CENTRO STUDI
CONSIGLIO NAZIONALE INGEGNERI

IL PUNTO DI VISTA DEL CENTRO STUDI: I DATI SULLA SICUREZZA ICT

RED 2016
Riviera Engineering Days

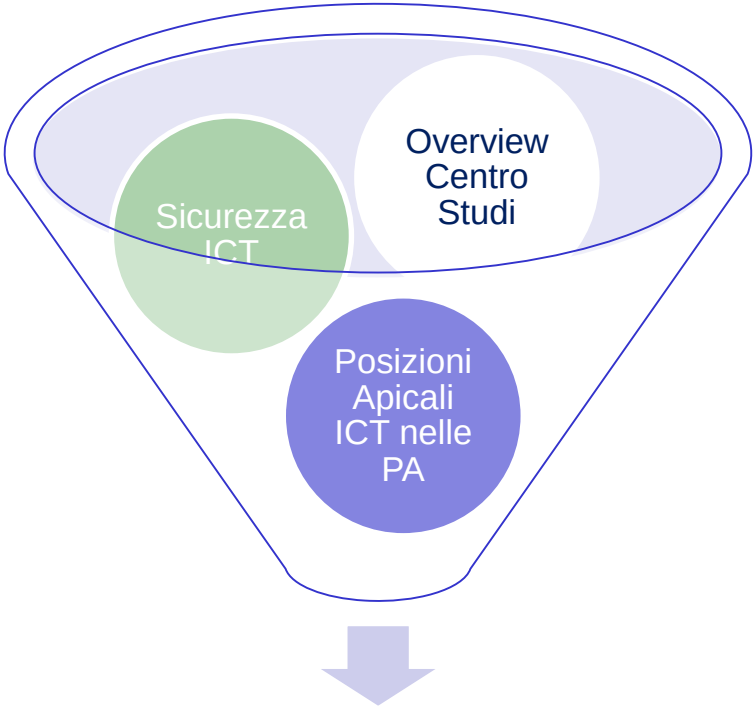
Savona 08.04.2016

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI
http://www.centrostudicni.it

Agenda

CENTRO STUDI
CONSIGLIO NAZIONALE INGEGNERI



RED 2016
Riviera Engineering Days

Conclusioni sul valore della sicurezza ICT

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

Il Centro Studi del CNI

Attività di supporto al CNI

Indagini quantitative e monitoraggi

Attività di approfondimento

Attività di servizio agli ordini e agli iscritti

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

Le Pubblicazioni

Le Pubblicazioni

Le pubblicazioni sono tutte disponibili sul sito e per tutti tra queste ve ne segnalo alcune :

- **N. 127/2011 «La sicurezza delle reti e dei sistemi informativi: il ruolo degli Ingegneri dell'informazione.»**
- **N. 148/2014 «Linee Guida sulla Certificazione degli Organismi Professionali secondo il sistema di gestione della Qualità ISO 9001:2008»**
- **N. 153/2015 « La formazione degli ingegneri Anno 2014»**
- **Ricerca n. 476 Maggio 2015 «Gli iscritti all'Ordine degli ingegneri nel 2015»**
- **Settembre 2015 : Posizioni apicali dell'ICT nella PA**

La Sicurezza ICT

CENTRO STUDI
CONSIGLIO NAZIONALE INGEGNERI

RED 2016
Riviera Engineering Days

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

Dati sui contratti sui servizi ICT (Fonte Centro Studi CNI - survey 2011)

- Secondo l'Autorità per la vigilanza sui contratti pubblici (oggi ANAC) nel 2010:
  - Il valore dei contratti aggiudicati relativamente ai servizi informatici (consulenza, sviluppo di software, Internet e supporto) è risultato pari a 2,41 miliardi di euro;
  - quello dei contratti aggiudicati per i servizi architettonici, di costruzione, ingegneria e ispezione si è fermato, nello stesso periodo, a 349 milioni di euro;

Dati sui contratti
(Fonte Centro Studi CNI)

- **Secondo l'ANAC (relazione di luglio 2013 a tutto il 2012)**
  - Il valore dei contratti aggiudicati relativamente ai servizi informatici (consulenza, sviluppo di software, Internet e supporto) è risultato pari a 2,23 miliardi di euro, dei quali la maggior parte circa 2,12 miliardi di € di importi superiori a 150 k€;
  - quello dei contratti aggiudicati per i servizi di ingegneria e ispezione si è fermato, nello stesso periodo, a 1,09 milioni di euro, dei quali la maggior parte circa 1,04 miliardi di € di importi superiori a 150 k€;

Rilevazione Bandi per il 2015 (Fonte Centro Studi CNI)

- Rispetto al totale dei bandi aggiudicati:
- Quelli in ambito ICT valgono 195,4 milioni di euro;
- Quelli per i servizi di ingegneria (senza esecuzione) 64,7 milioni di euro ;
- Ai precedenti si devono aggiungere i servizi di ingegneria con esecuzione (di cui non vi sono dati disponibili per poter individuare la componente dei soli servizi) che valgono 2.458,7 milioni di euro.
- I concorsi di progettazione, infine, valgono 0,4 milioni di euro.

Commento:
Quante OO.PP. In ambito ICT vengono erroneamente trattate come forniture di beni e servizi ?

