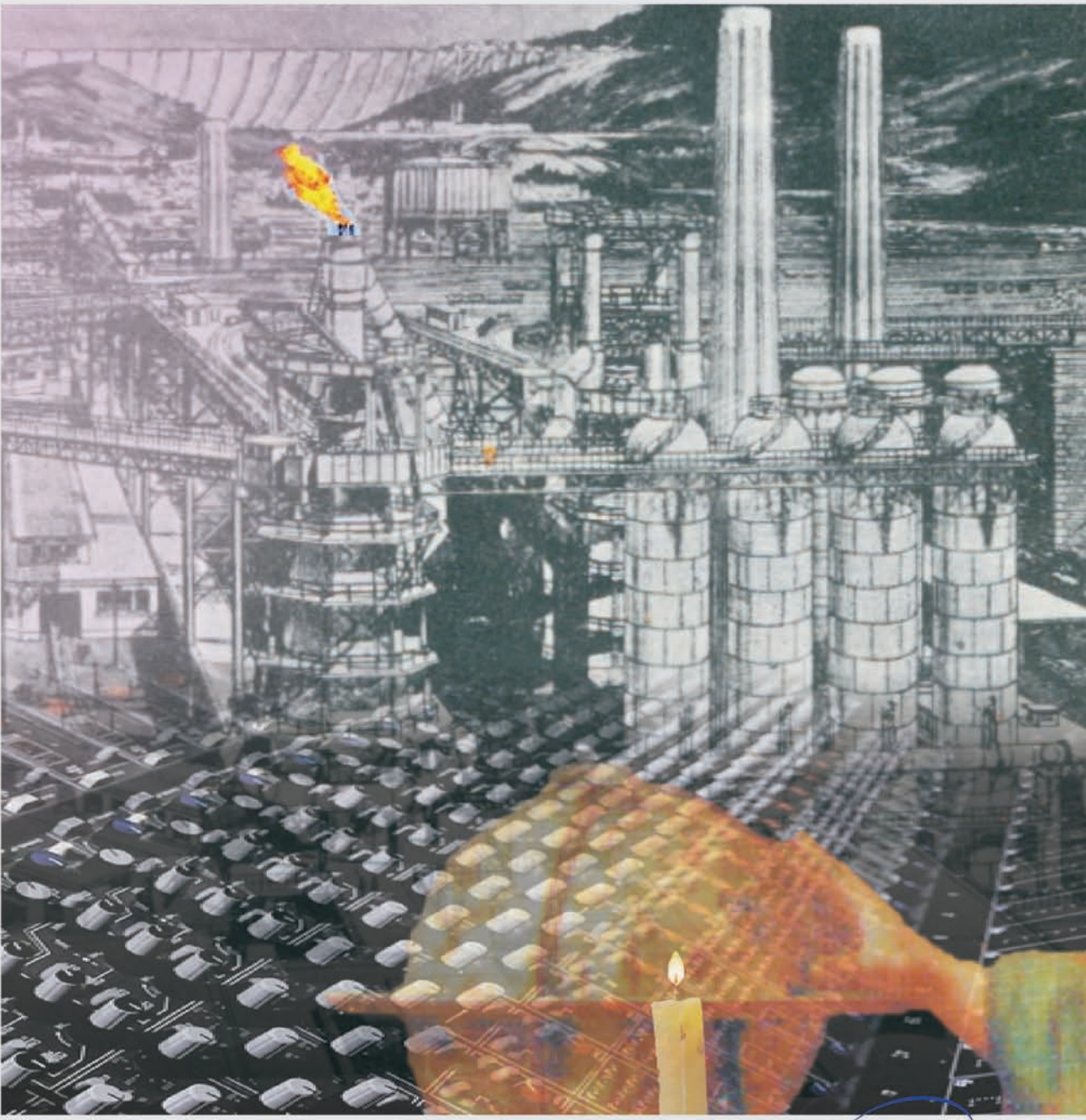
Ministero delle Comunicazioni

ISCOM
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

GESTIONE DELLE EMERGENZE LOCALI



Linee Guida ISCOM

La gestione delle emergenze locali

Il presente documento è stato realizzato da (in ordine alfabetico):

Luigi Carrozzi	AIEA
Annalisa Cocco	Bull, AIEA
Giuseppe Concordia	Ministero Economia e Finanze
Francesca Di Massimo	Microsoft
Luisa Franchina	ISCOM (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)
Matteo Lucchetti	ABI
Mariano Lupo	Ministero Economia e Finanze
Gianluigi Moxedano	Cnipa
Tommaso Palumbo	Ministero dell' Interno
Giuseppe Russo	Sun Microsystems
Federico Sandrucci	C. Amm. (Aus) Consulente Amm.ne Difesa TELEDIFE - SE.PRO TE.C. S.A.S
Enzo Maria Tieghi	Servitecno
Raffaele Visciano	Ministero Economia e Finanze

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.

Indice

Introduzione

La presente pubblicazione si inquadra in una serie di attività svolte dal Ministero delle Comunicazioni nel corso del 2005 e relative alla realizzazione di linee guida su:

- Gestione delle emergenze locali
- Risk analysis approfondimenti
- Qualità del servizio su UMTS
- Qualità dei servizi per le PMI su reti fisse a banda larga
- Certificazione della sicurezza ICT
- Outsourcing della sicurezza ICT

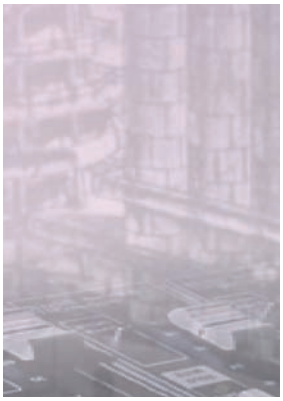
Si coglie volentieri l'occasione per ringraziare quanti hanno, con entusiasmo e professionalità, collaborato alla redazione e alla revisione del presente documento:

Luigi Carrozzi (AIEA), Annalisa Cocco (Bull, AIEA), Giuseppe Concordia (Ministero Economia e Finanze), Francesca Di Massimo (Microsoft), Matteo Lucchetti (ABI), Mariano Lupo (Ministero Economia e Finanze), Gianluigi Moxedano (Cnipa), Tommaso Palumbo (Ministero dell' Interno), Giuseppe Russo (Sun Microsystems), Federico Sandrucci (C. Amm. (Aus) Consulente Amm.ne Difesa - TELEDIFE-SE.PRO TE.C. S.A.S), Enzo Maria Tieghi (Servitecno), Raffaele Visciano (Ministero Economia e Finanze).

Roma, luglio 2006

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

Ing. Luisa Franchina



1 - Le infrastrutture critiche e la Sicurezza Ict

Il termine Infrastrutture Critiche è definito nella sezione 1016(e) dell'USA Patriot Act del 2001 e con esso si intendono quei *"sistemi e beni, sia fisici che virtuali, così vitali alla nazione che un loro malfunzionamento o una loro distruzione produrrebbe un impatto debilitante sulla sicurezza dei cittadini, sulla sicurezza economica della nazione, sulla salute pubblica nazionale e su una qualsiasi combinazione delle precedenti"*. Successivamente agli USA Patriot Act è nato il Dipartimento di Homeland Security degli Stati Uniti avente lo scopo, tra l'altro, di assicurare la protezione delle Infrastrutture Critiche Nazionali.

Anche l'Europa ha emanato un proprio programma di Protezione delle Infrastrutture Critiche nel quale viene fornita la seguente definizione di Infrastruttura Critica.

Una infrastruttura è critica quando una eventuale interruzione o distruzione delle sue risorse fisiche, dei suoi servizi, dei suoi sistemi di information technology, delle sue reti di comunicazione o di qualunque altro suo bene infrastrutturale comporta un serio impatto sulla salute, la sicurezza fisica, sociale ed economica dei cittadini e sulla efficacia di funzionamento dei governi.

Il *green paper* EPCIP (*European program for critical infrastructure protection*), presentato l'11 novembre 2005 dalla Commissione Europea, considera sia Infrastrutture Critiche a livello Europeo che a livello Nazionale. Questo ci consente di traslare questo approccio a livello di nazione Italia considerando sia le principali infrastrutture critiche a carattere nazionale sia le numerose realtà locali o regionali che, per le

loro attività lavorative quotidiane, rivestono un carattere di "criticità" in uno scenario di emergenza più ampio.

La situazione italiana prevede che *"(omissis) l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione assicuri i servizi di protezione informatica delle infrastrutture critiche nazionali individuate con decreto del Ministero dell'Interno"* (L. 31 luglio 2005, n 155). Dunque, l'dentificazione delle Infrastrutture Critiche Nazionali è a carico al Ministero dell'Interno, ma coinvolge comunque l'attiva partecipazione di istituzioni pubbliche e realtà private.

Un sistema di protezione che sia completo deve considerare ogni livello di intervento: fisico, logico, organizzativo. Inoltre, lo stesso sistema di protezione, deve prevedere delle accurate procedure di emergenza da implementare durante una fase di crisi.

Questa linea guida concentra la sua attenzione proprio sulla Gestione delle Emergenze in ambito Information e Communication Technology (ICT) e rappresenta un punto di continuità con il lavoro svolto lo scorso anno, presso l'Istituto Superiore delle Comunicazioni e della Tecnologia dell'Informazione, che ha prodotto diverse Linee Guida sulla Sicurezza delle Reti di Telecomunicazione.

In particolare le due linee guida *"LA SICUREZZA DELLE RETI - Dall'analisi del rischio alle strategie di protezione"* e *"LA SICUREZZA DELLE RETI - Nelle infrastrutture critiche"* hanno fornito gli spunti necessari all'opportuno approfondimento che questa linea guida vuole dare[1].

L'attuale sviluppo delle telecomunicazioni (TLC), nel settore pubblico come in quello privato, è caratterizzato da una sempre più stretta convergenza, interdipendenza ed integrazione tra i servizi tradizionali e servizi che utilizzano tecnologie informatiche (IT), sempre più caratterizzati da sistemi- fisici e logici - via via sempre più innovativi, in un'area definita sempre più dalla cibernetica (cyberspace).

Ciò riguarda anche e soprattutto le Infrastrutture Critiche

[1] *Cfr. paragrafo 3.3 della linea guida "LA SICUREZZA DELLE RETI - Nelle infrastrutture critiche", pag. 133 e seguenti*

Nazionali (NCI), composte da infrastrutture pubbliche e private interessanti settori e servizi critici per il sistema paese, la cui protezione CIP - (Critical Infrastructure Protection) è diventata vitale ed essenziale a causa della loro vulnerabilità agli attacchi, di qualunque natura o provenienza, e del forte impatto che loro guasti, di natura accidentale o dolosa, provocano nell'opinione pubblica o nel contesto socio-economico della nazione. Tra le prime misure di protezione delle NCI vi è la protezione delle infrastrutture TLC ed IT (ICT) CIIP - Critical Information Infrastructure Protection) le quali costituiscono la più importante ed essenziale porzione delle infrastrutture critiche, a qualunque settore appartengano. Salvaguardare tali risorse TLC ed IT significa salvaguardare le stesse infrastrutture critiche e, in sostanza, la sicurezza delle infrastrutture critiche della nazione.

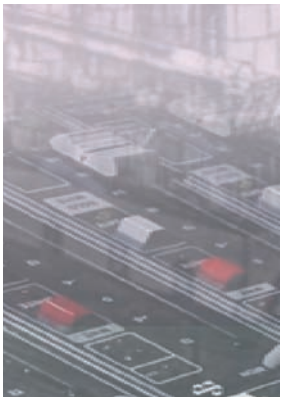
Le minacce alla sicurezza dei sistemi ICT e TLC sono diventate non solo più numerose e disparate ma anche più dannose e dirompenti ed emergono frequentemente nuovi tipi di incidenti.

Le attività di prevenzione, basate sui risultati della valutazione dei rischi, possono diminuire il numero di incidenti, ma gli incidenti non possono essere del tutto evitati.

Solo recentemente ci si è resi conto dell'inefficacia di un approccio totalmente mirato alla protezione in quanto, qualsiasi contromisura, anche la più efficace, non è in grado di garantire una protezione totale. È su questo presupposto che le definizioni più attuali e moderne di Sicurezza Informatica prevedono tre aree:

- Protezione dagli incidenti di sicurezza
- Rilevazione degli incidenti
- Reazione agli incidenti

Un sistema di gestione delle emergenze deve perciò contemplare tutta una serie di misure e procedure atte a implementare ed attuare le tre aree individuate.



2 - La protezione delle infrastrutture critiche e le realtà locali

2.1 LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE NAZIONALI: LA REALTÀ ITALIANA

Il tema dell'individuazione delle infrastrutture critiche informatizzate di un Paese è di grande rilevanza.

Sino allo scorso luglio, l'approccio italiano per la loro individuazione era esclusivamente metodologico, in quanto non esisteva alcuna normativa specifica in materia.

La legge 31 luglio 2005, n. 155, recante: "Misure urgenti per il contrasto del terrorismo internazionale", ha cambiato tutto ciò, in quanto ha inquadrato l'argomento nel contesto della tutela dell'ordine e della sicurezza pubblica, ponendo il focus sulla protezione da attacchi informatici di matrice criminale o terrorista di strutture che gestiscono servizi strategici per il Paese.

L'articolo 7 bis della citata legge ha, infatti, stabilito che sia il Ministro dell'Interno ad individuare con decreto quali siano le infrastrutture critiche informatizzate del Paese.

Lo stesso articolo impone, poi, alle infrastrutture che verranno citate nel decreto, di effettuare "collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate".

Tali collegamenti saranno effettuati con "l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di

telecomunicazione", che il decreto interministeriale del 19 gennaio 1999 ha individuato nel Servizio Polizia Postale e delle Comunicazioni.

Per il conseguimento degli obiettivi prefissati dalla legge, presso il Servizio Polizia Postale e delle Comunicazioni è in fase di realizzazione una struttura operativa dedicata: il CNAIPIC - Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, che avrà sede nei nuovi uffici del Dipartimento, siti in via Tuscolana.

I "…servizi di protezione informatica delle infrastrutture critiche informatizzate…" previsti dalla sopra citata disposizione normativa, verranno assicurati da un Ufficio costituito da risorse di elevato livello tecnologico e personale altamente qualificato che, permanendo nell'alveo delle specialistiche competenze istituzionali di Polizia giudiziaria affidate alla Polizia Postale e delle Comunicazioni è, in via esclusiva, incaricato della prevenzione e repressione dei crimini informatici in danno dei sistemi delle infrastrutture critiche nazionali.

Come tale, in alcun modo si occuperà della gestione diretta della sicurezza ICT delle Infrastrutture critiche, affidata a strutture interne o esterne alle medesime, e tanto meno procederà a controlli di gestione su tali competenze: il valore aggiunto derivante dal CNAIPIC è, infatti, rappresentato dalla realizzazione di una centrale operativa di riferimento, da collegamenti esclusivi e diretti per il trasferimento dati in funzione informativa ed investigativa e dalla predisposizione di procedure condivise ed adeguati strumenti di indagine atti a rendere tempestivo l'intervento - in funzione preventiva, repressiva o correttiva - al verificarsi di attacchi informatici o mere situazioni di pericolo.

Il CNAIPIC costituisce il punto di contatto 24/7 con le infrastrutture critiche collegate e, più in generale, con il mondo esterno.

Inoltre, il CNAIPIC espleta attività di intelligence ai fini della prevenzione dei crimini informatici, anche mediante la predisposizione di rapporti previsionali sull'evoluzione della minaccia e delle tecniche criminali, nonché delle vulnerabilità, che possono riguardare i sistemi gestiti dalle infrastrutture critiche singolarmente. L'attività viene espletata attraverso:

- il costante monitoraggio Internet (con riferimento a specifici

contesti informativi in materia di sicurezza informatica, hacking ed in ambienti ideologicamente caratterizzati);

- la raccolta e l'approfondimento, in chiave comparativa, di tutti i dati e le informazioni, in qualsiasi modo e da qualsiasi fonte, acquisiti dal CNAIPIC.

Di importanza fondamentale è poi l'attività di analisi dei dati relativi ad attacchi conclamati o situazioni anomale che riguardano i sistemi delle infrastrutture critiche e, da queste, segnalati al CNAIPIC tramite collegamenti telematici dedicati, quale immediata risposta operativa di polizia.

Il CNAIPIC, infine, è costantemente in contatto con le articolazioni investigative periferiche della Polizia Postale e delle Comunicazioni e con le forze di polizia di tutto il mondo, specializzate nel contrasto al cyber crime, sia per la raccolta e lo scambio d'informazioni di polizia, sia per le attività investigative.

Le procedure di costituzione della connessione infrastruttura critica informatizzata - CNAIPIC e le successive procedure di comunicazione dei flussi informativi tra le strutture connesse, saranno necessariamente fissate dopo aver proceduto ad un'attenta analisi delle peculiarità di ogni singola infrastruttura, sia riguardo alla topografia della rete ed alla natura degli apparati, ma soprattutto rispetto ai processi generati e rispetto all'importanza di quest'ultimi sulla creazione e la gestione di processi che sono alla base di servizi erogati da altre infrastrutture.

Se la legge dello scorso luglio ha previsto come verranno individuate nel prossimo futuro le infrastrutture critiche informatizzate del Paese, occorre sottolineare che esse non esauriranno l'ampio insieme delle strutture informatiche, la cui compromissione possa mettere in difficoltà, seppur parzialmente o localmente, l'erogazione di servizi strategici.

I criteri per la loro individuazione sono molto difficili da definire, pertanto occorrerebbe favorire un'attività endogena alle strutture aziendali atta a verificare quale sia il livello di impatto dei loro malfunzionamenti a livello nazionale e locale.

In realtà il discorso appare particolarmente importante per

quanto riguarda la valutazione dell'impatto sulle realtà locali, in quanto queste sono spesso soggette alla presenza di peculiarità difficilmente comprese e valutate appieno dagli analisti.

Ma soprattutto esiste un'alta probabilità che realtà aziendali nevralgiche a livello locale siano tentate di non destinare sufficienti risorse finanziarie per la gestione di una sicurezza informatica che superi, nell'ottica della sicurezza del Paese, la classica valutazione dell'analisi dei rischi strettamente ancorati alla visione dell'impatto sulla propria struttura.

Tali tematiche devono necessariamente essere affrontate con un approccio multidisciplinare, che tenga conto delle specificità locali, da parte di tutti gli organi interessati.

2.2. INFRASTRUTTURE CRITICHE: UNA SFIDA PER LE REALTÀ LOCALI E REGIONALI

Allo stesso modo in cui le grandi realtà nazionali rientrano in un più vasto schema di protezione, in quanto infrastrutture critiche nazionali, è altresì necessario che le aziende e le organizzazioni che operano a livello locale e regionale siano in grado di comprendere e di valutare quanto la loro attività quotidiana sia caratterizzata da un determinato livello di criticità. Non di rado realtà locali o regionali cooperano e collaborano ad attività nelle quali sono coinvolte organizzazioni nazionali. Ancora più spesso le infrastrutture informatiche e comunicative delle realtà locali e nazionali sono interdipendenti in termini operativi, logici e geografici. Queste considerazioni e le altre che troveremo all'interno di questa guida ci spingono ad inserire le realtà locali tra i destinatari fondamentali di questa linea guida per la gestione delle emergenze. Perciò la necessità di un accurato sistema per la gestione delle emergenze va esteso soprattutto alle realtà locali, forse più piccole ma non per questo meno critiche, onde poter minimizzare l'effetto domino, che estenderebbe l'ambito di una crisi a livello locale allargandola alle infrastrutture critiche nazionali.

È necessario promuovere una crescita della consapevolezza, peraltro già in atto dopo i fatti del 11 settembre 2001, nelle realtà che

operano su territorio locale. Per questo nel seguito di questo paragrafo si vuole fornire una sorta di self assessment minimale per realtà piccole e locali utile alle stesse per una forma di auto-valutazione circa la criticità delle loro attività quotidiane. Il self-assessment è posto sotto forma di mini questionario.

Q1. La tipologia di attività svolta dalla realtà locale rientra in uno dei settori classici di infrastrutture critiche quali: agricoltura e alimentazione, acque potabili, banca e finanza, difesa, energia, industria chimica e materiale pericoloso, protezione civile, servizi postali e spedizioni, salute, telecomunicazioni, trasporti?

Q2. Sono state identificati i beni (politiche, procedure, processi, sistemi, reti, applicazioni, dati, ecc.) che la realtà locale utilizza?

Q3. Quale è l'impatto di una perdita dei beni identificati alla domanda Q2?

Q4. Sono state identificate e caratterizzate le minacce a cui sono soggetti i beni al punto Q2?

Q5. Sono state identificate e analizzate le vulnerabilità cui sono soggetti i beni al punto Q2?

Q6. Conosco perfettamente quali sono le interdipendenze operative, logiche e geografiche con realtà critiche nazionali?

Q7. È stata effettuata una attività di Risk Analisys e di Business Impact Analisys per comprendere i rischi e determinare le priorità?

Q9. Sono state identificate opportune contromisure che tengano conto dei costi-benefici?

Q10. Una qualunque emergenza a livello locale quanto può avere un impatto ed un effetto domino sulle infrastrutture più grandi o nazionali con le quali sono in interdipendenza?

A titolo di esempio, una realtà locale che abbia una propria attività legata al mondo delle forniture elettriche e che voglia identificare il proprio livello di criticità, rispetto alle domande precedenti può ulteriormente chiedersi:

Se uno dei beni (o servizi) della domanda Q2 è stato seriamente interrotto o distrutto esiste un elevato potenziale di rischio che:

- si produca un effetto catastrofico
- ci sia una mancata fornitura di energia alle infrastrutture di servizio nazionale
- il livello di interdipendenza coinvolga altri settori considerati critici nella domanda Q1
- ci sia una mancata fornitura di energia a vaste aree urbane
- ci sia un effetto domino con i partner ed i fornitori dei servizi erogati dalla mia realtà
- siano possibili severi impatti ambientali
- siano possibili immediati e significativi impatti sulla comunità locale
- sia possibile che il tempo necessario al ripristino delle condizioni normali vada oltre il dovuto
- le capacità dei generatori di servizio ausiliari non siano disponibili o insufficienti?

Una riflessione accurata sulle precedenti, peraltro semplici, domande fa apparire chiara la necessità, per tutte quelle realtà minori o locali che congiuntamente alle infrastrutture critiche nazionali formano il tessuto connettivo e produttivo del sistema paese, di una accurata progettazione del sistema di gestione delle emergenze. L'intero sistema di gestione delle emergenze consentirà di minimizzare l'impatto di incidenti che possono accadere su quel sistema di sistemi connesso e alimentato dai sistemi ICT.

3 - Essere preparati a gestire le emergenze

3.1. DEFINIZIONI

3.1.1 Una definizione di incidente e di crisi

Nel momento in cui un'organizzazione decide di costruire un sistema di gestione delle emergenze, il primo aspetto che deve prendere in considerazione è quello definitorio. Le definizioni inerenti la gestione delle emergenze sono molto legate al settore di attività ed ai servizi erogati dall'organizzazione, ma in generale la situazione di emergenza è collegata all'indisponibilità temporanea/permanente o al malfunzionamento di risorse "critiche" che possono essere infrastrutturali e/o umane.

La definizione di emergenza è fortemente legata alla classificazione che viene fatta dell'evento o "incidente", in quanto si può trattare di una situazione di semplice "problema", che può non rientrare nel processo di gestione delle emergenze, fino al livello di criticità molto alta o "crisi" o "disastro" che invece richiede l'innesco di piani di azione mirati.

Ad esempio, dopo i tragici accadimenti dell'11 settembre 2001 è stata riconosciuta la vulnerabilità del sistema finanziario e sono state avviate diverse iniziative a livello internazionale (Financial Stability Forum) rivolte a definire principi comuni per garantire la continuità dei sistemi finanziari. A livello nazionale la Banca d'Italia ha condotto

diverse attività tra le quali quella di coordinamento, con Consob, di un Gruppo di lavoro che ha portato, tra i vari risultati, all'individuazione dei servizi critici di sistema e degli scenari di rischio da presidiare. La Banca d'Italia ha quindi definito ad esempio i seguenti scenari di crisi:

- distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche;
- indisponibilità di personale essenziale per il funzionamento dell'azienda;
- interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari);
- alterazione dei dati o indisponibilità dei sistemi a seguito di attacchi perpetrati dall'esterno attraverso reti telematiche;
- danneggiamenti gravi provocati da dipendenti.

Se si circoscrive l'attenzione alla sicurezza ICT, a livello nazionale ed internazionale si definisce incidente di sicurezza ICT *"la violazione o l'imminente minaccia di violazione della politica di sicurezza ICT o delle prassi di sicurezza standard"* (cfr. CERT Governativo italiano e NIST).

Viceversa, se si allarga il tema alla sicurezza nazionale, l'Homeland Security nel National Response Plan definisce, ad esempio, come "incidente" un evento che richiede una risposta di emergenza per proteggere la vita o la proprietà *("An occurrence or event, natural or human caused, that requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response").*

Rimanendo in tema di ICT, a seguito di quanto detto, è possibile definire diversi scenari di emergenze in funzione del tipo di servizio, in quanto l'interruzione di un servizio ICT per un periodo più o meno lungo può rappresentare un evento più o meno grave a seconda del servizio erogato mediante i sistemi ICT interessati. Come sarà dettagliato nel seguito, la definizione e la classificazione di un evento sono

legate alla tipologia ed al livello di gravità dell'impatto conseguente al verificarsi dell'evento ed alla valutazione dei rischi associati.

3.1.2. Classificazione degli incidenti secondo il livello di impatto

Qualsiasi attività di protezione non può prescindere dall'evidenziare in via preliminare quali sono le informazioni critiche per l'organizzazione e successivamente quantificare il loro valore ai fini della continuità e qualità del processo produttivo.

Ormai la totalità delle organizzazioni operanti sul mercato, indipendentemente dalle dimensioni dal settore industriale di appartenenza, hanno i loro processi critici largamente *'information based',* dipendenti cioè da qualche contenuto informativo trattato con strumenti ICT.

Una violazione dell'integrità, della disponibilità e della riservatezza delle informazioni può avere conseguenze di varia intensità in relazione alla criticità che tali informazioni assumono nel ciclo produttivo ed al contesto di rischio in cui l'organizzazione opera.

Gli impatti degli incidenti di sicurezza delle informazioni hanno diversa natura e specificità che ne consentono classificazioni articolate.

L'organizzazione può subire impatti diversificati a seguito di incidenti di sicurezza in termini di una limitazione o alterazione nella capacità di governo del sistema produttivo, con conseguenze anche sulla sicurezza fisica di persone (pensiamo ad es. all'impossibilità di evadere ordini di consegna merce, all'incapacità di un sistema di telecontrollo di evidenziare anomalie di funzionamento di un impianto industriale), la perdita di competitività a seguito di divulgazione di segreti industriali, la perdita di immagine e di reputazione sul mercato, l'incorrere in violazioni di leggi, norme, regolamenti, etc.

Ne consegue che il processo preventivo di classificazione delle informazioni e dei *related information assets* cioè di tutti i sistemi ICT (e non) deputati al trattamento di tali informazioni è un passo fondamentale per una corretta valutazione degli incidenti di sicurezza.

La figura seguente riporta una classificazione del valore degli information assets.

Valore dell'Information Asset		Descrizione
1	**Molto Basso**	Information Asset la cui perdita, distruzione o alterazione non ha impatto economico o al più lo è in misura molto ridotta.
2	**Basso**	Information Asset di Bassa rilevanza. Nel caso di distruzione o alterazione l'impatto economico è marginale.
3	**Medio**	Information Asset importanti. Nel caso di perdita, distruzione o alterazione possono essere rimpiazzati al fine di non incorrere in gravi perdite.
4	**Alto**	Information Asset di alto valore per i processi di business. La loro perdita, distruzione o alterazione può avere conseguenze molto rilevanti sulla capacità produttiva dell'organizzazione.
5	**Altissimo**	Information Asset di estremo valore per l'organizzazione. La loro perdita, distruzione o alterazione, può avere conseguenze sulla sopravvivenza stessa dell'organizzazione.

