando l'incapacità di trasmettere informazioni con i sistemi previsti, sia per mancanza di capacità trasmissiva sia per mancanza di rete).

Un esempio di realizzazione di rete d'emergenza sono le reti in radiofrequenza in banda HF (2 - 30 MHz).

Una Rete HF è realizzata da ricetrasmettitori HF e conseguen-

temente entrambe le funzioni di Accesso e Trasporto sono realizzate via radio.

La banda utilizzabile per la trasmissione dell'informazione (voce o dati) é dell'ordine dei 3 MHz massimo (corrispondente a circa 3 Kbit/sec) ed il sistema risulta in grado di supportare sia trasmissioni analogiche (voce e dati) che digitali (voce e dati).

Le portanti variano da decine di Km (onda di terra) a centinaia e migliaia di Km (onda di cielo che sfrutta la riflessione degli strati alti dell'atmosfera) e risultano altamente influenzate dalle condizioni meteorologiche e dall'ora del giorno (si sperimentano variazioni di attenuazione anche dell'ordine dei 90 dB).

Per tale ragione si consiglia caldamente l'uso della banda HF estesa in basso in modo da poter operare anche, ad esempio, h 24 durante il mese di agosto e in presenza di elevata attività di emissioni solari.

L'accesso alla rete può essere operato da un semplice sistema di radio portatile (hand held) o da terminali radio fissi di maggiore potenza.

Si ritiene che la Rete di Emergenza HF debba prevedere:

- la presenza di Frequenze di Emergenza per distribuire informazioni a tutti gli utenti e instaurare un collegamento al di fuori di quelli pianificati
- un piano di assegnazione ed utilizzo delle frequenza da parte degli utenti
- un sofisticato sistema di Supervisione e di *re-routing* dell'informazione che tenga conto della "attuale" disponibilità delle stazioni fisse che rappresentano i nodi della rete
- un supporto della comunicazione diretta tra gli utenti utilizzando collegamenti locali, regionali e nazionali basati sui soli sistemi mobili.

3.3 GLI ASPETTI GESTIONALI E ORGANIZZATIVI

Nel presente paragrafo verranno analizzati, sempre in una ottica di Buona Regola, i principali aspetti organizzativi legati alla gestione delle Reti di Comunicazioni, illustrando infine alcuni trend tecnologici legati ai concetti di Reti Sicure.

3.3.1 Gestione congiunta delle situazioni di crisi derivanti dalle infrastrutture ICT

Come già descritto, le infrastrutture critiche nazionali sono gestite da una pluralità di istituzioni pubbliche e private. L'utilizzo di tecnologie ICT ha condotto ad una così elevata interdipendenza fra le diverse infrastrutture critiche che un evento dannoso verificatosi in una struttura può ripercuotersi sulle altre, provocando dei disservizi anche ad utenti che non hanno rapporti diretti con l'infrastruttura inizialmente danneggiata.

Partendo dal presupposto che ogni istituzione dovrebbe possedere i propri piani di emergenza/*Disaster Recovery*/*Business Continuity*, come prevedono le ISO/IEC 17799/BS7799, all'interno di ogni struttura dovrebbe esistere una Unità di Gestione delle Crisi (UGC).

Parimenti, nell'ambito della cooperazione tra diverse istituzioni dovrebbe essere costituita una Unità di Gestione Congiunta delle Crisi (UGCC).

Affinché tale Unità possa operare, dovrebbe esistere una matrice delle interdipendenze dei servizi forniti dalle diverse aziende, che permetta di individuare, una volta che una o più istituzioni vengano colpite da un evento dannoso, quali siano le altre strutture coinvolte, le modalità ed i tempi probabili di propagazione degli effetti provocati dall'evento dannoso, nonché i tempi di fine dei disservizi. Ciò sarà utile anche per determinare i tempi di intervento e prevenire/limitare l'effetto domino.

3.3.1.1 Unità di crisi

È l'organo di governo che dovrebbe sovrintendere ai piani per la gestione di gravi emergenze (attentati fisici o informatici, disastri naturali o accidentali, severi guasti alle tecnologie, gravi problemi organizzativi) con un forte impatto sulle strutture di ICT di supporto alle CII. Esso potrebbe essere convocato anche in caso di previsione di un potenziale disastro per la classificazione dell'evento e/o per l'eventuale individuazione di possibili contromisure. In caso di emergenza, l'Unità di crisi potrebbe sovrintendere alle seguenti attività:

- valutazione della situazione (fase di gestione dell'allarme)
- attuazione del piano di *recovery* (fase di gestione del disastro)
- ritorno alle normali condizioni di esercizio (fase di rientro).

3.3.1.2 Definizione dei referenti della gestione delle emergenze CII e ICT

Per la costituzione di una UGCC occorrerà innanzi tutto definire i ruoli, individuare le figure professionali all'interno delle singole istituzioni/aziende con adeguato potere decisionale e definire i processi. Sarà quindi necessario definire procedure che stabiliscano quando deve essere dichiarato lo stato di crisi congiunta e come questa deve essere gestita sino al ripristino della normale operatività (Piano di Gestione Congiunta delle Crisi, PGCC).

L'UGCC potrà essere composta da un Coordinatore e dai referenti delle Unità di Gestione delle Crisi delle singole istituzioni/aziende che gestiscono le diverse infrastrutture critiche/ICT. Il ruolo di Coordinatore della UGCC potrà essere ricoperto anche da uno dei referenti della UGC delle singole istituzioni/aziende e, quindi, tale figura potrà possedere anche un duplice ruolo (*Fig. 19*).

La nomina di ogni singolo membro dell'UGCC all'interno delle diverse istituzioni/aziende, dovrà essere formalizzata dai vertici istituzionali/aziendali e poi comunicata al Coordinatore. La stessa formalizzazione dell'incarico dovrà essere effettuata per il Coordinatore, ma in questo caso, l'individuazione della persona e quindi la nomina

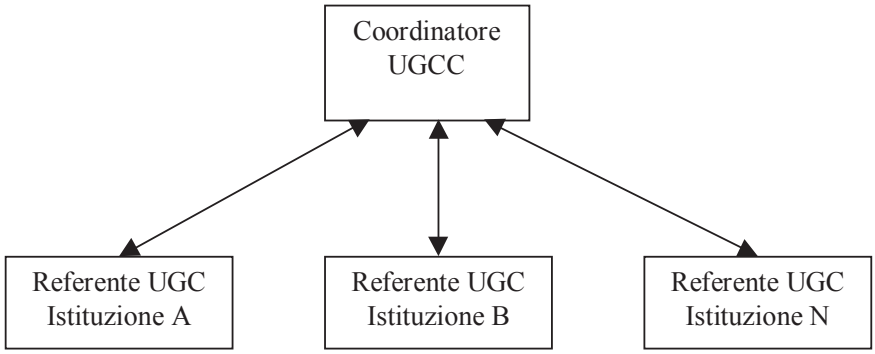


Fig. 19: Unità di Gestione Congiunta delle Crisi (UGCC)

dovrà essere concordata tra le varie istituzioni/aziende.

Tutti i referenti delle diverse UGC dovranno possedere in tempo reale tutte le informazioni concernenti la situazione di eventuali emergenze presenti all'interno della propria struttura.

Ogni componente della UGCC dovrà possedere un numero di telefono al quale è rintracciabile in caso di necessità ed una casella di posta elettronica alla quale dovranno essere indirizzate tutte le comunicazioni informative. La segnalazione di situazioni di emergenza, e le conseguenti convocazioni, dovranno essere effettuate tramite telefono e successivamente formalizzate tramite e-mail. I membri della UGCC dovranno essere sempre rintracciabili, anche in periodi di ferie, quindi dovrebbe essere disponibile un riferimento telefonico aziendale, tramite il quale sia sempre possibile rintracciare il referente della singola UGC od un suo sostituto.

È fondamentale per l'operatività dell'Unità che esista una comunicazione veloce ed efficiente tra tutti i membri. Ne consegue che gli strumenti utilizzati per comunicare dovrebbero essere sempre attivi e ad alta disponibilità.

3.3.1.3 Modalità di interazione, integrazione ed interoperabilità

Ogni volta che all'interno di una singola struttura viene attivata l'UGC a causa di un'emergenza (evento dannoso di tipo informatico o di qualunque altro genere), il relativo referente per l'UGCC deve essere in grado, in base alla matrice delle interdipendenze dei servizi precedentemente definita, di:

1) individuare il livello di criticità della situazione
2) effettuare una previsione realistica della durata dei disservizi in atto
3) prevedere gli eventuali impatti sulle altre infrastrutture
4) nel caso di possibili impatti esterni, allertare tutti i componenti dell'UGCC.

Una volta che l'UGCC si è riunita, occorrerà valutare se dichiarare o meno lo stato di Crisi Congiunta. In caso positivo, dovranno essere attuate le indicazioni del PGCC e quindi messe in atto le azioni per evitare che i disservizi si propaghino alle infrastrutture non ancora coinvolte fornendo supporto alle altre per limitare gli effetti/danni. In caso contrario, l'UGCC seguirà l'evolversi della situazione fino a che il livello di criticità si abbasserà e/o verrà dichiarata finita l'emergenza nell'infrastruttura colpita dal danno. Comunque, in tutte e due i casi, prima che l'UGCC si sciolga, dovrà essere dichiarata la fine dello stato di Gestione Congiunta della Crisi (GCC) e contestualmente preparato un documento nel quale siano registrate/descritte tutte le fasi di gestione dell'evento, per una successiva analisi.

Un possibile flusso operativo è riportato nella *Fig. 20*.

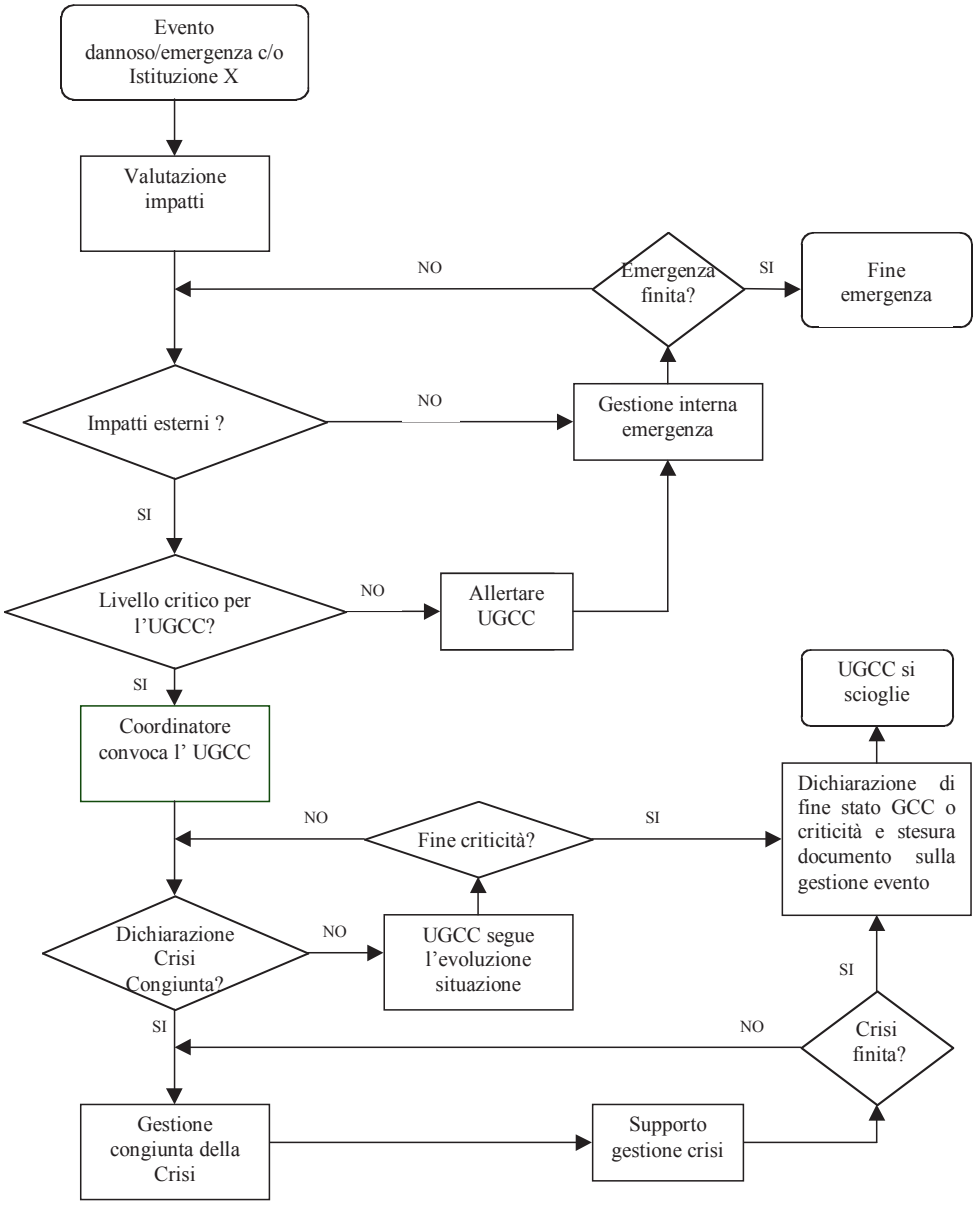


Fig. 20: Possibile flusso operativo

Affinché tale flusso possa dare dei risultati ottimali, ovviamente è fondamentale che sia stata effettuata una precedente analisi dei rischi relativa alla interdipendenza dei servizi forniti dai gestori delle infrastrutture critiche e ICT. Essa dovrà aver evidenziato quali siano le possibili minacce/vulnerabilità cui ogni infrastruttura può essere soggetta a causa di un evento dannoso verificatosi in una o più infrastrutture e la probabile durata dei conseguenti disservizi. Quindi dovrà essere già chiaro quali siano le relative contromisure da adottare al fine di evitare che le situazioni di emergenza/disservizio si propaghino.

Tali analisi potrebbero anche portare alla stipula di accordi relativi ad un eventuale supporto da parte delle aziende facenti parte dell'UGCC verso quelle colpite dal danno.

Qualora in caso di incidente, fosse possibile impedire la propagazione dei disservizi fra le diverse infrastrutture, sarà necessario che l'UGCC analizzi l'evento e la gestione fatta dell'emergenza, al fine di evitare il riverificarsi dello stessa situazione al ripresentarsi del medesimo evento.

Pertanto, periodicamente, l'UGCC dovrà riunirsi per discutere:

- sugli incidenti verificatisi nel periodo
- su come hanno reagito le singole istituzioni
- sulla valutazione degli impatti/portata dei danni/disservizi provocati da ogni incidente
- sulla determinazione di soluzioni atte ad evitare il ripetersi degli stessi problemi.

Quindi, oltre al PGCC, dovrebbe esistere un registro di tutte le emergenze verificatesi con il dettaglio delle attività svolte.

In caso di gravi situazioni di emergenza, l'UGCC dovrà emettere dei bollettini informativi per aggiornare sulla situazione i soggetti istituzionali preposti.

In caso di una minaccia nota che si stia diffondendo tra le differenti realtà ICT nazionali/mondiali (es. virus informatico), il Coordinatore dovrà convocare i membri dell'Unità per seguire l'evolversi della situazione, valutare le precauzioni/azioni che ogni singola

Istituzione avrà intrapreso ed eventualmente decidere di intraprendere un'azione comune per contrastare tale minaccia.