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

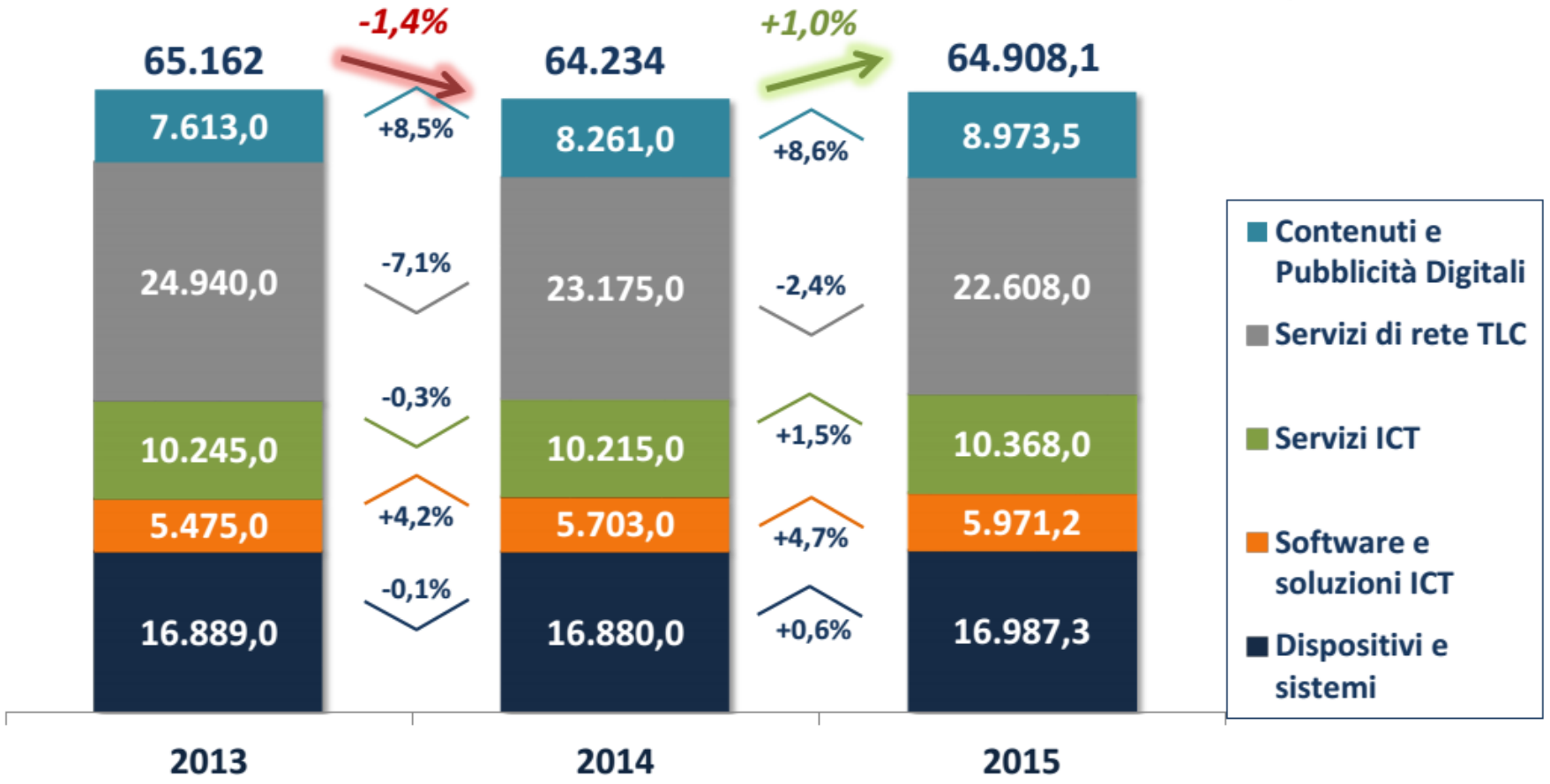
Valore filiera SW e Servizi (Fonte Assinform 2016)

- per la voce Software (valore **5,9 miliardi di euro nel 2015**) sono state considerate le seguenti voci: **SW Applicativo, Middleware e SW di sistema operativo**;
- per la voce **servizi (10,3 miliardi di euro nel 2015)** sono state incluse le seguenti sotto voci: sistemi embedded; servizi di elaborazione dati; formazione; system integration; outsourcing; consulenza; sviluppo e manutenzione.

