

Speciale Sicurezza.

Intervista a Luisa Franchina Direttore Generale dell'Istituto Superiore delle Comunicazioni e della Tecnologia dell'Informazione

Il ruolo dell'I.S.C.T.I., l'Osservatorio nazionale per la sicurezza delle reti e la tutela delle comunicazioni, il gruppo di lavoro per la protezione delle infrastrutture critiche informatiche.

<http://www.isacaroma.it/html/newsletter/?q=node/33>

<http://www.isacaroma.it/pdf/news/0411-franchina.pdf>



L'ing. Luisa Franchina è Direttore Generale del Ministero delle Comunicazioni. Precedentemente ha lavorato in Solving International, Xfera e Deloitte Consulting. È stata docente presso l'Università di Roma "La Sapienza".

Contatti:
luisa.franchina@comunicazioni.it

Cos'è l'Istituto Superiore delle comunicazioni e delle tecnologie dell'informazione presso il Ministero Comunicazioni?

L'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione è stato costituito nel 1907; nel 1923 vi è stata annessa la Scuola Superiore di Specializzazione in Telecomunicazioni.

L'Istituto ha numerosi ambiti di attività:

- misure (segnalo tra gli altri le misure su parametri di qualità del servizio e di sicurezza delle reti);
- omologazioni (obbligatorie e volontarie);
- certificazioni (obbligatorie e volontarie: segnalo tra le altre le certificazioni dell'Organismo per la Sicurezza);
- formazione;
- regolamentazione e standardizzazione (nazionale e internazionale);
- ricerca di base e applicata.

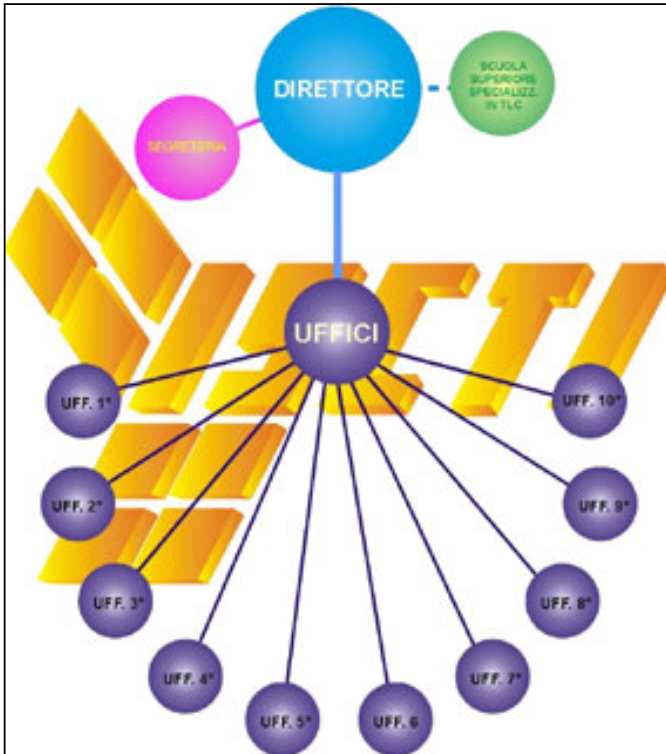
La normazione tecnica, soprattutto quella di carattere internazionale in cui l'Istituto è attore attivo e propositivo, riveste un ruolo sempre più rilevante vista anche l'esigenza, nata specialmente tra gli ormai



normativo.

numerosi gestori di reti e servizi di telecomunicazioni, di chiarezza e standardizzazione in ambito

L'ISCTI, tramite il CONCIT (ente formato da CEI, UNI e dallo stesso Istituto e riconosciuto a livello europeo) effettua la trasposizione nell'ordinamento nazionale delle norme europee emesse dall'ETSI. Per l'attività di normazione l'Istituto Superiore C.T.I. fornisce il personale qualificato a rappresentare l'Amministrazione con funzioni di Capo Delegazione dei gruppi nazionali presenti nelle varie commissioni e gruppi tecnici di studio.



Struttura dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (I.S.C.T.I.). Fonte: <http://www.comunicazioni.it/it/index.php?Mn1=9&Mn2=35>

Inoltre, aderendo ad una specifica richiesta della Presidenza del Consiglio dei Ministri, è stato allestito un Centro per la Valutazione della sicurezza informatica di prodotti e sistemi destinati a gestire dati coperti dal Segreto di Stato o di vietata divulgazione (CE.VA.).

Cos'è l'Organismo di Certificazione della sicurezza dei sistemi e prodotti informatici commerciali?