Un altro compito dell'UGCC sarà quello di divulgare informazioni all'interno delle singole infrastrutture e promuovere iniziative relative alla sicurezza, alla riduzione degli effetti di eventuali eventi dannosi, alla conseguente gestione dell'emergenza e alla risposta ad attacchi di tipo informatico.

Affinché vi possa essere una gestione proattiva delle eventuali emergenze, è fondamentale una condivisione tra i componenti dell'UGCC delle informazioni relative a nuove minacce o possibili eventi dannosi. È quindi auspicabile che l'UGCC possa usufruire di strumenti di Early Warning per ottenere tali informazioni e di *Information Sharing* per poterle condividere in tempo reale.

Tutte le informazioni confidenziali scambiate tra i membri della UGCC che riguardano le situazioni di emergenza, non dovranno passare a persone non autorizzate.

3.3.1.4 Attività di formazione comune e strumenti di supporto

Per i membri dell'UGCC, dovrà essere prevista una formazione volta all'addestramento cooperativo per la gestione congiunta delle crisi.

Dovranno inoltre essere messi a disposizione dell'UGCC strumenti atti a:

- definire modelli di realtà virtuale (VR) che consentano di determinare le aree che possono essere impattate da un'emergenza
- individuare i possibili scenari di intervento
- determinare gli elementi utili per la definizione delle strategie di gestione
- definire le varie strategie di addestramento
- effettuare una continua rivisitazione degli argomenti preceden-

ti considerando la realtà presente nelle strutture che partecipano all'UGCC.

Ogni nuovo membro dell'UGCC dovrà essere formato sugli argomenti prima indicati.

Ogni membro dell'UGCC dovrà possedere una conoscenza approfondita del piano di intervento in caso di Crisi (PGCC) e particolarmente di quelle parti del piano che lo coinvolgono direttamente. Ogni qualvolta che il PGCC venga modificato/aggiornato in qualche parte fondamentale, il Coordinatore dell'UGCC dovrà convocarne i membri per aggiornarli/formarli sul nuovo PGCC.

In corrispondenza di ogni variazione delle infrastrutture critiche/piattaforme ICT delle singole strutture che può apportare una modifica alla matrice delle interdipendenze dei servizi e/o al PGCC, dovrà essere effettuato un seminario di aggiornamento per i componenti dell'UGCC.

Dovranno inoltre essere effettuati dei corsi di aggiornamento periodici su eventuali nuove metodologie/strategie di gestione delle crisi dovute ad emergenze nelle diverse infrastrutture critiche/ICT e sull'utilizzo di nuovi strumenti che consentano di prevedere/gestire i comportamenti di tali infrastrutture al verificarsi di incidenti.

3.3.1.5 Buone regole circa la gestione delle emergenze ICT inclusa quella di Call Centre

Come già indicato in precedenza, le ISO/IEC 17799/BS7799 forniscono tutte le indicazioni su come deve essere realizzato un *Business Continuity Management Process* e quindi il *Business Continuity Plan*, fra le quali:

- individuare e concordare tutte le responsabilità e le procedure di emergenza
- implementare le procedure di emergenza che consentono il ripristino nei tempi predefiniti dei sistemi/servizi critici in caso di emergenza

- produrre la documentazione dei processi/procedure concordati per la gestione delle emergenze
- effettuare un adeguato addestramento del personale coinvolto nella gestione della crisi relativamente ai processi/procedure prima menzionati
- collaudare ed aggiornare i piani di gestione delle emergenze.

Senza queste attività preventive la gestione delle emergenze potrebbe risultare oltremodo problematica.

Ne consegue che le seguenti attività potrebbero essere considerate quali azioni minime da attuare per essere in grado di gestire le emergenze:

1. approvazione da parte dei vertici aziendali di un budget per garantire la continuità operativa dei sistemi/servizi critici
2. costituzione di una struttura (Unità di gestione della Crisi) che in caso di disastro o di interruzione del servizio coordini le azioni di ripristino
3. definizione di un processo, adeguatamente documentato (piano di gestione delle crisi), per gestire le emergenze ed operare il ripristino dei servizi
4. svolgimento di test periodici del piano di gestione delle crisi con simulazione delle emergenze
5. adeguamento periodico del piano, tenendo conto anche delle normative/standard/indirizzi vigenti e dei processi utilizzati nelle altre organizzazioni.

Durante una crisi è importante:

1. seguire, per quanto possibile, le indicazioni del Piano di Gestione delle Crisi (PGC)
2. tenere sempre aggiornati i vertici aziendali sullo stato della crisi
3. dare priorità alle procedure volte alla salvaguardia della incolumità delle persone
4. gestire i rapporti con i mezzi di informazione (stampa, televi-

sioni, radio), evitando sia di fornire inutili notizie che possano infondere panico alla cittadinanza sia di sospendere i canali di comunicazione con il pubblico

5. applicare tutte le procedure che consentono di evitare/limitare la diffusione dei danni ad altre organizzazioni
6. cercare di evitare/limitare il danno di immagine dell'azienda colpita dalla crisi
7. registrare tutte le informazioni che consentano di documentare l'evento dannoso i suoi effetti e le azioni messe in atto nella gestione della crisi, al fine di poter ricostruire ed analizzare il tutto.

Nel caso di gestioni congiunte delle emergenze, è evidente che il fattore comunicazione è fondamentale e quindi occorre che possano essere mantenuti attivi i contatti con le Forze dell'Ordine, le Istituzioni Statali, i centri che forniscono servizi di informazione per la cittadinanza o per le singole infrastrutture (informazioni sulle le minacce/danni, situazioni sul territorio) e con tutte le altre organizzazioni che cooperano nella gestione dell'emergenza.

Altro fattore importante, in caso di situazioni di emergenza, è la possibilità di contattare i vari *Call Centre* per ricevere informazioni/indicazioni sui disservizi venutisi a creare.

Il piano di *Disaster Recovery/Business Continuity* di ogni singola infrastruttura dovrà, quindi, includere tutte quelle attività/processi/procedure che permettono anche la continuità operativa dei rispettivi *Call Centre.* Ciò consentirà a tali strutture di fornire informazioni utili ai cittadini sugli eventuali disservizi in atto, utilizzando anche, sempre se la situazione di emergenza lo permette, gli eventuali servizi Web messi a disposizione degli utenti. Ovviamente, in caso di gestione di Crisi congiunta, l'UGCC dovrà far pervenire ai diversi *Call Centre*, tramite il referente dell'UGC della singola azienda, informazioni attendibili sulla situazione in atto e sulla probabile durata dei disservizi.

3.3.1.6 Opportunità e modalità di simulazioni di emergenze ICT

Allo scopo di verificare l'efficienza del processo di Gestione Congiunta delle Crisi, anche in funzione di evoluzioni tecnologiche/organizzative delle singole infrastrutture e quindi per mantenere un adeguato livello di preparazione/addestramento delle persone costituenti l'UGCC, sarà necessario effettuare periodicamente delle simulazioni di emergenze (almeno ogni sei mesi).

Per simulazione di situazioni di emergenza, s'intende lo svolgimento di tutte quelle attività previste nel PGCC, per esempio la convocazione dell'Unità, la valutazione degli impatti, dell'eventuale escalation e dei tempi di ripristino della normale operatività, l'emissione di comunicati, ecc. Ovviamente, tale simulazione non deve prevedere l'effettivo blocco dei sistemi/attività di una o più infrastrutture. Tale simulazione, affinché sia realistica, dovrebbe essere realizzata in un ambiente di test congiunto, dove ognuno abbia implementato la parte di propria competenza e che rappresenti in scala tutte le infrastrutture critiche, ICT e non, su cui si appoggiano i servizi erogati.

Sarebbe auspicabile inoltre che il Coordinatore della UGCC convocasse almeno una volta all'anno senza preavviso tutti i componenti della struttura per valutare la rintracciabilità ed i relativi tempi di risposta dei componenti dell'Unità.

Alla fine di ogni simulazione, i risultati dovranno essere registrati, valutati ed in base a queste analisi l'UGCC dovrà dichiarare la conformità del PGCC o eventualmente rivedere i processi/procedure di gestione delle crisi (adeguamento del PGCC) o decidere la ripetizione della simulazione.

Dai test di simulazione potrebbero nascere delle indicazioni utili anche per le singole infrastrutture.

L'eventuale utilizzo di Sistemi Intelligenti di Supporto alle Decisioni, IDSS (*Intelligent Decision Support System*), e/o di ambienti di simulazione (*Modelling and Simulation Environment*) può essere utile sia per la formazione interna sia per i componenti dell'UGCC per la valutazione dei possibili impatti di un incidente.

3.3.1.7 Gli aspetti Comunicazionali nella Gestione Congiunta delle Crisi

La presenza della UGCC impone la necessità di un sistema di comunicazioni in grado di supportare le relative operazioni.

Tale Rete di Comunicazione dovrà:

- Collezionare e fornire alla UGCC (sia in condizioni operative normali che in emergenza) lo stato attuale delle infrastrutture ed una previsione a breve e medio termine con eventuali richieste di assistenza legate sia alla struttura stessa sia alle relative comunicazioni
- Permettere alla UGCC di inviare informazioni e dati alle Infrastrutture Critiche al fine di gestire la situazione e supportarne le operazioni
- Permettere alla UGCC di scambiare informazioni con gli organismi dello Stato interessati
- Permettere qualsiasi altro scambio di informazioni che risultasse necessario per la gestione della crisi e la minimizzazione del danno.

La tipologia di operazioni che la UGCC deve condurre cade sotto la tipologia denominata *Network Centric Operations* e necessita di una soluzione di tipo *Network Centric Communications* che comporta l'**Interoperabilità** tra reti di comunicazione.

Infatti lo scambio dati prefigurato comporta che gli utenti ed i dati disponibili nella rete di comunicazioni A della Infrastruttura Critica A siano accessibili (gli utenti interagiscano tra loro condividendo dati ed informazioni) alla UGCC e che le informazioni e dati generati da questa siano utilizzati dagli utenti delle rete A.

A livello nazionale la soluzione che si può adottare è rappresentata da una rete *ad hoc* (*Fig. 21*) distribuita a livello nazionale che si dovrebbe interfacciare con:

- tutte le reti di comunicazione che supportano tutte le CII

- tutte le reti di comunicazione degli organismi dello Stato interessati
- tutte le reti di comunicazione degli Enti Operativi di Intervento

implementando lo scambio e la condivisione delle informazioni prefigurate. La rete di comunicazione UGCC:

- risulterà sempre connessa con le reti sopra indicate
- non renderà normalmente disponibile lo scambio diretto di dati tra Infrastrutture Critiche, scambio che risulterà possibile solamente su comando della UGCC
- risulterà sicura con un livello massimo di sicurezza in quanto dovrà trattare dati che per loro natura e per la funzionalità dell'UGCC sono da considerare sempre critici.

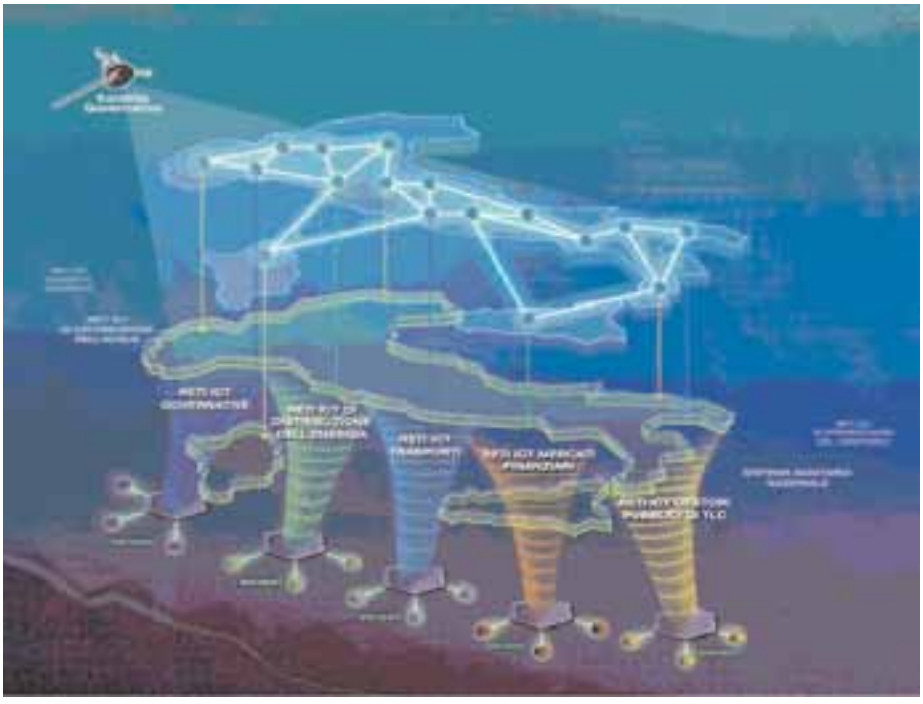


Fig. 21: Rete nazionale "ad hoc"

3.3.2 Trend nazionali e mondiali

3.3.2.1 Trend Tecnologici ed organizzativi

I trend tecnologici ed organizzativi, sia a livello Europeo che Mondiale, sono imperniati da un lato sulla ricerca di soluzioni tecnologiche atte a garantire una sicurezza "intrinseca" del complesso delle Reti di Comunicazione con l'adozione di nuovi protocolli e link protetti , dall'altro lato sulla diffusione del concetto e delle problematiche di "Sicurezza" verso i vari gestori con normative e Best Practice che consentano un uso "intelligente" del complesso di comunicazioni esistente adattandolo alle nuove esigenze di protezione.

Nel primo capitolo abbiamo segnalato la PARS (Preparatory Action for Research and Security) lanciata dalla Commissione Europea: ebbene delle 5 aree in cui è stata suddivisa la necessità di protezione "globale" Europea, ben 3 sono afferenti alle nuove tecnologie per reti di comunicazione, alla loro interoperabilità ed alla loro gestione inquadrata in un concetto di "Network Centric Operation".

La rete USA "Govnet" è un esempio di rete amministrativa indipendente che integra i due concetti sopramenzionati: è stata progettata come rete privata voce e dati basata sul protocollo Internet (IP) ma senza interconnessione alle reti commerciali e pubbliche.

3.3.2.1.1 Intelligent SW Agent

Tra le tecnologie di ultima generazione, che possono essere utilizzate nell'ambito delle reti di comunicazione per le infrastrutture critiche, gli agenti intelligenti rivestono una posizione di rilievo. Gli agenti intelligenti, anche noti come "software agent", sono in grado di eseguire in modo autonomo molte delle operazioni effettuate da normali utenti, in aggiunta a tutta una serie di altri compiti.

Ad esempio, l'architettura di sistema multi-agent RETSINA, sviluppata dalla Carnegie Mellon University di Pittsburgh (USA), è applicabile a una vasta gamma di dominii, tra i quali:

- Interoperabilità delle reti con particolare riguardo alle problematiche dell'accesso e condivisione dei dati in evoluzione verso il concetto di "Information Dissemination" della Network Centric Communication
- Pianificazione della logistica nelle operazioni militari
- Gestione personalizzata delle informazioni
- Gestione di telecomunicazioni mobili wireless
- Gestione dei portafogli finanziari
- Aste telematiche.

L'uso della tecnologia Intelligent SW Agent nell'ambito della protezione delle infrastrutture critiche interdipendenti riguarda sia gli aspetti di sviluppo di sistemi di controllo distribuito, come nel caso del progetto europeo SAFEGUARD teso all'incremento della robustezza del sistema di controllo della rete di distribuzione dell'energia elettrica, che gli aspetti di modellistica e simulazione delle infrastrutture critiche stesse. In quest'ultimo ambito possiamo ricordare le attività messe in essere dal NISAC (National Infrastructure Simulazione and Analysis Center negli USA, nato dalla collaborazione fra i Los Alamos National Laboratory e i Sandia National Laboratories insieme ad altre importanti strutture di ricerca americane) ed il progetto CISIA (Critical Infrastructure Simulation by Interdependent Agents) portato avanti da alcune Università Italiane[10].