Il mercato del Software e delle Soluzioni ICT

Valori in mln di Euro e in %

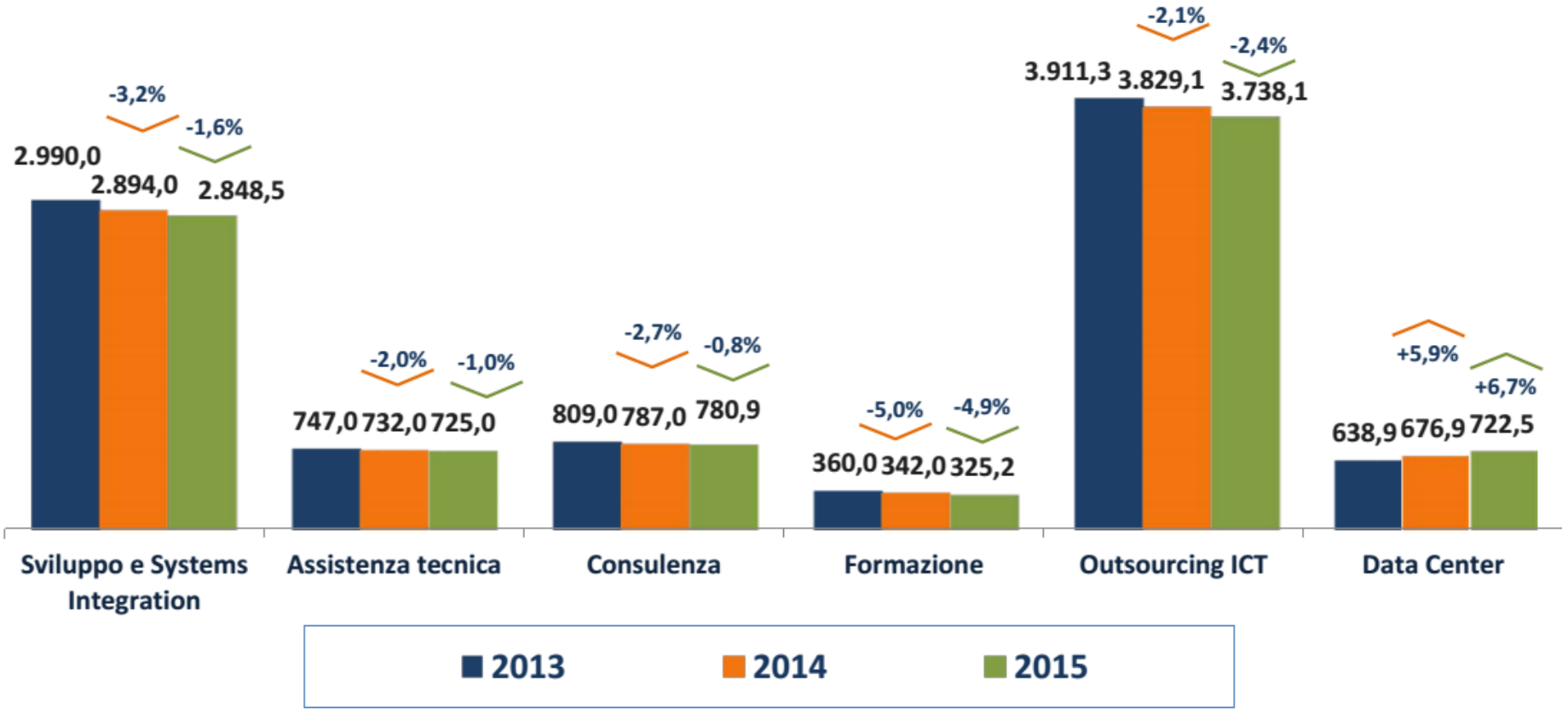
Fonte: Assinform / NetConsulting cube, Marzo 2016



I principali servizi ICT

Valori in Milioni di Euro e in %

Fonte: Assinform / NetConsulting cube, Marzo 2016



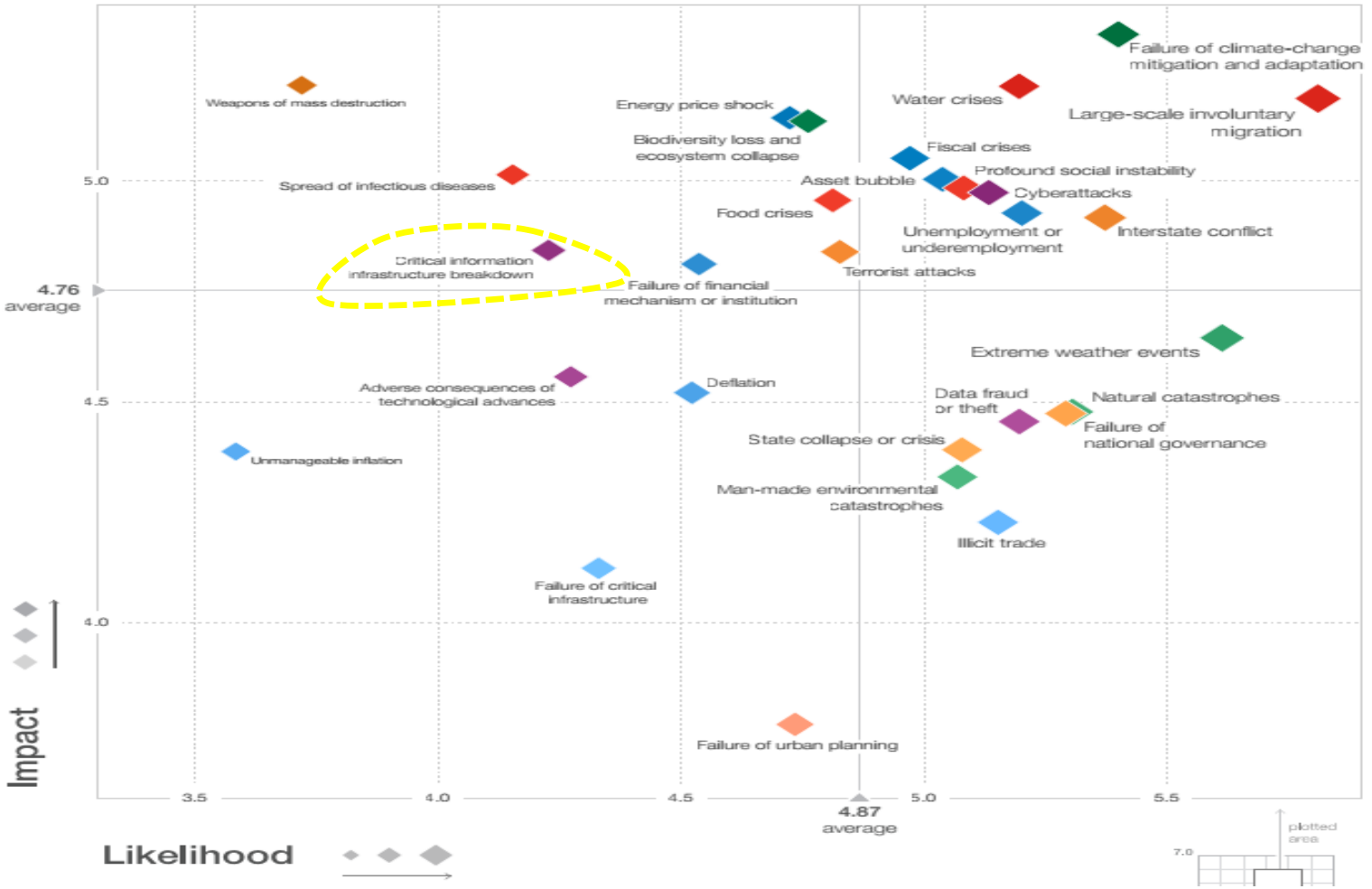
Dati su analisi del rischio down infrastrutture critiche e valutazione dei danni (Fonte The Global Risk Landscape 2016)