Figura 1 - Classificazione del valore degli information assets

Classificazione della gravità degli incidenti

Al riguardo, la Commissione europea, oltre al livello di gravità *("severity")* dell'impatto introduce due ulteriori dimensioni di analisi: l'estensione *("scope")* dell'incidente e la durata temporale dell'effetto *("Effects of time")*. La seguente definizione di impatto, fornita dalla Commissione, lega infatti quest'ultimo alla somma dei differenti effetti di un incidente misurati in termini quantitativi e qualitativi:

Impacts are the total sum of the different effects of an incident. This needs to take into account at least the following qualitative and quantitative effects:

- Scope - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, regional or local.

- Severity - The degree of the loss can be assessed as None, Minimal, Moderate or Major.
- Among the criteria which can be used to assess impact are:
  - Public (number of population affected, loss of life, medical illness, serious injury, evacuation);
  - Economic (GDP effect, significance of economic loss and/or degradation of products or services, interruption of transport or energy services, water or food shortages);
  - Environment (effect on the public and surrounding location);
  - Interdependency (between other critical infrastructure elements).
  - Political effects (confidence in the ability of government);
  - Psychological effects (may escalate otherwise minor events).

both during and after the incident and at different spatial levels (e.g. local, regional, national and international)

- Effects of time - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

La seguente tabella, tratta da *'FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems'*, del NIST identifica tre livelli di potenziale impatto sull'organizzazione e sugli individui rispetto alle tre categorie di violazioni della sicurezza e cioè riservatezza, integrità e disponibilità.

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

Vediamo più nel dettaglio l'articolazione di tale classificazione.

Il potenziale impatto è dichiarato **LOW** se:

*- The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. (Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law)*

AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality,integrity, or availability might:

(i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;

(ii) result in minor damage to organizational assets;

(iii) result in minor financial loss; or

(iv) result in minor harm to individuals.

Il potenziale impatto è dichiarato **MODERATE** se

- *The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.*

AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality,integrity, or availability might:

(i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;

(ii) result in significant damage to organizational assets;

(iii) result in significant financial loss; or

(iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

L'impatto potenziale è dichiarato **HIGH** se:

- *The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.*

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

(ii) result in major damage to organizational assets;

(iii) result in major financial loss; or

(iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

È possibile (cfr. figura 2) suddividere ulteriormente il livello di gravità dell'impatto in cinque diversi livelli:

1. irrilevante
2. lieve
3. importante
4. molto grave
5. catastrofico.

LIVELLI DI GRAVITÀ	1	2	3	4	5
	IRRILEVANTE	LIEVE	IMPORTANTE	MOLTO GRAVE	CATASTROFICO
DESCRIZIONE IMPATTO	Incidente che provoca un disturbo ma senza conseguenze nei confronti della clientela e della produzione di beni/servizi .Non ha impatti di ordine economico.	Incidente con impatto di entità minore. Può creare disagi alla clientela e comunque di impatto economico contenuto	Incidente di Impatto rilevanteHa conseguenze sul Business condotto e perdite economiche non trascurabili	Incidente con conseguenze molto rilevanti. Provoca ingenti danni economici con rilevanti conseguenze sulla capacità produttiva dell'organizzazione nel breve e medio termine.	Incidente che reca un danno di elevatissima entità economica. Si accompagna ad una sostanziale completa distruzione dei mezzi di produzione. dell'organizzazione. Il recupero, se possibile, è attuabile solo nel lungo termine e a fronte di ingenti investimenti

Figura 2 - Classificazione della gravità degli incidenti

3.1.3 Cosa si intende per "disastro"

Nel momento in cui un'organizzazione si appresta a definire una classificazione di un evento in relazione all'impatto, risulta spesso difficile definire i confini tra una classe ed un'altra e soprattutto definire il contesto nel quale l'impatto è tale da dover parlare di disastro. Le classificazioni descritte nei paragrafi precedenti ci riportano a definire "disastro" un evento il cui l'impatto è classificato come alto o catastrofico (gli aggettivi utilizzati a livello internazionale sono: high, severe, fatal, cathastrophic).

Il *Disaster Recovery Journal* americano fornisce, ad esempio, la seguente interessante definizione di Disastro:

A sudden, unplanned calamitous event causing great damage or loss as defined or determined by a risk assessment and Business Impact Analysis; 1) Any event that creates an inability on an organizations part to provide critical business functions for some predetermined period of time. 2) In the business environment, any event that creates an inability on an organization's part to provide the critical business functions for some predetermined period of time. 3) The period when company management decides to divert from normal production responses and exercises its disaster recovery plan. Typically signifies the beginning of a move from a primary to an alternate location.

Parallelamente con "Disaster Recovery" si fa riferimento alle attività ed ai piani definiti per ripristinare i servizi critici dell'organizzazione ad uno stato accettabile. I requisiti di ripristino e quindi i livelli minimi di tolleranza al disastro sono definiti dall'Unità di Business responsabile dei servizi critici e sono comunemente sintetizzati nei seguenti due parametri:

- **Recovery Point Objective (RPO)**, che indica la massima perdita di dati accettabile per un'applicazione informatica espressa in ore/minuti precedenti l'interruzione di servizio (la definizione del Disaster Recovery Journal è "*The point in time to which systems and data must be recovered after an outage as determined by the business unit*")
- **Recovery Time Objective (RTO)**, che indica la massima durata accettabile di interruzione del servizio e quindi il tempo massimo entro il quale i sistemi, le applicazioni o le funzioni

devono essere ripristinati (la definizione del Disaster Recovery Journal è "*The period of time within which systems, applications, or functions must be recovered after an outage -e.g. one business day. RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. Similar Terms: Maximum Allowable Downtime*").

Se, ad esempio, un'applicazione finanziaria ha un RPO=2 ore ed un RTO=6 ore significa che, dopo un disastro, l'organizzazione (in base a quanto dichiarato dalla Business Unit responsabile dell'applicazione) può tollerare al massimo (caso peggiore) un tempo di fermo dell'applicazione pari a 6 ore (dopo il disastro) e quindi l'applicazione, al più tardi dopo 6 ore, deve essere ripristinata con una base dati non più vecchia di 2 ore precedenti il disastro. Questo si traduce in pratica nell'aver definito una strategia di disaster recovery che consente di:

- mantenere in un sito alternativo (scelto in modo da non essere interessato dallo stesso disastro) una copia dei dati di esercizio allineata ogni 2 ore;
- disporre nel sito alternativo di sistemi tali da poter far ripartire l'applicazione entro le 6 ore dopo il disastro.

La posizione del sito alternativo (e quindi la distanza tra questo sito e quello di esercizio) dipende dalla tipologia di eventi disastrosi dai quali un'azienda si vuole proteggere (calamità naturali, danneggiamenti/interruzioni di reti di telecomunicazione o di energia, attacchi terroristici, ecc.).

La figura seguente, tratta dal "Federal Legislative and Regulatory Business Continuity Requirements for the IRS-Internal Revenue Service" emesso dal MITRE (Center for Enterprise Modernization) nel febbraio 2003, rappresenta i requisiti di RTO ed RPO in relazione alle attività da effettuare sui due siti.

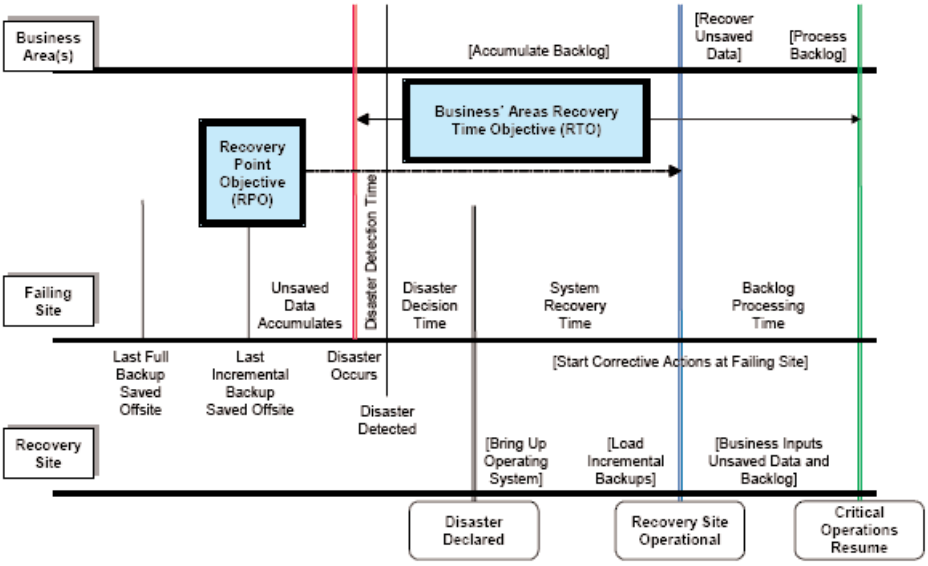


Figura 3 - Business Recovery Terminology and Timelines (fonte: MITRE, 2003)

3.1.4 Cosa si intende per "continuità operativa"

L'obiettivo finale di un'organizzazione è di ridurre al minimo gli effetti di un disastro o di un incidente e di garantire la continuità operativa. Al riguardo, sempre il Disaster Recovery Journal, definisce come continuità operativa ("business continuity") "*The ability of an organization to ensure continuity of service and support for its customers and to maintain its viability before after and during an event*".

Nel momento in cui un'applicazione ha un RTO ed un RPO prossimi allo zero generalmente si parla di "Business Continuity" ovvero di "continuità operativa".

A titolo esemplificativo, la Banca d'Italia, sempre con l'obiettivo di definire principi comuni per garantire la continuità dei sistemi finanziari, ha introdotto le seguenti definizioni circa la gestione della continuità operativa:

- La gestione della continuità operativa comprende tutte le iniziative volte a ridurre a un livello ritenuto accettabile i danni conseguenti a incidenti e catastrofi che colpiscono direttamente o indirettamente un'azienda.
- Il piano di continuità operativa, anche denominato piano di emergenza, è il documento che formalizza i principi, fissa gli obiettivi e descrive le procedure per la gestione della continuità operativa dei processi aziendali critici.
- Il piano di disaster recovery stabilisce le misure tecniche e organizzative per fronteggiare eventi che provochino la indisponibilità dei centri di elaborazione dati. Il piano, finalizzato a consentire il funzionamento delle procedure informatiche rilevanti in siti alternativi a quelli di produzione, costituisce parte integrante del piano di continuità operativa.

D'altra parte, come sarà articolato nel seguito, la definizione di tipologie di eventi/emergenze porta con se la definizione di diverse tipologie di piani di azione. Al riguardo, il NIST (National Institute of Standard Technology, U.S.) nel formulare le raccomandazioni per definire un Piano di Gestione delle Emergenze per i sistemi IT (si veda il documento "Contingency Planning Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology" pubblicato nel 2002) pone l'accento su come la Gestione delle Emergenze sottende un insieme di attività che hanno impatto su tipologie diverse di risorse (umane, fisiche ed informatiche) e per questo sono predisposti diversi Piani di azione che differiscono per obiettivi e focus:

- *Business Continuity Plan (B*CP), focalizzato sulla continuità delle funzioni di business di un'organizzazione durante e dopo un disastro.
- *Business Recovery Plan (BRP)*, focalizzato sul ripristino delle funzioni di business dopo un disastro, a differenza del BCP manca delle procedure per garantire la continuità dei processi critici durante un'emergenza o un disastro.
- *Continuity of Support Plan/IT Contingency Plan (COOP)*, focaliz-

zato sul ripristino in un sito alternativo delle funzioni essenziali di un'organizzazione (generalmente il quartier generale) per un periodo limitato fino al ripristino delle condizioni normali.

- *Continuity of Support Plan/IT Contingency Plan*, focalizzato sulla continuità dei sistemi di supporto e delle principali applicazioni (generalmente sono prodotti più piani, uno per ogni applicazione, da manutenere nell'ambito del BCP dell'organizzazione).
- *Crisis Communications Plan*, focalizzato sulle procedure di comunicazione verso l'interno e verso l'esterno. A crisis communications plan is often developed by the organization responsible for public outreach.
- *Cyber Incident Response Plan*, focalizzato sulle procedure per contrastare gli attacchi informatici contro i sistemi IT di un'organizzazione.
- *Disaster Recovery Plan (DRP)*, focalizzato sui principali, generalmente disastrosi, eventi che impediscono il normale accesso alle infrastrutture per un periodo prolungato e si riferisce alle procedure per ripristinare, sistemi e applicazioni in un sito alternativo dopo un'emergenza (generalmente include l'IT Contingency Plan)
- *Occupant Emergency Plan (OEP)*, focalizzato sulle procedure di gestione degli occupanti le infrastrutture in caso di situazione pericolosa (incendi, uragani, ecc.) per la salute e la sicurezza del personale e dell'ambiente.

La figura 4 riporta la descrizione del NIST circa gli obiettivi e l'ambito dei diversi Piani tra loro correlati.

Nell'ambito delle iniziative avviate per definire il Programma Europeo per la protezione delle Infrastrutture Critiche, la Commissione Europea (si veda il Green Paper "On a European Programme For Critical Infrastructure Protection" del 17.11.2005) ha introdotto la seguente definizione di Piano di Emergenza (Contingency Plan) che lega il Piano alle attività necessarie per rispondere a guasti o distruzioni di servizi essenziali:

"*A plan used by a Member State and critical infrastructure owner/operator on how to respond to a specific systems failure or disruption of essential service. Contingency plans would typically include the development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental and public-assistance programs to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration as well as development of initiatives to mitigate the effects of future incidents.*"

Plan	Purpose	Scope
Business Continuity Plan (BCP)	Provide procedures for sustaining essential business operations while recovering from a significant disruption	Addresses business processes; IT addressed based only on its support for business process
Business Recovery (or Resumption) Plan (BRP)	Provide procedures for recovering business operations immediately following a disaster	Addresses business processes; not IT-focused; IT addressed based only on its support for business process
Continuity of Operations Plan (COOP)	Provide procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days	Addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT-focused
Continuity of Support Plan/IT Contingency Plan	Provide procedures and capabilities for recovering a major application or general support system	Same as IT contingency plan; addresses IT system disruptions; not business process focused
Crisis Communications Plan	Provides procedures for disseminating status reports to personnel and the public	Addresses communications with personnel and the public; not IT focused
Cyber Incident Response Plan	Provide strategies to detect, respond to, and limit consequences of malicious cyber incident	Focuses on information security responses to incidents affecting systems and/or networks
Disaster Recovery Plan (DRP)	Provide detailed procedures to facilitate recovery of capabilities at an alternate site	Often IT-focused; limited to major disruptions with long-term effects
Occupant Emergency Plan (OEP)	Provide coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility; not business process or IT system functionality based

Figura 4 - Piani legati alla Gestione delle Emergenze (fonte: NIST, 2002)

3.2 COME COSTRUIRE E MANTENERE UN SISTEMA DI GESTIONE DELLE EMERGENZE

La gestione delle emergenze è un processo strategico per ogni organizzazione e per garantirne l'efficacia è necessario che sia integrato con tutto il ciclo di vita di sviluppo di un sistema ICT (SDC - *System Development Life Cycle*). Al riguardo, l'utilizzo di linee guida e standard riconosciuti a livello internazionale è fondamentale per avere un alto livello di garanzia che tutti gli aspetti siano presi in considerazione e strettamente collegati con i requisiti di business (tra i quali quello di continuità del servizio).

In particolare, la metodologia COBIT - *Control Objectives for Information and related Technology*, sviluppata dall'ISACA- *Information Systems Audit and Control Association* e dall'IT Governance Institute e quella proposta dal NIST - *National Institute of Standards and Technology* rappresentano sicuramente una linea guida importante.

In entrambi i casi, il modello di gestione si basa sull'approccio conosciuto come PDCA (*Plan, Do Check, Act*), caratterizzato dal miglioramento continuo e dalla visione per processi (propri anche dello standard ISO/IEC 27001:2005) e sulla garanzia di allineamento con i requisiti di business.

Il concetto che la metodologia COBIT propone è che affinché gli *obiettivi di business* siano soddisfatti, il Management deve istituire un sistema di controllo interno o *framework* e deve pensare al controllo nell'IT guardando alle *informazioni* che sono necessarie per gestire i *processi aziendali*, e guardando all'informazione come al risultato di una combinata applicazione di risorse correlate alla tecnologia informatica che devono essere gestite con processi propri dell'IT. In questo modo si crea un link fondamentale tra i requisiti di business e di IT governance, tra i processi IT (articolati in attività e raggruppati in domini) e le risorse (persone, infrastrutture, informazioni, applicazioni).

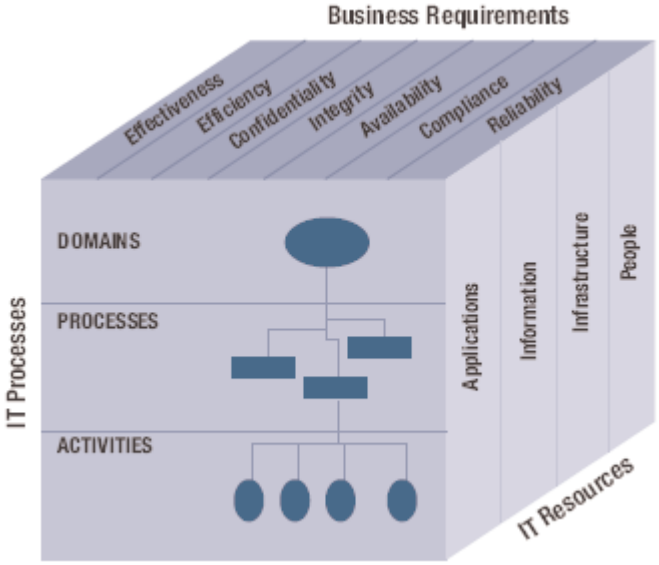


Figura 5 - Il modello COBIT (fonte: COBIT v4.0, © 2005 IT Governance Institute)

Tale approccio è utile nel momento in cui ci si trovi a dover definire un *framework* di gestione delle emergenze che investe trasversalmente l'organizzazione e tutto il ciclo di vita dei sistemi. In ognuna delle quattro fasi del ciclo di vita di un sistema ("Pianificazione e Organizzazione", "Acquisizione e Realizzazione", "Erogazione e Supporto" e "Monitoraggio e Valutazione") il COBIT propone sia obiettivi di controllo da attuare per garantire l'efficacia della gestione delle emergenze, sia una metrica per misurarne il raggiungimento. A titolo esemplificativo, nella figura 4 sono riportati i principali obiettivi di controllo, estratti dal COBIT ed applicabili alla Gestione delle Emergenze che sono trasversali al SDC e riguardano:

- Valutazione e gestione dei rischi,
- Gestione dei cambiamenti,
- Garanzia della continuità del servizio,
- Valutazione e controllo delle prestazioni.

In particolare, già a livello di pianificazione ed organizzazione, è necessario definire, formalizzare e condividere un *framework* per la valutazione e la gestione dei rischi dei sistemi IT ed integrarlo con il più ampio *framework* di gestione di rischi di business, mentre nella fase di erogazione e supporto è necessario sviluppare, mantenere e testare gli "IT Continuity Plans". Su questo ultimo aspetto, gli obiettivi di controllo da soddisfare sono i seguenti:

- sviluppare un *IT Continuity Framework*;
- sviluppare gli *IT Continuity Plans*;
- individuare le risorse IT critiche e definire le priorità per il ripristino;
- manutenere l'*IT Continuity Plan*, affinché sia in linea con l'evoluzione dei requisiti di business, dei processi e delle architetture;
- effettuare prove periodiche dell'*IT Continuity Plan*;
- effettuare sessioni periodiche di addestramento del personale sull'*IT Continuity Plan*;
- definire una strategia per distribuire l'*IT Continuity Plan* affinché sia distribuito in maniera sicura e disponibile a tutto il personale autorizzato;
- definire un piano d'azione per gestire il recupero ed il ripristino dei servizi IT;
- garantire la disponibilità e la gestione di uno storage di back-up in un altro sito con le risorse necessarie per il recupero ed il ripristino dei servizi IT;
- effettuare, a valle del ripristino, una valutazione dell'adeguatezza del piano e delle procedure per poi eventualmente procedere con la loro revisione, in ottica di miglioramento.

PO-Plan and Organise	AI-Acquire and Implement	DS-Deliver and Support	ME-Monitor and Evaluate
PO9 Assess and Manage IT Risks	**AI6 Manage Changes**	**DS4 Ensure Continuous Service**	**ME1 Monitor and Evaluate IT Performance**
PO9.1 IT and Business Risk Management Alignment	AI6.1 Change Standards and Procedures	DS4.1 IT Continuity Framework	ME1.1 Monitoring Approach
PO9.2 Establishment of Risk Context	AI6.2 Impact Assessment, Prioritisation and Authorisation	AI6.2 Impact Assessment, Prioritisation and Authorisation	ME1.2 Definition and Collection of Monitoring Data
PO9.3 Event Identification	AI6.3 Emergency Changes	DS4.3 Critical IT Resources	ME1.3 Monitoring Method
PO9.4 Risk Assessment	AI6.4 Change Status Tracking and Reporting	DS4.4 Maintenance of the IT Continuity Plan	ME1.4 Performance Assessment
PO9.5 Risk Response	AI6.5 Change Closure and Documentation	DS4.5 Testing of the IT Continuity Plan	ME1.5 Board and Executive Reporting
PO9.6 Maintenance and Monitoring of a Risk Action Plan		DS4.5 Testing of the IT Continuity Plan	ME1.6 Remedial Actions
		DS4.7 Distribution of the IT Continuity Plan	
		DS4.8 IT Services Recovery and Resumption	
		DS4.9 Offsite Backup Storage	
		DS4.10 Post-resumption Review	

Figura 6 - Obiettivi di controllo per i principali processi inerenti la gestione delle emergenze (fonte: COBIT v4.0, © 2005 IT Governance Institute)

3.3. MACROPROCESSO E ATTIVITÀ FONDAMENTALI DEL SISTEMA DI GESTIONE DEGLI INCIDENTI DI SICUREZZA DELLE INFORMAZIONI

3.3.1 Il flusso delle attività

Per far fronte compiutamente ad incidenti di sicurezza delle informazioni è necessario che l'azienda o l'amministrazione si doti al suo interno di una organizzazione specifica, anche se essenziale, in cui siano allocati ruoli e responsabilità delle attività di contrasto dell'incidente e che queste si svolgano secondo una procedura che all'interno sia già stabilita e condivisa.

È quindi auspicabile che anche (o forse soprattutto) le realtà più piccole evitino quanto più possibile attività di contrasto basate sull'improvvisazione. Purtroppo era frequente il caso che reputando remota la probabilità del verificarsi di un incidente, non si ritiene necessario investire risorse per una programmazione delle attività di gestione degli incidenti: si vedrà poi sul momento cosa fare magari chiedendo supporto a terze parti.

Questo approccio limita fortemente le capacità di reazione dell'organizzazione che si trova impreparata al verificarsi dell'emergenza e magari affida la reazione a personale esterno che non ha mai avuto a che fare con l'organizzazione. I fattori critici di successo sono invece la prontezza di reazione, la precisione e l'efficacia dell'azione (sapere come e dove agire) e l'instaurarsi delle corrette sinergie all'interno dell'organizzazione nei momenti 'caldi' delle attività di contrasto.

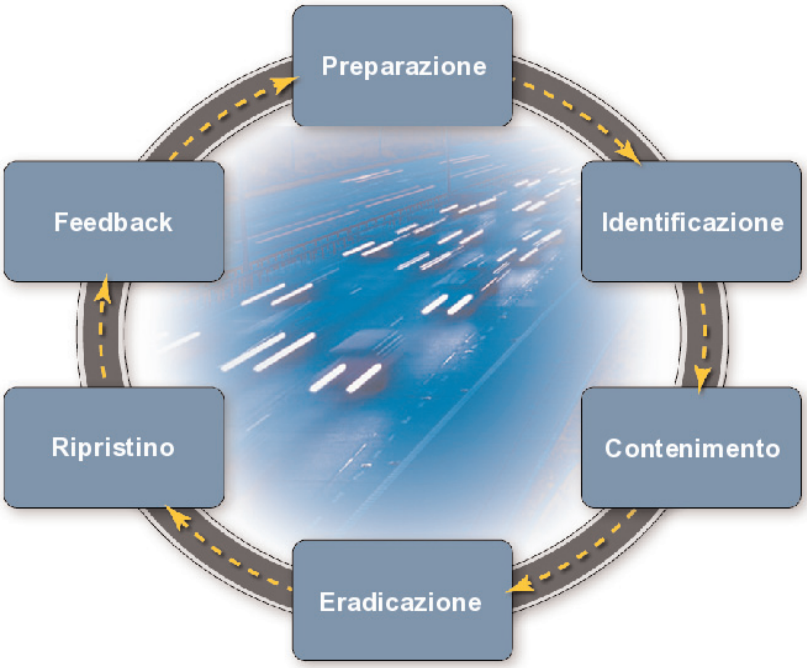


Figura 7 - Il flusso delle attività

La gestione degli incidenti dovrebbe svolgersi secondo un approccio specifico che vede come attività centrali l'identificazione della causa dell'incidente, la predisposizione di quanto necessario per evitare che l'incidente amplifichi l'impatto in termini di estensione e/o di intensità del danno, l'attività di eliminazione della causa ad origine dell'incidente e quindi il ripristino delle condizioni iniziali per il ritorno nel più breve tempo possibile alla normalità.

Queste attività 'operative centrali' sono precedute e seguite da due attività di natura gestionale ma fondamentali per il successo delle quattro attività operative citate, e cioè la *preparazione* che consiste sostanzialmente nella costruzione del sistema tecnico organizzativo per la prevenzione ed il contrasto degli incidenti ed il *feedback* che raccogliendo le esperienze (positive e negative) di come l'organizzazione si è comportata nelle attività di contrasto all'incidente e che alimenta il ciclo del miglioramento continuo.

La figura 7 illustra il flusso delle attività le cui singole fasi analizziamo di seguito nel dettaglio.

Fase di preparazione

È la fase di costituzione del sistema di gestione degli incidenti. In questa fase viene effettuata una accurata analisi dei rischi e definita la strategia di gestione del rischio, vengono definite le policy e le procedure operative, creata l'organizzazione ed i ruoli nelle condizioni di emergenza, stabilite ed allocate le risorse economiche e di personale ritenute necessarie.

A seguito di un incidente vengono messe in atto le azioni di miglioramento individuate nella fase di feedback.

La fase di preparazione è anche e soprattutto una fase di "prevenzione" ed è decisiva per la riuscita di un qualsiasi sistema di gestione delle emergenze. Al riguardo, la Comunità Europea definisce la "prevenzione" come l'insieme di decisioni, operazioni critiche ed attività necessarie per costruire, mantenere e migliorare la capacità operativa di prevenire, proteggere, rispondere e ripristinare a seguito di un incidente. La prevenzione viene anche caratterizzata come un processo continuo (*process of ongoing actions*), in quanto, come anticipato nel capitolo precedente, solo adottando un approccio di miglioramento continuo è possibile ridurre l'esposizione agli incidenti. Nel seguito la definizione di Prevenzione data dalla Commissione europea:

The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from an incident. Prevention involves efforts to identify threats, determine vulnerabilities and identify required resources. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity, and apprehending potential per-

petrators and bringing them to justice. Prevention involves the stopping of an incident before it happens with effective processes, guidelines, standards and certification. Seamless interactive systems, and comprehensive threat- and vulnerability analysis. Prevention is a continuous process of ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

Fase di identificazione

È la fase in cui si rileva e si qualifica l'incidente.

Generalmente si avvia con una segnalazione dell'evento, vengono raccolte rapidamente le informazioni del caso per comprendere la natura e l'intensità dell'evento. Sulla base di queste si decide se attribuire all'evento il valore di incidente e nel caso si attribuisce il relativo livello di gravità. È largamente consigliabile di predisporre questionari 'tipo' con le informazioni rilevanti ai fini del processo decisionale. Tali informazioni potranno in una prima fase essere raccolte per le vie brevi dal punto di contatto per la segnalazione degli incidenti (appositamente predisposto, con presidio continuativo) e veicolate ai referenti prestabiliti per le decisioni del caso. Dal momento che la segnalazione dell'evento può avvenire da fonte interna o esterna all'organizzazione (e la rapidità di intervento può essere decisiva per ridurre gli impatti) è consigliabile rendere facilmente reperibile il riferimento del punto di contatto per la segnalazione degli incidenti sia internamente che esternamente all'organizzazione. Nel caso di apertura di un incidente viene data tempestiva comunicazione a tutti gli interessati attraverso 'contact list' e mezzi di comunicazione appositamente predisposti.