3.3.2.1.2 Protocollo Ipv6

Il diffondersi degli accessi internet nel mondo sta rendendo rapidamente insufficiente la tecnologia a 32 bit su cui si basa la versione 4 del protocollo IP (IPv4) finora utilizzato.

IPv4, sviluppato ormai trenta anni fa dal Dipartimento della Difesa statunitense, mette infatti a disposizione circa quattro miliardi

[10] *Per la precisione dall'Università CAMPUS Bio-Medico di Roma e dall'Università degli Studi di Roma Tre.*

(pari a 2^{32}) di indirizzi IP: un numero apparentemente alto, che però rischia di non soddisfare pienamente le richieste di accesso alla Rete Globale.

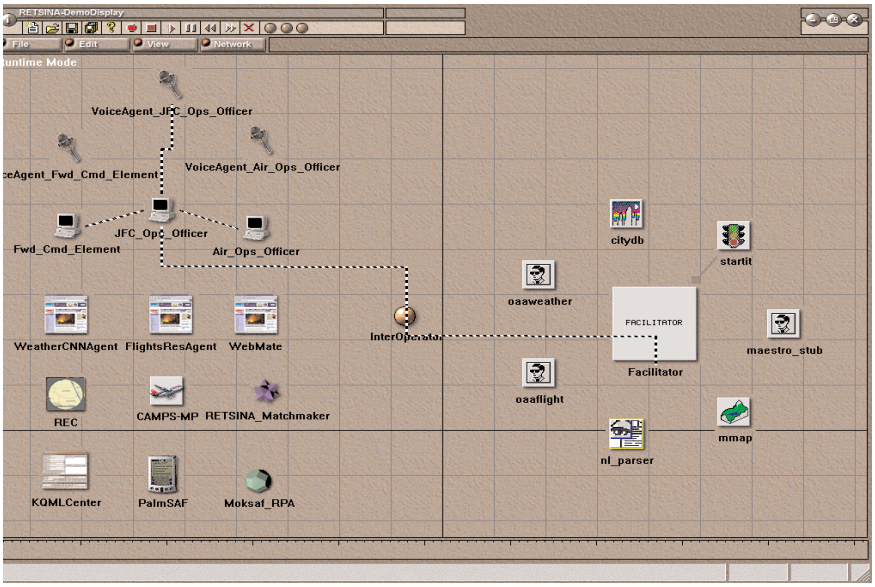


Fig. 22: Un'applicazione dell'architettura RETSINA

È così nata l'esigenza di un nuovo protocollo a 128 bit, chiamato in un primo momento IPng (IP next generation), ed ora noto come IPv6.

I benefici apportati da IPv6 sono:

- **Moltiplicazione esponenziale degli IP address disponibili (2^{128}):** grazie al nuovo protocollo, ogni nodo può disporre di un proprio indirizzo
- **Inclusione nativa di IPSec:** le intestazioni IPSec AH ed ESP fanno parte degli Extension Header di IPv6. Ne consegue che il supporto ad IPSec è ora una caratteristica obbligatoria, e non più semplicemente opzionale come nella precedente versione.

Ciò favorisce la diffusione di connessioni sicure end-to-end. Inoltre vengono agevolati servizi come FTP, IRC, SNMP, H323, SIP e RPC che erano resi difficoltosi dall'uso di Ipv4

- **Elevata velocità di elaborazione:** il formato dell'intestazione dei datagrammi è stato notevolmente semplificato, allo scopo di accelerare le operazioni svolte dagli apparati di rete
- **Eliminazione del NAT (Network Address Translation):** la disponibilità di un numero sufficientemente ampio di indirizzi IP permette di eliminare il NAT, un dispositivo usato per identificare un gruppo di macchine tramite un solo indirizzo IP pubblico. Inoltre il nuovo protocollo IP sfrutta pienamente le potenzialità di IPSec.

3.3.2.1.3 Nodi di Comunicazione Intelligenti (Smart Communication Node)

Il trend ormai condiviso da tutti gli attori nel panorama delle operazioni in ambienti complessi ed in particolare nei "sistemi di sistemi" risulta quello di prevedere l'interoperabilità di reti esistenti, "legacy" e di nuove reti (o di reti aggiornate in funzione dei requisiti operativi) come supporto alle operazioni in un concetto di "Network Centric Communication".

Tale evoluzione si basa su tre elementi : la componente di networking, quella di accesso e condivisione dei dati e la componente di sicurezza.

Gli Smart Communication Node rappresentano l'evoluzione delle attuali Centrali Multiprotocollo e sono destinati a fornire la soluzione alle problematiche di "networking" nella scenario evolutivo della interoperabilità delle reti.

Tali nodi risulteranno in grado di indirizzare l'informazione in transito su differenti percorsi operando contemporaneamente sui vari protocolli trasmissivi e sui differenti standard di trattamento dell'informazione presenti rendendo possibile, in tal modo, l'integrazione di reti e sistemi non omogenei ed il supporto contemporaneo di differenti protocolli e standard.

L'estensione ai nuovi standard quali Ipv6 e VoIP e la capacità di agire anche come Federation Agent fanno sì che tali nodi intelligenti possano rappresentare la soluzione alle problematiche di federazione ed interoperabilità evidenziate in precedenza.

3.3.3 Il Fattore Umano

In parallelo agli aspetti tecnici e tecnologici trattati ampiamente in precedenza nel presente documento, è di importanza fondamentale considerare anche il **fattore umano** che rappresenta un elemento cruciale per qualunque politica di sicurezza ICT.

Una parte delle vulnerabilità presenti nell'area ICT, derivano dalla mancanza di consapevolezza nei principali attori di questa infrastruttura (utenti e amministratori dei sistemi informatici e delle reti, progettisti della tecnologia, responsabili delle acquisizioni dei prodotti, ecc.) di quanto sia importante definire un adeguato approccio alla sicurezza ICT.

La mancanza di tale consapevolezza ha come conseguenza primaria l'assenza di adeguate procedure e processi per la gestione della sicurezza ICT e degli eventi anomali connessi. Ciò comporta anche una insufficiente attività informativa e formativa per dotarsi di personale adeguatamente addestrato e qualificato. Un tale scenario complica di fatto la possibilità di limitare a livelli accettabili le vulnerabilità ICT e di adottare efficaci contromisure.

Una adeguata strategia per rendere più sicura la specifica infrastruttura critica è pertanto quella di attivare iniziative che impattano su temi relativi alla consapevolezza, all'istruzione ed alla formazione degli attori, come ad esempio:

- la promozione di un programma globale per aumentare la consapevolezza a tutti i livelli di quanto sia importante una politica di sicurezza per i sistemi ICT
- l'adozione di programmi di istruzione e formazione per supportare le necessità di sicurezza ICT
- la promozione delle certificazioni di sicurezza (cfr. par. 3.2.2.2.4.1).

Di seguito vengono approfonditi i temi delle iniziative sopra citate.

3.3.3.1 La promozione di un programma per aumentare la consapevolezza

Una ridotta conoscenza e consapevolezza dell'esistenza di uno specifico problema di sicurezza relativo alle infrastrutture ICT, vanifica la ricerca e l'applicazione di eventuali soluzioni che, in molti casi, sarebbero già disponibili sul mercato.

In altri casi non esiste la consapevolezza di quanto possa essere importante rendere sicuro un elemento della rete; per esempio una azienda che non comprendesse che il sistema di identificazione ed autenticazione al suo server web non è adeguato, potrebbe permettere ad eventuali utenti non autorizzati di guadagnarne il controllo e sfruttarne le risorse.

Poiché l'insicurezza di un componente del Sistema può avere importanti impatti anche sulle altre componenti, le azioni intraprese per rendere sicura la propria parte di rete contribuiscono alla sicurezza di insieme del sistema stesso.

3.3.3.2 Azioni intraprese in altre realtà nazionali

I temi precedentemente trattati sono affrontati nel documento [5] emesso dal governo degli Stati Uniti, che descrive, fra le altre cose, le azioni previste per la gestione del fattore umano nel contesto della sicurezza ICT[11].

Si riportano in Tabella 12 le Azioni e le Raccomandazioni previste in tale documento.

---

[11] Il 25 novembre del 2002, il presidente Bush ha firmato l'atto legislativo per la creazione del Department of Homeland Security (DHS). Al DHS sono state attribuite importanti responsabilità relative alla sicurezza del Cyberspace.

La promozione di un programma nazionale globale per aumentare la consapevolezza	*Il DHS , in coordinamento con gli stati federali, gli enti locali e con il settore privato, promuoverà una campagna di sensibilizzazione sugli aspetti della sicurezza informatica e un programma di premi per quelle industrie che apporteranno significativi contributi al tema della sicurezza. (A/R 3-1)*
	Il DHS, in coordinamento con il Dipartimento dell'Educazione, incoraggerà e sosterrà, tenendo in opportuna considerazione le indicazioni di budget, le organizzazioni statali, locali e private nello sviluppo di programmi e linee guida per la sicurezza informatica per gli studenti delle scuole primarie e secondarie. (A/R 3-2)
	Le piccole aziende possono contribuire alla sicurezza del Cyberspace rendendo sicure le proprie connessioni ad esso tramite l'installazione di firewall ed il loro regolare aggiornamento, mantenendo aggiornati i software antivirus, i sistemi operativi e le principali applicazioni dei loro sistemi. Per facilitare queste attività il DHS creerà una task force pubblica- privata composta da aziende private per identificare modalità che consentano ai fornitori di prodotti IT e ad altre organizzazioni di rendere più facile agli utenti domestici e alle piccole aziende la messa in sicurezza dei propri sistemi. (A/R 3-3)
	Una partnership pubblica-privata dovrebbe contribuire a rendere più sicuro il Cyberspace con la partecipazione ad una " technology and R&D gap analysis" che fornisca input alla "federal cybersecurity research agenda" e contribuisca al coordinamento delle ricerche associate e allo sviluppo e disseminazione delle bestpractice per la cybersecurity. (A/R 3-6)
Adozione di adeguati programmi di istruzione e formazione a livello nazionale	*Il DHS implementerà ed incoraggerà la definizione di programmi avanzati per l'addestramento di professionisti di cybersecurity negli Stati Uniti. In coordinamento con il NSF, l'OPM e la NSA identificherà i modi per migliorare l'esistente "Cyber Corps Scholarship for Service program" così come i programmi per i laureati, i senior researcher, ecc. creati dal "Cyber Security Research and Development Act". (A/R 3-7)*
	Il DHS in coordinamento con altre agenzie con competenze di cybersecurity, svilupperà un meccanismo di coordinamento con i "federal cybersecurity and computer forensics training programs" (A/R 3-8).
La promozione di un supporto al settore privato per ottenere delle certificazioni di sicurezza	*La promozione di un supporto al settore privato per ottenere delle certificazioni di sicurezza. Il DHS incoraggerà gli sforzi necessari per la costruzione delle fondamenta per lo sviluppo di "security certification programs" universalmente riconosciuti e accettati sia dai settori privati che dai settori pubblici. Il DHS e le altre agenzie federali possono contribuire a questa attività coordinando le necessità delle "federal IT security community". (A/R 3-9).*

Tabella 12: Azioni e Raccomandazioni previste nel documento [5]

3.3.3.3 Contromisure di tipo procedurale e personale previste dall'Autorità Nazionale per la Sicurezza (ANS)

Sempre in tema "Fattore Umano" si fa un breve riferimento al documento [6] che tra i diversi argomenti trattati, affronta il tema delle misure di sicurezza, chiamate anche contromisure, che appartengono sostanzialmente a 4 categorie:

- Misure fisiche
- Misure personali
- Misure procedurali
- Misure tecniche hardware e software

Per rimanere nell'ambito del fattore umano, nei paragrafi "misure personali" e "misure procedurali" si trovano definite una serie di contromisure che, se opportunamente implementate, possono ridurre significativamente il livello di vulnerabilità dei sistemi ICT critici. Un estratto di tali contromisure è di seguito riportato:

Misure personali

Pe1	Nulla Osta di Segretezza (NOS)
Pe2	Assegnazione degli accessi alle informazioni secondo la necessità di conoscere
Pe3	Istruzioni sulla sicurezza e gestione del personale 1. Motivare il personale a seguire la politica della società o dell'Ente di appartenenza 2. Istruire il personale indicando le possibili minacce (es. divulgazione di password, e il modo di limitarne la portata) 3. Mantenere costante l'attenzione alle norme di sicurezza, adottando poster, lettere circolari, video didattici
Pe4	Addestramento del personale 1. Test di reparto per valutare il grado di alfabetizzazione informatica del personale 2. Corso interno di utilizzo delle procedure sulla base dei test effettuati 3. Esami finali di valutazione del grado di conoscenza aquisito
Pe5	Creazione di uno staff di supporto agli utenti, che effettui controlli sulla sicurezza e fornisca assistenza sulle problematiche legate alla sicurezza.

Misure procedurali

Pr1	Procedure per il backup del software e dei dati 1. Piano di backup 2. Rotazione delle memorie utilizzate per il backup 3. Backup effettuato a fine giornata 4. Assegnazione delle responsabilità e dei compiti 5. Creazione di più copie 6. Documentazione relativa alle copie
Pr2	...
Pr3	...
Pr4	Controllo dei contenitori adibiti alla raccolta dei rifiuti, per verificare se contengono oggetti (tabulati, dischetti, fogli) che possano rappresentare un rischio per la sicurezza.
Pr5	...
Pr6	Piano di emergenza 1. Manuale delle procedure da fornire al personale addetto 2. Posizionamento di quadri riassuntivi delle procedure di emergenza 3. Regole per verificare che esista realmente una situazione di emergenza 4. Pocedure per il ripristino dei dati danneggiati 5. Presenza di una check list per le procedure di emergenza 6. …. 7. Chiusura dei backup in casseforti ignifughe 8. ……

3.3.4 Cornici Contrattuali Raccomandate

Per concludere le panoramiche relative alla protezione delle reti di comunicazioni, dopo aver analizzato i fattori tecnici ed umani, è opportuno portare l'attenzione anche sugli aspetti relativi ai rapporti con i fornitori di servizi curando anche gli aspetti contrattuali.

Nella stesura di un contratto con società esterne per la fornitura di servizi la cui mancata disponibilità oltre tempi definiti possa condurre ad una situazione di emergenza/crisi all'interno di un'azienda, possono, tra gli altri, essere considerati almeno i seguenti aspetti:

1. verificare che il fornitore non ricorra ad altre strutture (risorse tecnologiche/umane) esterne. In caso contrario, verificare i processi/procedure esistenti presso tali strutture per le situazioni interne di emergenza/crisi, atti a garantire la continuità dei servizi da fornire alla CII, secondo i livelli prestazionali previsti dal contratto. Verificare l'assunzione di tutte le responsabilità senza deleghe o condivisione con terzi
2. verificare che il fornitore dei servizi abbia stipulato dei piani di intervento relativi a supporto nei casi di emergenza/crisi coinvolgenti più entità che prevedano tempi di ripristino servizi differenziati per aziende e priorità. In tal caso, sarebbe buona norma includere sul contratto una clausola inerente la priorità di intervento di ripristino
3. assicurare idonea documentazione (ad es. report mensile) circa i livelli di servizio erogati.