- La **probabilità** del down di una infrastruttura critica, in una scala da 1 a 7, è stato valutato pari a **4,3 nel 2016 dato uguale rispetto a quello 2015**.
- L'**impatto**, sempre in una scala da 1 a 7, è stato valutato pari a **4,8 in discesa rispetto al 2015 (5,1) comunque leggermente superiore alla media (4,76)**.
- Stime sull'impatto economico, dell'eventuale accadere di tali rischi, in termini di costi e/o mancati guadagni, non sono disponibili a causa di alcune difficoltà metodologiche !!!

Dati su analisi del rischio down infrastrutture critiche e valutazione dei danni (Fonte The Global Risk Landscape 2016)

CENTRO STUDI
CONSIGLIO NAZIONALE INGEGNERI

Figure 1: The Global Risks Landscape 2016



Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

Ingegneria dell'Informazione & Sicurezza dei sistemi

CENTRO STUDI
CONSIGLIO NAZIONALE INGEGNERI

Pillole di Informazioni:

Standard di riferimento : ISO/IEC 27001.

- **Si deve garantire:**
  - **L'integrità dei dati**
  - **La riservatezza dei dati**
  - **La disponibilità dei dati**

Controlli ai quali l'»Organizzazione» dovrebbe attenersi.

- **Ambiti di Applicazione:**
  - **Classificazione delle Informazioni.**
  - **Sicurezza accessi.**
  - **Gestione PDL**
  - **Segnalazione e trattamento degli «Incidenti»**

Policy Aziendale definita dal Responsabile della Sicurezza che riferisce alla Direzione

Ingegneria dell'Informazione & Sicurezza dei sistemi

Cos'è la Business Continuity (Continuità operativa):

è l'insieme di attività volte a minimizzare gli effetti distruttivi, o comunque dannosi, di un evento che ha colpito un'organizzazione o parte di essa, garantendo la continuità delle attività in generale.

Anch'essa non può prescindere dai seguenti elementi:

PERSONE

PROCESSI

TECNOLOGIA

INFRASTRUTTURA ICT

Ingegneria dell'Informazione & Sicurezza dei sistemi

CENTRO STUDI
CONSIGLIO NAZIONALE INGEGNERI

DISASTER RECOVERY (DR)

Erroneamente considerata come sinonimo della continuità operativa , la Disaster Recovery (DR) è una componente della Business Continuity e si occupa della reazione immediata al verificarsi di un evento, al fine di garantire la continuità tecnologica, che nel contesto delle pubbliche amministrazioni riguarda l'infrastruttura informatica e telecomunicativa (ICT - TELCO).

Costituita da step successivi configurati in una pianificazione a fasi, la DR comporta il fermare gli effetti che un evento avverso sta causando (falla nella sicurezza , incendio, terremoto, …)

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

Ingegneria dell'Informazione & Sicurezza dei sistemi

Due gli **indicatori chiave della continuità operativa:**

- **RTO (Recovery Time Objective): esprime l'arco** temporale massimo entro cui il ripristino delle risorse minime deve essere garantito, al fine di contenere gli impatti, legati all'indisponibilità, a livelli sopportabili;
- **RPO (Recovery Point Objective): rappresenta** l'intervallo temporale massimo a cui far riferimento per individuare il punto di ripristino dei dati e/o del sistema (dall' ultimo salvataggio delle informazioni disponibili). E' quindi un indicatore della quantità di dati che possono essere perduti.