Su richiesta della Presidenza del Consiglio dei Ministri, l'Istituto si è attivato per istituire l'Organismo di Certificazione della sicurezza dei sistemi e prodotti informatici commerciali. L'ISCTI collabora con l'IMQ insieme al quale svolge attività di verifica e controllo sui Sistemi di Qualità Aziendale in osservanza delle norme UNI EN ISO 9000, o nell'attività di controllo dei Laboratori Accreditati e degli Organismi Notificati a fronte della norma UNI CEI EN 45001.

L'Istituto, possedendo le competenze, i laboratori e le attrezzature per l'effettuazione delle prove tecniche è Organismo Notificato ai sensi delle Direttive "riguardanti le apparecchiature radio e le apparecchiature terminali di telecomunicazione e il reciproco riconoscimento in ambito europeo della loro

conformità" e ricopre il ruolo di "Competent Body" in materia di compatibilità elettromagnetica.

L'Istituto ha sottoscritto nel 2002 il contratto internazionale per diventare Ente di Certificazione Europeo per conto del TETRA MoU.

L'ISCTI detiene inoltre il database dei numeri "portati" in tecnologia GSM e UMTS e altri database relativi alle assegnazioni numeriche.

Lei dirige anche l'Osservatorio nazionale per la Sicurezza delle Reti e la Tutela delle Comunicazioni. Di che si tratta?

L'osservatorio interministeriale per la sicurezza delle reti e la tutela dell'informazione è presieduto dal Segretario Generale del Ministero delle comunicazioni con il supporto tecnico della sottoscritta ed è composto da rappresentanti dei ministeri delle comunicazioni, della giustizia, dell'interno, della difesa, delle attività

produttive e della Presidenza del Consiglio dei ministri – dipartimento per la funzione pubblica e dipartimento per l'innovazione e le tecnologie.

I compiti dell'osservatorio sono i seguenti:

- predisposizione degli atti normativi in materia di sicurezza delle reti, di tutela delle comunicazioni e di attività investigative ai fini di giustizia, comprendendo la rete Internet anche a tutela dei minori;
- tenuta dei rapporti con gli organismi nazionali ed internazionali che si occupano dell'argomento;
- monitoraggio delle attività e della condotta degli operatori assoggettati ad obblighi verso l'Autorità ed altri organismi;
- monitoraggio dello sviluppo tecnologico del settore, con specifico riguardo alla sicurezza;
- collaborazione e consulenza, per gli aspetti tecnologici, alle amministrazioni pubbliche che manifestino l'esigenza di implementare la sicurezza dei propri "punti sensibili";
- consulenza alle pubbliche amministrazioni nell'indicazione degli operatori che forniscono servizi di telecomunicazione anche in base al livello dell'offerta di sicurezza ed ai costi;
- definizione di un "livello minimo" di sicurezza indispensabile per ottenere l'accesso alle reti pubbliche;

- formulazione di suggerimenti per la protezione delle infrastrutture civili relativamente ai temi degli attacchi e dei rischi di tipi elettronico ed elettromagnetico;
- indicazioni circa la certificazione ed elaborazione degli standard di sicurezza dei servizi e delle infrastrutture di telecomunicazioni;
- promozione di azioni di sensibilizzazione con apposite campagne informative;
- collaborazione con il Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni



Che tipo di lavoro svolge l'Osservatorio?

L'Osservatorio lavora attraverso Gruppi di lavoro *ad hoc*; sono attualmente attivi sei gruppi di lavoro che si occupano di:

1. obblighi di legge degli operatori TLC;
2. regolamentazione sulla portabilità dei numeri (trasmesso all'Ufficio Legislativo del Ministero Comunicazioni in luglio 2004);
3. codice di autoregolamentazione sui servizi a sovrapprezzo e sullo SPAM (in collaborazione con il Garante della Privacy);
4. conservazione e trattamento dei dati (in collaborazione con il Garante della Privacy che sta lavorando al codice di autoregolamentazione relativo);
5. redazione di linee guida su Sicurezza delle Reti e delle infrastrutture TLC per le Infrastrutture Critiche informatizzate (in collaborazione con le infrastrutture critiche del Paese);
6. redazione di linee guida sui metodi di analisi dei rischi per la sicurezza delle reti (in collaborazione con aziende private esperte del settore).

Una prima versione dei documenti obiettivo degli ultimi due gruppi è già pronta ed in fase di "editing".

Può dirci qualcosa in più riguardo le linee guida sulla sicurezza?