Fase di contenimento

È la fase in cui si cerca di limitare gli effetti dell'incidente e di isolarlo per evitare che amplifichi e/o estenda i suoi effetti. Tale fase comporta che l'organizzazione abbia compreso la natura della minaccia, il meccanismo di propagazione ed abbia disponibili le conoscenze, i mezzi tecnici e le risorse per limitare i danni, in attesa delle risoluzio-

ne 'ab origine' (laddove possibile) del problema. Durante tale attività deve essere massima la capacità dell'organizzazione di far convergere verso il team di risposta le necessarie conoscenze/competenze tecniche e specialistiche e di attivare processi di comunicazione efficaci e tempestivi.

Fase di eradicazione

È la fase in cui una volta identificate le cause dell'incidente si interviene per rimuoverle. Si cerca inoltre di raccogliere tutte le evidenze possibili dell'accaduto sia per eventuali rivalse nel caso di azione dolosa sia per identificare le vulnerabilità che hanno causato l'incidente. Vengono valutati i danni e censite le risorse disponibili per attivare la fase successiva di ripristino. Quanto più esaustiva e dettagliata sarà la documentazione dell'accaduto tanto maggiore sarà il contributo che potrà essere fornito alla svolgimento dell''ultima fase, quella di feedback.

Fase di ripristino

È la fase in cui si mettono in campo le azioni necessarie per il ritorno alla normalità. Viene effettuato il 'restore' dei sistemi con le necessarie attività di valutazione e verifica dell'ambiente ripristinato prima dell'avvio in esercizio. Viene formalmente data comunicazione agli interessati di chiusura dell'incidente e di ritorno alla normale conduzione delle attività di business. È possibile che nel caso di incidenti gravi il ripristino sia graduale con la ripresa delle attività di business critiche in via prioritaria e il ripristino delle restanti attività e servizi secondo una scala di priorità già identificata nelle fasi di pianificazione della continuità operativa (se disponibile).

Feedback

Viene analizzata la documentazione raccolta e ripercorso criticamente quanto accaduto, analizzando le cause dell'incidente e valu-

tando nel complesso le performance dell'organizzazione coinvolta nel processo di gestione dell'incidente.

Per quello che riguarda il verificarsi dell'incidente è opportuno valutare se ciò sia dovuto ad una vulnerabilità non evidenziata nel corso della analisi dei rischi, o piuttosto a mutate condizioni di rischio ambientale o ad altre ragioni da individuare. Tale valutazione costituirà la base per l'adeguamento del sistema di protezione al fine di evitare il ripetersi dell'incidente.

In questa fase si analizza anche il comportamento del team di risposta. È opportuno sottolineare che per tale attività è richiesta estrema apertura e disponibilità al confronto all'interno dell'organizzazione. L'obiettivo non deve essere quello di 'mettere sotto processo' gruppi o singoli individui ma piuttosto quello di comprendere, condividendolo all'interno dell'organizzazione, cosa effettivamente non abbia funzionato per porvi da rimedio, rivedendo ad esempio l'attribuzione dei ruoli o piuttosto i meccanismi di comunicazione interni. Anche i comportamenti migliori e le 'storie di successo' devono entrare, con gli aspetti da migliorare, nel patrimonio di conoscenze operative dell'organizzazione acquisite nel corso della gestione dell'incidente e divenute 'Lessons Learned' al fine di avviare il successivo piano di miglioramento.

3.3.2 Cosa fare per costruire un Piano per la gestione delle emergenze

I passi fondamentali per la definizione e la manutenzione di un Piano per la gestione delle emergenze, sono i seguenti:

- *Sviluppare una Politica di gestione delle Emergenze* che sia formalizzata e condivisa dal personale. La politica deve essere integrata con i piani generali di gestione del rischio e della sicurezza.
- *Condurre la Business Impact Analysis (BIA) e l'Analisi dei Rischi* che consentono di definire: il livello di priorità dei processi in funzione del danno economico associato alla loro interruzione, il tempo di fermo del servizio ritenuto accettabile ed il livello di esposizione al rischio per ogni processo. I rischi sono valutati

determinando l'entità dei danni potenziali sul sistema che una o più minacce (eventi indesiderati in grado di provocare un malfunzionamento o un danno al sistema) potrebbero provocare in caso di accadimento, considerando la probabilità che la minaccia causi sempre il maggior danno possibile al suo verificarsi. L'attività viene svolta seguendo alcuni i passi fondamentali:

- identificazione dei processi aziendali (nell'ambito delle aree critiche del business e dell'azienda),
- valutazione dell'impatto economico-finanziario di una loro interruzione di attività per il business complessivo,
- determinazione dell'entità dell'impatto in funzione del tempo,
- identificazione delle risorse bloccanti a supporto dei processi,
- identificazione delle minacce e della relativa probabilità di accadimento su tutte le risorse bloccanti,
- definizione delle priorità di ripristino.

Tale processo consente di individuare "*the optimum point to recover the IT system*", bilanciando il costo del fermo con il costo delle risorse necessarie a ripristinare il sistema.

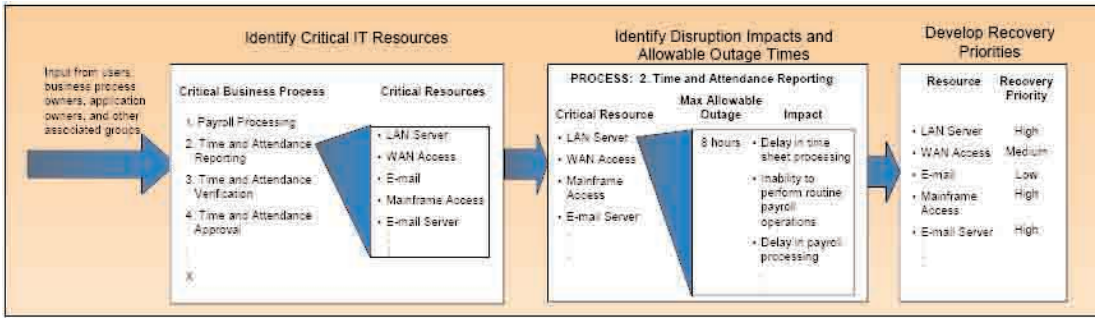


Figura 8 - Processo di Business Impact Analysis (fonte: NIST, 2002)

- *Definire controlli preventivi* da attuare per prevenire gli incidenti o limitarne gli effetti nel caso in cui si verifichino. Tali controlli devono essere documentati.
- *Definire la strategia di recovery* per la gestione del rischio residuo identificato (con i relativi impatti) nelle precedenti fasi di BIA e Analisi dei Rischi (e quindi per minimizzare il *Recovery Time Objective* e i costi associati). La strategia interessa aspetti tecnici ed organizzativi e deve includere un ampio spettro di soluzioni in grado di gestire le diverse situazioni di emergenza identificate.
- *Sviluppare e documentare il Piano di Gestione delle Emergenze* per la gestione dei rischi residui. Secondo quanto suggerito dal NIST, il Piano si compone di cinque parti fondamentali rappresentate nella figura seguente.
- *Pianificare attività di test, addestramento ed esercitazioni*. L'attività di test del Piano è fondamentale ed ogni elemento del Piano deve essere provato per verificare l'efficacia di ogni procedura e del Piano nel suo complesso.
- *Manutenere il Piano*. Affinché il Piano sia efficace è necessario che questo sia mantenuto allineato con le evoluzioni tecniche-organizzative. Il Piano deve quindi diventare parte integrante del processo di *Change Management*.

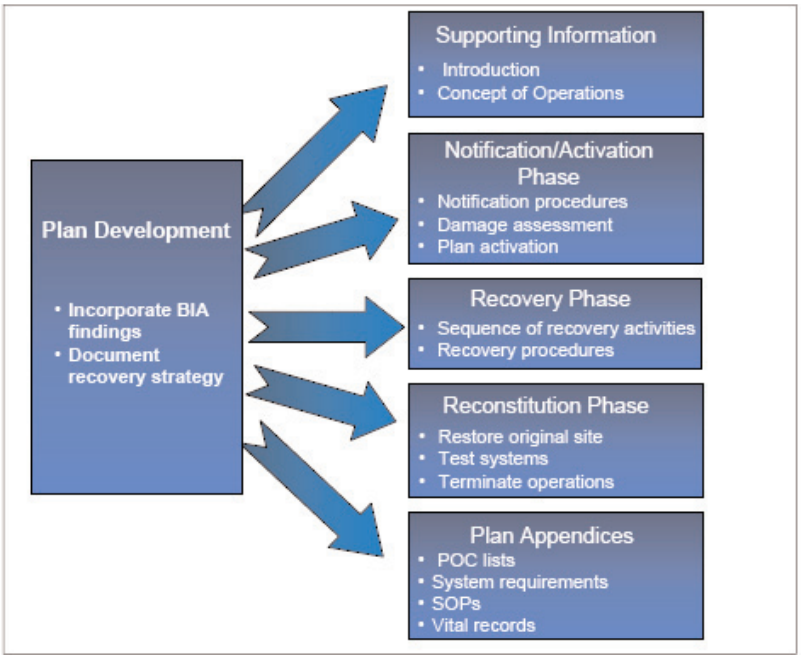


Figura 9 - Struttura di un Piano per la gestione delle emergenze (fonte: NIST, 2002)

Come rappresentato in figura 9, un Piano di gestione delle emergenze contiene generalmente le seguenti parti:

- *Supporting Information*, contenente un'introduzione (obiettivi, ambito, applicabilità, riferimenti, storia delle revisioni del documento) ed informazioni aggiuntive circa: descrizione del sistema, dei ruoli e delle responsabilità.
- *Notification/Activation Phase*, include le attività di comunicazione al personale che deve gestire l'emergenza, di assessment delle conseguenze sui sistemi e di attuazione del Piano.
- *Recovery Phase*, questa fase inizia dopo che il Piano di gestione delle emergenze è stato attivato e descrive le attività da fare per consentire l'esercizio temporaneo dei sistemi (eventualmente in un sito alternativo in caso di evento disastroso).
- *Reconstitution Phase*, questa fase dettaglia le attività necessarie al

rientro alle normali condizioni di esercizio. In taluni casi, questa fase può essere dettagliata in un documento separato (Piano di Ripristino).

- *Plan Appendices*, generalmente contengono i riferimenti del personale appartenente ai Team di gestione delle emergenze e dei fornitori, le procedure e l'elenco dei sistemi (hardware, software, firmware, ecc.) interessati dal Piano con le relative priorità di ripristino, gli accordi stabiliti con i fornitori, i riferimenti di siti alternativi da raggiungere in caso di disastro, i risultati della BIA.

In parallelo alla formulazione del Piano, va definita una metrica per controllare il processo ed il raggiungimento degli obiettivi di business. Ad esempio, la figura 10 riporta gli obiettivi e la metrica per la continuità del servizio secondo il COBIT v4.0.

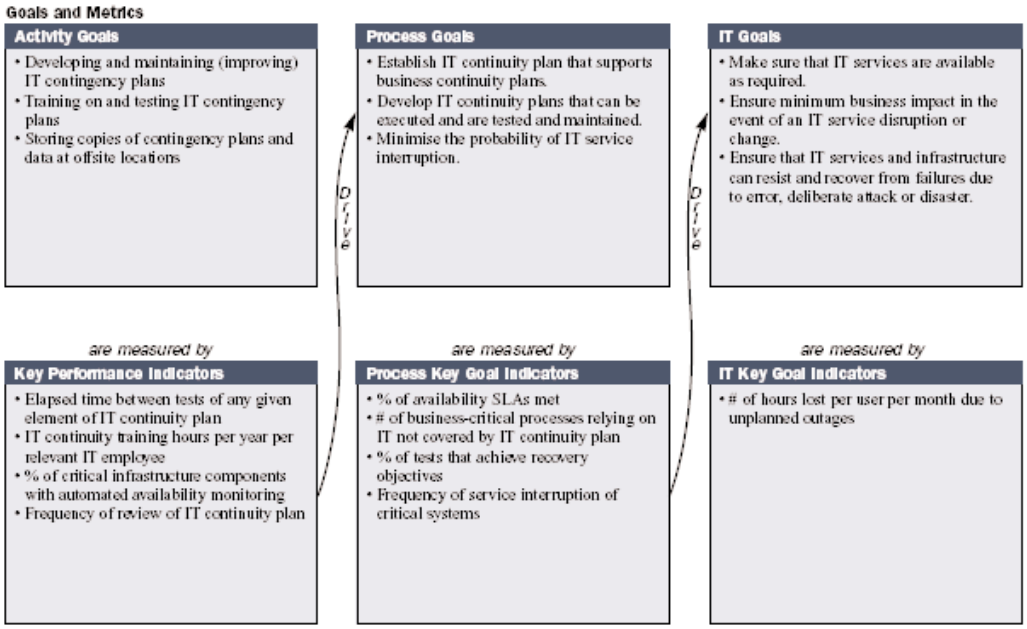


Figura 10 - Obiettivi di controllo per i principali processi inerenti la gestione delle emergenze (fonte: COBIT v4.0, © 2005 IT Governance Institute)

L'approccio è sempre circolare, ovvero gli obiettivi di business sono calati in obiettivi IT e in obiettivi di processo e di attività ed ognuno di questi obiettivi ha uno specifico insieme di indicatori. In tal modo si riesce a dare concretezza, e quindi a misurare, un processo che altrimenti sarebbe troppo complesso. Inoltre, la disponibilità di una metrica e quindi di indicatori consente di attuare la politica di miglioramento continuo che abbiamo detto essere fondamentale per l'efficacia del processo.

3.4. IL RUOLO DELL'ANALISI DEI RISCHI E LA BUSINESS IMPACT ANALYSIS

3.4.1 Il Risk Management per le infrastrutture critiche

Le infrastrutture critiche sono tipicamente fortemente dipendenti dal sistema di gestione e controllo informatizzato. Dai sistemi informativi di tipo più tradizionale ai sistemi che utilizzano elettronica specializzata (es: sistemi di telemetria e telecontrollo) il governo elettronico è vitale per tali infrastrutture ed un eventuale danno a tali sistemi può avere impatti totalizzanti sulla capacità produttiva dell'infrastruttura.

La protezione della componente informatizzata delle infrastrutture critiche viene messa in atto attraverso una sequenza ciclica che prevede, come anticipato nel capitolo precedente, la rilevazione del contesto e delle funzioni vitali, l'analisi e la gestione dei rischi, la selezione delle contromisure applicabili, la definizione del piano di implementazione e la sua realizzazione, l'attività di controllo per il necessario feedback di miglioramento.

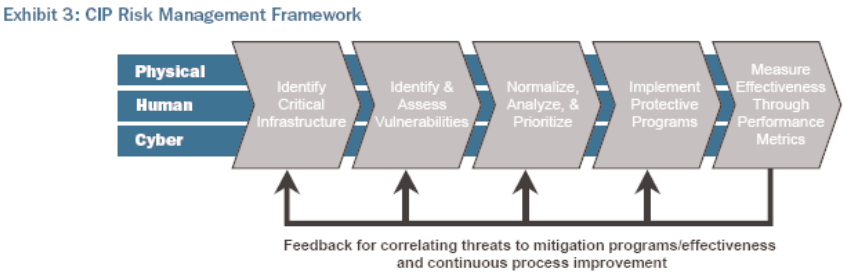


Figura 11 - Il Risk Management per la protezione delle infrastrutture critiche (Fonte: Interim Infrastructure Protection Plan- Homeland Security, 2005)

In termini generali possiamo definire come rischio la possibilità di incorrere in un danno od una perdita economica. Il livello di rischio è correlato a tre fattori: la probabilità che la minaccia si verifichi, la vulnerabilità dell'asset rispetto a quella minaccia, l'impatto (inteso come danno, perdita) nel caso che la minaccia si concretizzi.

La tabella in figura 12 presenta una modalità sintetica di calcolo del livello di rischio sulla base della probabilità che si verifichi la minaccia e la gravità dell'evento in termini di potenziale impatto sugli asset.

Vediamo ora come si articolano le macro fasi di analisi e gestione del rischio.

Ai fini della definizione del programma di protezione della struttura è necessario dapprima identificare e classificare le funzioni produttive secondo un ranking di criticità per la conduzione del business o dell'attività amministrativa

Ad esempio:

- Funzioni Critiche
- Funzioni Essenziali
- Funzioni di Supporto.

		GRAVITÀ DELL'EVENTO		
		ALTA	MEDIA	BASSA
PROBABILITÀ DELL'EVENTO	ALTA	ALTA	ALTO	MEDIO
	MEDIA	ALTO	MEDIO	BASSO
	BASSA	MEDIO	BASSO	BASSO

Figura 12 - Esempio di matrice per il calcolo del rischio

Tale classificazione sarà di guida per la definizione delle priorità d'intervento nell'attuazione del programma di protezione.

Seguirà l'analisi dei sistemi ICT di supporto a tali funzioni, con l'identificazione dei relativi information asset.

Verranno quindi valutate le minacce all'integrità, alla riservatezza ed alla disponibilità che gravano su tali asset (ad es: disastro naturale, attacco informatico, furto, accesso non autorizzato ai dati, introduzione ed esecuzione di codice dannoso, errore umano, divulgazione non autorizzata di dati confidenziali, ecc.). Si procede quindi con l'analisi delle vulnerabilità (cioè del corrente livello di esposizione degli asset alle minacce identificate) e con la valutatazione delle potenziali conseguenze (impatti) nel caso in cui tali minacce si concretizzassero.

3.4.2 Possibili impatti

Di seguito si riporta una lista esemplificativa dei possibili impatti per aziende ed amministrazioni pubbliche.

Impatti Fisici

- Perdita di vite umane, o danni alle persone
- Incendi, esplosioni e rilascio di sostanze nocive nell'ambiente
- Danni alle infrastrutture produttive

Impatti sulla capacità produttiva in termini di:

a) nel caso di aziende, impatti sulla capacità commerciale:
   - perdita di fatturato;
   - perdita della customer base;
   - perdita della competitività commerciale;
   - perdita di credibilità rispetto alla capacità commerciale ed alla solvibilità finanziaria;
   - perdita della fiducia degli azionisti;

b) nel caso di amministrazione pubblica, impatti sulla capacità di esercizio dell'attività amministrativa:
   - disagi alla cittadinanza nell'erogazione dei servizi essenziali;
   - conseguenze socio economiche della mancata o ridotta (in termini di quantità/qualità) azione amministrativa.

Impatto in termini di costi non preventivati

- Perdita di partite commerciali correnti, recupero di spazio aggiuntivo ai fini produttivi o di stoccaggio merce, riassetto del parco fornitori, indennizzi a terze parti, spese legali, ecc.

Impatti legali e sulla reputazione dell'azienda o dell'amministrazione

- Violazione a norme, leggi , regolamenti o impegni contrattuali precedentemente sottoscritti
- Perdita dell'immagine acquisita nella società e negli stakeholder per le aziende
- Perdita di credibilità del 'Sistema Paese' per le amministrazioni pubbliche

Giunti a questo punto si è in possesso degli elementi conoscitivi per il calcolo del rischio e la successiva gestione. Tipicamente nel caso in cui si identifichino aree di rischio di livello non accettabile si procede alla messa in campo di protezioni e contromisure di natura sia tecnica che organizzativa per mitigare il rischio.

Il processo di gestione del rischio è tipicamente ciclico dal momento che sia l'ambiente con le sue minacce sia le organizzazioni sono soggetti a continui mutamenti.

3.5. INFORMAZIONE E COMUNICAZIONE PER LA GESTIONE DELL'INCIDENTE

Nel momento in cui si verifica un incidente, il contenuto e la qualità dell'informazione che deve essere veicolata alle varie strutture con ruoli operativi e decisionali, al fine di una corretta e pronta gestione dell'incidente, è di fondamentale importanza.

Al momento della segnalazione dell'incidente ci si trova di fronte a due esigenze talvolta in contrasto. La prima è quella di veicolare in tempi rapidi la segnalazione dell'incidente per far partire quanto prima possibile l'azione di risposta. L'altra è che l'informazione sia quanto più accurata (aderente alla realtà dei fatti) e più dettagliata possibile per abilitare un efficace ed efficiente processo decisionale.

La segnalazione tempestiva dell'evento è quindi rilevante per il successo dell'attività di risposta ma una segnalazione generica e imprecisa può far perdere tempo prezioso o impegnare risorse inutilmente.

È importante in tal senso che la prima segnalazione abbia tutte le informazioni fondamentali per far partire il meccanismo di gestione dell'incidente consentendo così di agire con prontezza e precisione.

Nella tavola seguente viene riportata la struttura di informazioni essenziali da inserire in un "*Rapporto di segnalazione incidente per essere veicolata ai vari punti di contatto e centri di responsabilità*".

1) Dati identificativi del compilatore del report

- Nome, unità organizzativa di appartenenza, qualifica e ruolo, riferimenti (tel, mail, fax, etc.)

- luogo, data e ora di produzione del report

2) Notizie dell'incidente

- Provenienza della segnalazione (fonte interna, esterna; specificare e qualificare se possibile)

- Breve descrizione dell'incidente.

- tipologia di evento (Es.: Attacco di Denial of Service, modificazione non autorizzata di dati, Worm/Virus, evento fisico di origine naturale o dolosa, violazione di nome leggi, regolamenti etc..)

- luogo dell'incidente, data di inizio e fine o specificare se ancora in corso;

- risorse interessate;

- danni rilevati; danni presunti e/o potenziali.

- Prima classificazione dell'incidente sulla base delle informazioni disponibili (fare riferimento ad una matrice specifica da allegare al form.

- Personale di contatto dell'Unità Organizzativa coinvolta.

3) Prime azioni intraprese, esigenze

- Breve descrizione dei primi eventuali interventi effettuati per il contenimento dell'incidente

- Eventuale richiesta di assistenza (specificare)

4) Ulteriori informazioni utili

Figura 13 - Rilevazione e segnalazione dell'incidente: informazioni essenziali

Tali informazioni tipicamente vengono raccolte e veicolate da un referente autorizzato alla segnalazione dell'incidente. Tale ruolo può essere attribuito solo ad un numero ristretto di figure (ad esempio i responsabili di strutture tecnico-oganizzative) oppure la possibilità di attivare la segnalazione dell'incidente può essere lasciata ad una pluralità di soggetti (ad es. tutti i dipendenti di una azienda).

La segnalazione viene indirizzata ad un punto di contatto per la gestione degli incidenti; questo sulla base del contenuto del report (laddove ritenga abbia informazioni quali/quantitative adeguate), avvia il processo di gestione dell'incidente allertando i presidi specifici del Team di Risposta secondo quanto stabilito dalla procedura di Incident Handling.

3.6. ASPETTI ORGANIZZATIVI: ATTORI, RUOLI, RESPONSABILITÀ E ATTIVITÀ.

3.6.1 Il modello organizzativo interno

Il processo di gestione delle emergenze è trasversale a tutta l'organizzazione, ma coinvolge anche una serie di attori esterni a quest'ultima. Per quanto riguarda i ruoli e le responsabilità interne all'organizzazione una prima grande distinzione va fatta tra le figure che intervengono nella definizione/revisione/attivazione del Piano di gestione delle emergenze e quelle che intervengono nell'attuazione operativa del Piano stesso (queste ultime sono definite nella parte introduttiva del Piano).

La Mappa delle responsabilità ad alto livello è rappresentata nella figura seguente.

RACI Chart / Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Develop IT continuity framework.		C	C	A	C	R	R	R	C	C	R
Conduct business impact analysis and risk assessment.		C	C	C	C	A/R	C	C	C	C	C
Develop and maintain IT continuity plans.	I	C	C	C	I	A/R		C	C	C	C
Identify and categorise IT resources based on recovery objectives.				C		A/R		C	I	C	I
Define and execute change control procedures to ensure IT continuity plan is current.				I		A/R		R	R	R	I
Regularly test IT continuity plan.				I	I	A/R		C	C	I	I
Develop follow-on action plan from test results.				C	I	A/R	C	R	R	R	I
Plan and conduct IT continuity training.				I	R	A/R		C	R	I	I
Plan IT services recovery and resumption.		I	I	C	C	A/R	C	R	R	R	C
Plan and implement backup storage and protection.				I		A/R		C	C	I	I
Establish procedures for conducting post-resumption reviews.				C	I	A/R		C	C		C

Figura 14 - Mappa delle responsabilità per la continuità del servizio (fonte: COBIT v4.0, fonte: COBIT v4.0 © 2005 IT Governance Institute)

La Mappa usa il modello RACI dove le singole lettere indicano:

R = Responsible - owns the problem / project
A = to whom "R" is Accountable - who must sign off (Approve) on work before it is effective
C = to be Consulted - has information and/or capability necessary to complete the work
I = to be Informed - must be notified of results, but need not be consulted

A livello più operativo i principali ruoli per la gestione delle emergenze sono riportati nella figura 15.

Ruolo	Responsabilità
Unità di Crisi	È l'organo di governo che dirige i piani per la gestione di gravi emergenze o situazioni di "crisi" (cfr. capitolo sulle definizioni) con significativo impatto sulle strutture ICT. In caso di previsione di potenziale crisi la convocazione dell'Unità ha lo scopo di classificare l'evento ed eventualmente attivare l'attuazione del Piano. L'Unità di Crisi si compone di rappresentanti delle diverse funzioni aziendali (ICT, Risorse Umane, Acquisti, Comunicazione, ecc.)
Coordinatore dell'Emergenza	È la persona che riceve la segnalazione dell'emergenza e convoca il Team di Assessment per la classificazione dell'emergenza e, se necessario, avvisa l'Unità di Crisi. Dopo l'attivazione del Piano coordina le attività di gestione della crisi.
Emergency/Recovery Teams	Gli Emergency/Recovery Teams intervengono su convocazione del Coordinatore e provvedono, ognuno per le attività di competenza (Sistemi, Reti, Applicazioni, Immobili, ecc.), alla gestione della crisi/disastro (ed alle attività di ripristino).
Assessment Team	Il Team interfunzionale ha il compito di valutare gli impatti della segnalazione e gli eventuali danni, redigendo uno specifico rapporto.

Figura 15 - Principali ruoli e responsabilità per la gestione delle emergenze

La figura 16 rappresenta un esempio del NIST circa l'organizzazione interna specificatamente preposta alla gestione delle emergenze IT, ovvero che interviene dopo che il Team di Assessment ha valutato l'entità e la tipologia dell'emergenza. La figura rappresenta anche l'albero di notifica dell'emergenza.

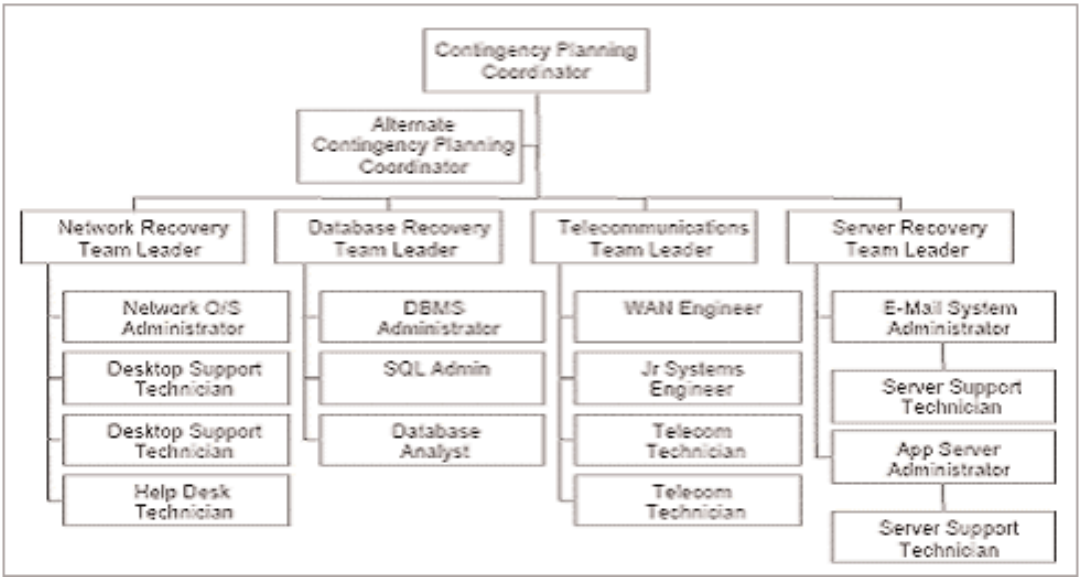


Figura 16 - Esempio di struttura organizzativa del team tecnico (Fonte NIST)

Un aspetto fondamentale è poi la formalizzazione e comunicazione dei ruoli e delle responsabilità all'interno dell'organizzazione.