Gartner Group propone di classificare i servizi erogati in termini di RTO e RPO:

- servizi di classe 1: con RTO e RPO prossimi a zero;
- servizi di classe 2: con RTO dell'ordine delle 24 ore, e RPO prossimo a 4 ore;
- servizi di classe 3: con RTO dell'ordine delle 72 ore, e RPO prossimo a 24 ore;
- servizi di classe 4: con RTO misurabile in giorni, e RPO superiore a 24 ore.

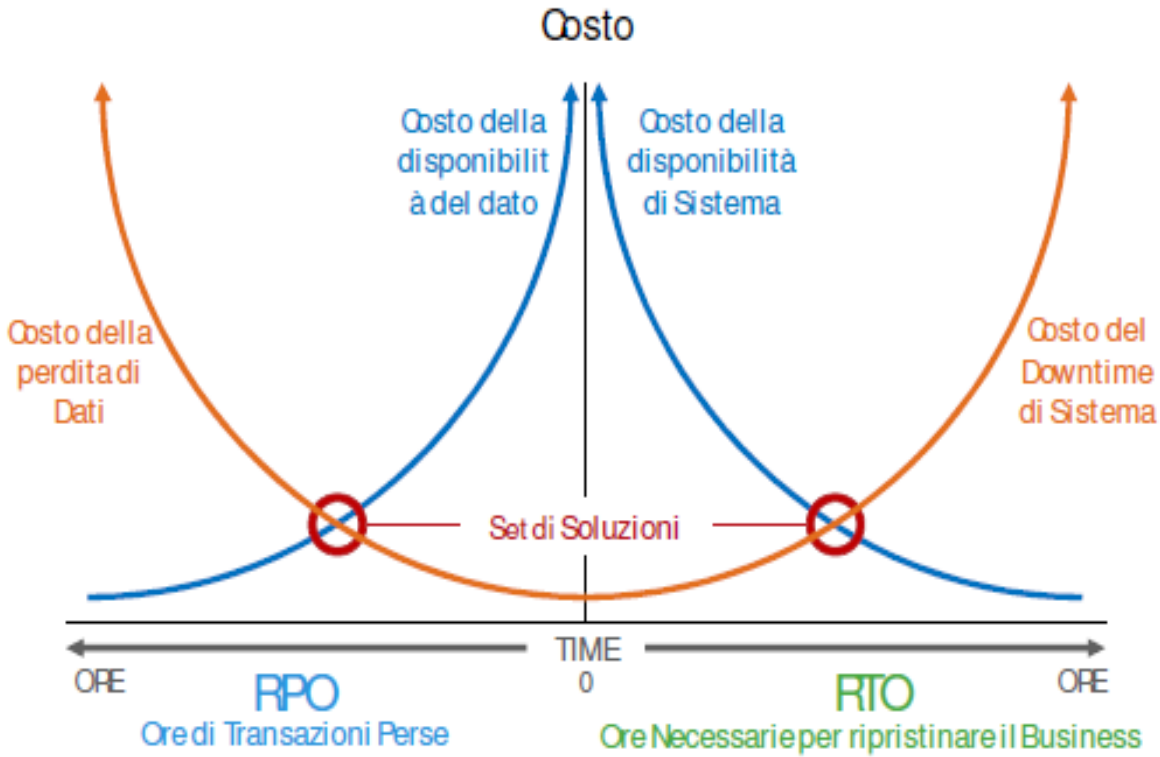
I servizi delle prime due classi sono, in generale, quelli da applicare alle c.d. **«Infrastrutture Critiche»** Quelli appartenenti alla terza e quarta classe possono essere protetti anche con un sistema di backup.

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

Ingegneria dell'Informazione & Sicurezza dei sistemi

L'ottimizzazione dei tempi RTO e RPO si traduce in un compromesso tra i costi dovuti alla perdita di dati e i costi d'implementazione di un'architettura ad alta affidabilità



Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

Ingegneria dell'Informazione & Sicurezza dei sistemi

La continuità operativa è un **impegno e obbligo istituzionale**

La continuità operativa rappresenta un aspetto di **estrema importanza per l'e-governement,** poiché consente di garantire realmente una disponibilità dei servizi on-line superiore a quella degli accessi tradizionali tramite sportello.

In tal modo, è possibile fornire al cittadino il pieno esercizio del suo diritto ad accedere ai servizi pubblici per via telematica, come previsto dall'**Articolo 3 del Codice dell'Amministrazione Digitale**.

L'importanza di questo tema ha trovato conferma in occasione della revisione del CAD operata dal **decreto legislativo 30 dicembre 2010 n. 235, che ha inserito un nuovo articolo, il 50-bis, "Continuità operativa".**

Continuità Operativa nella Pubblica Amministrazione è un obbligo (DLgs.235/10 Art.50-bis) – Attenzione lo vogliono abolire !!! – qui c'è un impegno del Centro Studi del CNI e della RPT.