Per quanto riguarda le linee guida su Sicurezza delle Reti e delle infrastrutture TLC per le Infrastrutture Critiche informatizzate, si tratta di un'attività di analisi specifica per le criticità legate all'interdipendenza delle CNI

tradizionali con le infrastrutture di Telecomunicazione, comprendendo in queste le reti informatiche e di telecomunicazione in senso stretto.

Le infrastrutture critiche (*CNI - Critical National Infrastructure*) sono aree appartenenti al settore pubblico o privato che sono ritenute critiche per il funzionamento economico, politico, sociale del paese.

Tra queste possiamo ricordare ad esempio il settore dei trasporti, quello dell'energia, del gas, dell'acqua, quello finanziario e quello della sanità.

Tali infrastrutture possono essere soggette ad eventi critici di varia natura in grado di comprometterne direttamente od indirettamente l'efficienza. Gli eventi critici sono, in prima approssimazione, riconducibili o ad attacchi intenzionali o a disastri naturali. Per il loro funzionamento, le CNI si basano sempre di più su infrastrutture di telecomunicazione (*CII - Critical Information Infrastructure*). Tali reti devono non solo permettere l'operatività della CNI in normali condizioni di funzionamento, ma anche e soprattutto garantire un'adeguata capacità operativa in caso d'eventi critici.

Si noti che gli eventi critici possono riguardare non solo la CNI ma anche direttamente la relativa infrastruttura di telecomunicazione. Inoltre sia le CNI sia le CII possono essere soggette a guasti, anche in assenza di eventi esterni.

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

Obiettivo del Gruppo di Lavoro è la redazione di un documento, un Libro Bianco, corredato da linee guida, che tratti con specifico riferimento alla situazione italiana, i seguenti aspetti:

- Qualità del Servizio e della Sicurezza delle Reti tenendo anche in considerazione gli Standard e le Normative di Riferimento Nazionali ed Internazionali;
- Le interdipendenze tra CNI e le CII;
- Individuazione di un'insieme comune di minacce da prevenire e contrastare;
- Individuazione un insieme minimo di parametri per la sicurezza;
- Individuazione di parametri tecnici minimi che garantiscano i livelli di QoS adeguati a garantire la minor criticità;

- Analisi dei parametri tecnici, degli elementi di trasparenza e dei termini legali che è consigliabile adottare all'interno delle relazioni contrattuali commerciali e nei Service Level Agreement (SLA) siglate con i Fornitori;
- Individuazione dei parametri minimi necessari al raggiungimento del necessario livello di resilienza e di business continuity;
- Adeguamento dei piani di disaster recovery alle esigenze date dalle interdipendenze;
- Descrizione del ruolo potenziale che possono svolgere le Istituzioni nell'individuazione e realizzazione di strategie comuni di protezione;
- Proposte di autoverifica sull'attuale livello di criticità ed organizzazione pertinente all'interno della propria CNI.



Può raccontarci qualcosa sull' incontro che l'Osservatorio ha organizzato sul tema delle infrastrutture critiche del marzo 2004?

Il Ministro Gasparri è molto attento e sensibile al tema della sicurezza delle reti e dell'informazione.

Fu lui ad aprire il convegno tenuto a marzo 2004 sulla protezione delle infrastrutture critiche e il ruolo dei Governi sul tema.

Il Ministero delle Comunicazioni, attraverso l'Osservatorio, ha organizzato a Roma questo incontro con tutti i Governi mondiali sul tema delle infrastrutture critiche: due giorni, di cui uno dedicato solo ai rappresentanti governativi e uno aperto alle esperienze industriali e allo scambio di opinioni con i produttori di sicurezza. Erano presenti tutti gli Stati Europei (EU 25) e molti Paesi stranieri, tra cui Giappone, India, Cina e USA. E' stato il primo esempio "reale" di impegno fattivo per l'information sharing. L'Italia ha aperto il dibattito "raccontando e raccontandosi" rispetto all'esperienza del blackout del 28 settembre 2003: hanno parlato gli esperti della Protezione civile e di varie altre infrastrutture. Questo esempio ha per così dire "aperto le acque" e tutti hanno poi partecipato al dibattito in modo anche informale, mettendo i reali problemi sul piatto e condividendo esperienza e best practice.