In un'organizzazione di dimensioni medio-piccole, può accadere che, per vincoli organizzativi, alcuni ruoli sia a livello alto (cfr. Figura 12) che a livello operativo (cfr. Figura 13) siano ricoperti dalla stessa persona, ma in tal caso è importante che i diversi ruoli e responsabilità siano definiti in modo che ogni aspetto sia preso in considerazione (l'attribuzione "ad personam" dei ruoli è un aspetto successivo).

3.6.2 Relazioni con enti esterni per il governo dell'incidente

L'organizzazione di recovery dell'ICT di un'infrastruttura critica (pensiamo esempio ad un governo locale o ad una infrastruttura critica di piccole o medie dimensioni presente sul territorio) potrebbe avere necessità di ricorrere a servizi specialistici esterni e di coordinar-

si con riferimenti istituzionali di più alto livello.

In tale contesto il ruolo delle terze parti può essere più o meno importante a seconda dei livelli di delega decisi dall'organizzazione rispetto alla gestione dell'ICT (ad es. in caso di outsourcing, per l'incidente prettamente informatico le attività di incident handling sono largamente delegate al fornitore dei servizi di gestione).

Nella tabella seguente vengono riportati i servizi tipici di un CSIRT (Computer Security Incident Response Team) che possono ad esempio essere richiesti ad enti esterni.

Il raccordo sia con strutture specialistiche esterne che con funzioni istituzionali a livello nazionale è rilevante per l'organizzazione colpita dall'incidente anche in ragione del fatto che questa può ricevere assistenza e supporto rispetto a risorse e mezzi non prontamente disponibili e che potrebbero risultare indispensabili per gestire l'incidente sin dalle prime fasi.

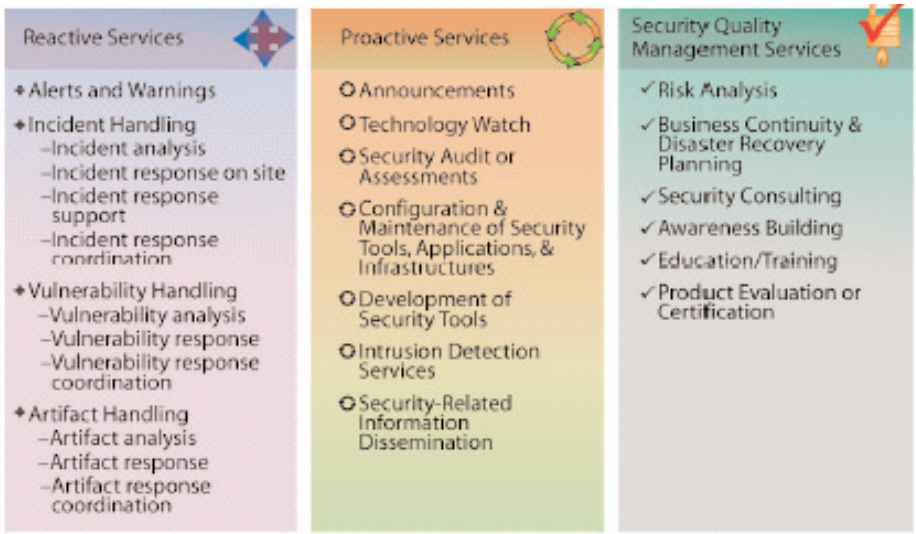


Figura 17 - Lista dei servizi tipici di un 'CSIRT' (Fonte: CMU/SEI)

Pensiamo ad esempio non solo alla disponibilità di risorse professionali ed equipaggiamenti tecnologici ma anche alla fornitura di combustibile per l'alimentazione dei gruppi di continuità o al supporto logistico per raggiungere i siti di recovery laddove necessario.

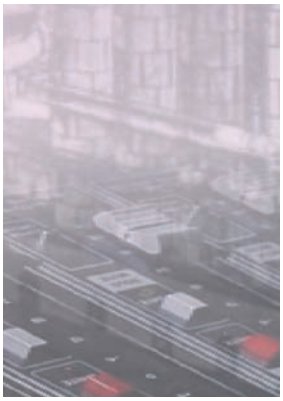
È opportuno che le amministrazioni e le aziende identifichino da subito ed inseriscano nel loro piano di risposta all'incidente i riferimenti istituzionali per questo tipo di eventualità.

Le organizzazioni possono trovare vantaggioso avviare relazioni con altri enti sia per eventuali richieste di supporto sia per scambio di informazioni talora preziose sulla dinamica dell'incidente e sui possibili rimedi.

Altri attori esterni poi possono comparire nel corso delle gestione dell'incidente con i quali l'organizzazione deve necessariamente interagire (media, istituzioni, forze dell'ordine). È quindi necessario identificare già in fase di stesura del piano i riferimenti e le modalità di relazione con tali entità esterne che potrebbero essere coinvolte. Laddove vi sia la necessità di ricorrere in ogni caso a servizi tecnici esterni nell'eventualità di un incidente, è consigliabile stipulare accordi di servizio preventivi con terze parti qualificate.

Figura 18 - Relazioni con terze parti nella gestione degli incidenti (Fonte NIST)

La figura 18 riporta alcuni tra i principali potenziali attori esterni all'organizzazione: (fonte: NIST Computer Security Incident Handling Guide- Special Publication 800-61).



4 - La gestione operativa dell'emergenza

4.1. DA EVENTO A DICHIARAZIONE DI CRISI

Prima di focalizzare l'attenzione sul processo decisionale occorre premettere che la gestione dell'emergenza, per essere efficiente ed efficace, presuppone l'esistenza di un'organizzazione strutturata dedicata la cui missione è **garantire la messa in campo di tutte le misure atte ad affrontare l'evento indesiderato (incidente o emergenza) al fine di ridurne l'impatto sul sistema, rendere disponibili eventuali risorse alternative, governare la fase critica, gestire il rientro alla normalità.** Una corretta definizione di ruoli e responsabilità determina il successo dell'organizzazione. Nelle ordinarie condizioni le attività saranno necessariamente diverse da quelle nelle condizioni di crisi. I dettagli di tale struttura saranno descritti nei paragrafi successivi, qui basta dire che la struttura dell'organizzazione di gestione delle emergenze si traduce nella presenza di diverse componenti: una componente di vertice, una componente di coordinamento, una componente tecnico-operativa.

Una gestione ottimale del processo decisionale di dichiarazione di passaggio da evento a crisi deve essere basato su una scala di severità dell'evento, necessariamente legata agli effetti prodotti dall'impatto di quest'ultimo sull'organizzazione, e questo anche per identificare le risorse da impiegare ed i processi da attuare. A parte l'operatività normale dove l'attività si può esaurire magari in un banale controllo di allarmi provenienti da diverse fonti, si possono definire dei livel-

li (basso, medio, alto) legati all'impatto (rispettivamente minimo, significativo, elevato) dell'evento sul sistema. L'estremo superiore di quest'ampia gamma di fenomeni assume i connotati di disastro, che comporta una drastica riduzione delle funzioni vitali per l'organizzazione.

In base alle caratteristiche dell'evento, quali la modalità di accadimento, l'impatto sull'operatività, la velocità di propagazione, la stima dell'impatto, viene effettuata la scalabilità della reazione ad un livello più alto.

Per il livello basso è individuata una possibile minaccia e si stabiliscono le misure da intraprendere. Se opportuno, sono inviati ai dipendenti dei messaggi con la richiesta delle azioni da intraprendere.

Per il livello significativo la minaccia si è manifestata e si stabiliscono le azioni da intraprendere per il contenimento e la rimozione della causa. Se opportuno, sono inviati ai dipendenti dei messaggi con la richiesta delle azioni da intraprendere.

Per il livello alto la minaccia si è diffusa ampiamente e l'impatto è elevato e si stabiliscono le azioni da intraprendere per il contenimento e la rimozione della causa. Si invia un messaggio agli utenti. Si intraprendono, eventualmente, azioni legali.

L'escalation degli effetti dell'evento determina il riposizionamento delle risorse da impiegare (umane e tecnologiche) e dei processi da innescare, e quindi l'intervento di quelle componenti dell'organizzazione di gestione dell'emergenza, prima individuate. Una cosa è certa: non appena ci si rende conto di un incidente si deve immediatamente cominciare a lavorare sul contenimento.

Per quanto riguarda gli eventi manifestatisi al sistema, è fortemente consigliabile avere a disposizione un opportuno elenco contenente le condizioni di attenzione, superate le quali, l'evento deve essere riportato alle altre componenti della struttura di gestione. Normalmente le condizioni di attenzione sono espresse in termini di percentuale di rendimento minimo del sistema accettabile, e di massima durata del periodo di disponibilità del servizio al di sotto di un livello minimo. Un apposito gruppo all'interno della componente tecnica avrà il compito di gestire il processo di escalation dove, man mano che l'impatto dell'incidente diventa più significativo, il coinvolgimento delle

risorse secondo il piano prestabilito diventa sempre crescente.

Il ruolo portante del processo decisionale e gestionale dell'emergenza è svolto dal piano di reazione il cui fine è quello di essere un riferimento a tutte le componenti impegnate nell'affrontare l'evento non desiderato. I principali obiettivi da raggiungere sono:

- individuare le modalità di accadimento dell'evento avverso;
- limitare gli effetti dovuti all'impatto;
- evitare o quanto meno limitare al massimo l'escalation;
- ricondurre il sistema nelle normali condizioni di funzionamento;
- ripristinare le normali attività operative;
- determinare, se possibile, l'origine dell'evento avverso;
- aggiornare politiche di sicurezza e procedure;
- valutare il danno e l'impatto in termini di perdite economiche, di immagine, ecc.

Come già detto in precedenza, occorre dunque un'identificazione del livello di severità dell'evento indesiderato, fondamentale per la scelta delle risorse da mettere in campo. Per quanto riguarda i livelli di cui sopra qui si può aggiungere che nella pratica le normali attività di controllo appartengono all'operatività ordinaria, la classica infezione da virus o un normale SPAM comporta un minimo impatto, i ritardi nel fornire un servizio già comporta un impatto significativo, accessi non autorizzati, penetrazioni indesiderate nel sistema, alterazione o distruzione di dati, danneggiamenti di apparecchiature hanno un impatto elevato e, nella forma più estrema, comportano l'attivazione di un processo di disaster recovery.

Naturalmente il piano ha una struttura articolata in fasi logiche legate al susseguirsi delle azioni che devono essere svolte: sicuramente c'è una fase di preparazione, ossia il piano deve essere formalizzato e pronto all'uso (sapere cosa fare in caso di incidente fornisce un prezioso aiuto per dominare il fenomeno). Alla fase preparatoria segue una fase identificativa, ossia bisogna accorgersi che un dato evento è acca-

duto, ovvero occorre rilevare l'evento per avviare le azioni più opportune. A dare una mano in questa fase possono essere di aiuto alcuni indicatori quali: crash di sistemi; presenza di nuovi account o insolita attività per un dato account; file non riconosciuti o sospetti come data e dimensione; anomalie nei file di log e di accounting; mancata disponibilità di sistemi e servizi; inspiegabile mancanza di risorse di elaborazione o di prestazioni negli apparati.

Una volta conclusa la fase identificativa viene avviata quella di contenimento, ossia una volta che ci si è resi conto di un evento indesiderato occorre lavorare per contenere al minimo gli effetti sull'intera organizzazione. Segue, poi, la fase di rimozione degli effetti attraverso variazioni di configurazione o aggiornamenti del software. Ripristinare il sistema rappresenta la fase successiva: occorre riportare il sistema nelle ordinarie condizioni. Si rammenti che nella fase di maggiore crisi questa rappresenta la fase di rientro dalle condizioni di disaster recovery avviate nelle fasi precedenti. L'ultima fase è quella di relazionare sull'evento indesiderato e sugli effetti da esso provocati. Questa fase è delicata in quanto è basilare per eventuali azioni legali e soprattutto influenza l'analisi del rischio e può comportare la modifica delle politiche di sicurezza.

Nella fase di contenimento sono altresì attivate tutte le misure necessarie ad identificare l'ambito della crisi. In particolare, se essa è locale alla organizzazione oppure se si è estesa fuori dai suoi confini. In tal caso occorre identificare i canali sui quali l'emergenza si sta estendendo e contattare immediatamente i referenti delle organizzazioni che sono interdipenti alla organizzazione che è fonte dell'emergenza.

Nel seguito si illustra un esempio di emergenza causata in un Caso di attacco informatico al software (WORM):

Watch. Continuous state of normal watchfulness. The emergency process moves into the Alert phase when a First Responder (CERT/ISAC etc.) is made aware of a potential emergency.

Alert. All First Responders are contacted, One of three things can occur during this phase: 1) the First Responders declare an emergency, 2) the First Responders declare that the incident is manageable without declaring an emergency, or 3) the First Responders cannot

reach a decision and call in director-level management (GOV.CERT) for further clarification. Should the emergency declaration be warranted, the next phase, Mobilize, begins.

Mobilize. If an emergency is declared, the First Responders convene the Leadership Summit and call leads from additional teams. After the summit, the teams split into three groups, the Technical Team , the Emergency Communication Team , and the Emergency Executive Team. The ECT in turn will mobilize the Emergency Response Teams in each CI Organization involved. Once all teams are mobilized and briefed, the process moves to the next phase, Assess and Stabilize.

Assess and Stabilize. Teams mobilize any and all resources required to quickly identify/create remediation option(s). The teams should work at an accelerated pace to understand the problem, develop an emergency plan to address the situation, and deliver a workaround or fix. The TT team diagnoses the problem and defines a fix, workaround, or remediation. It is then tested to ensure it works and distributes the fix and/or workaround information. The ECT develops communications. the process transitions to the Recover phase.

Recover. The TT refine the fix (if needed) and develop additional tools that can aid in remediation (if applicable). These updates and additions are posted to the Web with updated messaging.

Resolve. Emergency operations are shut down and crisis information is archived. A post-mortem is held to gather lessons learned and suggestions for improving the response process. Teams return to normal watchfulness.

4.2. GRUPPI DI GESTIONE DELLA CRISI

Sono state individuate, dunque, tre componenti: una di vertice, una di coordinamento, una tecnico operativa. Tutte insieme costituiscono la struttura dedicata alla gestione dell'emergenza. Questa sezione chiarirà le loro caratteristiche ed i compiti nelle condizioni ordinarie e nelle condizioni di crisi.

La componente di vertice

La componente di vertice è la massima struttura dell'organizzazione preposta alla gestione dell'emergenza ed è responsabile delle scelte più critiche (quando si entra in un vero e proprio stato di crisi ossia si è in condizioni di disaster) e del coordinamento strategico dell'iniziativa, assumendo il controllo di tutte le operazioni e avendo responsabilità piena sulle decisioni che condizionano il buon esito delle misure messe in atto. Ovviamente la sua azione è diretta o indiretta attraverso le altre componenti, ma ad ogni modo mantiene il controllo su tutto il processo. La componente di vertice, dunque, promuove le necessarie iniziative per avere successo nelle operazioni, si avvale della componente di coordinamento affinché abbia disponibilità di strumenti e competenze per tutte le decisioni da prendere ed ha competenza in particolare nelle aree di:

- dichiarazione di crisi
- avvio della fase di ripristino
- comunicazioni e rapporti con l'esterno (mezzi di comunicazione, cittadini, organizzazioni pubbliche e private)
- implicazioni legali
- rapporti con l'interno
- fase di rientro
- dichiarazione di rientro.

I rapporti con l'esterno e le implicazioni legali possono passare attraverso le classiche componenti organizzative del tipo: ufficio stampa, ufficio comunicazioni, ufficio legale laddove esistenti come strutture. Particolare cura va posta nei rapporti interni: chiarezza, precisione e tempistica sono parametri per avere successo e questo perché una situazione di emergenza si accompagna sempre a incertezza, difficoltà di comunicazione, necessità di esprimersi al massimo al fine di governare delle fasi difficili. La comunicazione con i diretti addetti all'organizzazione di gestione si basa sul fatto che chi ha l'incarico di operare comunica, su richiesta all'organismo superiore lo stato dell'ar-

te ed apprende le decisioni che lo riguardano. La fase di rientro, pur attuata dai gruppi operativi, deve essere continuamente monitorata dalla componente di vertice.

Nelle normali condizioni la componente di vertice si riunisce, con periodicità almeno annuale, al solo scopo di esaminare lo stato progettuale, dal punto di vista delle criticità, della gestione delle emergenze con particolare riferimento al passaggio allo stato di crisi ossia di recovery. Non è escluso l'allestimento di simulazioni per la verifica e la tenuta della componente decisionale.

In caso di escalation legata ad eventi disastrosi, la componente di vertice viene coinvolta da quella di coordinamento o da quella tecnica. Dal momento del coinvolgimento prende il controllo di tutte le operazioni. Per primo acquisisce lo stato dell'arte e valuta misure immediate di contenimento degli effetti legati agli eventi appena appresi. Particolare attenzione va indirizzata alla salvaguardia della salute di chi è coinvolto nell'evento ed alla salvaguardia delle principali infrastrutture di cui l'organizzazione si serve. Verificata l'incapacità di erogare servizi adeguati all'utenza, la componente di vertice avvia la fase di ripristino, che può anche contemplare l'attivazione di un sito alternativo di recovery, nel caso in cui la crisi evolve in disastro, tale decisione viene immediatamente rappresentata alle altre due componenti. Da questo momento questa componente governa l'intero processo di gestione vigilando affinché si operi in coerenza con la missione istituzionale.

Per meglio svolgere le attività di gestione dovrà essere predisposto apposito elenco contenente, per la componente di vertice i dovuti riferimenti di titolari, loro delegati e/o assistenti. Tale elenco sarà mantenuto ed aggiornato dalla componente di coordinamento, sarà riservato, sarà depositato in luogo sicuro e conterrà per ogni componente almeno i seguenti dati: indirizzo privato, indirizzo pubblico, numeri telefonici fissi e mobili, indirizzo di posta elettronica. La componente di coordinamento assicura supporto diretto alla componente di vertice, poiché quest'ultima dovrà prendere decisioni rapide e mirate. In caso di crisi, la componente di vertice ha bisogno di contare su un supporto operativo a 360° per le attività legate alle seguenti aree:

- logistica a garanzia di eventuali spostamenti, anche in collabo-

razione con altri organi e di adeguate sale attrezzate alla gestione durante la fase di crisi, tali sale vanno descritte in apposito documento;

- tecnica a garanzia del funzionamento e dell'accesso alle infrastrutture ICT predisposte;
- informativa a garanzia di un continuo e preciso aggiornamento delle notizie provenienti dai canali pubblici di comunicazione;
- comunicativa di processo a garanzia della raccolta di tutti i rapporti di stato provenienti dalla componente di coordinamento e da quella tecnica e di rapida diffusione di tutte le istruzioni da impartire ai gruppi dell'organizzazione di gestione;

Il supporto alla componente di vertice da parte di quella di coordinamento si estende anche alla valutazione di strategie di comunicazione verso l'esterno e l'interno ed alla valutazione dei relativi mezzi da utilizzare per le diverse tipologie di comunicato; alla definizione di iniziative a carattere finanziario necessarie ad assicurare risorse tempestive; alla definizione di comportamenti e formulazione di specifici messaggi volti a sensibilizzare chi è direttamente coinvolto nelle operazioni di gestione e a valorizzare il relativo ruolo; alla verifica del grado di sicurezza offerto dalle configurazioni adottate per affrontare la crisi e protezione dei dati in tutte le situazioni.

Dovrà essere, poi, disponibile un ulteriore elenco di persone che sono chiamate a fornire supporto specifico. Tale elenco sarà mantenuto ed aggiornato dalla componente di coordinamento, sarà riservato, sarà depositato in luogo sicuro e conterrà per ogni componente almeno i dati seguenti indirizzo privato, indirizzo pubblico, numeri telefonici fissi e mobili, indirizzo di posta elettronica.

Per quanto riguarda l'aspetto comunicativo giova dare qualche chiarimento in più. Alla componente di vertice sono riservate le decisioni definizioni di messaggi significativi come l'entrata nello stato di crisi, la dichiarazione di rientro e qualunque altra dichiarazione che riguarda profondi cambiamenti sulla conduzione dei processi e dei servizi erogati, nonché, per la comunicazione esterna, informativa sulla

situazione, le ragioni della crisi, le misure messe in atto e le prospettive di ripristino della normalità.

La componente di coordinamento

La componente di coordinamento costituisce il collegamento tra la componente di vertice ed eventuali strutture di vari centri di responsabilità (laddove esistenti) con particolare attenzione alla disponibilità delle informazioni ed alla continuità operativa in funzione delle esigenze legate alle attività amministrative e dei vincoli esistenti. Essa supporta la componente di vertice nel processo di gestione e coordina le iniziative indirizzate ai centri di responsabilità, attraverso i referenti di questi ultimi. Promuove, inoltre, l'aggiornamento, da parte dei referenti, della lista dei processi amministrativi; aggiorna, con la collaborazione della componente tecnica, la lista dei processi supportati e non, da parte dei servizi informatici in eventuale situazione di crisi che sta assumendo i connotati del disaster (indicazioni utili a definire delle procedure alternative).

Nelle ordinarie condizioni la componente di coordinamento promuove la cultura della continuità operativa presso tutte le strutture, anche grazie al supporto dei referenti dei centri di responsabilità; documenta eventuali scenari legati a particolari situazioni e stati di crisi, affinché possano essere comprese eventuali misure alternative da prevedere; promuove l'iniziativa di revisione periodica, in relazione a mutate esigenze, della cosiddetta analisi di impatto, essenziale quando la crisi assume i connotati di disaster; promuove la realizzazione, presso i vari centri di responsabilità, di procedure alternative per quei processi critici non supportati dallo strumento automatico; mantiene documenti ed elenchi necessari al coordinamento delle operazioni; prepara ed organizza test; pianifica le necessarie attività di sensibilizzazione e formazione.

Nelle condizioni di crisi la componente di coordinamento raccoglie, grazie ai predetti referenti, le indicazioni sulle aree critiche; coordina gli interventi di portata limitata e sottopone alla componente di vertice, in caso di escalation, tutte le situazioni gravi; diffonde le iniziative prese dalla componente di vertice presso i centri di respon-

sabilità e ne verifica l'attuazione, con l'ausilio dei referenti; supporta la componente di vertice nella gestione della crisi. Anche in questo caso occorre un elenco dei membri della componente di coordinamento, con tutti i riferimenti, mantenuto ed aggiornato dalla stessa.

La componente tecnico operativa

La componente tecnico operativa gestisce gli aspetti tecnici, in particolare il processo di escalation dove, man mano che l'impatto dell'evento emergenza diventa sempre più significativo, il numero di risorse coinvolte diventa sempre crescente. Essa avrà ovviamente un responsabile nei confronti delle altre due componenti ed un coordinatore dei vari gruppi e sarà composta a sua volta da diversi gruppi con compiti ben precisi e delineati:

- *gruppo di valutazione,* ossia specialisti di sicurezza informatica e di conduzione di sistemi di elaborazione, con il compito di reperire le informazioni riportate da fonti selezionate e produrre report informativi; durante la crisi, individua ad esempio l'impatto nelle risorse dei virus informatici e definisce il piano degli interventi da trasmettere al gruppo di supporto tecnico;
- *gruppo di supporto tecnico,* ossia specialisti hardware, software e di infrastrutture di comunicazione, con il compito di rimuovere gli effetti causati dall'incidente;
- *gruppo di comunicazione,* ossia di specialisti con il compito di trasmettere messaggi agli utenti, interagendo con i referenti tecnici delle diverse strutture e la parte dedicata al help-desk.
- *gruppo di rientro,* ossia di specialisti con il compito di garantire l'efficacia della procedura di rientro presso il sito di esercizio e la ripresa delle attività in regime normale. Particolare attenzione va posta a questa attività, in quanto i toni del disastro vanno dallo spostamento di alcuni servizi informatici per un tempo non molto lungo al sito di recovery alla distruzione del sito di esercizio che comporta necessariamente una situazione precaria per molti mesi.

La scalabilità della reazione verso un livello superiore, è in relazione alle caratteristiche dell'evento incidente, quali:

- la modalità di diffusione dell'evento;
- l'impatto sull'operatività;
- la velocità di propagazione;
- la stima dell'impatto stesso.

Nelle condizioni di *operatività normale* il gruppo di valutazione controlla le fonti di allarmi e le notifiche di minacce.

Nelle condizioni di i*mpatto minimo* (livello basso) una possibile minaccia è stata individuata e vengono stabilite le contromisure. All'occorrenza ci sono messaggi con la richiesta delle azioni da intraprendere. Il gruppo di valutazione stabilisce le iniziali azioni, attiva il gruppo di supporto ed il coordinatore valuta l'escalation verso il livello significativo. Il coordinatore, ricevuta l'informativa la trasmette agli utenti insieme alle azioni difensive attuali e future.

Nelle condizioni di *impatto significativo* (livello medio) la minaccia si è manifestata; si stabiliscono le azioni da intraprendere per contenere l'effetto e rimuovere la causa. All'occorrenza ci sono messaggi con la richiesta delle azioni da intraprendere. Il gruppo di valutazione comunica al gruppo di supporto tecnico le azioni richieste, avverte il coordinatore circa la nuova minaccia, fornisce al coordinatore un rendiconto della situazione creatasi. Il gruppo di supporto tecnico delinea, in collaborazione col gruppo di valutazione, la sequenza di azioni ai fini del contenimento degli effetti, e verifica funzionalmente le azioni definite. Il coordinatore comunica al responsabile il piano degli interventi ed appronta un documento contenente informazioni sui tempi di verifica degli eventi e sui dati e programmi coinvolti. Il responsabile allerta il gruppo di comunicazione ed i referenti applicativi, definisce il contenuto della comunicazione e valuta le condizioni di possibile innesco di un livello successivo. Il gruppo di comunicazione invia messaggi indicanti le azioni che si devono intraprendere.

Nelle condizioni di *impatto elevato* la minaccia si è diffusa ampiamente; si stabiliscono le azioni da intraprendere per contenere l'effet-

to e rimuovere la causa. All'occorrenza ci sono messaggi con la richiesta delle azioni da intraprendere e si intraprendono le eventuali azioni legali. Il responsabile attiva l'unità di crisi, mantiene un collegamento verso i referenti dei centri di responsabilità e verso il management. In caso di disastro si attiva la componente di vertice (con l'ausilio della componente di coordinamento). Sono definiti i messaggi e la raccolta di quanto necessario per eventuali azioni legali. Il coordinatore coordina l'unità di crisi ed avvia la registrazione cronologica degli eventi accaduti e degli eventuali effetti ed interagisce col responsabile. Il gruppo di comunicazione invia i messaggi predisposti. Il gruppo di valutazione continua nella sua azione di controllo delle fonti di allarme, e avvia un controllo continuo sull'efficacia delle azioni in corso per respingere la minaccia. Il gruppo di supporto tecnico continua nell'applicazione delle azioni di contrasto alla minaccia sintetizzandole in un report.