Ing. Bruno Lo Torto

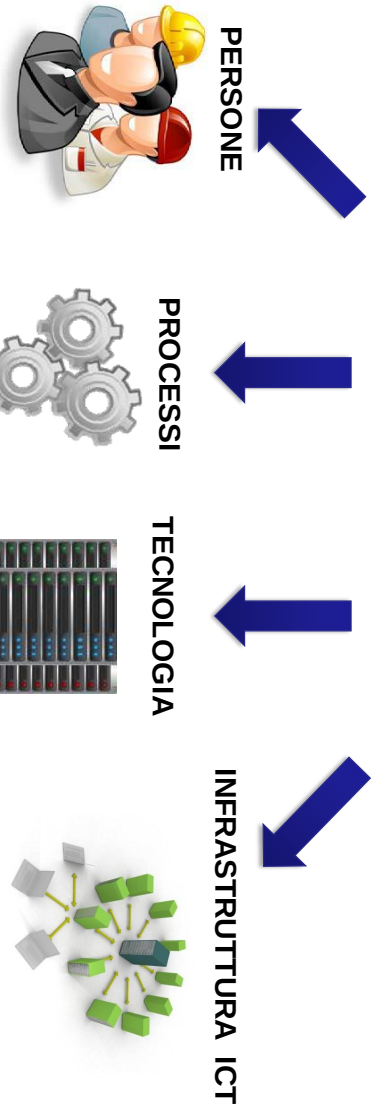
Consigliere Centro Studi CNI

Ingegneria dell'Informazione & Sicurezza dei sistemi

CENTRO STUDI
CONSIGLIO NAZIONALE INGEGNERI

Analisi per un corretto piano di Continuità Operativa

- **Tecnologia:**
  - Analisi dei servizi critici (risk assessment)
  - Affidabilità HW dei singoli sistemi (non solo server)
  - Ridondanza HW e SW dei sistemi
  - Replica dei dati
- **Persone:**
  - Individuazione delle "Persone chiave".
  - Creazione di know-how interno
- **Infrastruttura ICT:**
  - Analisi della collocazione delle macchine
  - Analisi e adeguamento della rete esistente
- **Processi:**
  - Analisi e revisione dei processi di ripristino



Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

Ingegneria dell'Informazione & BIM – PRIMA SUGGESTIONE

Ciò che subito risulta evidente a chiunque si approcci al BIM è che vi sono forti interazioni con competenze tipiche dell'Ingegneria dell'Informazione per gli aspetti connessi con l'Ingegneria Gestionale, con l'Ingegneria Elettronica ed Informatica.

Il BIM, infatti, non può prescindere dai seguenti elementi:

PERSONE

PROCESSI

TECNOLOGIA

INFRASTRUTTURA ICT

Indagine sulle posizioni apicali nell'ICT della PA

CENTRO STUDI
CONSIGLIO NAZIONALE INGEGNERI

RED 2016
Riviera Engineering Days

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

CENTROSTUDI
CONSIGLIO NAZIONALE INGEGNERI

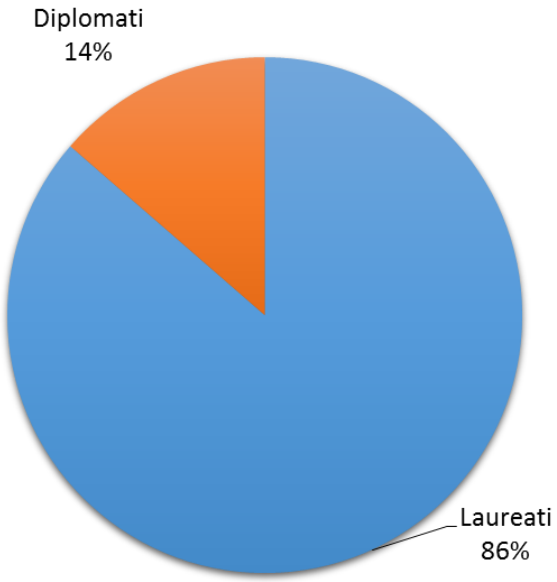
Indagine sulle posizioni apicali nei sistemi di gestione ICT nelle Pubbliche amministrazioni

Risultati di sintesi

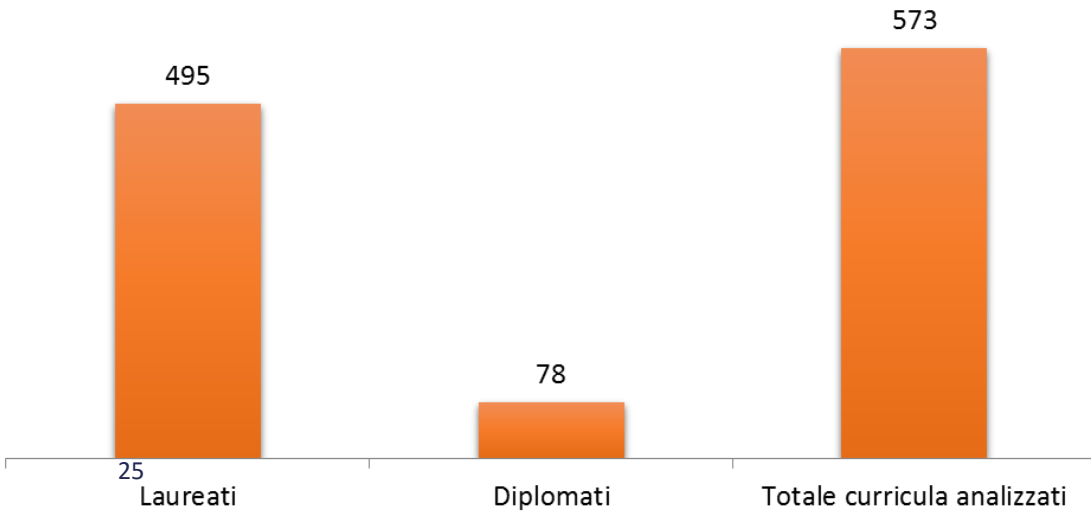
(4 sett. 2015)