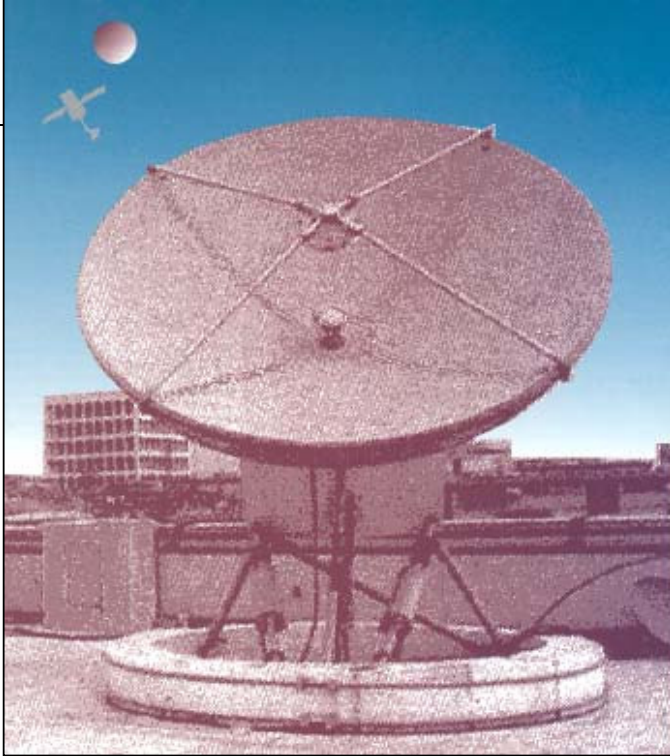
Una prima importante occasione per aumentare la consapevolezza del problema, era stata il Workshop on Critical Information Infrastructure Protection organizzato dall'Ufficio del Primo Ministro e l'Ambasciata Americana a Roma nel Maggio 2002. Si è poi appena concluso un terzo incontro bilaterale tra Italia e USA sul tema delle Infrastrutture critiche informatizzate, svolto a Washington dal 15 al 17 novembre 2004, al quale hanno partecipato tutti i dicasteri coinvolti nella protezione delle CIIP. Il principale risultato è stata una condivisione delle best practice organizzative per il coordinamento della protezione delle CIIP a livello governativo. In quell'occasione abbiamo rincontrato i colleghi statunitensi che avevano partecipato al Convegno di Roma e che ci hanno espressamente chiesto di ripetere l'iniziativa nel prossimo anno per farci promotori anche di un "ponte" tra Europa e Stati Uniti sul tema dell'information sharing. Nel 2005 è previsto un follow up dell'incontro di marzo 2004, sempre a Roma e con la cooperazione, se possibile, dell'ENISA (*European Network and Information Security Agency*).

Sul tema della difesa delle infrastrutture critiche: che rapporto c'è fra l'Osservatorio ed il "Gruppo di lavoro per la protezione delle infrastrutture critiche informatiche" presso il Ministero delle Innovazione Tecnologica?

Nel Maggio 2002 la Commissione dei Ministri per la Società dell'Informazione ha realizzato il documento Linee Guida del Governo per lo sviluppo della Società dell'Informazione. Le Linee Guida descrivono e definiscono l'impegno del Governo a condurre l'Italia in una posizione di protagonista nell'era digitale, modernizzando il Paese attraverso un utilizzo diffuso delle nuove tecnologie ICT sia nel pubblico che nel privato.

Copertina de "La Comunicazione, Note Recensioni & Notizie", Pubblicazioni dell' Istituto Superiore C.T.I
<http://www.comunicazioni.it/it/index.php?Mn1=9&Mn2=84>

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



Nelle Linee Guida viene trattato anche il problema della sicurezza delle reti e viene introdotto un piano nazionale per la sicurezza ICT e la privacy basato sulle seguenti azioni:

- Direttiva sulla sicurezza ICT: tale direttiva definisce una "Base minima di sicurezza" a cui tutte le Amministrazioni devono allinearsi dopo avere effettuato una autovalutazione sul proprio livello di sicurezza ICT.
- Comitato Tecnico Nazionale sulla sicurezza ICT: ha il compito di indirizzare e coordinare tutte le attività e gli sforzi relativi al fine di definire il Modello Nazionale di Sicurezza e quindi di predisporre gli interventi di natura organizzativa e tecnica. La composizione e l'attività del comitato si basa sulla piena collaborazione tra il Ministero delle Comunicazioni ed il Dipartimento per l'Innovazione e le Tecnologie.
- Modello organizzativo sulla sicurezza ICT: realizzazione di un'architettura nazionale in termini di strutture e responsabilità sulla sicurezza ICT, capace di sviluppare linee guida, raccomandazioni, standard e tutte le procedure di certificazione.
- Piano Nazionale sulla sicurezza: predisposizione di un Piano Nazionale di Sicurezza che definisce attività, responsabilità, tempi per l'introduzione degli standard e delle metodologie necessarie per pervenire alla certificazione di sicurezza nella Pubblica Amministrazione.
- Certificazione di sicurezza: le Amministrazioni più aperte e con uffici in rete hanno bisogno di più sicurezza certificata. Occorre richiedere sempre

prodotti e servizi certificati. In Italia abbiamo un Ente di certificazione internazionale per la sicurezza di prodotti e servizi che è l'Istituto Superiore delle Comunicazioni, interno al Ministero delle Comunicazioni.