La fase di chiusura dell'incidente presuppone un rapporto per il management, da parte del responsabile, contenente l'anagrafica di quanto accaduto a partire dalla registrazione cronologica degli eventi, azioni ed impegni che sono stati richiesti dal piano di reazione, la stima dell'impatto, l'efficacia delle azioni intraprese, eventuali accorgimenti a politiche e procedure, eventuali coinvolgimenti di strutture (interne ed esterne).

Nel caso che si rientri da una situazione di disaster recovery il gruppo di rientro dalla crisi avrà una lunga serie di azioni da svolgere, dalla pianificazione delle attività di rientro al rilevamento delle strutture danneggiate o distrutte, all'elencazione di eventuali apparati da sostituire e quindi da acquistare, alle attività di verifica dell'infrastruttura ripristinata, alla predisposizione di relazioni per la componente di vertice sullo stato di avanzamento del rientro. Nelle ordinarie condizioni è coinvolto nello studio di diverse strategie di rientro in relazione ai diversi scenari di disastro. (vedasi il paragrafo sul rientro alla normalità).

4.3. RUOLO DELLA COMUNICAZIONE DURANTE LA CRISI

La comunicazione riveste un ruolo fondamentale per l'efficacia di tutta l'organizzazione preposta alla gestione dell'emergenza. Deve essere predisposta la natura e la tipologia della comunicazione nelle varie condizioni di verifica con dei tag ben precisi e stili ben delineati, in relazione a chi è rivolto (comunicazione esterna e comunicazione interna). In generale alla componente di vertice è riservata la definizione dei messaggi più significativi quali ad esempio la dichiarazione dello stato di crisi e la dichiarazione dello stato di rientro, o dichiarazioni ritenute particolarmente significative che comportano, ad esempio, cambi nella conduzione di processi amministrativi o variazioni di livelli di servizi erogati. Nella pura gestione della comunicazione esterna, particolare attenzione a non diffondere paure ingiustificate. Inoltre riveste particolare importanza tutta la comunicazione rivolta verso i gruppi esterni quali Computer Emergency Response Team (CERT) e Information Sharing And Analysis Center (ISAC). Tali gruppi, come illustrato al capitolo 6 vanno considerati come gruppi a valore aggiunto per un monitoraggio proattivo ed una fonte pregiata e formativa per il *lesson learned*.

Per quanto riguarda l'utilizzo di canali trasmissivi messi a disposizione dai media la messaggistica conterrà, ad esempio, una sintetica descrizione della nuova situazione venutasi a creare, le ragioni e le prospettive di riconduzione alla normalità. Per quanto riguarda la comunicazione interna probabilmente questa è meno problematica in quanto impatta personale specializzato e collaudato alle attività da svolgere, con qualche attenzione in più per la normale utenza al fine di non creare disarmonie di comportamento (con l'ausilio anche della componente sindacale).

Durante le emergenze le telecomunicazioni rivestono un ruolo primario perché sono indispensabili al coordinamento delle attività. Inoltre possono risentire di pesanti effetti durante le emergenze, sia perché oggetto di attacchi (fisici e logici) sia perché congestionate dal traffico che si innesca. Si rimanda, per un loro approfondimento al capitolo 5.

4.4. RIENTRO ALLA NORMALITÀ

Il rientro alla normalità rappresenta un aspetto molto variabile e sensibile in tutte le emergenze, può diventare infatti attività molto lunga e complessa in relazione ai danni subiti. Il gruppo che gestisce il rientro sarà pertanto responsabile di aspetti che potrebbero rivelarsi anche molto lunghi e complessi.

Il rientro alla normalità richiede un'attenta attività di preparazione e predisposizione, infatti, non potendo prevedere i tipi di danni subiti, i possibili scenari che si possono presentare sono dei più diversi e giungono fino alla completa distruzione del sito ordinario. Pertanto può essere necessaria anche un'attività di ripristino molto lunga. Vanno innanzi tutto valutate le condizioni di rientro, va poi fatto un piano di dettaglio e quindi va gestita la comunicazione sia interna sia esterna.

Le decisioni sui tempi e sulle modalità di rientro spettano alla componente di vertice, la quale si avvale delle informazioni fornite dalla componente di coordinamento. Fin dalla dichiarazione di crisi (che nella sua accezione più alta significa recovery) la squadra di rientro della componente tecnica acquisisce informazioni sui danni subiti dall'infrastruttura di esercizio e valuta i possibili scenari di recupero e ripristino delle normali condizioni di funzionamento. Gli scenari sono forniti alla componente di vertice, che li analizza in base ai tempi, ai modi, ai costi e ad eventuali rischi connessi. Per meglio svolgere il proprio compito, si è detto, che ci si avvale delle informazioni fornite dalla componente di coordinamento, tali informazioni, in generale, riguardano i processi fermi, i sistemi posti sotto recovery e quelli andati perduti, i dati da verificare ai fini dell'integrità e quelli accumulati con procedure manuali.

Quanto finora detto corrisponde a quella tecnicamente definita come la fase della valutazione delle condizioni di rientro.

Dopo di questa ci si predispone al rientro, il che significa che è stata scelta la soluzione di rientro e sono noti i tempi di attuazione. In base a tale soluzione saranno attivate tutte le azioni di ripristino delle ordinarie condizioni. L'elemento di riferimento è il cosiddetto piano di rientro, ossia un vero e proprio piano di azione da attivare

quando la componente di vertice darà il via alle operazioni di rientro. Il piano viene predisposto dalla squadra di rientro della componente tecnica e approvato dalla componente di vertice. Il piano, per essere efficace, dovrà comprendere:

- procedure di riattivazione dei sistemi di esercizio;
- procedure di allineamento dei dati con l'eventuale sito di ripristino;
- procedure di verifica dell'integrità dei dati;
- procedure di ripristino dei dati corrotti;
- sequenza di passaggio dell'elaborazione in esercizio;
- sequenza di riattivazione dei servizi non destinati al recovery;
- sequenza di riattivazione di eventuali collegamenti periferici;
- sequenze di test e controlli.

L'inizio delle attività di rientro viene comunicato all'intera organizzazione, quest'ultima si atterrà al piano e procederà con le necessarie attività.

Apposite comunicazioni vengono studiate per l'esterno, ossia cittadini, aziende, enti, allo scopo di informare sui tempi di ripristino delle ordinarie condizioni e su quanto necessario per le fasi di rientro. Per il periodo di passaggio dal sito di ripristino a quello di esercizio può accadere che il livello di servizio assicurato sia inferiore anche a quello minimo garantito per il periodo di transizione e quindi risulta necessario predisporre misure opportune.

La gestione del rientro prevede, dunque, una serie di azioni che devono seguire il piano predisposto all'occorrenza. L'esecuzione delle operazioni pianificate per la ripartenza del sistema e dell'allineamento dati sono di responsabilità della squadra di rientro della componente tecnica, mentre alla componente di vertice spetta la vigilanza sul rispetto del piano, in collaborazione con la componente di coordinamento.

La componente di coordinamento e la componente tecnica hanno la responsabilità di coordinare tutti gli interventi necessari per aggiornare i sistemi informatici con i dati raccolti con procedure alter-

native durante il periodo di recovery. Allorquando saranno stati ripristinati i dati ospitati sui sistemi critici, i proprietari dei processi amministrativi avviano il processo di riallineamento delle basi informative con i dati eventualmente raccolti secondo modalità alternative.

Una volta che tutte le verifiche previste saranno felicemente concluse, la componente di vertice dichiarerà la fine del periodo transitorio ed il controllo dell'organizzazione tornerà alle ordinarie strutture. Nelle immediate fasi seguenti il ripristino della normalità, la componente di coordinamento raccoglierà le eventuali segnalazioni di problemi legati al ripristino dei processi amministrativi e coordinerà gli interventi a supporto.

La componente coordinamento e la componente tecnica potranno valutare la creazione di strutture dedicate al supporto degli utenti e di strutture tecniche di valutazione in grado di rispondere a tutti i problemi non convenzionali derivanti dal carattere eccezionale degli eventi.

Quando anche la sequenza di problemi post rientro sarà esaurita e l'organizzazione preposta alla gestione dell'emergenza non ha più oneri specifici, può essere promosso, dalla componente di coordinamento in collaborazione con quella tecnica, un vero e proprio processo analitico degli eventi trascorsi, delle reazioni, delle soluzioni adottate, delle criticità emerse.

Quest'attività ha un'importanza notevole in quanto permette la scoperta il ritrovamento di eventuali punti deboli nell'organizzazione e ne promuove il miglioramento. Si parte dalla raccolta ed analisi dei documenti prodotti durante la crisi, allo scopo di rappresentare i processi decisionali e le sequenze operative. Si esamina, poi, l'esito di ogni importante decisione, in relazione alle aspettative ed agli eventi. Si valuta l'efficacia delle sequenze operative e si modificano eventualmente organizzazione, metodi e tecnologie.

5 - La gestione delle telecomunicazioni nelle situazioni di emergenza

La difesa e la protezione civile sono rappresentate dal complesso delle misure da predisporre e dalle attività da porre in atto al fine di fronteggiare emergenze determinate da eventi naturali, incidenti volontari o casuali, da fatti calamitosi, da crisi internazionali o in caso di conflitto bellico.

Costituiscono materia della difesa e della protezione civile i seguenti settori:

- Continuità dell'azione del governo
- Telecomunicazioni e sistema di allarme
- Salvaguardia dell'apparato economico e logistico
- Salvaguardia della sanità pubblica
- Informazione pubblica, addestramento alla protezione e salvaguardia dei beni artistici e culturali.

Per quanto riguarda la competenza specifica del Ministero delle comunicazioni i settori di interesse sono il secondo ed in parte il sesto.

In particolare il settore "Telecomunicazioni e sistema di allarme" comprende tutto ciò che è necessario per assicurare:

- La funzionalità delle telecomunicazioni
- La diramazione degli stadi e stati di allarme

Per quanto riguarda il settore "Informazione pubblica, addestramento alla popolazione ecc." il Ministero delle comunicazioni può essere interessato in quanto organismo che rilascia le licenze, le concessioni e le autorizzazioni soprattutto nel settore radiotelevisivo, e come tale essere parte attiva nel coinvolgimento degli operatori del settore nella fase di informazione della popolazione sui possibili pericoli e relativi stati di emergenza e di allarme.

5.1. IMPORTANZA DELLE TELECOMUNICAZIONI NEL SETTORE DELLA DIFESA CIVILE E NELLA PROTEZIONE CIVILE

In qualsiasi situazione di emergenza la possibilità di "**comunicare**" è di vitale importanza, in quanto solo attraverso le comunicazioni si possono ricevere informazioni sull'evolversi delle situazioni e di conseguenza impartire disposizioni e raccogliere risorse. In particolare, nel caso di eventi catastrofici, riveste speciale importanza il mezzo di comunicazione via radio. Infatti le caratteristiche di flessibilità e di facilità di installazione rendono il mezzo radio indispensabile nella gestione delle emergenze, soprattutto nelle fasi iniziali quando la facilità di dispiegamento e di mobilità consentono di allestire in tempi brevi le strutture necessarie a far fronte alle esigenze di comunicazione, quando ancora non è pensabile di far ricorso ai mezzi fissi quali centrali telefoniche di emergenza, che peraltro, anche in fase di operatività hanno bisogno di collegamenti via radio per poter essere connessi alla rete fissa.

5.2. IMPIEGO DELLE TELECOMUNICAZIONI NELLE DIVERSE FASI DELL'INTERVENTO

I sistemi di telecomunicazioni trovano ampio impiego in tutte le fasi connesse ad un intervento di emergenza, in alcuni casi, già a partire dalla fase precedente al manifestarsi dell'evento; l'uso del mezzo radio è vitale nel compito di monitoraggio dei segnali che possano dare una notizia del possibile avverarsi di un evento. In particolare l'utilizzo dei mezzi di TLC avviene in ciascuna delle seguenti fasi:

- Allerta al verificarsi dell'evento
- Uso delle TLC sul teatro dell'evento
- Ripristino dei sistemi di TLC pubblici
- Informativa alla popolazione
- Intensificazione dei controlli a protezione delle comunicazioni.

5.2.1 Segnalazione di allerta per un evento che richieda un intervento di protezione civile

Il ruolo dei sistemi di telecomunicazione, specialmente quelli che utilizzano il mezzo radio, è di importanza cruciale sia nell'allertamento tempestivo al verificarsi di un evento sia, in alcuni casi, nel prevedere il sopraggiungere di una emergenza. In ogni caso il verificarsi o la previsione di un evento che richiede l'attivazione dei mezzi della protezione civile si basa, per raggiungere la massima efficienza, su reti di telecomunicazioni che trovano impiego nei seguenti campi:

- Raccolta dati da reti di monitoraggio
- Segnalazione degli eventi agli Enti preposti
- Segnalazione e raccolta ed inoltro informazioni tramite il mezzo radio

5.2.1.1 Reti di monitoraggio

È ben noto che gli Enti addetti alla protezione civile gestiscono complesse reti che, attraverso il mezzo radio, consentono il trasferimento in tempo reale, a centri di studio e ricerca o a centrali operative della protezione civile, di dati di monitoraggio raccolti in località normalmente o eccezionalmente a rischio. Tipici esempi di reti di questa natura sono le reti di monitoraggio delle aree sismiche o vulcaniche e dei bacini idrografici delle zone soggette ad alluvioni. Lo scopo di tali reti, il cui utilizzo viene autorizzato dal Ministero delle comunicazioni, che assicura anche, attraverso i suoi organi periferici, la protezione contro le interferenze, è quello di mantenere un continuo controllo

delle situazioni di rischio, onde attivare azioni preventive di tutela della popolazione, in caso di raggiungimento di valori di soglia pericolosi per i parametri sotto controllo.

Come accennato, e come meglio si dirà in seguito, di estrema importanza è l'azione di prevenzione delle interferenze svolta dal Ministero delle comunicazioni per quei collegamenti, e sono molti, che viaggiano sui mezzi radioelettrici. Si veda in proposito il D.M. 22.12.98 che, all'art. 1, riserva una coppia di frequenze in gamma UHF per il sistema multiaccesso di sorveglianza sismica e vulcanica della Sicilia orientale, nell'ambito del progetto "Poseidon", e per l'integrazione delle reti di monitoraggio esistenti.

5.2.1.2 Segnalazione degli eventi agli enti preposti

Tutte le strutture di telecomunicazioni pubbliche e private possono, in sostanza, essere considerate, nel loro complesso, come un sistema di telecomunicazioni disponibile per svolgere le attività ed i compiti del servizio nazionale della protezione civile per quanto riguarda la previsione e la prevenzione dell'emergenza. Pertanto il Servizio nazionale della protezione civile può sempre acquisire, anche avvalendosi della collaborazione del Ministero delle comunicazioni, tutti i servizi di telecomunicazione terrestri, satellitari fissi e mobili di cui avesse bisogno per la gestione dell'emergenza.

5.2.1.3 Segnalazione ed inoltro informazioni tramite il mezzo radio

Può verificarsi che l'evento calamitoso metta fuori uso, nella zona interessata all'evento medesimo, tutte le strutture di telecomunicazione terrestre ordinarie; in tal caso si rende necessario ricorrere a mezzi alternativi che non siano stati danneggiati quali i **sistemi satellitari**, sia mobili che diffusivi, gli apparati terminali **mobili cellulare GSM e TACS**, gli apparati **Campali**, gli apparati **radioamatoriali** eventualmente presenti nell'area. In particolare questi ultimi possono essere molto utili nelle prime fasi dell'emergenza, grazie alla loro capillarità e semplicità di installazione ed uso, soprattutto per la raccolta di

informazioni vitali sull'entità dei danni, il tipo di assistenza richiesta, la praticabilità delle strade di accesso e informazioni simili; ovviamente la natura di tale tipo di comunicazione fa sì che la stessa diventi meno utile, man mano che vengono ripristinate o dispiegate le strutture di comunicazione pubbliche su rete fissa.

5.2.2 Uso delle telecomunicazioni sul teatro dell'evento

Superata la fase della prima emergenza la gestione delle comunicazione viene svolta non più dai mezzi di cui si è detto in precedenza ma dalle reti istituzionalmente gestite dal Dipartimento della protezione civile, che ha a disposizione apparati funzionanti su 10 coppie di frequenze in VHF ed UHF, assegnate sull'intero territorio nazionale dal D.M. 22.12.1998.

La rete che utilizza tali frequenze è tale da essere repentinamente dispiegata sul territorio, e può consentire il ripristino delle comunicazioni più essenziali per l'organizzazione dei soccorsi in attesa che gli organi istituzionali di TLC provvedano a ripristinare i propri servizi sia attraverso lo spostamento sul territorio di apparecchiature trasportabili sia tramite la "riparazione" delle proprie strutture danneggiate. Gli stessi organi istituzionali possono installare, in attesa del ripristino della funzionalità delle reti, strutture provvisorie, ed in particolari le reti dei servizi mobili possono essere installate sul teatro dell'evento strutture trasportabili collegati alle reti fisse tramite ponti radio.

5.2.3 Ripristino dei sistemi di comunicazione pubblici

La fase di ripristino ha per scopo di restituire operatività alle strutture pubbliche e private di telecomunicazioni al fine di consentire la fine della fase di emergenza e ritornare all'utilizzo, anche da parte della popolazione civile, dei mezzi di comunicazione. Un ruolo importante giocano in questa operazione la società TELECOM Italia per la telefonia fissa e la società RAI per la radiodiffusione, le quali hanno proprie strutture pronte ad intervenire in situazioni di emergenza, sia per fornire supporto durante la gestione dell'emergenza sia per avvia-

re in tempi rapidi il ripristino di una situazione di operatività, il più vicino possibile alla normalità, in tempi brevi. Peraltro le dette società testano periodicamente le loro strutture attraverso la partecipazione alle esercitazioni di difesa del territorio (DITEX), coordinate dalle prefetture e simulano situazioni di emergenza al fine di testare la capacità di risposta del sistema. Il Ministero delle comunicazioni svolge in tale ambito, come del resto sarebbe chiamato a fare nei casi di effettiva emergenza, compiti di coordinamento nei confronti degli operatori del settore TLC. A tale proposito partecipa ai Comitati Provinciali di Difesa Civile (C.P.D.C.), a livello nazionale, ed ai Comitati Consultivi Compartimentali delle TLC (CCCTLC), a livello locale, tramite gli Ispettorati territoriali.

La nuova realtà conseguente alla liberalizzazione dei servizi di TLC ha portato alla nascita di numerosi altri operatori privati il cui contributo può essere molto importante nelle situazioni di emergenza, soprattutto per quanto attiene agli operatori di telefonia mobile, in quanto le caratteristiche del servizio svolto da essi li rende particolarmente idonei a fornire servizio in situazioni di emergenza. In proposito il Ministero ha avviato con le società TIM, OMNITEL e WIND dei contatti per definire un documento congiunto sulla "Utilizzazione del GSM nei periodi di emergenza".

5.2.4 Informativa alla popolazione della zona teatro dell'evento

La possibilità di informare la popolazione sull'evento in atto e di diffondere istruzioni in merito alle strutture di emergenza attivate, sul modo in cui usufruirne e sulle iniziative intraprese è di vitale importanza sia per tenere sotto controllo e limitare fenomeni di allarmismo sia per attivare azioni preventive di difesa da pericoli imminenti. In tale ottica appare essenziale il compito delle stazioni di radiodiffusione televisiva e radiofonica a livello nazionale e locale, sia pubbliche che privare. Nell'attività di coinvolgimento delle società interessate risulta essenziale il ruolo di coordinamento proprio del Ministero delle comunicazioni.

5.2.4.1 Ruolo delle emittenti locali

È ovvio che l'informazione relativa ad una situazione di emergenza deve raggiungere specificamente l'area interessata dall'emergenza stessa, per cui appare evidente l'importanza di poter coinvolgere l'emittenza radiofonica e televisiva locale, che ha capillarità anche a livello provinciale. In tali situazioni il Ministero delle comunicazioni può svolgere sia il compito di interfaccia tra le autorità di protezione civile e le emittenti, sia quello di attivazione di queste ultime e di reperimento e tutela delle risorse spettrali necessarie. A tal proposito una situazione del genere si è verificata nel 1998 in occasione dell'alluvione di Sarno, quando l'Ispettorato Territoriale di Napoli è stato chiamato a reperire, di intesa con la RAI, una frequenza da assegnare ad una emittente radiofonica privata della zona che aveva sottoscritto un accordo con un comune della zona interessata all'alluvione per consentire di diffondere tra la popolazione i preavvisi per eventuali sgomberi in caso di concreto pericolo di nuove frane. In tale occasione il Ministero delle comunicazioni è intervenuto sia a livello locale, per individuare e proteggere la frequenza utilizzata, sia centrale per disporre in tempi rapidi le necessarie autorizzazioni.

5.2.4.2 Ruolo delle emittenti nazionali

Analoga collaborazione può essere immaginata per le emittenti radiofoniche e televisive nazionali nel caso in cui si rendesse necessario estendere a livello nazionale le informazioni particolari non comprese tra quelle normalmente diffuse nei notiziari. Esempi di situazioni del genere sono rintracciabili nella storia di tutte le più grandi emergenze nazionali, durante le quali si è fatto costante ricorso all'emittenza nazionale privata e soprattutto pubblica per diffondere notizie di interesse generale necessarie alla organizzazione dei soccorsi ed alla loro gestione.

5.2.4.3 Circuito nazionale di emergenza

Di recente, sotto il patrocinio del Ministero delle comunicazioni e dell'Autorità per le garanzie nelle comunicazioni, sono stati sottoscritte due convenzioni rispettivamente con gli operatori del servizio di comunicazione mobile e personale e con le Associazioni rappresentative delle imprese di radiodiffusione sonora e televisiva in ambito nazionale e locale, aventi per oggetto la costituzione del *"circuito nazionale dell'informazione d'emergenza"*.

Con tali convenzioni gli operatori radiomobili e le emittenti nazionali e locali si impegnano, con modalità adeguate ai rispettivi mezzi trasmissivi e risorse disponibili a trasmettere ai cittadini informazioni loro fornite dal Dipartimento della protezione civile, nei casi di emergenze, di calamità naturali, di catastrofi o di grandi eventi.

Le emittenti radiofoniche e televisive dirameranno i messaggi in radiodiffusione circolare sulle aree interessate, mentre gli operatori di telefonia mobile invieranno i messaggi tramite SMS.

Il Ministro delle comunicazioni e l'Autorità, in quanto promotori dell'iniziativa, hanno costituito un gruppo di lavoro che ha l'incarico di monitorare la fase operativa dell'accordo.

5.3. IMPORTANZA DEL RUOLO DEL MINISTERO DELLE COMUNICAZIONI

Il ruolo del Ministero delle comunicazioni nella gestione dei sistemi di telecomunicazioni nelle situazioni di crisi è andato modificandosi nel tempo, diventando sempre meno legato ad interventi diretti, sulla scena degli eventi, con proprie strutture e, rivestendo sempre più compiti di coordinamento sia in fase di intervento sia in fase di prevenzione.

Infatti, nell'arco di un decennio, il Ministero ha perduto il ruolo di gestore diretto di servizi di telecomunicazione, quali la rete dorsale interurbana una volta gestita dall'ASST, i servizi di radiocomunicazione mobile marittima, il servizio telex ed il servizio di trasmissione dati, per non parlare di servizi di "comunicazione" quali le poste. La

perdita di tali servizi ha sottratto al Ministero delle comunicazioni gran parte del ruolo attivo, comportando, peraltro, un ampliamento dei compiti di coordinamento.

In effetti nel campo delle TLC si è avuta una trasformazione sostanziale dell'intero sistema con la realizzazione delle privatizzazioni, che hanno comportato la cessione, da parte dello Stato, di attività un tempo gestite direttamente o tramite aziende a totale capitale pubblico. Contemporaneamente si è avuta l'apertura del mercato nel settore con la fine del monopolio di poche aziende (Telecom per la telefonia e RAI per la radiodiffusione) e la comparsa di una pluralità di soggetti, con la conseguenza che la natura privatistica dell'assetto societario dei nuovi e vecchi soggetti ha spinto le aziende a privilegiare l'aspetto commerciale del servizio offerto. Ciò significa che, in assenza di un intervento correttore ed incentivante dello Stato, le aziende sono portate a privilegiare le attività economicamente remunerative abbandonando, o non attivando per niente, strutture destinate ad operare in situazione di emergenza, qualora il mantenimento di tali strutture sia economicamente penalizzante.

Appare quindi evidente quale debba essere in proposito il compito di coordinamento del Ministero delle comunicazioni che può sollecitare le aziende a mantenere attive le strutture di emergenza, anche al di là dello stretto necessario al ripristino, in caso di crisi, del servizio commerciale. Gli strumenti utilizzati per garantire la disponibilità minima indispensabile di risorse di telecomunicazioni nelle emergenze sono due :

- la definizione della figura del concessionario del servizio pubblico
- la definizione degli obblighi di servizio universale.

Il primo caso è quello relativo alla società RAI, che risulta ancora concessionaria del servizio pubblico e come tale ha degli obblighi verso lo Stato che "concede" il servizio. Il secondo invece si applica nella telefonia fissa attraverso l'individuazione di obblighi cui le società licenziatarie, nel caso specifico la sola Telecom Italia, si assoggettano nel fornire prestazioni commercialmente non remunerative a fronte di un compenso economico concordato con la pubblica ammi-

nistrazione. Tale compenso viene prelevato da un fondo cui contribuiscono gli altri operatori del settore che non avendo obblighi speciali possono trascurare le attività utili socialmente me economicamente non convenienti.

Il compito di coordinamento ed iniziativa del Ministero si manifesta anche in via preventiva attraverso l'attività delle gestione e pianificazione delle frequenze, sia in ambito nazionale che internazionale. A tale proposito l'Italia nel corso dell'ultima conferenza mondiale delle telecomunicazioni ha svolto un ruolo attivo nella decisione di inserire nell'agenda della prossima conferenza del 2003 l'argomento relativo agli studi, in ambito internazionale, per l'individuazione di frequenze armonizzate a livello mondiale da utilizzare per la "public safety", al fine di evitare che, in caso di operazioni svolte da organismi provenienti da diversi paesi, ciascuno utilizzi, per gli apparati radio, gamme di frequenze diverse rendendo estremamente difficile lo scambio di informazioni tramite il mezzo radio. Anche per quanto riguarda la partecipazione agli studi preparatori l'Italia sta rivestendo un ruolo primario, avendo assunto il coordinamento degli studi svolti in ambito europeo sull'argomento.

Anche nella nuova ottica quindi il ruolo del Ministero delle comunicazioni nella gestione delle varie fasi dell'emergenza nel campo delle TLC è essenziale in quanto è fondamentale che tra i servizi di protezione civile e i gestori dei servizi vi sia una interfaccia che abbia l'autorità di disporre e coordinare gli interventi dei vari operatori.

Tuttavia il Ministero delle comunicazioni continua, sotto certi aspetti, ad avere un ruolo attivo nella gestione delle telecomunicazioni durante le crisi. Infatti le comunicazioni che maggiormente vengono utilizzate nella fase di emergenza sono quelle via radio, le quali sono quelle che maggiormente possono essere oggetto di interferenza, per cui nell'ambito della difesa civile assume una rilevanza notevole la protezione dalle interferenze, che è compito istituzionale del Ministero stesso e che richiede una partecipazione diretta del personale dello stesso al fine di rendere più efficace la protezione delle comunicazioni nelle situazioni di crisi. Per tale compito il Ministro può avvalersi delle strutture periferiche, gli Ispettorati territoriali, che hanno capillarità regionale e dispongono di strutture tecniche fisse e mobili adibite al

monitoraggio dello spettro operanti anche a livello provinciale, e con capacità di intervento sull'intero territorio regionale di propria competenza.

Un esempio del ruolo di coordinamento del Ministero delle comunicazioni nella gestione di una situazione di emergenza, volta alla prevenzione di rischi per l'intero sistema industriale ed economico del paese, si è avuta in occasione della costituzione e del dispiegamento delle strutture destinate ad affrontare il rischio del Millennium Bug.