Si riporta di seguito una lista di raccomandazioni sugli aspetti di sicurezza che si ritiene utile verificare nelle cornici contrattuali e negli SLA (Service Level Agreement) con i fornitori di servizi di telecomunicazioni.

Garanzie e certificazioni

- Assistenza per comprendere le complessità della rete per la CII e collaborazione secondo modalità concordate per cercare soluzioni che assicurino la massima resilienza

- Impegno di risorse tecnicamente valide al fine di garantire la sicurezza della CII
- Impegno ad operare congiuntamente con la CII per quel che concerne la pianificazione ai fini della continuità dei servizi e per quel che riguarda il "disaster recovery", ivi comprese le prove per verificare e garantire la sicurezza

  Le CII sono responsabili della pianificazione della continuità dei loro servizi e della pianificazione del "disaster recovery"; molti Fornitori garantiscono assistenza in queste attività, ma il loro supporto può non essere coperto dai contratti per la fornitura dei servizi di rete
- Certificazione circa la completa "separazione" e diversità dei servizi al fine di ottemperare ai requisiti della CII
- Certificazione circa la "separazione" e la diversità mantengano la loro resilienza nel tempo.

Contratti e Trasparenza

- Prevedere il giusto grado di trasparenza
- Nel caso in cui avere "separazione" dei servizi sia un requisito primario di progetto, richiedere la piena visibilità delle infrastrutture di rete necessarie per garantire la separazione da estremo a estremo
- Disporre di opportuni piani per la gestione delle emergenze, e assicurare che tali piani vengono periodicamente sottoposti a verifica
- Disporre di opportune procedure di escalation in modo da garantire che la specifica problematica sia gestita con un livello adeguato con la l'importanza dell'evento
- Legare le clausole di recesso al rispetto degli SLA
- Concordare gli ambiti e i meccanismi di audit tecnico periodici.

Misure di Disponibilità

- Prevedere disponibilità, tempi di ripristino, ed altri indicatori di qualità ben definiti e con precisi meccanismi di calcolo
- Determinare chiaramente le responsabilità circa le garanzie di disponibilità.

Valutazione delle Minacce

- Valutare le minacce contro le infrastrutture di rete, ed esplicitare come il fornitore di servizi possa venir coinvolto nello sforzo teso a diminuire i rischi a fronte di tali minacce
- Verificare la resilienza dei servizi di rete acquistati tramite subfornitura.

3.3.4.1 Ulteriori suggerimenti

Oltre a quanto riportato nel paragrafo precedente si forniscono alcuni suggerimenti che rappresentano delle "Best Practice" organizzative in relazione ai contratti con i fornitori di servizi:

- Accertare la possibilità che i servizi che vengono forniti alla CII si possano adattare a nuove situazioni successive alla stipula del contratto
- Verificare che il fornitore disponga di opportuni piani di emergenza da attuare in caso di mancanza di energia elettrica e che esso attui le prescritte verifiche periodiche
- Verificare che la rete fornita alla CII si mantenga resiliente nel tempo
- In presenza di contratti di outsourcing che riguardano attività particolarmente sensibili ai fini della sicurezza e della continuità del servizio, prevedere che il Fornitore dei Servizi consegni almeno con cadenza mensile tutta la documentazione relativa ai livelli di servizio fornito. Se tale Fornitore dovesse prestare servizi relativi a sistemi critici (gestione di sistemi di sicurezza

informatica, gestione di apparati della rete di telecomunicazione aziendale, gestione centri di elaborazione dati critici aziendali, ecc.), prevedere la messa a disposizione dell'Azienda di strumenti di monitoraggio in tempo reale dei sistemi controllati dall'outsourcer e comunque della documentazione relativa ai log con cadenza quindicinale.

4 - Conclusioni

Questo volume è stato rivolto a tutti i gestori di infrastrutture critiche nazionali, private o pubbliche, con l'obiettivo di creare una maggiore attenzione e consapevolezza circa quelle che possono essere le relazioni e le interdipendenze esistenti tra queste e le infrastrutture di telecomunicazioni.

Le comunicazioni elettroniche sono una risorsa trasversale a tutte le infrastrutture (critiche e non) di un Paese e rivestono un ruolo particolarmente delicato sia per quel che concerne la normale funzionalità delle diverse infrastrutture sia per quel che riguarda gli aspetti legati alla gestione di situazioni di emergenza e le attività di ripristino.

In particolare la diffusione delle tecnologie informatiche e la convergenza dei canali trasmissivi hanno amplificato il ruolo strategico svolto dalle telecomunicazioni per quel che concerne il supporto che esse offrono alle diverse infrastrutture nazionali. Questi stessi fenomeni hanno, per altro, contribuito ad amplificare il livello di interdipendenza esistente fra le diverse infrastrutture.

Questo mutato scenario e le accresciute minacce connesse soprattutto con il rischio terroristico, hanno spinto i governi a delineare strategie atte a migliorare la robustezza e la sicurezza del sistema di

infrastrutture che sono alla base di ogni nazione sviluppata.

In quest'ottica, parallelamente alla protezione fisica delle infrastrutture, è fondamentale considerare gli aspetti di sicurezza connessi con i sistemi informatici che sovrintendono al funzionamento della stragrande maggioranza delle infrastrutture nazionali.

Questo volume ha voluto evidenziare appunto, i principali elementi che occorre considerare nell'analisi di vulnerabilità di questi sistemi informatici ed alcune delle possibili contro-misure che possono attuarsi.

La crescente importanza, infatti, che le tecnologie dello ICT rivestono per la continuità di servizio delle diverse infrastrutture impone di considerare con grande attenzione gli aspetti di sicurezza, protezione e robustezza dei diversi sistemi informativi e delle reti di comunicazione da questi impiegati (Capitolo 1).

Tale attività deve partire dall'analisi delle vulnerabilità del sistema, andando a considerare con attenzione gli elementi di interdipendenza e le possibili minacce oltre che dall'individuazione degli asset da proteggere. Questi elementi costituiscono il punto di partenza per la definizione di opportune strategie di sicurezza tese a ridurre il rischio al di sotto di un livello compatibile con la criticità dell'infrastruttura in esame (Capitolo 2).

Concentrando l'attenzione sulle reti di telecomunicazioni a servizio dei sistemi informativi di monitoraggio e controllo delle diverse infrastrutture, occorre analizzare l'importanza e la strategicità delle informazioni da esse veicolate e le caratteristiche che la rete sottostante deve possedere.

Tale analisi porta ad una loro classificazione in termini di: reti di massima sicurezza, reti sicure e reti robuste. Tali classi presentano un decrescente livello di resilienza e sono caratterizzate da elementi architetturali, topologici, procedurali e di funzionamento differenti,

tali da preservare gli standard di sicurezza richiesti per le diverse applicazioni.

Analoga attenzione va posta anche agli strati superiori al livello fisico, ove occorre predisporre adeguate infrastrutture di sicurezza in grado di garantire l'identificazione, l'autenticazione e la certificazione dei soggetti operanti sull'infrastruttura e delle informazioni da questa veicolate. È indubbio, poi, che il fattore umano rappresenta la più valida delle risorse per gestire nel migliore dei modi situazioni anomale o di crisi, ma nel contempo, in presenza di personale non adeguatamente formato e motivato, esso può rappresentare un elemento di vulnerabilità per l'intero sistema. Ciò impone la necessità di attivare adeguati processi di informazione e formazione per quel che concerne i diversi aspetti della sicurezza, adozione di standard internazionali e il ricorso alla certificazioni.

Specificatamente la certificazione rappresenta un elemento di notevole importanza sia per quel che riguarda la valutazione di sicurezza dei singoli prodotti (certificazione basata sui Commom Criteria) che per quel che riguarda il processo (certificazione basata sulla BS7799).

Naturalmente la sicurezza delle reti di comunicazioni deve prendere in esame, oltre che gli aspetti più strettamente informatici, anche i servizi e le infrastrutture di supporto. In quest'ottica particolare attenzione va posta nel garantire una adeguata fornitura elettrica.

La presenza di interdipendenze fra le diverse infrastrutture fa sorgere la necessità di gestire in modo congiunto eventi di crisi al fine di circoscriverne e limitarne le conseguenze. A tal fine è ipotizzabile la costituzione di una apposita unità di gestione della crisi in cui siano rappresentati esponenti delle diverse infrastrutture coinvolte. Tale unità di crisi, che dovrebbe essere composta da persone adeguatamente formate e supportate da appositi strumenti metodologici e tecnologici coordina le iniziative necessarie per la gestione i diversi aspetti della crisi.

Le appendici che sono state incluse completano il lavoro riportando le azioni intraprese in questo settore da un importante operatore italiano (sono evidenziati gli aspetti di analisi e gestione del rischio, nonché gli aspetti procedurali, metodologici ed operativi che occorre attivare in presenza di eventi di crisi) e aggiungendo un questionario di sussidio che i diversi operatori potranno usare per effettuare una autovalutazione del proprio livello di dipendenza dalle infrastrutture di telecomunicazione e di rischio al fine di prendere una più chiara coscienza delle proprie vulnerabilità.

Il questionario riguarda gli elementi che in un contratto sono specificati negli SLA. Essi mirano ad assicurare che il servizio offerto sia caratterizzato da un concordato, predefinito, verificabile livello di qualità, prevedendo specifici oneri contrattuali nel caso in cui il Fornitore non ottemperi agli obblighi previsti. Tali garanzie e oneri dipendono sia in forma esplicita sia, più spesso, in forma implicita, anche da azioni procedurali e misure tecniche che devono essere attuate dal committente. Un'eventuale mancanza organizzativa o tecnica del committente può essere alla base di contestazioni sulla interpretazione dello SLA, soprattutto per le clausole riguardanti il risarcimento del danno dovuto a una presunta inadempienza da parte del Fornitore.

Per evitare tali situazioni e, soprattutto, per tutelare maggiormente il committente rispetto alla attuazione effettiva di quanto previsto nello SLA, è fortemente raccomandato concordare con il Fornitore di Servizi in forma esplicita e dettagliata l'insieme delle condizioni che devono essere rispettate dall'Organizzazione affinché lo SLA possa ritenersi valido.

Tali condizioni costituiscono normalmente un nuovo documento contrattuale denominato Operation Level Agreement (OLA).

In linea del tutto generale, gli OLA e gli SLA dovrebbero essere documenti paralleli, in cui ad ogni prescrizione contrattuale prevista per il Fornitore nello SLA corrisponde l'insieme delle prescrizioni

(OLA) che devono essere soddisfatte dall'Organizzazione affinché lo SLA possa essere applicato nel modo desiderato.

In presenza di una coppia SLA-OLA ben coordinati, in caso di controversie non dovrebbero esserci contestazioni riguardo a *quali* fossero gli obblighi procedurali e tecnici del Fornitore e del committente, ma solamente riguardo a *se* quelle particolari procedure e misure tecniche siano state attuate.

Per risolvere questo ultimo aspetto del problema possono essere previste due soluzioni.

La prima consiste nel prevedere che il Fornitore controlli le azioni intraprese dal committente. Questo approccio, però, potrebbe essere considerato dal committente troppo invasivo o di difficile realizzazione pratica.

La seconda soluzione prevede di affidare i suddetti controlli a una terza parte fidata e riconosciuta sia da parte del Fornitore sia da parte del committente. Questa terza parte fidata potrebbe essere un soggetto che opera nell'ambito dello Schema Nazionale per la Certificazione della Sicurezza Informatica, sia esso un Laboratorio per la Valutazione della Sicurezza (LVS) o un Assistente.

L'importanza della robustezza e della resilienza delle infrastrutture di comunicazione è al centro di un dibattito proposto a livello europeo dalla presidenza olandese: le esperienze degli ultimi anni, dalle torri gemelle allo tsunami, ci hanno posti di fronte a un dato di fatto, e cioè che la sola prevenzione non basta, occorre lavorare sulla organizzazione preventiva della gestione emergenze (anche a livello locale) e sui piani di recupero.

L'Italia conta su una esperienza profonda e ricca di esemplari successi nella gestione di emergenze e nel recupero (si pensi al black out del 2003, solo per fare un esempio) e viene percepita a livello mondiale come un Paese di riferimento per tali aspetti.

Questo volume ha voluto essere un punto di partenza per promuovere lo scambio di informazioni e la diffusione di Best Practice sul rapporto tra infrastrutture di comunicazione e infrastrutture critiche nazionali.

Allegato 1 - Acronimi e abbreviazioni

Acron./Abbrev.	***Descrizione***
ACL	*Access Control List*
CA	*Certification Authority*
CAO	*Certification Authority Operator*
CII	*Critical Information Infrastructure (Infrastruttura Critica Informatizzata)*
CIIP	*Critical Information Infrastructure Protection (Protezione delle Infrastrutture Critiche Informatizzate)*
CMD	*Carta Multiservizi della Difesa*
CNI	*Critical National Infrastructure (Infrastruttura Critica Nazionale)*
CNII	*Critical National Information Infrastructure (Infrastruttura Critica Nazionale Informatizzata)*
COTS	*Commercial Off The Shelf*
CRL	*Certificate Revocation List*
CRM	*Customer Relationship Management*
CTI	*Computer Telephony Integration*
DMZ	*DeMilitarized Zone*
D-OCSP	*Distributed On Line Certificate Status Protocol*
DOS	*Denial of Service*
DR	*Disaster Recovery*
EAL	*Evaluation Assurance Level*
GCC	*Gestione Congiunta della Crisi*
HA	*High Availability*
HIDS	*Host Intrusion Detection System*
HSM	*Hardware Security Module*
ICT	*Information and Communication Technologies*

IDSS	*Intelligent Decision Support System*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IPng	*IP next generation*
ITSEC	*Information Technology Security Evaluation Criteria*
ITSEM	*Information Technology Security Evaluation Methodology*
ITU	*International Telecommunication Union (Unione Internazionale delle Telecomunicazioni – ente internazionale che nell'ambito dell'Organizzazione delle Nazioni Unite cura la standardizzazione per il coordinamento delle reti e dei servizi di telecomunicazione)*
IVR	*Interactive Voice Response*
LDAP	*Lightweight Directory Access Protocol*
MLPP	*Multi-Level Precedence and Pre-emption*
NAT	*Network Address Translation*
NIDS	*Network Intrusion Detection System*
OCSI	*Organismo di Certificazione della sicurezza dei sistemi e prodotti informatici commerciali*
OCSP	*On Line Certificate Status Protocol*
OHSAS	*Occupation Health and Safety Assessment*
OSS	*Operations Support System*
OU	*Organizational Unit*
PdR	*Porta di Rete*
PGC	*Piano di Gestione delle Crisi*
PGCC	*Piano di Gestione Congiunta delle Crisi*
PKI	*Public Key Infrastructure*
PSTN	*Public Switched Telephone Network*
RA	*Registration Authority*
RTC	*Real Time Certification*
RFC	*Request for Quotation*
SLA	*Service Level Agreement*
TBD	*To Be Defined*
TOE	*Target Of Evaluation*
UGC	*Unità di Gestione delle Crisi*
UGCC	*Unità di Gestione Congiunta delle Crisi*
VR	*Virtual Reality*
VPN	*Virtual Private Network*

Allegato 2
Documenti di riferimento

[1] PIC - Protezione delle Infrastrutture Critiche Informatizzate - La realtà Italiana - *Dipartimento per l'Innovazione e le Tecnologie, rapporto del Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate - Marzo 2004*

[2] Linee Guida del Governo per lo sviluppo della Società dell'Informazione - *Commissione dei Ministri per la Società dell'Informazione - Maggio 2002*

[3] Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la Pubblica Amministrazione - *Comitato Tecnico Nazionale sulla sicurezza ICT - Marzo 2004*

[4] National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products (NSTISSC) - *National Security Telecommunications and Information Systems Security Committee, Security Policy (NSTISSP) No. 11 - Gennaio 2000*

[5] SEC_CYBERSPACE - The National strategy to Secure Cyberspace February 2003 - The White House.