Nel Marzo 2003, è stato istituito il Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate, nel quale hanno collaborato sia i rappresentanti dei diversi dicasteri interessati alla gestione di infrastrutture critiche (Ministero dell'Interno, delle Infrastrutture, delle Comunicazioni, Dipartimento per l'Innovazione tecnologica, ecc.), sia i principali operatori privati (ABI, ASI, CESI, GRTN,

RFI, Snam Rete Gas, Telecom Italia, Wind e altri), oltre che esponenti del mondo della ricerca e dell'accademia.

L'obiettivo di tale Gruppo di Lavoro è stato quello di aiutare le istituzioni ad una migliore comprensione dei problemi associati alla CIIP, in particolare guasti accidentali e volontari, e di fornire una base per l'individuazione di requisiti organizzativi e di iniziative volte ad incrementare la robustezza delle infrastrutture critiche.

Il Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate ha rilasciato nell'Ottobre del 2003 il documento Protezione delle Infrastrutture Critiche Informatizzate - La realtà Italiana che rappresenta il risultato del lavoro svolto. Il documento descrive molti elementi delle Infrastrutture del nostro Paese, enfatizzando le loro interdipendenze e suggerendo strategie per la CIIP.

In particolare il Gruppo di Lavoro suggerisce che la piena responsabilità per la corretta implementazione delle politiche di sicurezza dovrebbe essere attribuita ai singoli proprietari ed operatori delle infrastrutture critiche, mentre le istituzioni sono ritenute responsabili della definizione dell'insieme delle indicazioni utili per minimizzare le interdipendenze e gli effetti di guasti a cascata.

Il documento suggerisce inoltre:

- La costituzione di un Gruppo di Interesse Nazionale con il compito di controllare i requisiti dei vari proprietari ed operatori.
- La definizione di un ambito di ricerca e sviluppo nazionale nell'area della Protezione delle Infrastrutture Critiche.

- La realizzazione di un Centro Virtuale di Simulazione e Analisi delle Interdipendenze
- Il lavoro dell'Osservatorio fa seguito a quella del Gruppo di lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate e ne mantiene buona parte dei partecipanti, pur avendo inserito molti altri attori.

Abbiamo un ottimo rapporto con tutti gli attori del tema sicurezza delle reti in Italia e poniamo molta attenzione a coinvolgere sempre tutti in ogni iniziativa. Non va poi dimenticato il contributo fondamentale della Fondazione Ugo Bordoni, i cui ingegneri sono sempre al mio fianco nella trattazione di questi argomenti con un'esperienza e una preparazione ineguagliabili.

L'ottimo rapporto con i colleghi del CNIPA e del Dipartimento Innovazione Tecnologica, del Ministero dell'Interno, del Ministero della Difesa, del Ministero Attività Produttive, del Dipartimento della Protezione Civile e della Presidenza del Consiglio è all'origine del nostro entusiasmo e dei molti risultati raggiunti dalle Istituzioni in questo settore.

Che consigli può dare ai nostri associati sul "mestiere" di "Security Manager"?

Consiglio una laurea in informatica o in ingegneria (meglio se con specializzazione in elettronica).

È ormai indispensabile l'esperienza all'estero e magari un master di stampo economico, che non fa mai male per imparare ad avere contatti personali con i manager responsabili della strategia di impresa e per capire la fattibilità economica delle proprie idee tecniche.

Raccomando inoltre la conoscenza ottima dell'inglese e magari di un'altra lingua.

Grazie ingegnere.

Grazie a voi

Articoli collegati

Intervista ad Andrea Pirotti, *executive*

director di ENISA, ISACAROMA Newsletter, numero 7, ottobre 2004

<http://www.isacaroma.it/html/newsletter/?q=node/17>

Link ed approfondimenti

Ministero delle Comunicazioni:

<http://www.comunicazioni.it/it/index.php>

Organismo di certificazione della sicurezza informatica (O.C.S.I.):

<http://www.ocsi.it>

e-mail: ocsi@istsupcti.it

CNIPA:

<http://www.cnipa.it>