Infatti in tale occasione è stato resa operativa una "Unità di gestione", composta da personale designato da diversi Ministeri, tra cui quello delle Comunicazioni, che ha seduto in permanenza presso Forte Braschi dalle ore 09.00 del giorno 31.12.1999 alle ore 12.00 del 4.01.2000. Il compito di tale unità è stato quello di verificare l'eventuale manifestarsi di malfunzionamenti nei sistemi informatici in corrispondenza con il passaggio dall'anno 1999 all'anno 2000, informando un comitato dei Ministri coordinato dal Dipartimento della funzione pubblica, sull'entità di eventuali malfunzionamenti in settori vitali dell'apparato industriale, indicando anche le misure da porre in atto per fronteggiare eventuali emergenze. Il Ministero delle comunicazioni, attraverso un delegato del Ministro, coadiuvato da due collaboratori, ha rappresentato l'interfaccia tra gli operatori del settore delle TLC ed il Comitato; in sostanza i rappresentanti del Ministero delle comunicazioni avevano il compito di acquisire direttamente dagli operatori l'evolversi della situazione, valutare l'impatto di eventuali disservizi e contribuire, per la parte TLC alla definizione del rapporto sullo stato della situazione. In sostanza i rapporti tra gli operatori direttamente presenti presso l'unità di gestione o collegati con lo stesso dalle proprie sale di emergenza, erano curati esclusivamente dal Ministero delle comunicazioni, D'altro canto, nel caso in cui si fossero presentati dei disservizi, sarebbe toccato agli stessi rappresentanti del Ministero definire, di intesa con gli operatori, i possibili interventi necessari a ridurre l'impatto negativo sul sistema paese e dare le necessarie indicazioni al comitato dei Ministri.

Il Ministero delle comunicazioni, nella fase preparatoria, ha svolto il compito di coordinamento degli operatori TLC e di raccordo tra le strutture costituite dagli stessi per la gestione dell'emergenza

Y2K ed il gruppo incaricato di gestire la crisi. In particolare hanno fornito il loro supporto, con presenza diretta, quale back-line del Ministero, presso la sala di controllo le società RAI, TELECOM Italia e TIM, mentre le società OMNITEL, WIND, MEDIASET, Albacom e Poste Italiane S.p.A. avevano allestito unità operative presso le loro sedi, che avevano come terminale per l'invio e la raccolta delle informazioni i rappresentanti del Ministero presso l'Unità di crisi.

La struttura descritta, pur non essendo stata chiamata a gestire situazioni di reale emergenza, in quanto il paese si è dimostrato preparato ad affrontare il problema Millennium Bug, ha comunque dimostrato la capacità di gestire eventuali situazioni di crisi, soprattutto nel settore delle TLC.

6 - Gruppi di monitoraggio e controllo proattivo

Tra le azioni tese ad innalzare il livello di sicurezza, affidabilità e disponibilità delle infrastrutture critiche che utilizzano, in tutto od in parte, una qualunque infrastruttura ICT, particolare importanza rivestono le azioni intese ad assicurare efficienti meccanismi di condivisione ed analisi delle informazioni per fare fronte alle emergenze ICT; ciò in considerazione dell'inestimabile vantaggio che la tempestiva conoscenza del verificarsi di un evento pericoloso offre ai responsabili della protezione e della sicurezza di un'infrastruttura vitale.

L'inadeguato coordinamento, sia a livello internazionale che a livello interno, ed una diffusa inadeguata capacità organizzativa, tecnica e legale sono fra le maggiori cause di insuccesso o di insicurezza nella gestione delle emergenze ICT, la cui trattazione è stata constatata spesso difficoltosa a causa di:

- incapacità d'intervento tempestivo sulle vulnerabilità più critiche per il sovraccarico e cortocircuito delle informazioni;
- difficoltà nell'identificazione di una sorgente affidabile e certificata di informazioni in grado di fornire servizi di allarme;
- difficoltà nel reperimento in tempo reale di informazioni ed istruzioni utili a far fronte ad un'emergenza ICT;
- l'impossibilità di valutare le proprie risorse di sicurezza e di confrontarle con altre realtà simili nell'ambito di uno scambio di esperienze.

Due gli aspetti individuati come particolarmente critici nella realizzazione di sistemi di risposta alle emergenze ICT, specie del tipo attacco informatico (cybercrime):

- *Information Sharing*, inteso come la possibilità di condividere informazioni ed esperienze relative ad emergenze o vulnerabilitàICT;
- *Early Warning*, inteso come capacità di avviso tempestivo dei responsabili delle infrastrutture ICT sulla presenza di nuove vulnerabilità, nuovi pericoli e possibili nuove emergenze.

Appare evidente che fattore determinante per affrontare le emergenze ICT, tra le quali riveste particolare attualità la lotta al crimine informatico rivolta contro le infrastrutture critiche, è la cooperazione tra i settori pubblico e privato, inclusa la comunità scientifica, finalizzata principalmente a:

- individuare congiuntamente sia le vulnerabilità ICT specifiche per ogni singola infrastruttura critica sia comuni a più settori;
- meglio comprendere la natura e l'impatto degli attacchi;
- individuare strategie comuni per rispondere alle emergenze e mitigare in modo coordinato il loro effetti.

Solo la collaborazione tra pubblico e privato può consentire, dunque, un adeguato livello di protezione e di intervento all'insorgere delle emergenze.

Il riconoscimento e la convinzione che solo l'unione degli sforzi di soggetti pubblici e privati ha portato, sulla spinta delle recenti vicende internazionali legate al terrorismo ed al cybercrime, alla costituzione di un sistema misto, pubblico e privato, di strutture e gruppi di controllo e di monitoraggio dedicati espressamente per fronteggiare le emergenze ICT quale parte di un sistema più ampio per la protezione delle NCI.

Tra le componenti essenziali del citato sistema, sviluppato e codificato in maniera diversa nelle diverse nazioni a seconda delle diverse esigenze e realtà organizzative, particolare rilievo hanno i gruppi di controllo e di monitoraggio CERT, CSIRT ed ISAC.

6.1. CERT/CSIRT

In una fase di emergenza, a fronte dell'insorgere di un problema di sicurezza informatica il fattore critico è la capacità di rispondere in modo veloce ed efficace. La rapidità, con la quale l'organizzazione è in grado riconoscere un incidente o un attacco e successivamente analizzarlo e contrastarlo, limiterà in modo importante il danno inferto o potenziale ed abbasserà il costo del ripristino e pertanto la capacità di rispondere prontamente ed in modo efficace ad una minaccia alla sicurezza, è un elemento critico per un ambiente informatico sicuro.

Un'attenta analisi della natura dell'attacco o dell'incidente può inoltre permettere di individuare misure preventive efficaci ed a largo spettro volte a contrastare eventi simili.

Una risposta efficace agli incidenti è un attività complessa e pertanto la creazione di una buona capacità di risposta richiede una significativa pianificazione e notevoli risorse.

Un modo per fornire tale risposta passa per la creazione di un gruppo, designato o istituito in modo formale, cui è data la responsabilità della gestione degli eventi di sicurezza.

L'istituzione di un gruppo focalizzato sulle attività di gestione degli incidenti permette di sviluppare la competenza nella comprensione degli attacchi e nelle intrusioni insieme all'acquisizione della conoscenza delle metodologie di risposta agli incidenti.

Il primo gruppo di risposta agli incidenti fu creato dal governo statunitense pochi giorni dopo il 2 novembre del 1988, data in cui accadde il primo grave incidente di sicurezza su Internet: l'Internet worm.

L'organismo prese il nome di Computer Emergency Response Team (CERT™). Quel CERT ha continuato ad operare ed è divenuto il CERT Coordination Center, organismo internazionale che ha anche la finalità di condividere e divulgare linee guida sulla creazione e la gestione di gruppi di risposta agli incidenti.

Tali gruppi vengono generalmente denominati con i seguenti acronimi:

- IRT - Incident Response Team
- CIRT - Computer Incident Response Team
- CSIRT - Computer Security Incident Response Team
- SIRT - Security Incident Response Team
- SERT - Security Emergency Response Team
- CSERT - Computer Security Emergency Response Team

Nel seguito del documento utilizzeremo, per indicare tali strutture, la denominazione più comunemente usata di Computer Security Incident Response Team (CSIRT).

Ad oggi sono formalmente riconosciuti nel mondo 170 gruppi CSIRT affiliati all'organismo statunitense FIRST (Forum of Incident Response and Security Teams), anche se il numero effettivo di CSIRT ad oggi costituiti è di gran lunga superiore. Dei 170 CSIRT ufficialmente registrati, 46 appartengono ad entità governative e gli altri (in proporzione di due a uno) ad aziende e ad enti di ricerca ed accademici.

Nell'ambito dell'organismo TERENA (Trans European Research and Education Networking Association) è inoltre attiva una struttura denominata TF-CSIRT (Task Force CSIRT) per il supporto ed il coordinamento dei CSIRT europei che conta attualmente 42 aderenti, alcuni dei quali affiliati anche al FIRST.

I CSIRT governativi in Europa sono attualmente 19 di cui 16 in rappresentanza dei paesi che hanno già aderito all'Unione Europea.

Un CSIRT costituisce un singolo punto di contatto per la segnalazione di problemi ed incidenti di sicurezza informatica e si caratterizza in base ad alcuni principali elementi:

- la comunità di riferimento;
- il modello organizzativo;
- i servizi erogati e le capacità intrinseche;
- le relazioni con entità ed organismi esterni.

La comunità di riferimento di un CSIRT è costituita dagli utenti, dagli enti e dalle organizzazioni cui il CSIRT eroga i suoi servizi.

La comunità di riferimento del CSIRT, inclusa la sua composizione, la sua localizzazione o distribuzione fisica o geografica, il settore in cui opera (governativo, pubblico, privato, accademico) costituisce un fattore decisivo nella scelta del modello organizzativo.

Un CSIRT istituito formalmente può essere organizzato in una delle tre seguenti modalità:

- **Gruppo centralizzato:** un singolo gruppo gestisce gli incidenti per tutta l'organizzazione di appartenenza;
- **Gruppo distribuito:** l'organizzazione dispone di più gruppi distribuiti in diversi settori fisici o logici;
- **Gruppo di coordinamento:** un gruppo fornisce supporto, guida e consulenza ad altri gruppi; è il caso di un CSIRT di CSIRT.

Se un gruppo opera come un CSIRT senza che gli sia stata attribuita una responsabilità formale viene indicato genericamente come gruppo di sicurezza.

6.1.1 Risorse utilizzate da un CSIRT

I gruppi di risposta agli incidenti possono utilizzare uno qualsiasi dei seguenti tre modelli di struttura delle risorse.

risorse interne: l'organizzazione effettua tutte le attività di risposta ai propri incidenti, eventualmente con un limitato supporto tecnico ed amministrativo da parte di terzi;

esternalizzazione parziale: l'organizzazione affida a società esterne parte delle attività di risposta agli incidenti; sebbene le modalità di suddivisone con terze parti possano essere diverse, due sono le più adottate:

- la modalità più diffusa è l'esternalizzazione 24 ore al giorno, sette giorni la settimana, ad un fornitore di servizi di gestione

remota del controllo dei sensori di rilevazione delle intrusioni, dei firewall e di altri dispositivi di sicurezza;

- alcune organizzazioni effettuano internamente una prima risposta ma si avvalgono di società esterne per le attività successive specialmente in caso di incidenti importanti ed estesi. I servizi che più spesso sono assegnati ad una terza parte sono l'analisi forense, l'analisi avanzata dell'incidente, il contenimento, l'eradicazione e la mitigazione della vulnerabilità;

completamente esternalizzato: l'organizzazione affida completamente il lavoro di risposta gli incidenti ad una società esterne e le attività vengono effettuate sul proprio sito.

6.1.2 I servizi erogati da un CSIRT

Possiamo raggruppare i servizi erogati da un CSIRT in tre grandi categorie:

- servizi reattivi
- servizi proattivi
- servizi per la qualità della sicurezza

6.1.2.1 Servizi reattivi

Questi servizi sono innescati da un evento o da una richiesta, quali la segnalazione della compromissione di un sistema, la diffusione di un codice maligno, la scoperta di una vulnerabilità software, o da un evento sospetto identificato da un sistema di rilevazione delle intrusioni o da un sistema di tracciamento. I servizi reattivi sono la componente base del lavoro di un CSIRT.

I servizi di questa categoria comprendono i seguenti.

Early warning: questo servizio consiste nella diffusione di informazioni che descrivono un attacco dì tipo intrusivo, una vulnerabilità, un allarme di intrusione, un codice maligno e fornisce raccomandazioni per azioni a breve termine per il trattamento dei problemi risultanti.

Gestione degli incidenti: questo servizio riguarda la ricezione, la valutazione e la risposta a richieste e segnalazioni, l'analisi degli incidenti e degli eventi. Specifiche attività di gestione includono:

- l'analisi dell'incidente: la raccolta di evidenze forensi ed il tracciamento;
- la risposta all'incidente sul sito;
- il supporto alla risposta all'incidente;
- il coordinamento della risposta all'incidente.

Gestione delle vulnerabilità: la gestione delle vulnerabilità implica la ricezione di informazioni e rapporti concernenti le vulnerabilità hardware e software, l'analisi della natura, della meccanica e degli effetti delle vulnerabilità e lo sviluppo di strategie di risposta per la rilevazione e le modalità di contrasto. Questo servizio può assumere varie forme: analisi delle vulnerabilità; risposta alle vulnerabilità; coordinamento della risposta alle vulnerabilità.

Gestione dei codici pericolosi: questo servizio riguarda la ricezione di informazioni e di copie di codici pericolosi che sono usati in attività intrusive, di ricognizione ed in altre attività non autorizzate, illecite o dannose. In questo caso intendiamo per codice pericoloso qualsiasi file o oggetto trovato su un sistema che potrebbe riguardare attività esplorative o di attacco. I codici pericolosi includono ma non sono limitati a virus, cavalli di Troia, worm, script e toolkit.

6.1.2.2 Servizi proattivi

Questi servizi forniscono assistenza ed informazioni per aiutare a proteggere i sistemi della comunità di riferimento in anticipazione di attacchi, problemi o eventi pericolosi. Questi servizi, se erogati con efficacia, riducono nel tempo il numero degli incidenti.

I servizi di questa categoria comprendono.

Annunci: questo servizio include (ma non è limitato a questi)

gli avvisi per intrusioni e vulnerabilità. Queste comunicazioni informano la comunità circa i nuovi sviluppi con impatto a medio lungo termine.

Osservatorio tecnologico: il CSIRT effettua il monitoraggio di nuovi sviluppi tecnici, attività di intrusione e le relative tendenze in aiuto all'identificazione di future minacce. Gli elementi sotto osservazione possono essere espansi per includere aspetti legali e giuridici, minacce sociali o politiche e tecnologie emergenti.

Verifiche e valutazioni: questo servizio fornisce una dettagliata revisione ed analisi di un'infrastruttura di sicurezza di un'organizzazione, basata sui requisiti definiti dalla stessa organizzazione o da altri standard applicati. Il servizio può anche includere una revisione delle prassi di sicurezza di un'organizzazione. Sono possibili diversi tipi di revisioni o valutazioni includendo: la revisione dell'infrastruttura; la revisione delle migliori prassi; la scansione; i test di penetrazione.

Configurazione e manutenzione: questo servizio identifica o fornisce la guida appropriata su come configurare e mantenere strumenti, applicazioni, e l'infrastruttura informatica generale usata dal CSIRT stesso. Il CSIRT può effettuare aggiornamenti di configurazione e manutenzione di strumenti, servizi di sicurezza quali IDS, strumenti di scansione o monitoraggio, filtri, wrapper, firewall, VPN o meccanismi di autenticazione. Il CSIRT può anche configurare e mantenere server, desktop, laptop, PDA ed altri dispositivi wireless in conformità alle linee guida di sicurezza.

Intrusion Detection: un CSIRT che effettua questo servizio revisiona i log generati da IDS, analizza ed inizia una risposta per qualsiasi evento che supera una certa soglia o inoltra allarmi in conformità ad un predeterminato livello di servizio o strategia di escalation.

Diffusione di informazioni relative alla sicurezza: questo servizio fornisce alla comunità di riferimento una completa collezione di informazioni utili ad aiutare a migliorare la sicurezza. Tali di informazioni possono includere:

- linee guida per le segnalazioni e le informazioni di contatto per il CSIRT
- archivi di allarmi, avvisi ed altri annunci

- documentazione relativa alle migliori prassi correnti
- guide generali alla sicurezza
- politiche, procedure e liste di controllo
- sviluppo di patch ed informazioni di distribuzione
- riferimenti dei fornitori
- statistiche correnti e tendenze sugli incidenti
- altre informazioni che possano migliorare le prassi di sicurezza

Raccolta e diffusione informazioni: questo servizio permette di creare ed accrescere nel tempo una base dati di conoscenza, indispensabile non solo per finalità statistiche, ma per valutare le tendenze ed orientare gli interventi nell'ambito della comunità di riferimento.

6.1.2.3 Servizi per la qualità della sicurezza

Questi servizi ampliano quelli già esistenti tradizionalmente erogati da altre aree di un'organizzazione quali l'IT, l'audit, la formazione.

Se il CSIRT eroga questi servizi, il punto di vista e la competenza del CSIRT possono essere d'aiuto nel migliorare la sicurezza complessiva dell'organizzazione e nell'identificare rischi, minacce e debolezze dei sistemi.

I servizi di questa categoria comprendono:

- Analisi dei rischi;
- Continuità di servizio;
- Consulenza;
- Sensibilizzazione, formazione ed aggiornamento.

6.2. ISAC

6.2.1 Definizione, origini e storia

Già dal 1998, gli USA hanno riconosciuto il problema di assicurare la protezione delle CNI da attacchi convenzionali e non, specie di natura informatica, ed hanno avviato numerose iniziative, in ambito interno ed internazionale, per eliminare ogni vulnerabilità ai propri sistemi ICT dovuti soprattutto ad attacchi fisici ed informatici. Tra gli strumenti organizzativi individuati negli USA, per meglio realizzare la cooperazione tra i settori governativi e privati, è stata disposta la creazione, per ogni settore ritenuto di importanza strategica, di Centri per la condivisione e l'analisi delle informazioni (ISAC - Information Sharing And Analysis Center). Gli ISAC sono associazioni di imprese private le quali, ciascuna per il proprio settore di competenza, raccolgono, distribuiscono, analizzano e condividono informazioni relative a minacce, vulnerabilità, allarmi e linee guida per la protezione delle NCI.

Gli eventi del settembre 2001 e la creazione negli USA del Dipartimento per la Sicurezza Interna (HSD) hanno evidenziato la necessità di una più stretta collaborazione all'interno della stesse strutture governative e tra le agenzie governative e le strutture private responsabili delle CNI e l'importanza degli ISAC è cresciuta per le capacità strategiche di prevenzione e di intervento e gestione delle emergenze. Le organizzazioni operative degli ISAC raccolgono informazioni e dati relativi alle emergenze ed alle vulnerabilità ICT dai propri membri e da altre fonti esterne e li diffondono ai propri membri dopo averli opportunamente analizzati ed integrati in un'immagine coerente che rispecchia lo stato dell'emergenza o della minaccia.

Iniziative analoghe sono state successivamente intraprese da altre nazioni ma, sostanzialmente, lo schema funzionale di un ISAC è quello riportato nella seguente figura 19 dal quale è possibile comprendere come i benefici portati dalla creazione di un'infrastruttura avente le caratteristiche descritte, risultano essere molteplici:

- eliminazione del sovraccarico di informazioni;
- diffusione mirata di in formazioni e soluzioni precedentemente vagliate e valutate;

- diminuzione del tempo di reazione agli incidenti ed alle crisi informatiche;
- diminuzione dei tempi di attualizzazione delle proprie misure di sicurezza;
- più stretta collaborazione tra aziende dello stesso ambito e quindi aumento degli scambi di esperienze e di conoscenze tra ambienti con simili esigenze e problematiche informatiche.

In tal modo è possibile sfruttare tutti i benefici derivati dalla creazione di una sorta di comunità virtuale di settore, gestita in modo automatico, sicuro, certificato, autenticato con condivisione di informazioni anche rese anonime all'occorrenza.

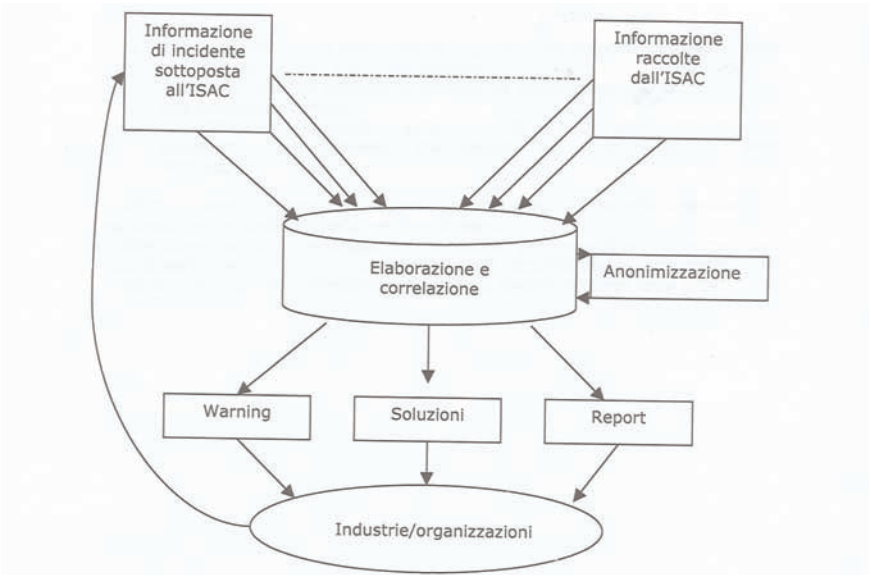


Figura 19 - Schema funzionale di un ISAC

6.2.2 La situazione negli U.S.A.

Sin dal 1996 l'Amministrazione federale ha riconosciuto la necessità di trovare una soluzione per fare fronte all'elevato numero di

vulnerabilità alle quali le infrastrutture ICT governative e private erano soggette e difficili da affrontare per riconosciuta incapacità d'intervento tempestivo. Un'apposita Commissione sulla CIP convenne sulla necessità di unire sia i settori pubblici che privati delle aree critiche all'interno di infrastrutture in grado di condividere le conoscenze e fornire supporto per far fronte alle emergenze di natura informatica.

Nel 1998 una Direttiva presidenziale sanciva,tra l'altro, la creazione, entro cinque anni, degli ISAC per ciascuno dei settori ritenuti critici per la sicurezza della nazione. Con questa Direttiva, l'Amministrazione USA intendeva realizzare un sistema per la condivisione dei dati relativi agli attacchi e alle vulnerabilità informatiche, la loro raccolta, analisi e diffusione all'interno del sistema ISAC di un quadro di situazione delle vulnerabilità, delle minacce e degli avvenimenti dei sistemi informatici propri di uno specifico settore critico.

Successive Direttive presidenziali del 2003 hanno rafforzato l'impegno dell'Amministrazione per la salvaguardia delle CNI meglio chiarendo ruoli, compiti e responsabilità di entrambi i settori pubblico e privato nel pieno riconoscimento che solo dalla loro cooperazione è possibile prevenire ed affrontare con successo le vulnerabilità ed i rischi degli specifici settori.

Proposed Framework as depicted in the I-NIPP

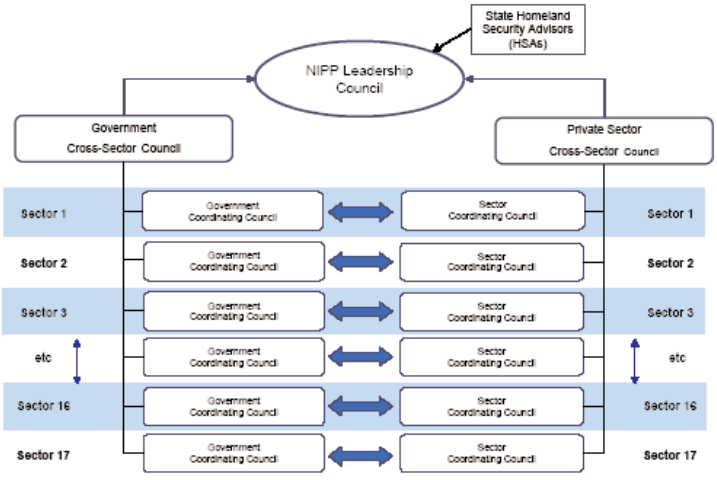


Figura 20 - Schema funzionale di un ISAC

Al momento, la struttura organizzativa USA vede il Segretario del Dipartimento della Sicurezza Interna (HDS) responsabile del coordinamento delle attività per la protezione delle CNI che viene attuato attraverso il National Infrastructure Advisory Council (NIAC). In Figura 20 è rappresentato il modello organizzativo previsto, di recente, dal NIAC e raccomandato per l'inclusione nell'Interim National Infrastructure Protection Plan (I-NIPP) in corso di esame da parte del HDS.

Attualmente sono attivi negli USA numerosi ISAC. Gli ISAC sono coordinati da un Consiglio (ISAC Council) che costituisce la principale interfaccia tra l'autorità governativa, in particolare con l'HSD, e le organizzazioni private.

Tra gli ISAC statunitensi più significative vi sono il NCC ISAC, l'ISAC per le telecomunicazioni, ed l'IT-ISAC i quali costituiscono un significativo esempio di come possono convergere gli interessi pubblici e privati o rimanere separati nella gestione di settori di elevata importanza per la sicurezza e delle emergenze nazionali. .

Dal 1999, infine, negli Stati Uniti è operante anche il WorldWide ISAC i cui servizi sono espletati dalla Science Applications International Corporation (SAIC) considerata tra le società leader mondiali che si occupano di reti TLC ed IT con estesa esperienza nel fornire un'elevata protezione ai sistemi ICT delle organizzazioni governative e private.

6.2.3 La situazione in Europa

Dalla fine 1999 la Commissione Europea ha avviato l'iniziativa eEurope con i seguenti obiettivi chiave:

- consentire a tutti i cittadini europei di entrare nell'era digitale e di disporre di un collegamento on-line;
- creare un'Europa capace di padroneggiare i sistemi digitali, sostenuta da una cultura imprenditoriale;
- garantire che il processo non ingeneri esclusione e contribuisca a creare fiducia nei consumatori.

Nel giugno 2000, il Consiglio Europeo di Feira ha adottato il piano d'azione eEurope 2002, che precisava le azioni politiche necessarie a conseguire tali obiettivi entro il 2002.

Nell'ambito del predetto piano, è stato deciso un primo intervento inteso a rafforzare la cooperazione pubblico/privato in materia di affidabilità dell'infrastruttura dell'informazione (tra cui lo sviluppo di sistemi di allarme preventivo) e a migliorare la cooperazione tra i vari CERT (Computer Emergency Response Team) creati negli ambiti nazionali.

Il 21 giugno 2002, presso il Consiglio Europeo di Siviglia, viene presentato il piano d'azione eEurope200s (C0M2002 263), naturale prosecuzione della filosofia che aveva portato allo sviluppo del precedente piano.

Stando a tale piano, entro il 2005, i diversi paesi europei dovranno dotarsi, tra l'altro, di moderni servizi pubblici on line, e-government, servizi di e-learning, servizi di e-health e di un ambiente dinamico di e-business.

Tra i presupposti alla base di tali sviluppi è stato esplicitamente indicato lo sviluppo di infrastrutture di protezione dell'informazione compresi:

- i Computer Emergency Response Systems, in grado, in particolare, di condividere tra partner privati e pubblici informazioni riguardanti la diffusione e la natura di virus e bug nonché lo scambio e la condivisione delle informazioni;
- gli Information Sharing and Analisys Center (ISAC), nell'ambito della creazione di una comunità telematica europea sicura, per il cui sviluppo, un successivo studio europeo ha indicato i CERT nazionali gli elementi preferenziali.

Successivamente, il regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio del 10 marzo 2004 ha istituito l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) ed ha fissato il quadro ed i presupposti per la sua attività. L'Agenzia con sede a Corfù, è diventata operativa. nell'autunno del 2005.

La missione dell'Agenzia è di assistere la Commissione nel

compito di assicurare un livello particolarmente elevato di sicurezza delle reti e dell'informazione. L'Agenzia contribuirà, pertanto, allo sviluppo di una cultura della sicurezza delle reti e dell'informazione a beneficio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico dell'Unione europea, contribuendo in tal modo all'ordinato funzionamento del mercato interno.