Sono stati esaminati 573 curricula (su oltre 1.000 strutture analizzate) di dipendenti e collaboratori operanti nella PA collocati in posizione apicale presso direzioni o strutture di gestione di sistemi informatici. In più di 400 casi di siti Internet della Pubblica Amministrazione – Sezione *Amministrazione trasparente*, i curricula delle posizioni apicali non erano accessibili o disponibili

Distribuzione % tra laureati e diplomati nella scuola media superiore con posizioni apicali nalla direzione ICT della PA

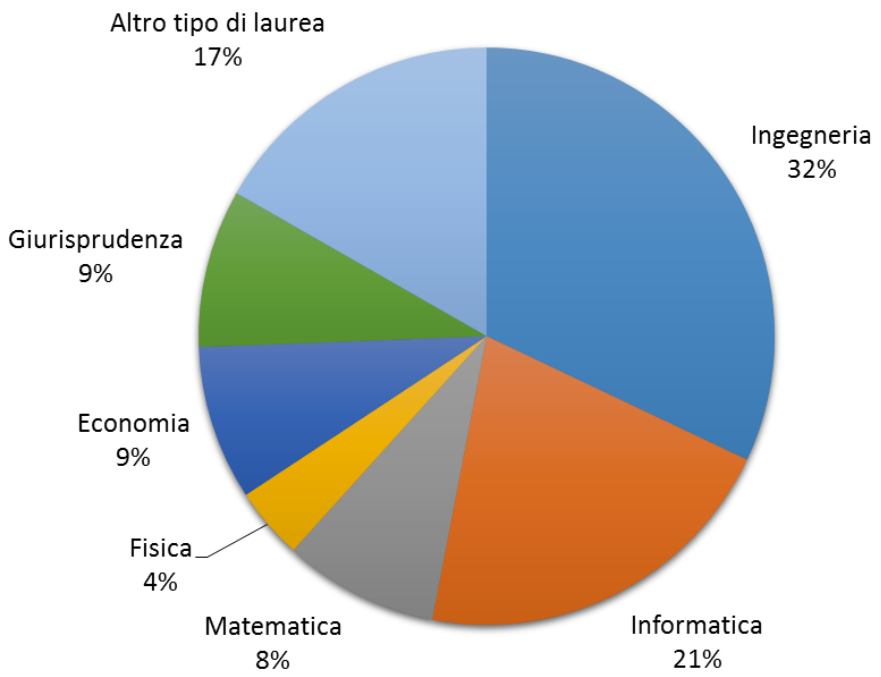


Numero di curricula esaminati di personale in posizioni apicali nella direzione di sistemi ICT nella PA, personale con laurea o diploma di scuola media superiore



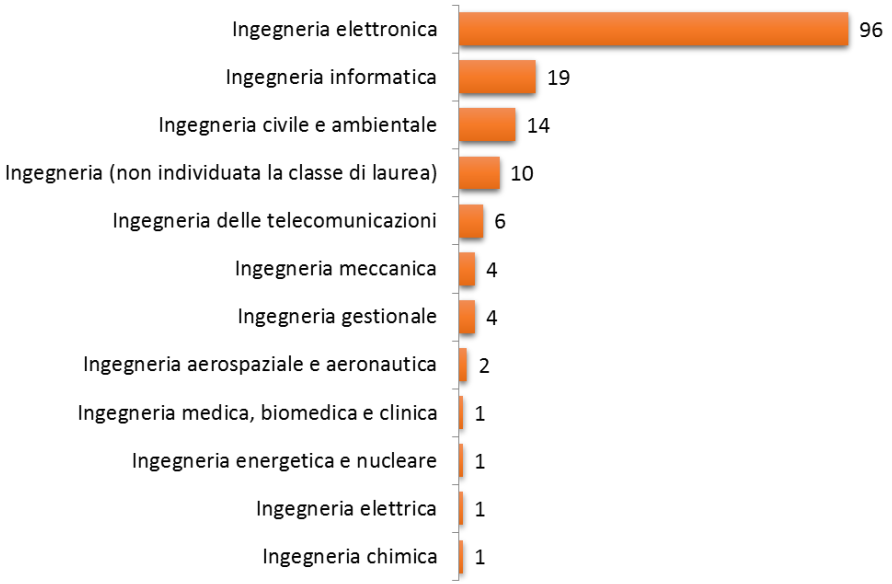
I laureati in informatica e ingegneria rappresentano appena il 53% delle posizioni apicali analizzate. Si arriva al 65% con i laureati in matematica e fisica. La parte restante è ricoperta da personale con percorso formativo universitario poco attinente alla complessità e tecnicalità del ruolo

Totale laureati in posizioni apicali in ambito ICT nella PA (495 laureati), per laurea conseguita