[6] STANDARD_SICUREZZA - Standard di Sicurezza per Sistemi/reti EAD militari - *Presidenza del Consiglio dei Ministri - Autorità Nazionale per la Sicurezza - PCM - ANS /TI002 -*

[7] "National Security Telecommunications and Information Systems" - *National Security Telecommunications and Information Systems Security Committee (NSTISSC)*

[8] CANADA - Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, *Threats to Canada's Critical Infrastructure,* TA03-001, 12 Marzo 2003.

[9] ETH - A. Wenger, J. Metzger, M. Dunn, I. Wigert (edited by) *International CIIP Handbook 2004*, ETH, the Swiss Federal Institute of Technology Zurich, 2004. www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdf

Allegato 3

Standard e normativa di riferimento

Nel compilare il documento ci si è riferiti agli standard e alle normative nazionali e internazionali di cui di seguito viene riportato un elenco non esaustivo.

ITU-T

- E.106 "International Emergency Preference Scheme for disaster relief operations (IEPS)", Ottobre 2003 [per reti PSTN, ISDN, e PLMN]F.706, "Service Description for an International Emergency Multimedia Service (IEMS)", (Draft - Novembre 2002) [estensione della E.106 per servizi multimediali su reti a pacchetto, ad es. IP]
- M.ets (futura M.3350), "TMN service management requirements for information interchange across the TMN X-interface to support provisioning of telecommunication capabilities for disaster relief operations and mitigation", Aprile 2004
- Y.roec (futura Y.1271), "Framework(s) on network requirements and capabilities to support emergency communications over evolving circuit-switched and packet-switched networks", draft H.460.4, "Call priority designation for H.323 calls", Novembre 2002
- H.460.14, "Support for Multi-Level Precedence and Preemption (MLPP) within H.323 systems", Marzo 2004
- I.255.3, "Community of interest supplementary services:

Multi-level precedence and preemption service (MLPP)", Luglio 1990

- Q.735.3, "Stage 3 description for community of interest supplementary services using Signalling System No. 7 : Multi-level precedence and pre-emption", Marzo 1993
- Q.955.3, "Stage 3 description for community of interest supplementary services using DSS 1 : Multi-level precedence and preemption (MLPP)", Marzo 1993
- Q.761 (1999) Amendment 2, "Support for the International Emergency Preference Scheme", 12/2002
- Q.762 (1999) Amendment 1, "Support for the International Emergency Preference Scheme", 12/2002
- Q.763 (1999) Amendment 2, "Support for the International Emergency Preference Scheme", 12/2002
- Q.764 (1999) Amendment 2, "Support for the International Emergency Preference Scheme", 12/2002
- Q.1902.1 (2001) Amendment 1, "Support for the international emergency preference scheme", 12/2002
- Q.1902.2 (2001) Amendment 1, "Support for the international emergency preference scheme", 12/2002
- Q.1902.3 (2001) Amendment 1, "Support for the international emergency preference scheme", 12/2002
- Q.1902.4 (2001) Amendment 1, "Support for the international emergency preference scheme", 12/2002
- Q.2761 (1999) Amendment 1, "Support for the international emergency preference scheme", 12/2002
- Q.2762 (1999) Amendment 1, "Support for the international emergency preference scheme", 12/2002
- Q.2763 (1999) Amendment 1, "Support for the international emergency preference scheme", 12/2002
- Q.2764 (1999) Amendment 1, "Support for the international emergency preference scheme", 12/2002

- Q.Sup47 "Emergency services for IMT-2000 networks - Requirements for harmonization and convergence", 11/2003

ETSI

- TR 101 300, "Telecommunications and Internet Protocol Harmonisation Over Networks (TIPHON)", v.2.1.1, Ottobre 1999

NSTAC

- "Network Security/Vulnerability Assesments Task Force Report", Marzo 2002, http://www.ncs.gov/nstac/reports/2002/NSVATF-Report-(FINAL).htm
- White Paper, "The Emergency telecommunications Service (ETS) in Evolving Networks", v.3.0, 4 Febbraio 2002

IETF

- RFC 3487, "Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP)", Schulzrinne, Febbraio 2003
- RFC 3523, "Internet Emergency Preparedness (IEPREP) Telephony Topology Terminology", Polk, Aprile 2003
- RFC 3690, "IP Telephony Requirements for Emergency Telecommunication Service (ETS)", Carlberg-Atkinson, Febbraio 2004
- RFC 3689, "General Requirements for Emergency Telecommunication Service (ETS)", Carlberg-Atkinson, Febbraio 2004
- INTERNET DRAFT Draft-ietf-sip-resource-priority-03, "Communications Resource Priority for the Session Initiation Protocol (SIP)", Schulzrinne-Polk, 20 Marzo 2004
- INTERNET DRAFT Draft-ietf-ieprep-framework-09.txt, "Framework for Supporting ETS in IP telephony", Carlberg-

Brown-Beard, 5 Febbraio 2004

- INTERNET DRAFT Draft-ietf-ieprep-domain-req-02.txt, "Emergency Telecommunication Services (ETS) Requirements for a Single Administrative Domain", Carlberg, 21 Settembre 2004
- INTERNET DRAFT draft-ietf-ieprep-domain-frame-03.txt, "A Framework for Supporting Emergency Relecommunication Services (ETS) within a single Administrative Domain", Carlberg, 17 Settembre 2004
- INTERNET DRAFT draft-polk-reason-header-for-preemption-00.txt, "Extending the Session Initiation Protocol Reason Header to account for Preemption Events", Polk, 8 Ottobre 2003
- RFC 3326, "The Reason Header Field for the Session Initiation Protocol (SIP)", Schulzrinne-Oran-Camarillo, Dicembre 2002
- INTERNET DRAFT Draft-pierce-tsvwg-pref-treat-examples-00.txt, "Examples for Provision of Preferential Treatment in Voice over IP", Pierce-Choi, Aprile 2004
- INTERNET DRAFT Draft-pierce-tsvwg-assured-service-req-00.txt, "Requirements for Assured Service Capabilities in Voice over IP", Pierce-Choi, Aprile 2004
- INTERNET DRAFT Draft-pierce-tsvwg-assured-service-arch-00.txt, "Architecture for Assured Service Capabilities in Voice over IP", Pierce-Choi, Aprile 2004
- INTERNET DRAFT Draft-silverman-tsvwg-mlefphb-01.txt, "Multi-Level Expedited Forwarding Per Hop Behaviour (MLEF PHB)", Pierce-Choi, 1 Ottobre 2004
- INTERNET DRAFT Draft-baker-tsvwg-mlpp-that-works-02.txt, "Implementing MLPP for Voice and Video in the Internet Protocol Suite", Baker-Polk, 2 Ottobre 2004
- INTERNET DRAFT Draft-baker-tsvwg-mlef-concerns-02.txt, "MLEF without Capacity Admission Does not Satisfy MLPP Requirements", Baker-Polk, 5 Ottobre 2004

ISO

- ISO 17799, "Information Security (INFOSEC)"
- ISO/IEC 2382-8 "Information technology - Vocabulary" - Part 8: Security, 1998
- ISO/IEC TR 15446 "Information technology - Security techniques - Guide for the production of Protection Profiles and Security Targets", Dicembre 2003
- ISO/IEC 17799:2000, Code of Practice for Information Security Management

COMMON CRITERIA E CERTIFICAZIONE DI SISTEMI/PRODOTTI

- CCIMB-2004-01-001, "Common Criteria for Information Technology Security Evaluation, Part 1 - Introduction and general model", version 2.2, Gennaio 2004
- CCIMB-2004-01-002, "Common Criteria for Information Technology Security Evaluation, Part 2 - Security functional requirements", version 2.2, Gennaio 2004
- CCIMB-2004-01-003, "Common Criteria for Information Technology Security Evaluation, Part 3 - Security assurance requirements", version 2.2, Gennaio 2004
- CCIMB-2004-02-09, "Assurance Continuity: CCRA Requirements"; Febbraio 2004
- CEM-97/017, "Common Evaluation Methodology for Information Technology Security Evaluation, Part 1 - Introduction and general model"; version 0.6, Gennaio 1997
- CCIMB-2004-01-004, "Common Evaluation Methodology for Information Technology Security Evaluation, Part 2 - Evaluation Methodology", version 2.2, Gennaio 2004

NIST e ISO

- Draft SP 800-70 The NIST Security Configuration Checklists Program
- SP 800-64 NIST Security Considerations in the Information System Development Life Cycle, October 2003
- SP 800-63 NIST Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, June 2004
- SP 800-61 NIST Computer Security Incident Handling Guide, January 2004
- SP 800-60 NIST Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004
- SP 800-59 NIST Guideline for Identifying an Information System as a National Security System, August 2003
- SP 800-55 NIST Security Metrics Guide for Information Technology Systems, July 2003 Draft SP
- SP 800-50 NIST Building an Information Technology Security Awareness and Training Program, October 2003
- SP 800-47 NIST Security Guide for Interconnecting Information Technology Systems, September 2002
- SP 800-46 NIST Security for Telecommuting and Broadband Communications, September 2002
- SP 800-42 Guideline on Network Security Testing, October 2003
- SP 800-41 Guidelines on Firewalls and Firewall Policy, January 2002
- SP 800-40 Procedures for Handling Security Patches, September 2002
- SP 800-36 Guide to Selecting Information Security Products, October 2003
- SP 800-35 Guide to Information Technology Security

Services, October 2003

- SP 800-34 Contingency Planning Guide for Information Technology Systems, June 2002
- SP 800-33 Underlying Technical Models for Information Technology Security, December 2001
- SP 800-31 Intrusion Detection Systems (IDS), November 2001
- SP 800-30 Risk Management Guide for Information Technology Systems, July 2002
- SP 800-27 Rev. A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, June 2004
- SP 800-26 Security Self-Assessment Guide for Information Technology Systems, November 2001
- SP 800-24 PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does, August 2000
- SP 800-23 Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, August 2000
- SP 800-18 Guide for Developing Security Plans for Information Technology Systems, December 1998
- SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
- SP 800-13 Telecommunications Security Guidelines for Telecommunications Management Network, October 1995
- SP 800-12 An Introduction to Computer Security: The NIST Handbook, October 1995
- INCITS/ISO/IEC TR 13335 Information technology - Guidelines for the management of IT Security

  Part 1: Concepts and models for IT Security

  Part 2: Managing and planning IT Security

Part 3: Techniques for the management of IT Security

Part 4: Selection of safeguards

Part 5: Management guidance on network security

- 1. ISO/IEC IS 17799-1 - Information security management - Part 1: Code of practice for information security management - Standard.
- 2. BS7799-2 - Information security management systems - Specification with guidance for use.
- 3. 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
- 4. ISO/IEC TR 13335-2, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 2: Managing and planning IT security
- 5. 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
- 6. ISO/IEC TR 13335-4, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 4: Selection of safeguards
- 7. ISO/IEC TR 13335-5, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 5: Management guidance on network security
- 8. ISO/IEC IS 15408-1 Evaluation Criteria for Information Technology Security - Part 1: Introduction and general model.
- 9. ISO/IEC IS 15408-2 Evaluation Criteria for Information Technology Security - Part 2: Security functional requirements.
- 10. ISO/IEC IS 15408-3 Evaluation Criteria for Information Technology Security - Part 3: Security assurance requirements.

Allegato 4
Una applicazione di gestione del rischio: il caso TERNA

INTRODUZIONE

Terna, società proprietaria in Italia della Rete di Trasmissione Nazionale dell'energia elettrica (RTN), ha sviluppato negli ultimi anni una diretta esperienza nel campo della gestione del rischio, ottenendo significativi risultati nell'ottica del raggiungimento degli obiettivi aziendali di qualità del servizio e di eccellenza operativa.

Nel presente documento vengono illustrati gli elementi caratteristici di uno dei processi fondamentali di *Business Continuity* messi a punto nella società: l'applicazione dell'analisi del rischio alle funzioni strategiche di conduzione e monitoraggio degli impianti elettrici della RTN.

In forma sintetica, vengono presentate la metodologia utilizzata per l'individuazione e la valutazione del rischio ed il piano di azioni per ricondurre ogni situazione di rischio a livelli sostenibili, nei casi maggiormente critici per la sicurezza del sistema elettrico nazionale, analizzando e valutando, a partire dalle esperienze di esercizio, un quadro ampio di potenziali minacce esterne e vulnerabilità interne.

Il documento descrive inoltre il ciclo di controllo, parte integrante della gestione operativa del rischio, finalizzato ad effettuare in modo sistematico le verifiche sulla realizzazione effettiva delle azioni

di prevenzione/mitigazione, sulla predisposizione di un efficace sistema di attuazione di *Disaster Recovery* e sulla corretta definizione dell'organizzazione preposta ad operare nel processo, a tutti i livelli.

L'ambito descritto rappresenta di fatto uno dei processi primari di *Business Continuity* per Terna, in quanto ad esso fanno capo il presidio continuo della RTN e le operazioni di esercizio, le attività di controllo ed attuazione delle riprese del servizio elettrico nei casi di black-out e le strutture organizzative necessarie alla gestione ordinaria ed a quella per fronteggiare eventuali situazioni di crisi.

GLI ASSET DI TERNA - CNI/CII

Terna è proprietaria di oltre il 90% della rete elettrica di trasmissione nazionale, con un parco impianti composto da quasi 300 stazioni elettriche, 566 trasformatori ed oltre 38.600 km di linee elettriche a 380/220/130 kV; si tratta di una infrastruttura distribuita su tutto il territorio nazionale *A4.1*), dedicata al trasferimento di energia in alta ed altissima tensione dagli impianti di produzione e dalla linee di interconnessione con l'estero fino ai punti di prelievo di alcuni grandi clienti (alimentati direttamente in alta tensione) e soprattutto delle varie aziende che effettuano la distribuzione dell'energia elettrica alla clientela diffusa.

Terna ha la responsabilità della gestione efficace ed efficiente della rete, in accordo con le procedure stabilite dal GRTN. Con gli obiettivi primari della sicurezza e della qualità del servizio (disponibilità degli elementi di rete, continuità, capacità di recovery) e della riduzione dei tempi di indisponibilità e dei costi, Terna effettua le operazioni di esercizio, monitoraggio e controllo in tempo reale della configurazione della rete tramite tre centri operativi (c.d. Centri di Teleconduzione - CTI) e provvede, tramite la sua organizzazione territoriale, alle attività di manutenzione ordinaria e straordinaria ed a quelle di sviluppo rete deliberate dal GRTN (per esigenze funzionali, per razionalizzazioni, per modifiche oppure per obblighi normativi).

Fig. A4.1: La CNI di Terna

Nell'ambito dei compiti attribuiti, Terna ha l'obbligo di mantenere rapporti operativi, oltre che con il GRTN, con le altre società di produzione e distribuzione del sistema elettrico nazionale, con i Terzi, con le Autorità e con gli Enti (Prefetture, Corpo Forestale e Protezione Civile).

Di seguito sono elencate alcune delle definizioni che ricorrono nel documento.