L'Agenzia aiuterà la Commissione, gli Stati membri e gli operatori economici a rispettare i requisiti relativi alla sicurezza delle reti e dell'informazione, ivi compresi i requisiti previsti dalla vigente e dalla futura normativa comunitaria.

L'Agenzia fungerà, infine, da centro di consulenza per gli Stati membri e le Istituzioni dell'Unione europea su questioni relative alla sicurezza delle reti e dell'informazione.

Al fine di assicurare la realizzazione degli obiettivi che le sono stati fissati, l'Agenzia svolgerà in particolare i seguenti compiti:

- raccogliere e analizzare i dati relativi agli incidenti connessi con la sicurezza e ai rischi emergenti;
- cooperare con i diversi soggetti che operano nel settore, in particolare tramite la creazione di un partenariato pubblico/privato con le imprese del settore operanti a livello dell'Unione europea e/o a livello mondiale;
- svolgere attività di sensibilizzazione e di promozione dei metodi di valutazione dei rischi e delle migliori pratiche in materia di soluzioni interoperabili di gestione dei rischi;
- seguire l'evoluzione delle norme sulla sicurezza delle reti e dell'informazione per prodotti e servizi.

Al momento, nelle altre nazioni europee una significativa iniziativa organizzativa è rappresentata in Gran Bretagna dal National Infrastructure Security Co-ordination Centre (NISCC) che è una organizzazione interministeriale creata per coordinare e promuovere le attività in atto presso i diversi dipartimenti ed agenzie governative e le organizzazioni del settore privato per difendere le NCI da attacchi di natura elettronica. All'interno della struttura del Consiglio dei Ministri opera, invece, un unità centrale per la sicurezza (CSIA - Central

Sponsor Information Assurance) per la salvaguardia dei servizi di comunicazioni ICT del paese d'intesa con le organizzazioni statali, pubbliche ed internazionali. NISCC e CSIA collaborano per lo scambio di informazioni al fine di ridurre il rischio di compromissioni e di attacchi al sistema di comunicazioni nazionale. Del NISCC fanno inoltre parte i punti WARP (Warning, Advice and Reporting Points) quali parti di una strategia e di una catena informativa diffusa per settori d'impiego, località, standard tecnologici, gruppi a rischio e quant'altro d'importante per gli interessi vitali della nazione. I membri WARP usufruiscono di una rete e di un sistema informativo dedicati con benefici in termini di costo/efficacia e sicurezza a costi minimi fornendo ai partecipanti al sistema:

- un ambiente sicuro;
- un sistema filtrato di informazioni di sicurezza;
- l'accesso ad esperti in sicurezza,
- allarmi sulle minacce;
- supporto alle decisioni strategiche;
- conoscenze sperimentate.

In Francia il sistema di sicurezza dei sistemi di comunicazione ed informatici è ben radicato nella struttura statale come è possibile vedere in figura 21. Da questa è possibile desumere che il CERT governativo è inserito nella struttura della Direzione Centrale per la sicurezza dei sistemi informativi del Segretariato generale della difesa nazionale (SGDN); in Francia esistono alcuni CERT relativi ai settori più strategici, collegati al CERTA, non è prevista la creazione di ISAC le cui funzioni sono assolte dai predetti CERT.

Per quanto noto, infine,negli altri paesi europei non vi sono iniziative od attività di organismi ISAC; le attività riferibili agli ISAC sono svolte dai CERT/CSIRT operanti nei diversi paesi.

Figura 21 - Gruppo di monitoraggio in Francia

6.2.4 Funzionalità generiche raccomandate per un ISAC

Si riportano di seguito le funzionalità che, secondo uno studio del CLUSIT, un ISAC dovrebbe essere in grado di fornire:

- notificare i rischi per la sicurezza e le vulnerabilità di tipo informatico;
- valutare i rischi in termini di gravità, intensità, pericolo potenziale e tempi di diffusione;
- definire le priorità di intervento e di comunicazione;
- elaborare rapporti statistici che offrano una vista globale delle vulnerabilità e delle minacce;
- fornire istruzioni mirate per il rafforzamento della sicurezza a fronte di una minaccia informatica.

6.2.5 Funzionalità specifiche raccomandate per un ISAC

Più in dettaglio, sempre il CLUSIT raccomanda che il sistema dovrebbe essere in grado di fornire le caratteristiche di seguito indicate:

- **Condivisione ed anonimato delle informazioni condivise.** L'infrastruttura dovrà essere cioè in grado di consentire la condivisione delle informazioni come incidenti, vulnerabilità e soluzioni, alternativamente, secondo il tipo, in modo autenticato o anonimo.
- **Suddivisione delle informazioni condivise in categorie:** le informazioni raccolte dovranno essere suddivise nelle seguenti categorie:
  - Incidenti
    - Buchi di sicurezza od esperienze di incidente di nuova natura;
    - Buchi di sicurezza od esperienze di incidente aventi un impatto significativo sui sistemi dei membri;
  - Minacce
  - Vulnerabilità
    - Riportate da CERT, FIRST, bugtraq, vendor bulletin;
    - Riportate da altre fonti attendibili;
    - Risultati di investigazioni di vulnerabilità specifiche;
  - Soluzioni
    - Indicazioni provenienti dai CERT e dai vendor report;
    - Indicazioni provenienti da esperienze proposte dai membri del sistema;
    - Indicazioni provenienti internamente dagli esperti ISAC.
- Fonti delle informazioni. Le istituzioni/aziende membri potranno inviare le informazioni relative ad attacchi/minacce in modo anonimo od attribuibile. Altre informazioni potranno provenire da agenzie governative o da centri scientifici di comprovata affidabilità.

- Analisi delle informazioni
    - Le notifiche di incidente ricevute od ottenute, saranno analizzate per determinarne la validità tecnica, per ottenere indicazioni, trends, soluzioni.

- Trattamento preventivo delle informazioni inviate
    - Tutte le informazioni di incidente, dove richiesto, dovranno poter essere anonimizzate per salvaguardare il diritto alla privacy del fornitore dell'informazione.

6.3. RAPPORTI CON LE AUTORITÀ PREPOSTE

Soprattutto negli USA, dove lo strumento degli ISAC a sostegno delle attività di protezione delle infrastrutture critiche è già operante da alcuni anni, è riconosciuta e sentita di particolare importanza la necessità, nel sistema di relazioni tra la strutture governative e quelle private, di:

- definire e chiarire i ruoli dell'autorità/organizzazioni governative responsabili della protezione delle infrastrutture critiche, dei gestori delle infrastrutture e degli ISAC nel rispetto delle reciproche prerogative;
- definire chiaramente le relazioni e le interfacce tra i diversi attori del sistema pubblico-privato;
- definire chiaramente e realizzare i requisiti governativi e del settore privato relativi ai dati ed alle informazioni da scambiare;
- definire e realizzare sistemi sicuri per lo scambio dei dati e delle informazioni nonché il database delle vulnerabilità dei sistemi critici;
- valutare il sistema nazionale di diffusione degli allarmi e la sua applicabilità ai settori critici e sviluppare sistemi per meglio utilizzare le informazioni raccolte per la diffusione dei livelli di allarme su base geografica, di settore o specifica;
- definire una raccolta di linee guida ed un manuale di risposte prepianificate da attuare all'insorgere di specifiche esigenze;

- poter disporre di esperti riconosciuti e di conoscenze approfondite in entrambi i settori pubblico e privato per poter meglio comprendere i potenziali fenomeni di attacco o pericolo alle infrastrutture critiche.

Il soddisfacimento delle predette esigenze è importante per il consolidamento della collaborazione e del coordinamento tra gli organismi governativi e quelli privati al pari della messa in opera di un sistema nazionale, unico e comune, per rendere il processo di diffusione delle informazioni il più rapido e sicuro possibile.

Allo scopo una stretta collaborazione fra GovCERT, il SinCERT, il CNAIPIC, altri CERT aziendali/di settore (nazionali o locali) e gli ISAC di settore, sempre più auspicati, sono chiamati a collaborare allo scopo di consentire una più ampia diffusione delle informazioni e una partecipazione, ognuno secondo i propri ruoli, alla gestione delle emergenze.

7 - La lezione dell'uragano Katrina ai sistemi di controllo: cosa un disastro naturale può insegnare all'industria

I recenti uragani che hanno devastato la costa sud degli Stati Uniti tra agosto e settembre del 2005 sono stati tra i peggiori disastri naturali mai subiti in Nord America.

Un elevato numero di impianti e infrastrutture critiche in quella regione sono stati chiusi, disattivati, molti danneggiati o addirittura distrutti dalla forza della natura.

Tra questi impianti industriali ed infrastrutture critiche troviamo:

1. elettricità, tra produzione, trasmissione e distribuzione
2. gas, tra produzione e distribuzione
3. raffinazione e trasporto di prodotti petroliferi
4. erogazione di acqua
5. depurazione e trattamento delle acque e reflui
6. produzione di alimenti e bevande
7. processi chimici
8. produzioni discrete
9. molti altri impianti critici

Questi processi critici sono nella maggior parte dei casi monitorati e controllati da sistemi specializzati che rientrano nella categoria

dei sistemi di controllo: una combinazione di computer, hardware e software, dispositivi per il controllo di processo, sistemi per interfacciarsi al processo, e tutte le applicazioni associate che tutti insieme contribuiscono a tenere sotto controllo le variabili di un processo tecnico e gestiscono la corretta esecuzione del processo stesso.

Per assistere i responsabili di aziende industriali, enti ed organizzazioni, gli operatori, i fornitori e tutti gli addetti all'installazione e funzionamento dei sistemi di controllo che devono essere riavviati in modo "sicuro", anche se in circostanze di emergenza, il **DHS** (Department of Homeland Security, il ministero USA responsabile per la sicurezza interna) per il tramite del Centro per la Sicurezza dei Sistemi di Controllo (**CSSC**, Control Systems Security Center) che fa parte del Team di Intervento per le Emergenze sui Computer (**US-CERT** United States Computer Emergency Readiness Team) ha messo a punto una sorta di "guida" con una serie di punti da prendere in considerazione e suggerimenti da seguire nel momento in cui sia necessario rimettere insieme e fare ripartire il sistema di controllo. Il CSSC mette a disposizione degli interessati anche un team di specialisti ed un punto di contatto per fornire tutta l'assistenza necessaria, per chiarire dubbi ed aiutare nel caso a svolgere al meglio il compito.

7.1. PROBLEMI DI SICUREZZA NEL FARE RIPARTIRE I SISTEMI DI CONTROLLO

Il CSSC riconosce che la preoccupazione principale per tutti i proprietari ed operatori di sistemi di controllo che gestiscono impianti ed infrastrutture critiche è riportare l'impianto e quindi il sistema di controllo stesso in funzione nel minor tempo possibile ed in sicurezza.

Al tempo stesso non si devono dimenticare le difficoltà in cui tale operazioni devono essere eseguite: spesso i sistemi, i loro componenti, le comunicazioni e quanto altro sono ancora in condizioni diverse dalla situazione antecedente, e quindi a come venivano utilizzati prima degli uragani. Può essere necessario prendere delle "scorciatoie" o forzatamente cambiare le configurazioni, e questo potrebbe esporre i sistemi a minacce e vulnerabilità quali ad esempio attacchi

informatici che potrebbero indurre altri problemi, a volte anche gravi.

Nella regione del Golfo degli USA, la perdita di infrastrutture critiche primarie e dei sistemi di controllo associati ha provocato anche un effetto "domino" con impatti a cascata indotti da altre e su altre infrastrutture critiche.

Nei giorni successivi al disastro naturale, "persone minacciose" armate di cattive intenzioni potrebbero tentare di sfruttare le nuove vulnerabilità o di approfittare delle vulnerabilità esistenti mentre gli sforzi e le risorse più significative sono diretti verso persone nel bisogno.

È quindi importante per i membri della comunità addetta ai sistemi di controllo essere consci delle minacce e di quali eventi potrebbero generarsi in una situazione che vede i sistemi più vulnerabili dia dal punto di vista fisico sia ai cosiddetti attacchi informatici: minacce che potrebbero venire da persone che prendono di mira uno specifico sistema o anche arrivare anche da altre strade con worm, Trojan, virus o altro software o codice maligno che purtroppo sono diventati molto comuni nel mondo "connesso" di oggi.

7.2. FACCIAMO RIPARTIRE I SISTEMI IN SICUREZZA ("SAFETY" & "SECURITY")

Per fare ripartire i sistemi di controllo nel modo più "sicuro" (teniamo presente sia il tema "Safety" sia l'aspetto "Security") il CSSC ha messo a punto un elenco di argomenti, una sorta di check-list, che devono essere presi in considerazione come risultato di tutta una serie di esperienze ed input raccolti nel tempo e pervenuti da specialisti di security di sistemi di controllo sia del settore pubblico ed infrastrutture critiche che di quello dell'industria privata.

Ma quanto qui di seguito suggerito non deve essere preso come un sostituto di Disaster Recovery Plan (DRP), di Business Continuity Plan (BCP) o di Continuity of Operation Plan (COOP) che l'azienda dovrebbe già avere perlomeno abbozzato e che dovrebbe comunque guidare gli addetti su quanto sia necessario fare durante e dopo un evento increscioso come quello causato dagli uragani.

Questo elenco di attività è solo un memorandum per assicurarsi che tra tutti gli altri temi affrontati ci sia anche l'aspetto della Security in tutte le aree di pertinenza dei sistemi di controllo prima che questi vengano rimessi in funzione.

Ci si aspetta che sia stato già fatto qualche assessment per la verifica dei danni subiti per determinare se i sistemi di controllo, loro componenti, le comunicazioni ecc. abbiano bisogno di essere riparati e/o sostituiti prima di una ripartenza.

Il CSSC rimane comunque a disposizione per ogni dubbio o assistenza sia richiesta per queste attività.

7.2.1 Determinare e mettere in atto una "Sicurezza Fisica"

- E' importante stabilire una "Sicurezza Fisica" in tutte le sedi, sia che abbiano subito danni o che siano rimaste integre, per evitare che chiunque abbia accesso non controllato per sottrarre, cambiare o anche solo fare atti di vandalismo ai componenti del sistema e della rete.
- Decidiamo chi può avere accesso ai sistemi o suoi componenti, sistemi di comunicazione inclusi, e limitiamo gli accessi solo a queste persone:
  - Definiamo le procedure per il controllo ed autorizzazione degli accessi
  - Inventariamo e teniamo traccia di tutti gli spostamenti di ogni componente dei sistemi di controllo, sistemi di comunicazione, reti, ecc.: controlliamo periodicamente questi registri fino a quando tutti i sistemi siano tornati in funzione nei luoghi definiti

7.2.2 Determinare e mettere in atto la "Sicurezza dell'organizzazione"

- Scegliamo chi sono le persone che possono aver accesso ai sistemi di controllo, e controlliamo che siano persone "fidate", delle quali si conosce la provenienza e le referenze
- Cerchiamo se possibile di utilizzare personale conosciuto, di fornitori conosciuti, che abbiano già avuto esperienza di lavoro sui nostri sistemi; se ciò non fosse possibile, chiediamo a fornitori di servizi che abbiano referenze comprovabili ed esperienza in impianti e sistemi simili al nostro, a nostro expersonale in pensione, o persone con esperienze almeno vicine alle nostre.

7.2.3 Determinare un sistema o procedura per il controllo delle configurazioni

- Dobbiamo avere un documentato controllo della configurazione mantenendo traccia di tutti i componenti rimpiazzati o modificati. C'è la tendenza, in momenti di fretta, a installare parti e ricambi (sia hw che sw) non perfettamente corrispondenti agli originali: e spesso questi rimedi temporanei divengono definitivi.
- Teniamo sotto osservazione dove mettiamo e che fine fanno computer e sistemi di storage, soprattutto quelli che decidiamo di dismettere: sinceriamoci che dischi fissi o CD con nostri dati non vadano in mani di persone che possano compromettere i nostri sistemi grazie a dati ed informazioni per l'accesso (User ID, Password, informazioni sulle configurazioni, ecc.)
- Assicuriamoci di avere adeguate procedure e policy per avere traccia della destinazione, della "pulizia", della dismissione e della distruzione del materiale danneggiato sia hardware che software.

7.2.4 Verifica dell'Hardware

- Per la sostituzione di sistemi e componenti utilizziamo solo materiale "approvato" di accertata qualità, acquistato possibilmente da rivenditori "ufficiali" del sistema di controllo o di comunicazione: evitiamo l'utilizzo di componenti "dubbi".
- Eseguiamo test per la calibrazione di tutti i sensori e convalida di tutti i componenti del sistema e del sistema intero su possibile ed adeguato: farlo prima della installazione ci consentirà di isolare eventuali problemi. Riparare, tarare, riconfigurare e/o sostituire se e quanto necessario.
- Alcuni componenti chiave possono essere stati asportati, causando problemi di funzionamento a tutto il sistema. Facciamo quindi un controllo punto per punto su tutto il sistema per identificare se ci sono componenti mancanti o danneggiati. Controlliamo l'alimentazione, la terra, i cablaggi, i collegamenti degli I/O, le canaline con cavi, ecc.
- Verifichiamo che l'alimentazione elettrica sia a posto. Se utilizziamo un gruppo di continuità e stabilizzazione della tensione (UPS Uninterruptible power supply) controlliamo che sia in ordine prima di qualsiasi collegamento. Se dobbiamo fare a meno di un UPS, controlliamo che i circuiti siano adeguati. Controlliamo anche le batterie di back-up che potrebbero essere esaurite o danneggiate.
- I sistemi di alimentazione potrebbero rimanere bloccati: controlliamo che non ci siano eventuali cortocircuiti a valle o a monte che possano bloccare tutto il sistema o parti di esso.
- Assicuriamoci che l'hardware sia aggiornato con versioni di firmware adeguato (con gli aggiornamenti di security)
- Assicuriamoci che i sistemi siano impostati e configurati per funzionare in modo "sicuro"
- Controlliamo che l'hardware sia installato in conformità alle nostre policy e procedure di security
- Se possibile facciamo test su tutti i componenti e su tutte le funzioni in "manuale" prima di mettere tutto in "automatico"

7.2.5 Verifica del Software

- La mancanza di alimentazione elettrica (batterie di back-up incluse) a volte provoca un reset totale del sistema di controllo, riportandolo esattamente allo stato iniziale con tutti i parametri di default impostati dal fornitore, come se fosse appena uscito dalla fabbrica, incluse password e tutti gli altri settaggi di security. Controlliamo quindi che siano montati i programmi più aggiornati e che le password siano accettabilmente "sicure" (non quelle di default e secondo le nostre policy).
- Prima di fare ripartire i sistemi, verifichiamo che siano correttamente aggiornate anche le liste di accesso dei firewall e router, senza accessi e password settati di default.
  - Rivediamo tutti i settaggi per assicurarci che siano abilitate connessioni solo le connessioni strettamente necessarie (valutiamo bene gli accessi su reti dell'azienda o di altri sistemi di fabbrica)
- Approfittiamo di questo intervallo in cui i sistemi sono off-line per assicurarci che tutto il software (ed anche l'hardware) sia allineato alle ultime versioni con patch ed antivirus aggiornati e correttamente funzionanti.
  - Apportiamo e testiamo accuratamente le patch ai sistemi esistenti.
  - Facciamo lo stesso anche con tutti i sistemi nuovi ed ogni altro nuovo componente aggiunto.
  - Testiamo che i sistemi antivirus (approvati dai fornitori del sistema di controllo) non abbiamo impatti funzionali e di prestazioni su tutto il sistema di controllo.
- Controlliamo che tutti i sistemi siano impostati per funzionare in modo "safe"
- Verifichiamo che tutto il software (sistemi operativi, programmi e software applicativo) sia configurato in modo conforme sia alle specifiche tecniche e del fornitore che alle policy e procedure di sicurezza aziendali.

- Ogni sistema dovrebbe essere accuratamente testato e "messo in sicurezza" prima di essere collegato alla rete. Eseguiamo tutti i download da sistemi isolati o dei quali siamo assolutamente sicuri.

7.2.6 Supporto per connessioni remote sicure

- Valutiamo bene la richiesta e necessità di connessioni remote per fornitori di sistemi, componenti e servizi, siano essi i fornitori del sistema di controllo, integratori, manutentori, operatori, ecc.
  - Se è richiesto un accesso remoto, facciamo in modo che sia abilitato con la sicurezza in mente (identificazione/autenticazione sicura, autorizzazione ed eventuale crittografia) e venga registrato un log di tutte le connessioni che dovremo monitorare con continuità
  - Autorizziamo le connessioni remote solo per determinati periodi di tempo e da specifici indirizzi.
  - Se possibile dotiamoci di sistemi di allarme e prevenzione per intrusioni non autorizzate, i cosiddetti IDS (Intrusion Detection Systems) ed IPS (Intrusion Prevention System) e che siano possibilmente pensati per applicazioni industriali.

7.2.7 Connessioni sicure con altre reti

- Riguardo alle connessioni dai/ai nostri sistemi di controllo con altre reti sia in azienda che soprattutto esterne:
  - Proteggiamo e segreghiamo le reti dei sistemi di controllo sia da internet che dalle altre reti dell'azienda che abbiamo accesso a internet o ad altri collegamenti esterni (anche email)
  - Soprattutto nella fase iniziale è meglio che sia le reti dei sistemi di controllo che qualunque altra collegata ad essi abbiano un accesso limitato ed estremamente controllato con l'esterno

  - Identifichiamo ogni singola richiesta di connessione, valutiamo e richiediamo esplicita approvazione ed assunzione di responsabilità
  - Sviluppiamo e mettiamo in opera meccanismi per connessioni esterne solo in sicurezza
  - Tutte le connessioni esterne siano filtrate da adeguati firewall o altri dispositivi equivalenti
  - Mettiamo tutte le connessioni sotto IDS (Intrusion Detection Systems) e/o IPS (Intrusion Prevention Systems (possibilmente espressamente pensati per le applicazioni in sistemi e reti di controllo), e soprattutto verifichiamo regolarmente i log generati
  - Se abbiamo connessioni verso fornitori, clienti o enti esterni, facciamo audit periodici: ogni compromissione dei loro sistemi è una potenziale minaccia per i nostri

- Mettiamo in sicurezza tutte le connessioni ai sistemi di controllo via telefono/modem
  - Autorizziamo solo se configurate in modo sicuro connessioni via modem per periodi di tempo assolutamente necessari, per specifici user e da indirizzi identificati
  - Mettiamo in sicurezza le connessioni wireless
  - Se intendiamo mettere in funzione o aumentare le connessioni wireless (anche per diminuire costi e lavori di cablaggio) tra i diversi componenti della rete e del sistema di controllo, pensiamo bene ad implementare appropriate misure di sicurezza per le comunicazioni wireless
- Se utilizziamo vie di comunicazioni di back-up per assicurare una continuità di funzionamento ai nostri sistemi, come ad esempio connessioni a tronconi di rete pubblica "aperta" (ADSL? Fibra?) da utilizzare solo quanto la nostra rete interna "protetta" è fuori uso, e quindi "al di fuori" dei nostri firewall aziendali, assicuriamoci di avere adeguati presidi anche su queste connessioni.
- Non dimentichiamoci le misure di sicurezza anche per tutti i componenti della nostra rete di controllo: router, switch, fire-

wall, dispositivi per VPN (Virtual Private Network), dispositivi per identificazione, autorizzazione, autenticazione ed ogni altro componente della rete e del sistema di controllo deve essere configurato in conformità alle policy e procedure di security stabilite dall'azienda (senza lasciare settaggi di default, ecc.).

7.2.8 Ripartenza dei processi controllati in "Safety" e in "Security"

- Assicuriamoci che per ogni sistema e componente riparato o sostituito (sistema di controllo, attuatori, sensori, router, firewall, software, ecc.) ci sia una persona responsabile al quale fare riferimento e che venga messo in funzione rispettando appropriate misure di security
- Tutti i sistemi per la sicurezza fisica devono essere installati e testati prima di fare "le prove" di ripartenza
- Verificare accuratamente tutte le messe a terra e relativi sistemi di protezione: ispezionarli, misurarli e rimetterli in efficienza secondo quanto necessario. La messa a terra è sempre un aspetto critico quando si viene colpiti da calamità quali venti molto forti, alluvioni ed allagamenti o quando gli impianti elettrici vengono esposti ad elementi chimici, corrosivi o tossici o anche solo eccessiva umidità che possano avere impatti sulla conduttività e provocare cortocircuiti.
- Controllare tutti gli interruttori e le protezioni di emergenza, anche quelli di gruppi e generatori per l'alimentazione di riserva.
- Finalmente facciamo ripartire il processo e controlliamo che gli impianti funzionino secondo quanto atteso:
  - Specialmente durante la ripartenza, teniamo particolarmente d'occhio tutti gli aspetti con un impatto sulla sicurezza e il controllo del processo
  - Annotiamoci ogni anomalia sospetta e valutiamo al momento ogni indizio di eventuali prestazioni differenti da quelle previste.

- Se abbiamo condizioni assolutamente diverse dal normale, attiviamoci per fermare e portare in modo sicuro l'impianto ed il processo e rieseguiamo la configurazione ed i test secondo necessità.

- Soltanto dopo aver verificato che tutto nel nostro processo e nei nostri sistemi di controllo funzioni e proceda correttamente e come previsto, potremo riaprire le connessioni necessarie come in precedenza indicato.

7.3. LA LEZIONE

Ricordiamoci di documentare e prendere nota di tutte le decisioni, di ogni passo fatto ed ogni evento al quale abbiamo assistito sia durante la ricostruzione, la riconfigurazione ed anche durante tutto il processo di ripartenza: questa esperienza potrà essere utile per ogni futura necessità di fermata e ripartenza sia in condizioni di emergenza sia programmate.

Tutto questo materiale sarà prezioso per stendere ed aggiornare tutti i nostri documenti, le nostre policy e procedure di ripartenza, eventuale Disaster Recovery Plan (DRP), il Business Continuity Plan (BCP) e il Continuity of Operation Plan (COOP).

A questo punto dobbiamo anche pensare ad un nuovo Risk Assessment, che comprenda anche un nuovo Vulnerability Assessment, per identificare qualsiasi vulnerabilità che possa essere evidenziata e risultare da tutti i cambiamenti effettuati sui sistemi e sulle condizioni al contorno.

7.4. NOTE FINALI

Pur augurandoci di non aver la necessità di dover ricostruire in parte o addirittura integralmente un sistema di controllo a causa degli effetti dovuti a cause esterne, da questo esercizio risultano evidenti alcuni punti sui quali è necessario riflettere:

1. non è possibile rimettere insieme un sistema se non abbiamo una traccia documentata di come era fatto e quindi una gestione della configurazione. Sono oggi disponibili molti tool spe-

cifici, pensati per l'industria ed i sistemi di fabbrica, per tenere sotto controllo la vita e l'evoluzione dei nostri sistemi: dalla progettazione, alla installazione iniziale, alla implementazione e commissioning, alle manutenzioni ordinaria e straordinaria che ogni sistema "vivo" nel tempo inevitabilmente subisce, fino alla sua dismissione.

2. A parte la tracciabilità dei componenti hardware, è di vitale importanza per la ripartenza avere dei back-up aggiornati di tutti i componenti software e dei dati gestiti. Anche per questo aspetto, sono oggi disponibili tool appropriati per il salvataggio gestito dei software dei sistemi di controllo, che spesso sono assolutamente diversi da quelli del tradizionale mondo dell'Information Technology: come ad esempio gestire i back-up dei software su PLC e sistemi DCS?
3. Parlando di back-up, risulta evidente che è necessaria anche una procedura che stabilisca quando devono essere effettuati e dove tenere i supporti: averli nella stessa location del sistema principale li espone agli stessi rischi (es. alluvione, fuoco, contaminazione RF, ecc.)
4. L'identificazione ed eliminazione dei cosiddetti "single-point-of-failure" che possano essere emersi nell'evento avverso ci devono guidare nella riprogettazione dei sistemi.
5. Il fattore umano è forse l'aspetto più importante ed a volte destabilizzante in tutte queste esperienze: cerchiamo quindi di imparare da quello che è successo, e pensiamoci a fondo non solo nelle disegno dei sistemi di controllo, ma anche in tutte le policy e procedure relative alla security dell'azienda relative all'ambiente del processo.