Black-out	*Totale assenza di tensione su impianti o porzioni di rete elettrica a seguito di disservizi che, per durata e/o estensione, possono provocare estese e rilevanti disalimentazioni di utenze*
Business Continuity	*Processo finalizzato ad assicurare la prevenzione e la gestione efficace di eventi critici mediante sistemi di prevenzione, strutture organizzative, regole operative e mezzi tra loro coerenti. Il processo si sviluppa nelle seguenti macro fasi:* *fase preventiva: analisi e valutazione dei rischi, predisposizione e realizzazione dei sistemi di prevenzione, del piano operativo di gestione degli eventi (piano di emergenza e piano di Disaster Recovery) e formazione del personale* *fase gestione: governo degli eventi critici e contenimento dei danni e ritorno alla normalità* *fase follow up: verifica dell'efficacia dei sistemi di prevenzione e di recovery e garanzia del loro aggiornamento - valutazione a posteriori delle modalità di gestione di eventi critici e messa in opera di azioni migliorative secondo la logica del miglioramento continuo*
Crisi	*Evento dannoso caratterizzato da un impatto aziendale eccezionale e che ha generalmente una risonanza straordinaria sull'opinione pubblica. Lo stato di crisi richiede di essere affrontato con strumenti di gestione straordinaria (es. Comitato di Crisi)*

Danno	*Impatto negativo derivante dal verificarsi di un evento, stimabile in termini economici*
Disaster Recovery (DR)	*Complesso di interventi organizzativi, tecnologici e logistici che consentono di ripristinare la continuità dei processi e delle infrastrutture aziendali resi non operanti o inaccessibili a seguito di eventi critici*
Emergenza	*Evento dannoso che devia il normale corso delle attività aziendali e che può essere prevenuto e/o gestito con appositi piani (piani di emergenza). Nell'ambito del processo Conduzione e monitoraggio impianti le situazioni di emergenza si identificano in due livelli "Condizione normale di allarme" e "Condizione perturbata"*
Evento critico	*Qualsiasi incidente o situazione che accade in un determinato luogo e in un certo tempo e che può determinare condizioni di emergenza e/o crisi*
Impatto	*"Conseguenza" derivante dal verificarsi di un evento. Può generare sia effetti positivi che negativi per l'azienda. Può essere espresso sia in termini qualitativi che quantitativi*
Ipotesi	*Assunzioni di base circa le possibili situazioni di disastro per tipologie di fenomeni diversi, a fronte dei quali il piano di recovery deve essere sviluppato. Le ipotesi possono essere di due tipi:* - *basate sulla frequenza (probabilità attesa, diagramma di Pareto)* - *basate sulla condizione peggiore (attacchi, ecc.).*
Livello di esposizione al rischio	*Valore ottenuto attraverso la correlazione tra il valore della probabilità di accadimento dell'evennto e il valore del danno causato dall'evento*
Minaccia	*Particolare evento o situazione, generalmente esterno all'organizzazione aziendale, il cui verificarsi determinerebbe un impatto negativo*
Probabilità	*Frequenza di accadimento di un evento, valutata/misura-*

	ta in un periodo di tempo sufficiente in relazione al processo
Unità di rischio	*Parte di sistema potenzialmente soggetta a eventi dannosi*
Vulnerabilità	*Elemento, generalmente interno al perimetro aziendale, che eleva il profilo di rischio determinando un aumento della probabilità e/o dell'impatto*

CONTESTO DI APPLICAZIONE DELLA GESTIONE DEL RISCHIO

Le funzioni di conduzione e monitoraggio in tempo reale degli asset della rete elettrica sono attuate da personale tecnico ad alta specializzazione con il supporto di un complesso sistema tecnologico integrato, costituito da componenti ICT, di diverso tipo e funzionalità, (nodi di acquisizione dati, reti di comunicazione, centri di controllo, server SCADA, Database e software dedicati, applicativi di grid management, ecc.) distribuiti sul territorio nazionale.

Come appare dalla *Fig. A4.2*, si tratta di un processo basato sulla combinazione di attività (cioè organizzazione e risorse, con fattori chiave professionalità, formazione, reclutamento, procedure, ecc.) e di tecnologie (con fattori chiave l'innovazione, le architetture, gli standard, le diversificazioni, ecc.).

Tale infrastruttura logica e fisica può essere considerata il "nucleo" della CII di Terna, per il ruolo che svolge nella gestione del sistema elettrico, infatti:

- gestisce i flussi informativi da/verso le stazioni elettriche assicurandone integrità e sicurezza
- esegue la rappresentazione in tempo reale agli operatori dello stato del sistema elettrico (topologia della rete, segnali e misure)

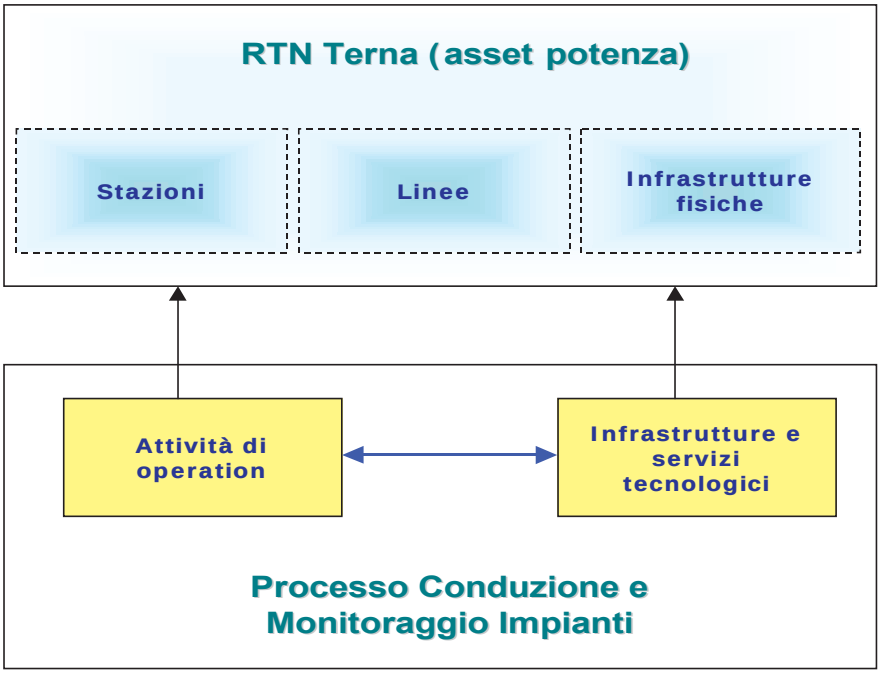


fig. A4.2 -Componenti del processo di conduzione e monitoraggio della RTN

- supporta tutte le azioni dirette a soddisfare la conduzione ed il controllo a distanza delle apparecchiature di potenza
- garantisce gli strumenti di comunicazione per la attività di emergenza.

L'infrastruttura utilizza al suo interno *Fig. A4.3*) specifiche componenti distribuite per l'interfacciamento con gli impianti di potenza e vari componenti ICT dedicati, come sistemi di elaborazione, HMI, Database, reti di telecomunicazioni implementate ad hoc, costituite, quest'ultime, sia da piattaforme geografiche di trasmissione dati (c.d. SCTI-NET, composta da nodi, router, sistemi di supervisione, sistemi di protezione) che da sistemi telefonici specificamente ottimizzati per fornire un supporto adeguato alle attività di esercizio della RTN.

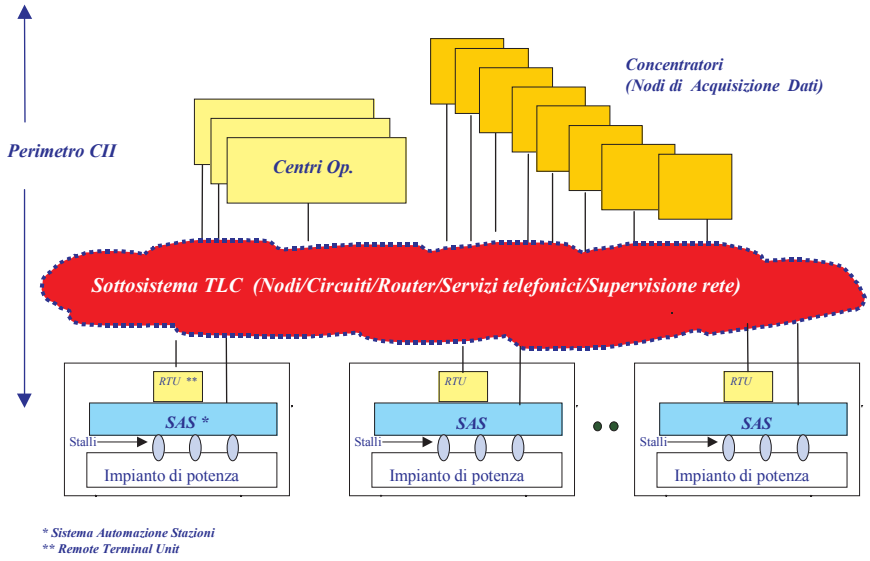


fig. A4.3 - Rappresentazione a blocchi funzionali della CII

Attraverso le attività di conduzione e monitoraggio, la Rete di Trasmissione Nazionale dell'energia elettrica deve essere mantenuta nelle condizioni (o stati) ottimali di esercizio: il processo globale è caratterizzato da un insieme coordinato di attività organizzative, funzionali, operative e progettuali finalizzate ad una gestione ottimale delle "*operation*", in cui ha un ruolo fondamentale la stretta interazione tra l'organizzazione e le tecnologie di supporto.

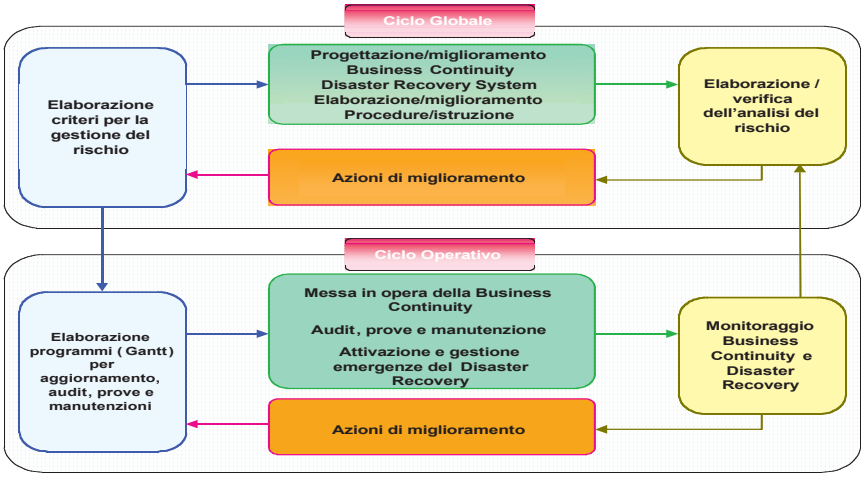
LE FASI DEL PROCESSO DI GESTIONE DEL RISCHIO PER LA CII

Alla luce di quanto detto, la gestione del rischio per l'infrastruttura di controllo e comunicazione rappresenta un vero e proprio processo a sé, destinato all'ingegneria, all'innovazione ed alla manutenzione della CII, estremamente critico per le attività rilevanti ai fini della sicurezza della rete elettrica (specie in condizioni perturbate) che svolgono le relative componenti tecnologiche.

La gestione del rischio per la CII è stata sviluppata secondo lo schema gerarchico, adottato tipicamente in Terna, a doppio ciclo - Globale ed Operativo - PDCA (Plan, Do, Check, Act).

Per la CII sono state definite ed indagate 3 categorie di rischio: rischio funzionale (relativo alla continuità del servizio), rischio fisico (relativo alla disponibilità degli asset ed alla loro integrità) e rischio logico-informatico (relativo alla sicurezza del software e dei dati).

La prima fase del processo ha sottoposto le funzioni elementari del sistema infrastrutturale ad un'analisi approfondita sull'impatto



dei potenziali eventi critici in grado di condizionarne il corretto funzionamento, con lo scopo di individuare eventuali soluzioni progettuali (sistemi di prevenzione), operative, di manutenzione, di esercizio necessarie a minimizzare gli effetti degli eventi stessi.

L'obiettivo finale di questa fase è fornire al *management* un quadro completo sulle criticità pendenti sul funzionamento di un processo operativo primario ed una rosa di possibili alternative per assicurare migliori condizioni di sicurezza, ovviamente in rapporto a considerazioni economiche ed avendo valutato in modo approfondito il grado di dipendenza degli obiettivi aziendali ed il relativo danno derivabile da una perdurante indisponibilità del processo stesso. Per raggiungere lo scopo è stato attuato un approccio top-down, strutturato secondo lo schema seguente:

I. analisi degli scenari di rischio (calamità naturali, eventi dolosi, guasti estesi, ecc.)

II. modellizzazione del processo e individuazione (identificazione) degli eventi critici (minacce, vulnerabilità)

III. valutazione del rischio mediante tecniche di esame di impatto e probabilità di accadimento delle conseguenze sul processo primario, tenendo conto dei possibili fenomeni di minaccia/disturbo e del loro effetto sulle funzioni e le prestazioni del processo

IV. individuazione e progetto delle azioni di mitigazione/correzione: scelta delle azioni tecniche che consentono di ridurre l'influenza dei fattori considerati entro misure accettabili;

V. realizzazione, messa in opera e verifica delle azioni di mitigazione/correzione e delle strutture di backup

VI. definizione e attuazione dei piani esecutivi per la messa in opera delle azioni di mitigazione/correzione per affrontare l'evenienza degli eventi critici previsti (minacce, vulnerabilità), con metodologie prefissate e con organizzazione di emergenza/crisi (Disaster Recovery)

VII. monitoraggio dell'intero processo e strutturazione dei controlli.

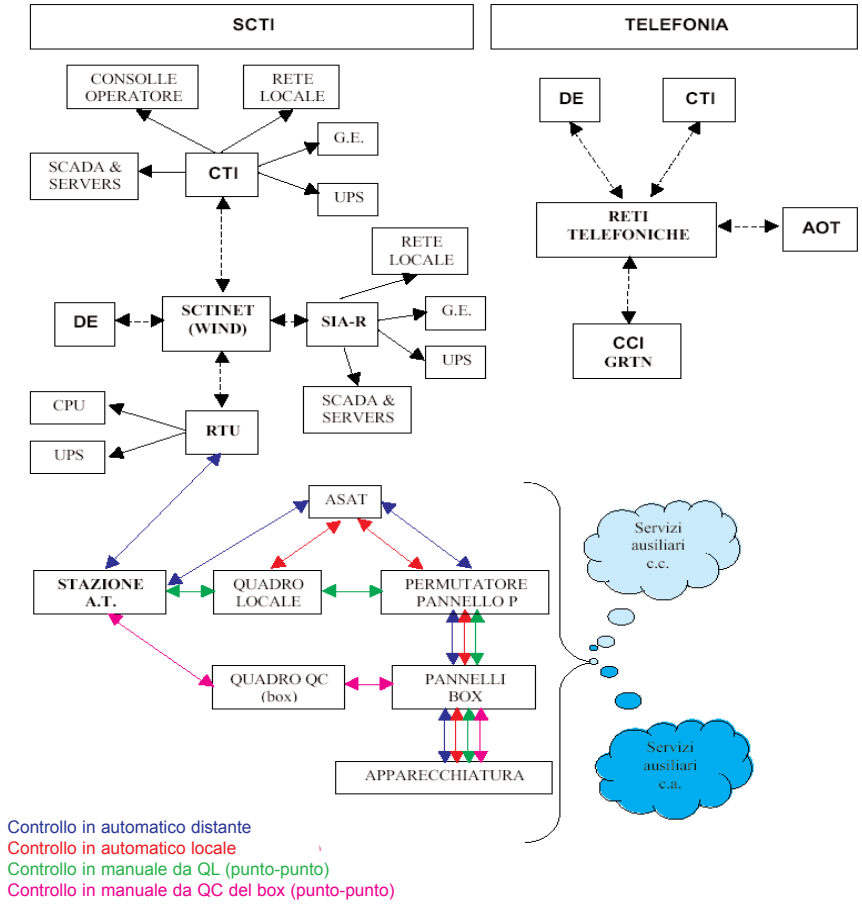


fig.A4. 4 - Parti oggetto di potenziali minacce/vulnerabilità

Nella pratica, è stata realizzata una rappresentazione grafica suddividendo la CII in sezioni elementari, oggetto di possibili eventi critici e tali da generare e/o propagare un'anomalia (*Fig. A4.4*).

Partendo dalla mappa di rappresentazione delle componenti elementari, è stato ricercato ogni evento/scenario potenzialmente sfavorevole, in grado di rappresentare una minaccia/vulnerabilità per il

patrimonio fisico ed umano dell'azienda e/o per le sue capacità organizzative, gestionali e di reddito. Questa fase, che costituisce il momento più critico di tutto il processo di analisi e ne influenza inevitabilmente la qualità dei risultati, è stata attuata con il metodo del problem solving (es. diagramma causa/effetto), a partire dall'individuazione degli eventi critici/scenari e dalla loro associazione all'unità di rischio, fino ad individuare la causa generante l'evento/scenario e l'effetto determinato sul processo.

La *Fig. A4.5* rappresenta schematicamente l'esito della scomposizione successiva in sottosistemi funzionali sempre più elementari, in modo da individuare più agevolmente ed isolare le parti soggette ad eventi potenzialmente dannosi.

Gli eventi critici individuati sono stati classificati secondo "minacce" e "vulnerabilità", in relazione alla loro origine esterna ed interna e descritti nelle loro cause e nelle caratteristiche più rilevanti.

Quanto migliore risulta l'accuratezza e la qualità dell'individuazione degli eventi, tanto più soddisfacenti saranno i risultati: in questa fase è importante non tralasciare nessuna possibile eventualità, poiché un evento rischioso non individuato può lasciare senza difesa, così come è importante pesare correttamente l'impatto di qualsiasi evento, per evitare ad esempio spese improduttive.

L'individuazione delle vulnerabilità richiede analisi approfondite e sostenute da competenze tecniche specialistiche: per ogni evento critico/scenario sfavorevole individuato, deve essere infatti fornita una stima della relativa probabilità di accadimento, ricorrendo a tutti gli elementi informativi disponibili ed evidenziandone l'origine, le fonti ed i criteri utilizzati (dati storici, analisi di affidabilità, dati di progetto, ecc.). Devono essere valutate inoltre le potenziali conseguenze dell'evento ed in particolare i suoi effetti diretti, indiretti e consequenziali sui differenti elementi del processo interessati, trascurando in questa fase gli effetti di eventuali sistemi di difesa già implementati.

Quando possibile, il danno/impatto sulle performance aziendali conseguente all'evento deve essere quantificato in termini economici, in quanto le valutazioni/decisioni aziendali non possono prescindere da un vincolo di economicità; per stimare il danno economico si è fatto ricorso ad una serie di assunzioni, tra cui le ricadute in caso di

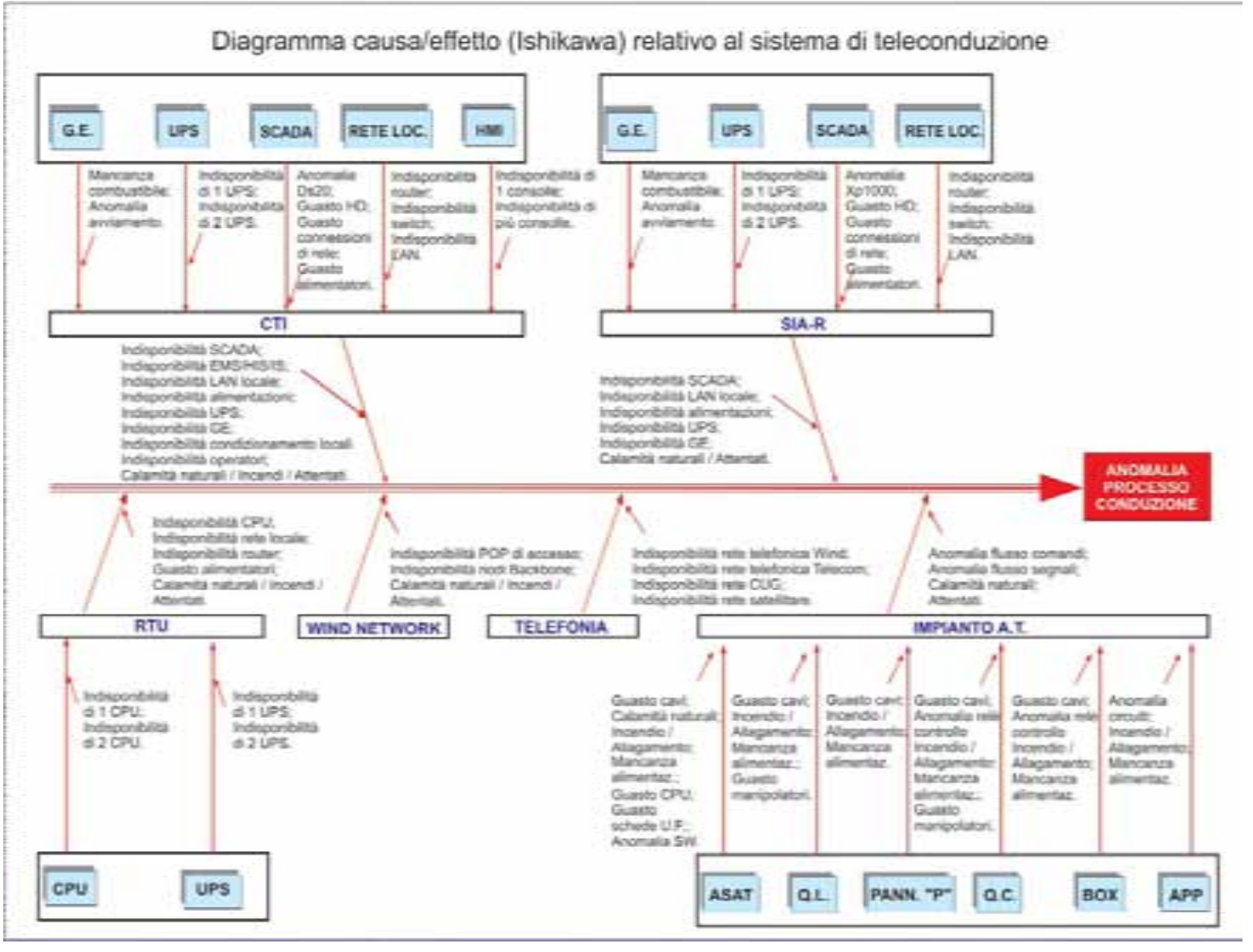


fig. A4.5 - Diagramma causa-effetto (Ishikawa)

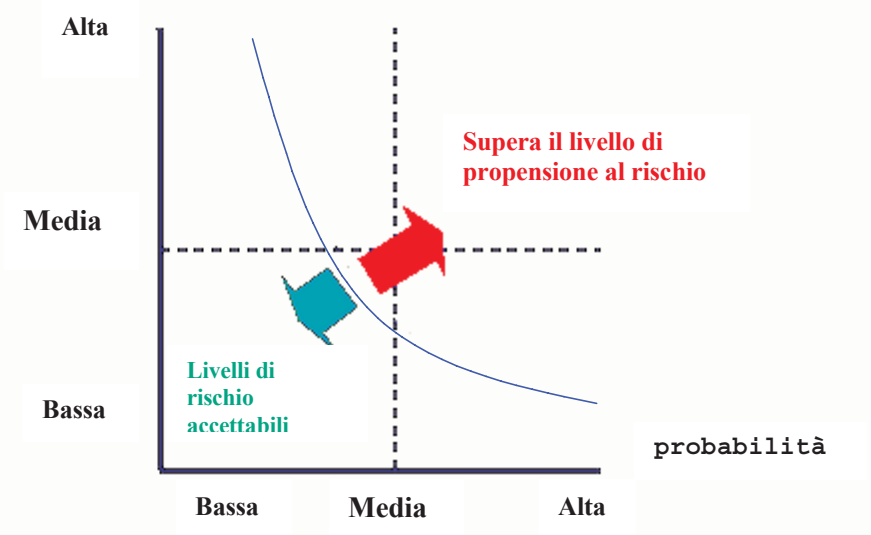


fig. A4.6 - Es. di curva probabilità/impatto

mancato rispetto degli obblighi di esercizio sulla RTN, i costi interni sorgenti, i danni causati a terzi.

Gli eventi critici/scenari, per i quali prevedere sistemi di prevenzione, sono stati individuati in funzione del "Livello di esposizione al rischio potenziale", valutato attraverso il confronto con una curva di accettabilità (genericamente rappresentata in *Fig. A4.6*), mappati successivamente in una Matrice (tabella seguente), dove il livello di esposizione è dato, convenzionalmente, dalla combinazione tra la "probabilità dell'evento" in un tempo ragionevole di osservazione e il valore del "danno", fissate opportunamente le fasce della probabilità e quelle del danno, in coerenza con gli obiettivi e le strategie aziendali.

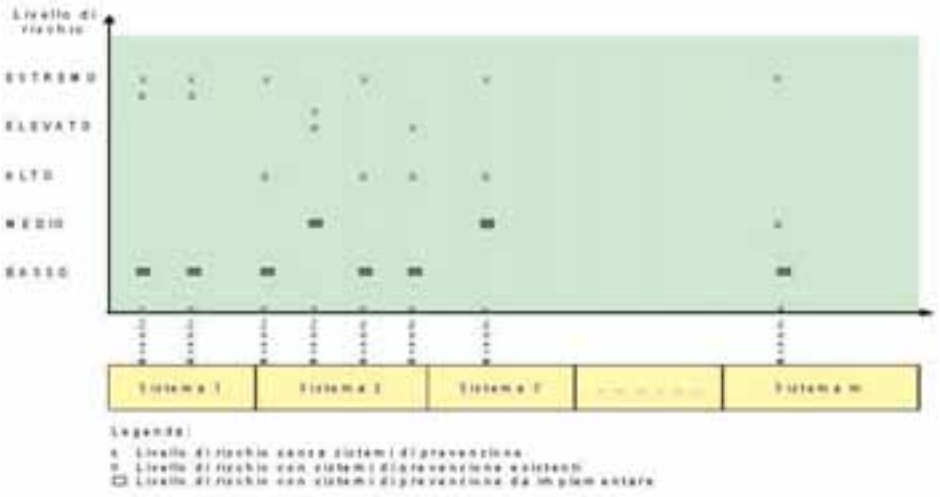
Per il processo in esame l'introduzione di sistemi di prevenzione è stata definita assolutamente necessaria nel caso di livello di esposizione al rischio "estremo" o "elevato", mentre per i casi in cui il livello è risultato "alto" o "medio" si è ritenuto opportuno prevedere, di volta in volta, una valutazione approfondita, con criteri costi/benefici, sulle modalità con cui accettare, ridurre o trasferire altrove il rischio.

Una volta individuati i sistemi di prevenzione necessari per contenere le criticità degli eventi/scenari ritenuti critici, è stata effet-

Valore della probabilità	Valore del danno									
	BASSO		MEDIO		ALTO		ELEVATO		ESTREMO	
NULLA (< 0,1)	BASSO	1	BASSO	1	BASSO	1	BASSO	1	MEDIO	2
BASSA (0,1-0,4)	BASSO	1	MEDIO	2	ALTO	3	ALTO	3	ELEVATO	4
MEDIA (0,4- 0,7)	MEDIO	2	ALTO	3	ELEVATO	4	ELEVATO	4	ESTREMO	5
ALTA (> 0,7)	MEDIO	2	ALTO	3	ELEVATO	4	ESTREMO	5	ESTREMO	5

tuata la valutazione delle criticità degli eventi/scenari tenendo conto dei sistemi di prevenzione individuati (secondo lo schema della tabella successiva): se si individua una riduzione della criticità a livelli accettabili, i sistemi stessi vanno a far parte di un piano di azioni di miglioramento, con relative priorità.

Tale fase è stata effettuata sulla base dell'esperienza di esercizio (eventi verificatisi), degli scenari ipotizzabili, dell'evoluzione del mercato dei sistemi ICT di controllo e di un'approfondita analisi economica (valutazione economica della sicurezza e del costo del rischio, scelta del grado di sicurezza, rapporto costi/benefici delle scelte alternative).



La progettazione del sistema di Business Continuity ha definito, a livello del minimo dettaglio, gli adempimenti procedurali, le figure da coinvolgere nelle diverse attività, le risorse software ed hardware e quanto necessario a tradurre in termini tecnici il complesso coordinato di tutte le azioni di modifica o integrazione dei sistemi di prevenzione.

Le valutazioni hanno principalmente interessato i livelli di affidabilità di apparati, componenti e reti, la stabilità dei sistemi IT, la certificazione dei moduli, l'introduzione di ridondanze in grado di sostenere guasti multipli (es. SCADA in hot stand-by, RTU con doppia CPU, dislocazione di risorse in siti diversificati, vie di comunicazione ridondate e su percorsi fisici alternativi), il potenziamento delle attività di supervisione della CII, l'impiego delle professionalità idonee e l'adeguatezza dei sistemi di prevenzione del rischio logico-informatico.

All'interno di uno specifico "Piano di azione" sono stati definiti i requisiti di fattibilità ed i programmi operativi dei sistemi di prevenzione, in relazione agli obiettivi ed alle responsabilità aziendali e nel rispetto degli adempimenti procedurali (dall'acquisizione delle risorse, alla formazione del personale coinvolto, all'elaborazione di check list dei controlli da effettuare per garantire il buon funzionamento del Sistema di Business Continuity, ecc).

Al termine di una fase omogenea di progettazione e di realizzazione, così come in occasione di eventi inattesi, di opportunità fornite dalle innovazioni o di qualsiasi altro nuovo fenomeno in grado di impattare sul processo, è necessario effettuare sul processo periodiche analisi di feedback che portino alla verifica della tenuta dei sistemi di prevenzione o all'eventuale inserimento di elementi correttivi.

IL SISTEMA DI DISASTER RECOVERY (DR) ED IL PIANO DI EMERGENZA

Un sistema di *Disaster Recovery* ha per obiettivo il ripristino entro un tempo limitato (e/o il mantenimento) delle funzionalità di un processo aziendale di particolare criticità, per fronteggiare gli eventi

critici (minacce, vulnerabilità), attraverso l'utilizzo metodologico, con organizzazione di emergenza e/o di crisi, delle azioni di mitigazione/correzione individuate e realizzate nell'ambito del piano di sviluppo dei sistemi di prevenzione (Sistema BC).

È in sostanza lo strumento organizzativo che consente di gestire il periodo che intercorre dalla dichiarazione dello stato di emergenza/crisi fino al ripristino delle condizioni normali.

Nel caso di Terna, partendo dalle iniziative descritte all'interno del piano di Business Continuity, sono state codificate una serie di procedure per rispondere, sul piano operativo, a qualsiasi condizione o scenario, definendo così il Sistema di Disaster Recovery (DR) del processo primario di conduzione e monitoraggio degli impianti della RTU.