Appendice A

In questa appendice si fornisce un esempio concreto di una procedura di emergenza ottenuta implementando le raccomandazioni fornite nella prima parte di questa linea guida. Si tratta di una procedura da usare come guida alle aziende che si occupano di fornitura di acque potabili durante la preparazione del proprio Piano di Gestione delle Emergenze.

In questa procedura sono state differenziate le situazioni di emergenza in base ai seguenti criteri.

Livello I. Problemi di Routine

Livello II. Emergenze di tipo Alert/Minori

Livello III. Emergenze Importanti

Livello IV. Disastro naturale

Livello V. Disastro Nucleare/Atti Terroristici Importanti

Nel seguito per ognuno dei livelli si forniscono le schede di emergenza per i singoli livelli.

Livello I	Problemi di Routine
Descrizione	Questi incidenti sono di minore rilevanza per il sistema dell'acqua che interessano il 10% o meno del sistema ed è previsto che vengano risolti in 24 ore o meno.
Esempio	Rotture della conduttura dell'acqua e problemi meccanici alle stazioni di pompaggio
Risposta Iniziale	1.Iniziare i log della documentazione (Emergency Response Checklist) alla prima notifica del problema. 2.Studiare il problema e valutazione della situazione per determinare il livello dell'emergenza.
Procedure di risposta	3.Attivare il team di risposta alle emergenze in conformità con il Piano di risposta alle emergenze. 4.Mantenere i record di tutte le attività svolte durante l'incidente. Archiviazione delle annotazioni come riferimento futuro. 5.Monitorare la risoluzione dell'emergenza e definizione delle azioni necessarie a seguito di una modifica del livello di emergenza.
Note	- Se avviene una violazione che richiede un avviso pubblico di tipo tier 1 in conformità con 310 CMR 22.16, il PWS deve mettersi in contatto consultare il personale di DEP entro 24 ore dalla prima scoperta di violazione del sistema pubblico dell'acqua. - Se avviene una violazione di un bacillo coliforme, il sistema pubblico dell'acqua deve mettere a file una Indagine valutazione di Violazione da bacillo coliforme (appendice H) con l'ufficio regionale locale di DEP. Questa indagine non verrà usata per scopi di compliance ma fornirà al DEP le informazioni sulle cause e sulle azioni correttive per le violazioni da bacillo coliforme.

Livello II	Emergenze di tipo Alert/Minori
Descrizione	Questi incidenti sono più significativi per il sistema dell'acqua, possono interessare fino al 50% dell'intero sistema ed è previsto che siano risolti entro 72 ore o meno.
Esempio	Rilevazione totale locale del bacillo coliforme, rotture principali importanti, rotture principali multiple, problemi meccanici importanti alle stazioni di pompaggio, o guasto dei sistemi chimici di alimentazione.
Risposta Iniziale	1.Iniziare i log della documentazione (Emergency Response Checklist) alla prima notifica del problema. 2.Studiare il problema e valutazione della situazione per determinare il livello dell'emergenza.
Procedure di risposta	3.Attivare il team di risposta alle emergenze in conformità con il Piano di risposta alle emergenze. 4.Contattare l'autorità responsabile locale, incluso l'Ufficio Regionale del DEP, per informarli delle condizioni del sistema e per discutere eventuali azioni speciali che possono rendersi necessarie. Queste azioni possono includere le seguenti, ma non sono limitate a queste: - Raccogliere speciali campioni di qualità dell'acqua riferiti alla natura dell'emergenza

Livello II	Emergenze di tipo Alert/Minori *(cont.)*
Procedure di risposta	- Raccogliere i campioni adeguati di qualità dell'acqua nei siti lungo tutto il sistema di distribuzione in cui si sono verificati i problemi. Questi campioni devono essere prelevati sia durante che dopo l'incidente. Se si rileva che il problema è relativo al bacillo coliforme, seguire il flusso relativo alla Determinazione della Violazione MCL coliforme contenuto nell'allegato G. - Dare notifica ai soggetti/reparti impattati dall'incidente. - Fornire una fonte alternative di acqua per i soggetti/reparti impattati dall'incidente, se necessario. - Contattare i media locali per informare dell'incidente , se necessario. - Dare notifica pubblica di qualsiasi violazione delle norme di DEP, se necessario. 5.Contattare l'autorità responsabile locale, incluso l'Ufficio Regionale del DEP, per informarli del completamento delle azioni di ripristino e dei risultati di tutti i test di qualità dell'acqua. 6.Mantenere i record di tutte le attività svolte durante l'incidente. Archiviazione delle annotazioni come riferimento futuro. 7.Monitorare la risoluzione dell'emergenza e definizione delle azioni necessarie a seguito di una modifica del livello di emergenza.
Note	- Se avviene una violazione che richiede un avviso pubblico di tipo tier 1 in conformità con 310 CMR 22.16, il PWS deve mettersi in contatto consultare il personale di DEP entro 24 ore dalla prima scoperta di violazione del sistema pubblico dell'acqua. - Se avviene una violazione di un bacillo coliforme, il sistema pubblico dell'acqua deve mettere a file una Indagine valutazione di Violazione da bacillo coliforme (appendice H) con l'ufficio regionale locale di DEP. Questa indagine non verrà usata per scopi di compliance ma fornirà al DEP le informazioni sulle cause e sulle azioni correttive per le violazioni da bacillo coliforme.

Livello III	Emergenze Importanti
Descrizione	Questi incidenti sono molto significativi per il sistema dell'acqua, possono interessare più del 50% dell'intero sistema ed è previsto che siano risolti in più di 72 . Le emergenze importanti possono richiedere una Dichiarazione di Emergenza dello stato della fornitura dell'acqua e/o un ordine di bollire l'acqua, un ordine di non berla o un ordine di non utilizzarla.
Esempio	Rottura nella conduttura principale della trasmissione, perdita o guasto della funzione di trattamento, perdita della fornitura (rottura della diga, scarsità del rifornimento idrico, contaminazione, ecc.), perdita di pressione nel sistema, scoppio totale diffuso del bacillo coliforme, rilevazione del bacillo coliforme fecale o di E. Coli, o atti di vandalismo.

Livello III	Emergenze Importanti
Risposta Iniziale	1. Iniziare i log della documentazione (Emergency Response Checklist) alla prima notifica del problema. 2. Studiare il problema e valutazione della situazione per determinare il livello dell'emergenza.
Procedure di risposta	**<u>Contaminazione batterica</u>** 3. Iniziare la consultazione con il DEP e seguire I requisiti di Notifica Pubblica. 4. Attivare il team di risposta alle emergenze in conformità con il Piano di risposta alle emergenze per raccogliere i campioni e fare analisi preliminari per determinare la potenziale contaminazione della fornitura dell'acqua. 5. Utilizzare i dati per seguire il flusso relativo alla Determinazione della Violazione MCL coliforme contenuto nell'allegato G. 6. Contattare l'autorità responsabile locale, incluso l'Ufficio Regionale del DEP, per informarli delle condizioni del sistema e per discutere eventuali azioni speciali che possono rendersi necessarie. Queste azioni possono includere le seguenti, ma non sono limitate a queste: - Raccogliere speciali campioni di qualità dell'acqua riferiti alla natura dell'emergenza - Raccogliere i campioni adeguati di qualità dell'acqua nei siti lungo tutto il sistema di distribuzione in cui si sono verificati i problemi. Questi campioni devono essere prelevati sia durante che dopo l'incidente. Se si rileva che il problema è relativo al bacillo coliforme, seguire il flusso relativo alla Determinazione della Violazione MCL coliforme contenuto nell'allegato G. - Dare notifica ai soggetti/reparti impattati dall'incidente. - Con l'approvazione del DEP, fornire una fonte alternativa di acqua se necessario. Le fonti d'acqua alternative dovrebbero essere identificate nel piano di risposta alle emergenze e possono includere l'acqua in bottiglia, connessioni con altri sistemi di fornitura dell'acqua, acqua in lattina, etc. - Contattare i media locali per informare dell'incidente , se necessario. - Se il DEP emette una dichiarazione di emergenza dello stato della fornitura dell'acqua e/o un ordine di bollire l'acqua, un ordine di non berla o un ordine di non utilizzarla, seguire le procedure necessarie. 7. Una volta identificato il problema, attivare le azioni per risolverlo. 8. Contattare l'autorità responsabile locale, incluso l'Ufficio Regionale del DEP, per informarli del completamento delle azioni di ripristino e dei risultati di tutti i test di qualità dell'acqua. 9. Mantenere i record di tutte le attività svolte durante l'incidente. Archiviazione delle annotazioni come riferimento futuro. 10 Monitorare della risoluzione dell'emergenza e definizione delle azioni necessarie a seguito di una modifica del livello di emergenza.

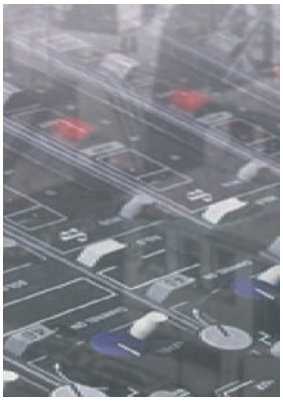
Livello III	Emergenze Importanti *(cont.)*
Procedure di risposta *(cont.)*	11. Contattare l'autorità responsabile locale, incluso l'Ufficio Regionale del DEP, per informarli del completamento delle azioni di ripristino e dei risultati di tutti i test di qualità dell'acqua. 12. Mantenere i record di tutte le attività svolte durante l'incidente. Archiviazione delle annotazioni come riferimento futuro. 13.Monitorare la risoluzione dell'emergenza e definizione delle azioni necessarie a seguito di una modifica del livello di emergenza. **<u>Danneggiamento del sistema:</u>** 14. Attivare il team di risposta alle emergenze per valutare the extent of the problem and determine the type and quantity of support needed to initiate corrective action. 15. Contattare l'autorità responsabile locale, incluso l'Ufficio Regionale del DEP, per informarli delle condizioni del sistema e per discutere eventuali azioni speciali che possono rendersi necessarie. Queste azioni possono includere le seguenti, ma non sono limitate a queste: ·- Completare le analisi preliminari di qualità dell'acqua per determinare la contaminazione potenziale del rifornimento idrico come conseguenza del guasto del sistema. ·- Dare notifica ai soggetti/reparti impattati dall'incidente. ·- Con l'approvazione del DEP, fornire una fonte alternativa di acqua se necessario. Le fonti d'acqua alternative dovrebbero essere identificate nel piano di risposta alle emergenze e possono includere l'acqua in bottiglia, connessioni con altri sistemi di fornitura dell'acqua, acqua in lattina, etc. · Contattare i media locali per informare dell'incidente , se necessario. - Se il DEP emette una dichiarazione di emergenza dello stato della fornitura dell'acqua e/o un ordine di bollire l'acqua, un ordine di non berla o un ordine di non utilizzarla, seguire le procedure necessarie. 16. Una volta identificato il problema, attivare le azioni per risolverlo.
Note	- Se avviene una violazione che richiede un avviso pubblico di tipo tier 1 in conformità con 310 CMR 22.16, il PWS deve mettersi in contatto consultare il personale di DEP entro 24 ore dalla prima scoperta di violazione del sistema pubblico dell'acqua. - Se avviene una violazione di un bacillo coliforme, il sistema pubblico dell'acqua deve mettere a file una Indagine valutazione di Violazione da bacillo coliforme (appendice H) con l'ufficio regionale locale di DEP. Questa indagine non verrà usata per scopi di compliance ma fornirà al DEP le informazioni sulle cause e sulle azioni correttive per le violazioni da bacillo coliforme.

Livello IV	Disastro naturale
Descrizione	Questi incidenti sono causati generalmente da un evento meteorologico o geologico diffuso che interrompe il sistema dell'acqua e che interessa più del 50% dell'intero sistema e richiedono più di una settimana per il ripristino dei servizi. Tali eventi possono creare danni strutturali alla funzione di trattamento delle acque o contaminare una fonte con acque luride non trattate, con un prodotto chimico tossico, o con materiale radioattivo. Le emergenze importanti possono richiedere una Dichiarazione di Emergenza dello stato della fornitura dell'acqua e/o un ordine di bollire l'acqua, un ordine di non berla o un ordine di non utilizzarla. *Se la rottura del sistema causa il guasto di apparecchiatura e/o contaminazione causata da attività batteriologica, seguire la procedura di risposta alle emergenze per il LIVELLO III. Se la contaminazione è causata da un composto (o composti) chimico, seguire la seguente procedura*
Esempio	Uragani, cicloni, terremoti, o inondazioni
Risposta Iniziale	1. Iniziare i log della documentazione (Emergency Response Checklist) alla prima notifica del problema. 2. Studiare il problema e valutazione della situazione per determinare il livello dell'emergenza.
Procedure di risposta	**<u>Contaminazione chimica</u>** 3. Se possibile, rimuovere la fonte interessata del rifornimento idrico o chiudere il sistema di distribuzione fino a quando sia stato valutato il livello di contaminazione. 4. Contattare l'Ufficio regionale di DEP per ulteriori istruzioni. 5. Informare le agenzie/autorità locali competenti attivare immediatamente la squadra di risposta e risponda in conformità con il programma di risposta di emergenza. L'autorità o le autorità responsabile pubblicherà "gli ordini" necessari. Vedi appendice D - procedure che coinvolgono le agenzie ed il personale esterno. 6. Informare il pubblico attraverso i media elettronici locali/regionali circa l'emergenza, la zona interessata, e il rifornimento idrico alternativo. Tenere il pubblico informato circa i nuovi sviluppi con "i rapporti speciali e le notizie di servizio pubblico". 7. Con approvazione di DEP, attivare il rifornimento idrico alternativo quale l'acqua in bottiglia, connessioni con altri sistemi di fornitura dell'acqua, acqua in lattina, etc. 8. Valutare la situazione per informare le autorità e il pubblico. Se necessario, approntare altre misure precauzionali per salvaguardare la sanità pubblica. 9. Raccogliere i nuovi campioni per le analisi e implementare un sistema di controllo per garantire la qualità dell'acqua. 10. Mantenimento dei record di tutte le attività svolte durante l'incidente. Archiviazione delle annotazioni come riferimento futuro.

Livello IV	Disastro naturale
Procedure di risposta *(cont.)*	11. Monitoraggio della risoluzione dell'emergenza e definizione delle azioni necessarie a seguito di una modifica del livello di emergenza. 12. Completare la checklist e allegare i moduli/memorandum necessari. Trasmettere all'Ufficio Regionale del Reparto (2) copie della checklist completata e di tutti gli allegati. Non sarà necessario trasmettere queste specifiche informazioni di emergenza al DEP se altri processi già forniscono quanto necessario (es.procedura dichiarazione di emergenza). dine di non berla o un ordine di non utilizzarla.
Note	- Se avviene una violazione che richiede un avviso pubblico di tipo tier 1 in conformità con 310 CMR 22.16, il PWS deve mettersi in contatto consultare il personale di DEP entro 24 ore dalla prima scoperta di violazione del sistema pubblico dell'acqua. - Se avviene una violazione di un bacillo coliforme, il sistema pubblico dell'acqua deve mettere a file una Indagine valutazione di Violazione da bacillo coliforme (appendice H) con l'ufficio regionale locale di DEP. Questa indagine non verrà usata per scopi di compliance ma fornirà al DEP le informazioni sulle cause e sulle azioni correttive per le violazioni da bacillo coliforme.

Livello V	Disastro Nucleare/Atti Terroristici Importanti
Descrizione	Questi incidenti provocano una fuoriuscita vasta e incontrollata di materiali o composti radioattivi nelle sorgenti che alimentano il sistema di acque potabili (atti terroristici). In caso di disastro nucleare le sorgenti di superficie in un raggio di 50 miglia possono essere immediatamente contaminate. Le sorgenti sotterranee possono rimanere sicure per un breve periodo di tempo. Va richiesta una dichiarazione di Emergenza nella fornitura d'acqua ed un ordine di "Non bere acqua di fonte".
Esempio	Impianto di Energia Nucleare che rilascia nelle falde acquifere, causa incidente o sabotaggio, materiale altamente tossico.
Risposta Iniziale	1.Iniziare i log della documentazione (Emergency Response Checklist) alla prima notifica del problema. 2.Studiare il problema e valutazione della situazione per determinare il livello dell'emergenza.

Livello V	Disastro Nucleare/Atti Terroristici Importanti
Procedure di risposta	3 Se possibile, rimuovere la fonte interessata del rifornimento idrico o chiudere il sistema di distribuzione fino a quando sia stato valutato il livello di contaminazione. 4. Contattare l'Ufficio regionale di DEP per ulteriori istruzioni. 5. Informare le agenzie/autorità locali competenti attivare immediatamente la squadra di risposta e risponda in conformità con il programma di risposta di emergenza. L'autorità o le autorità responsabile pubblicherà "gli ordini" necessari. Vedi appendice D - procedure che coinvolgono le agenzie ed il personale esterno. 6. Informare il pubblico attraverso i media elettronici locali/regionali circa l'emergenza, la zona interessata, e il rifornimento idrico alternativo. Tenere il pubblico informato circa i nuovi sviluppi con "i rapporti speciali e le notizie di servizio pubblico". 7. Con approvazione di DEP, attivare il rifornimento idrico alternativo quale l'acqua in bottiglia, connessioni con altri sistemi di fornitura dell'acqua, acqua in lattina, etc. 8. Valutare la situazione per informare le autorità e il pubblico. Se necessario, approntare altre misure precauzionali per salvaguardare la sanità pubblica. 9. Raccogliere i nuovi campioni per le analisi e implementare un sistema di controllo per garantire la qualità dell'acqua. 10. Mantenimento dei record di tutte le attività svolte durante l'incidente. Archiviazione delle annotazioni come riferimento futuro. 11. Monitoraggio della risoluzione dell'emergenza e definizione delle azioni necessarie a seguito di una modifica del livello di emergenza. 12. Completare la checklist e allegare i moduli/memorandum necessari. Trasmettere all'Ufficio Regionale del Reparto (2) copie della checklist completata e di tutti gli allegati. Non sarà necessario trasmettere queste specifiche informazioni di emergenza al DEP se altri processi già forniscono quanto necessario (es.procedura dichiarazione di emergenza).
Note	- Se avviene una violazione che richiede un avviso pubblico di tipo tier 1 in conformità con 310 CMR 22.16, il PWS deve mettersi in contatto consultare il personale di DEP entro 24 ore dalla prima scoperta di violazione del sistema pubblico dell'acqua. - Se avviene una violazione di un bacillo coliforme, il sistema pubblico dell'acqua deve mettere a file una Indagine valutazione di Violazione da bacillo coliforme (appendice H) con l'ufficio regionale locale di DEP. Questa indagine non verrà usata per scopi di compliance ma fornirà al DEP le informazioni sulle cause e sulle azioni correttive per le violazioni da bacillo coliforme.



Bibliografia

FONTI

Computer Security Incident Handling Guide. NIST -National Institute of Standard and technology - Special Publication 800-61. USA January 2004

Guide to malware prevention and Incident handling. NIST - USA National Institute of Standard and technology - Special Publication 800-63. November 2005.

Incident Command System: A Developing National Standard of Incident Management in the U.S. Stephen E. Hannestad. Center for Information Policy, College of Information Studies, University of Maryland. Proceedings of the 2nd International ISCRAM -Brussels, Belgium, April 2005.

National Incident Management System -, Homeland Security. USA March 1, 2004

Interim National Infrastructure Protection Plan - USA Homeland Security. February 2005

National Preparadness Guidance. USA Homeland Security. April 27, 2005

Standards for Security Categorization of Federal Information and Information Systems. USA FIPS PUB 199: Federal Information Processing Standards Publication

Control Systems Cyber Security Awareness, US-CERT - Informational Focus Paper . USA, July 7, 2005

Computer Security Information . Technology Division Laboratory, NIST National Institute of Standards and Technology. USA, February 2004

Telecommunications Infrastructure In Disasters: Preparing Cities for Crisis Communications Anthony M. Townsend Mitchell L. Moss Center for Catastrophe Preparedness and Response & Robert F. Wagner Graduate School of Public Service New York University USA, April 2005.

Common Sense Guide to Cyber Security for Small Businesses: Recommended Actions for Information Security. Internet Security Alliance. USA 1st Edition - March 2004

Handbook for Computer Security Incident Response Teams (CSIRTs). CMU/SEI USA April 2003BIT

'Contingency Planning Guide for Information Technology Systems, NIST-National Institute of Standard and Technology,USA, Giugno 2002

"Federal Legislative and Regulatory Business Continuity Requirements for the IRS" version 1.0, MITRE-Center for Enterprise Modernization,USA, 28 Febbraio 2003

European Commission, "Green Paper On a European Programme For Critical Infrastructure Protection" COM(2005) 576 final, Brussels, 17 Novembre 2005

Incident Response Managing Security at Microsoft, Technical White Paper Published: January 2003
"COBIT® 4.0 *(Control Objectives for Information and related Technology)*, IT Governance Institute, UK, 2005

"*National incident Management system*", Homeland Securit,y USA, 1 Marzo 2004

'*Code of practice for information security management*' International Standard ISO/IEC Second edition 2005-06-15

Presidenza del Consiglio dei Ministri, *Dipartimento per l'Innovazione e le Tecnologie: Protezione delle Infrastrutture Critiche Informatizzate*

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, *LA SICUREZZA DELLE RETI nelle infrastrutture critiche,* Ministero delle Comunicazioni, 2005

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, *NETWORK SECURITY in critical infrastructures,* Ministry of Communications, 2005

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, *LA SICUREZZA DELLE RETI. Dall'analisi del rischio alle strategie di protezione*, Ministero delle Comunicazioni, 2005

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, *NETWORK SECURITY. From risk analysis to protection strategies*, Ministero delle Comunicazioni, 2005

CNIPA: *Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la Pubblica Amministrazione*

CLUSIT: *Progetto ITAISAC*

D. Perucchini, *FUB: ISAC*, Note preliminari

THE WHITE HOUSE: *The National Strategy to Secure Cyberspace*

THE WHITE HOUSE: *Homeland Security Presidential Directive - 7 (HSPD-7)*, Critical infrastructure Identification, Prioritization and Protection

THE WHITE HOUSE: *Presidential Decision Directive 63 (PDD63),* Critical Infrastructure Protection

G. Brunette, *Toward Systemically Secure It Architectures, Sun Microsystems* BluePrints OnLine, February 2006

NIAC: *Sector Partnership Model Working Group*

United States General Accounting Office: *Information sharing responsibilities, challenges and key management issue*

ISAC Council White Paper: *Government - Private sector relations*

ISAC Council White Paper: *A functional model for critical infrastructure information sharing and analysis maturing and expanding efforts*

National Infrastructure Security Co-ordination Centre (NISCC): *First Responder's Guide: Policy and Principles*

Decisione del Consiglio europeo 92/242/EEC del 21 marzo 1992: *Sicurezza delle informazioni*

Proposta di Decisione-quadro del Consiglio Europeo relativa agli attacchi contro i sistemi di informazione (COM(2002))

Risoluzione del Consiglio europeo del 18 febbraio 2003: *Un approccio europeo per una cultura della sicurezza delle reti e dell'informazione*

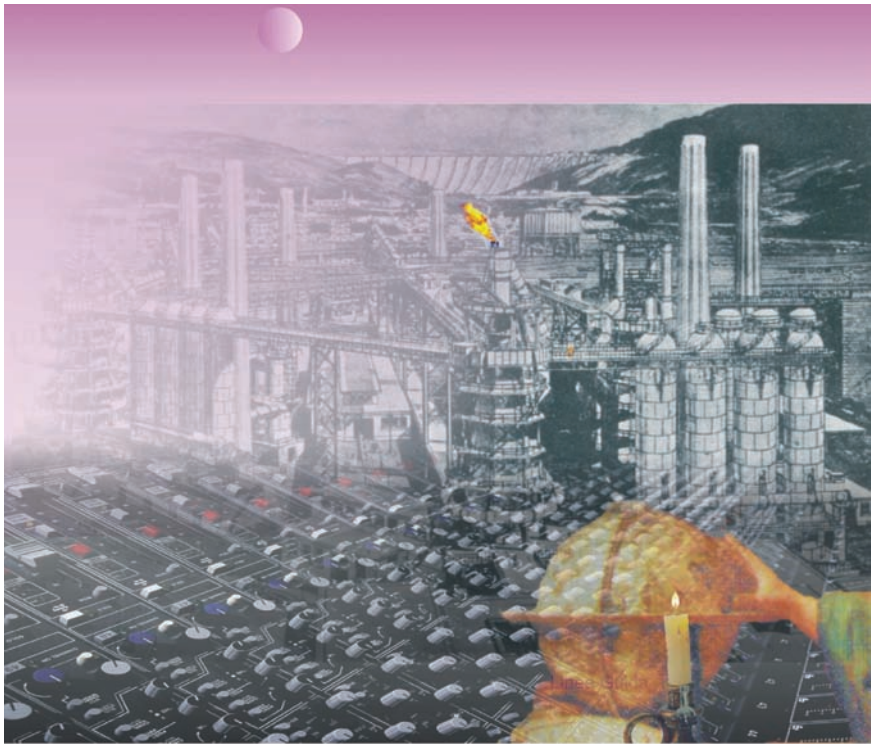
Decisione n° 2256/2003/CE del parlamento europeo e del Consiglio europeo del 17 novembre 2005: *adozione di un programma pluriennale (2003-2005) per il monitoraggio del piano d'azione eEurope 2005, la diffusione delle buone prassi ed il miglioramento della sicurezza delle reti e dell'informazione (MODINIS)*

L'Altra P.A: *I Cert di tutta Europa cooperano per la sicurezza informatica* - Intervista con Gianluigi Moxedano - Direttore del GovCERT del CNIPA

Gianluigi Moxedano: *Il CERT governativo, Seminari di studio CNIPA* - 13 giugno 2005

LINK

www.iscom.gov.it
www.innovazione.gov.it
www.cnipa.gov.it
www.cnipa.gov.it/site/_files/govcert-seminario-cnipa.pdf
www.clusit.it
www.whitehouse.gov/pcipb
www.fedcirc.gov/library/legislation/presDec
Directive63.html
www.dhs.gov/interweb/assetlibrary/NIAC_SectorPartnershi
pModelWorkingGroupUpdateOct05.pdf
www.gao.gov
www.isaccouncil.org
www.it-isac.org
www.ncs.gov
www.ncs.gov/services.html#isac
www.us-cert.gov
www.crime-research.org/library/Saytarly_apr.html
europa.eu.int/information_society/index_ithtm
www.enisa.eu.ini
www.niscc.gov.uk
www.cabinetoffice.gov.uk/csia
www.cesg.gov.uk
www.iaac.org.uk
www.cse.dnd.ca
www.bsi.bund.de
www.ssi.gouv.fr/fr/dcssi
www.certa.ssi.gouv.fr



Tutte le Linee Guida Iscom sono scaricabili dal sito
www.iscom.gov.it

realizzazione GRAPHICLAB
SETTORE DIVULGAZIONE E COMUNICAZIONE ESTERNA ISCOM

Stampa: Gruppo Grafiche Editoriali - Roma

Ministero delle Comunicazioni

iscom
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

DIVULGAZIONE E COMUNICAZIONE ESTERNA

LINEE GUIDA ISCOM PUBBLICATE

SICUREZZA DELLE RETI DALL'ANALISI DEL RISCHIO ALLE STRATEGIE DI PROTEZIONE

SICUREZZA DELLE RETI NELLE INFRASTRUTTURE CRITICHE

LA QUALITÀ DEI SERVIZI NELLE RETI ICT

GESTIONE DELLE EMERGENZE LOCALI

RISK ANALYSIS APPROFONDIMENTI

QUALITÀ DEL SERVIZIO SU UMTS

QUALITÀ DEI SERVIZI PER LE PMI SU RETI FISSE A LARGA BANDA

CERTIFICAZIONE DELLA SICUREZZA ICT

OUTSOURCING E SICUREZZA