Il sistema di DR utilizza i sistemi di prevenzione realizzati in conformità al piano di Business Continuity, attuando mediante un piano ed una organizzazione di emergenza preposta alla gestione delle singole situazioni di emergenza e/o addirittura crisi.

Si tratta di un piano contenente precise disposizioni, sia tecniche sia procedurali, rese note al personale interessato mediante iniziative mirate, che comporta l'adozione di figure professionali, flussi di comunicazione, attrezzature e tecnologie (quali ad esempio sale di emergenza equipaggiate per la gestione delle fasi di crisi) tutte specificatamente dedicate a fronteggiare situazioni eccezionali che interessano la CII.

Concorrono alla definizione del piano i seguenti elementi:

- individuazione dei sottosistemi interni/esterni che concorrono al funzionamento del sistema di DR
- evidenziazione dei sottosistemi che, in caso di guasto, richiedono il ricorso a sistemi di backup
- determinazione del numero minimo di persone necessarie per erogare il servizio in condizioni di operatività in emergenza
- determinazione del flusso di allarmi e modalità di escalation nel livello delle persone coinvolte fino alla Direzione per la dichiarazione dello stato di emergenza

- definizione delle esigenze di reperibilità delle persone coinvolte nel piano di ripristino
- predisposizione del diagramma delle attività e dei tempi per presidiare i siti di emergenza.

Un evento disastroso, in grado di turbare il normale funzionamento e lo svolgersi ordinario delle attività, impone una specifica organizzazione che, disponendo delle adeguate competenze e delle necessarie deleghe, sia preposta a gestire le complesse problematiche connesse ad una situazione eccezionale: tenendo ovviamente conto della struttura organizzativa preposta al governo della sicurezza aziendale, è necessario delineare un assetto gerarchico funzionale per l'emergenza, ossia individuare gli organi chiamati a dichiarare uno stato di crisi e ad operare in caso di evento disastroso (black-out parziali o totale della rete nazionale, fuori servizio contemporaneo di più centri di controllo per minacce esterne e/o vulnerabilità interna) e definire le rispettive responsabilità e attribuzioni. Durante lo sviluppo di una emergenza/crisi le azioni di comunicazione, coordinamento, di mantenimento rapporti devono essere messe in atto in maniera ordinata, tempestiva e puntuale a partire dall'evento scatenante.

ATTIVITÀ, RUOLI E COMPITI - PIANO DI COMUNICAZIONE/FORMAZIONE

Tutte le azioni che riguardano la BC ed il DR devono essere conosciute ed acquisite da tutti i soggetti coinvolti: nasce dunque l'esigenza di sviluppare e rendere operativi piani mirati di formazione del personale, cioè un percorso formativo continuo e incisivo che assicuri il costante aggiornamento in ambito tecnologico ed in ambito di sviluppo delle capacità comportamentali.

I principali obiettivi della formazione sulla gestione del rischio e l'attuazione dei piani di emergenza sono:

- far maturare la consapevolezza delle minacce che i cambiamenti interni ed esterni all'azienda potrebbero determinare; es. le nuove opportunità create dallo sviluppo tecnologico potreb-

bero portare con sé nuovi rischi da assumere e gestire consapevolmente

- far comprendere i comportamenti e le relative responsabilità operative nell'attività di conduzione della CNI sia nel caso di stato normale del processo, sia nei casi di scenari previsti dalla gestione del rischio tecnico-operativo
- illustrare i processi da attuare nel caso di anomalie/guasti dei principali componenti/sistemi/infrastrutture che supportano il processo oppure, comunque, al manifestarsi di eventi che potrebbero generarne impatti disastrosi
- illustrare le migliori metodologie di monitoraggio e manutenzione dei sistemi interessati nella BC e DR.

La formazione deve essere in ogni caso effettuata ogni qualvolta si proceda ad un aggiornamento delle procedure/istruzioni relative alla gestione del rischio tecnico-operativo e, ovviamente, all'atto delle nuove assunzioni di personale da inserire nelle Unità coinvolte dai Sistemi di BC e DR.

I ruoli e i compiti, i cicli di aggiornamento, i programmi di azione specifici (audit, prove e test dei sistemi, ecc.), i flow-chart operativi, i controlli periodici con le relative check-list e le azioni di miglioramento sono stati tutti riportati in dettaglio in appositi documenti di natura riservata che, in alcuni casi, sono stati vincolati addirittura ad una diffusione ristretta all'interno della azienda.

MANUTENZIONE ED EVOLUZIONE DEI SISTEMI DI BUSINESS CONTINUITY E DISASTER RECOVERY

Fattori quali l'evoluzione tecnologica dei sistemi hardware e software, riferita in particolare al contesto delle tecnologie per il controllo di processo, l'evoluzione organizzativa e logistica dell'azienda, la caduta di attenzione delle persone coinvolte, il cambiamento delle persone che occupano ruoli interessati, possono portare ad una rapida

obsolescenza dei sistemi di BC e DR, che devono pertanto essere soggetti a periodica rivisitazione.

Il mantenimento in uno stato di efficienza tecnico/operativa dei sistemi di BC e DR in esercizio e la sussistenza di eventuali ulteriori fattori di rischio precedentemente non inseriti nel processo di gestione rischi devono essere quindi valutati periodicamente.

In ambito Terna, queste azioni di monitoraggio si concretizzano attraverso l'esecuzione di test ciclici, l'estrazione dai sistemi informatici di tutti gli eventi che hanno un impatto sulla continuità del processo conduzione e monitoraggio impianti, l'*audit* e infine il presidio continuo sulle innovazioni offerte dal mercato.

Allegato 5

Questionario di autovalutazione sui requisiti minimi di sicurezza delle reti

Il presente questionario di autovalutazione è focalizzato sugli aspetti di sicurezza direttamente connessi alle infrastrutture di telecomunicazione, e viene proposto con l'obiettivo di facilitare lo sviluppo di sistemi ed architetture di rete con intrinseche caratteristiche di affidabilità e sicurezza a fronte di eventi accidentali e/o dolosi provenienti dall'interno o dall'esterno dell'Organizzazione cui è indirizzato il questionario.

È possibile che una Organizzazione, in relazione ai vari servizi di cui ha bisogno, si rivolga a Fornitori diversi, ma può anche accadere che richieda l'erogazione di uno stesso servizio a più Fornitori, con lo scopo di garantire il normale funzionamento dei propri sistemi critici anche in caso di interruzione del servizio da parte di uno specifico fornitore. In tale caso il questionario può essere utilizzato anche per avviare un confronto su come diversi Fornitori possono cooperare per minimizzare e mitigare i rischi.

Il presente questionario intende essere di aiuto nella verifica dei requisiti dell'infrastruttura di comunicazione di una Organizzazione e non intende avere carattere di esaustività.

Per un esame più approfondito delle specifiche tematiche relative alla Sicurezza Informatica si fa riferimento alle normative del Ministero per l'Innovazione e le Tecnologie.

A - Infrastrutture

La presente sezione propone considerazioni in merito alle infrastrutture di telecomunicazione impiegate nell'organizzazione, riguardo al fatto che la continuità operativa dipende tipicamente dalla disponibilità di tali infrastrutture.

A1 Disponete di una descrizione completa delle infrastrutture di telecomunicazione critiche per la vostra attività?

A2 Potete qualificare le vostre infrastrutture di telecomunicazione per grado di importanza e/o criticità tra alta/ vitale; media; bassa?

A3 Potete identificare i sistemi critici che sostengono le vostre infrastrutture di telecomunicazione?

A4 Avete una pianificazione di aggiornamento periodico dei sistemi critici che sostengono le vostre infrastrutture di telecomunicazione?

A5 Potete identificare univocamente le varie parti dell'infrastruttura di telecomunicazione utilizzata a sostegno dei vostri sistemi critici?

Dovrebbe essere possibile poter identificare univocamente ogni parte di impianto, circuito o tronco, per esempio mediante l'impiego di una codifica composta da un acronimo breve e/o da un numero di riferimento.

A6 Il sistema di identificazione di cui al punto precedente è condiviso tra la vostra Organizzazione ed il vostro Fornitore?

In caso si renda necessaria un'azione urgente sui sistemi di telecomunicazione, è importante per entrambi utilizzare una stessa nomenclatura.

B - Instradamento di rete (Network routing)

La presente sezione propone considerazioni su come i vostri servizi critici sono connessi alla rete di comunicazione.

B1 Sapete dove e come sono attestate le connessioni tra la vostra rete e la rete del Fornitore?

B2 Siete a conoscenza del percorso fisico che seguono i vostri servizi di rete fuori dalle vostre sedi?

Il cosiddetto "ultimo miglio" è frequentemente il tratto in cui i requisiti qualitativi non sono puntualmente garantiti, per esempio nel caso in cui il Fornitore offre i propri servizi di connessione sino alla centrale telefonica, ma non ha controllo sui servizi forniti nel tratto dalla centrale sino all'utente finale.

B3 Nel caso in cui, al fine di disporre di ridondanze, abbiate optato per due Fornitori che provvedano il medesimo servizio, vi siete assicurati che non sussistano percorsi fisici e/o punti di guasto comuni per entrambi i Fornitori?

C - Dipendenza

La presente sezione propone considerazioni su ulteriori componenti installati sia nella rete propria che in quella del Fornitore e che sono fondamentali per la fornitura dei servizi.

C1 Avete intera visibilità di come all'interno della vostra infrastruttura di rete i vostri servizi di telecomunicazione giungono fino all'interfaccia col Fornitore?

C2 Esistono parti dei collegamenti gestiti da appaltatori esterni e/o fuori dal vostro controllo?

C3 Esistono componenti di terze parti (quali router, modem e apparati di accesso wireless) che possono cadere ai confini fra zone di responsabilità?

C4 Conoscete chi abbia la responsabilità ai fini della integrità di tali collegamenti e componenti ?

D - Diversificazione (Diversity)

La presente sezione propone considerazioni su singoli punti di guasto, per i quali la perdita di uno specifico componente della rete potrebbe avere effetti negativi su molteplici servizi critici.

D1 Tutti i vostri collegamenti lasciano i Centri di Comunicazione nello stesso mezzo fisico (ad es. nello stesso cavo)?

D2 Sono tutti nella stessa canalizzazione?

D3 Nel caso di più Fornitori, condividono il medesimo percorso fisico?

Si dovrebbe considerare anche il caso in cui Centri di Comunicazione differenti utilizzati dalla vostra organizzazione, siano collegati ai medesimi punti all'interno della rete del Fornitore.

E - Separazione

La presente sezione propone considerazioni su come i differenti servizi critici sono indirizzati all'esterno dei locali di proprietà ed attraverso la rete del Fornitore.

E1 Siete a conoscenza se i vostri servizi critici sono indirizzati attraverso distinti componenti della rete in modo che l'eventuale guasto di uno dei componenti non pregiudichi la totalità dei servizi stessi?

E2 Avete avanzato ai vostri fornitori specifiche richieste in merito?

F - Nuovi Servizi

Non sempre il ricorso a due diversi Fornitori costituisce garanzia di separazione. Accade spesso, all'interno dell'industria delle telecomunicazioni, che circuiti di accesso locali (fra la rete ed i Centri di Comunicazione dell'Organizzazione), siano forniti dai terze parti. In questo caso è possibile che tali circuiti, pur offerti da differenti Fornitori, abbiano un percorso comune.

F1 Quando richiedete nuovi servizi al vostro Fornitore, esaminate anche la strutturazione dei vostri attuali servizi per accertarvi che, in merito ai requisiti di separazione o di diversificazione, non siano fatte scelte pericolose?

F2 Effettuate, in questo caso, una nuova verifica dei vostri requisiti al fine di prevenire compromissioni dello stato attuale?

G - Cambiamenti alla struttura della rete

La presente sezione propone considerazioni su come i Fornitori gestiscono i cambiamenti alla infrastruttura delle loro reti.

Non si dovrebbe pensare che la rete dei Fornitori sia statica:

avvengono continui cambiamenti che possono essere provvisori, in quanto dovuti ad un lavoro pianificato, o permanenti nel caso di ristrutturazione della rete, ivi compresa la rimozione di vecchi componenti e l'introduzione di nuovi.

Con il tempo, servizi che erano distinti o separati potrebbero essere interessati da tali cambiamenti, anche se al riguardo è necessario notare che i Fornitori dovrebbero normalmente tenere traccia delle modifiche apportate, per assicurare quanto stabilito da contratto in merito a separazione e diversificazione.

G1 Effettuate con il Fornitore una verifica periodica dei vostri specifici requisiti di resistenza alle minacce e capacità di recupero?

G2 Avete richiesto che venga inviata una precisa notifica dal vostro Fornitore sugli aggiornamenti della rete, sui tempi di indisponibilità per manutenzione o sugli altri cambiamenti rispetto al normale stato ed assetto?

H - Alimentazione elettrica

La mancanza di alimentazione elettrica, sia nei locali di proprietà che all'interno della rete del Fornitore, rappresenta una minaccia significativa alla continuità del servizio di telecomunicazioni. Tale minaccia è ovviamente di intensità proporzionale alla durata della interruzione dell'alimentazione elettrica.

H1 I vostri Centri di Comunicazione sono dotati di gruppi di continuità?

H2 Sono verificati nel funzionamento e manutenuti con regolarità?

H3 Avete visibilità di quanto il vostro Fornitore ha previsto in merito alla sua alimentazione di emergenza e siete consapevoli delle conseguenze che un guasto (anche prolungato) alla sua alimentazione elettrica potrebbe arrecare all'erogazione dei vostri servizi?

I - Contatto in caso di crisi

La presente sezione propone considerazioni sulle modalità di contatto con il/i vostro/i Fornitore/i in caso di un evento con effetti catastrofici sulla rete di telecomunicazioni.

I1 *Avete definito un piano di emergenza ed il relativo gruppo di risposta?*

I2 *Avete concordato i vostri piani d'emergenza con il Fornitore?*

I3 *Avete previsto metodi primari ed alternativi da utilizzare per mettervi in contatto con il vostro Fornitore (per esempio telefono, E-mail)?*

I4 *Il vostro Fornitore dispone di dettagli sui contatti alternativi con il vostro gruppo di emergenza?*

I5 *Quali puntuali aggiornamenti vi aspettate dal vostro Fornitore in caso di incidente?*

I6 *Avete trattato espressamente tale argomento con il Fornitore? Tali aspetti sono stati considerati nel rapporto contrattuale o mediante SLA?*

L - Sicurezza informatica

La presente sezione propone considerazioni su alcuni aspetti di sicurezza IT, al fine di valutare anche questo aspetto nelle problematiche di Infrastrutture Critiche. Possono essere considerati ad es. i seguenti punti, che si riferiscono solamente ad alcuni degli aspetti generali ritenuti di maggiore importanza:

L1 *Esiste un registro con l'inventario dell'hardware/software posseduto?*

L2 *I salvataggi dei dati (backup) vengono eseguiti con frequenza sufficiente a garantire un eventuale rapido e pieno ripristino della funzionalità del sistema?*

L3 *Esiste un piano procedurale per garantire la disponibilità e l'integrità dei dati?*

L4 *Esistono procedure operative e periodiche di test sul ripristino dei dati a fronte di minacce e/o perdite degli stessi?*

L5 *Esiste una ridondanza delle infrastrutture informatiche capace di assicurare la continuità operativa?*

Istituto Superiore
delle Comunicazioni e delle
Tecnologie dell'Informazione

Ministero delle Comunicazioni