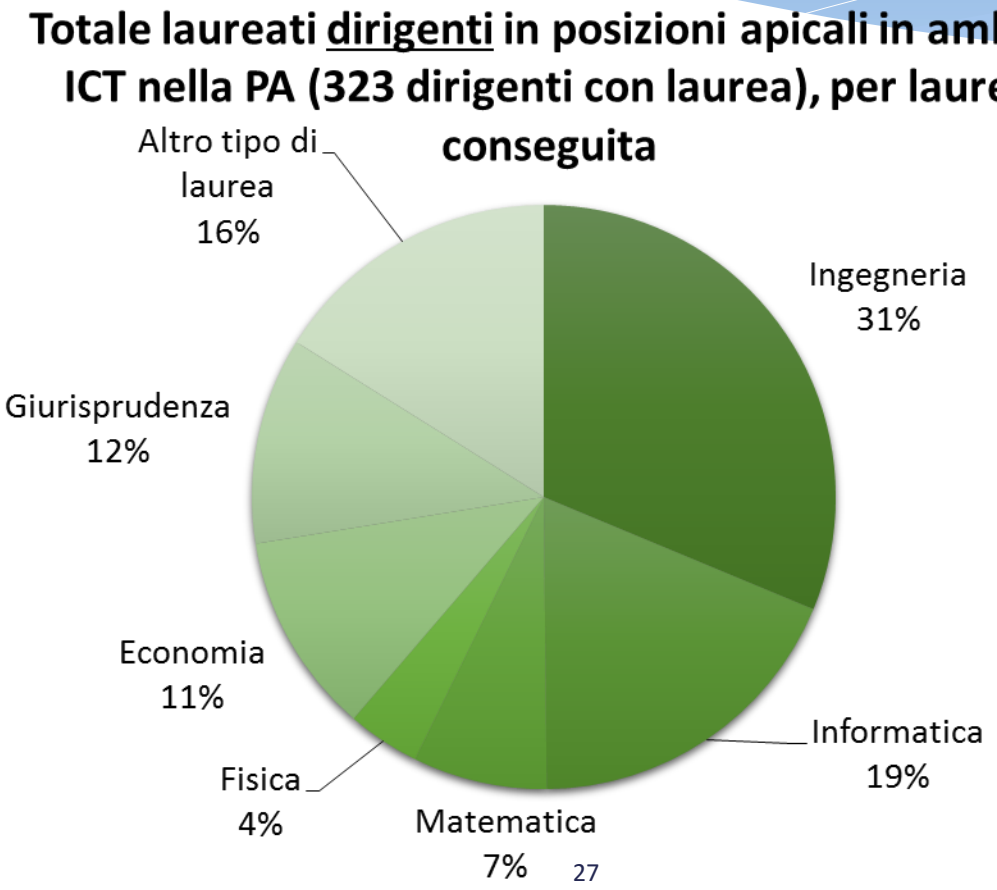


Dei 159 ingegneri rilevati, 19 sono laureati in ingegneria informatica

Laureati in ingegneria in posizione apicale rilevati

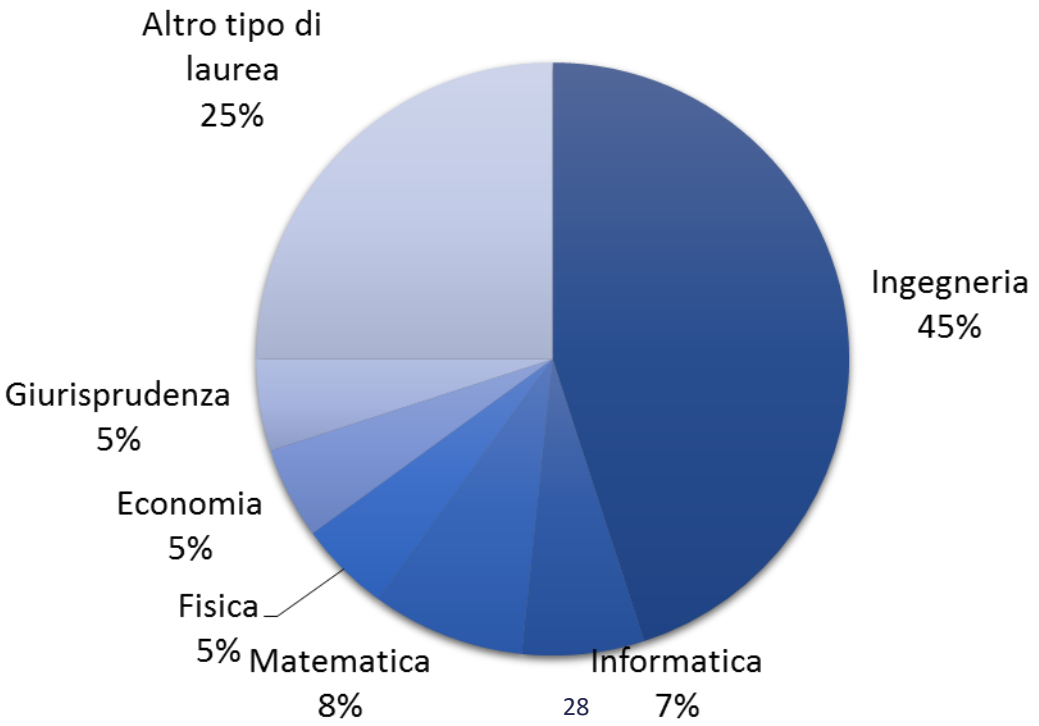


Poco meno di un terzo delle posizioni dirigenziali ha la laurea in ingegneria, appena il 19% è laureato in informatica

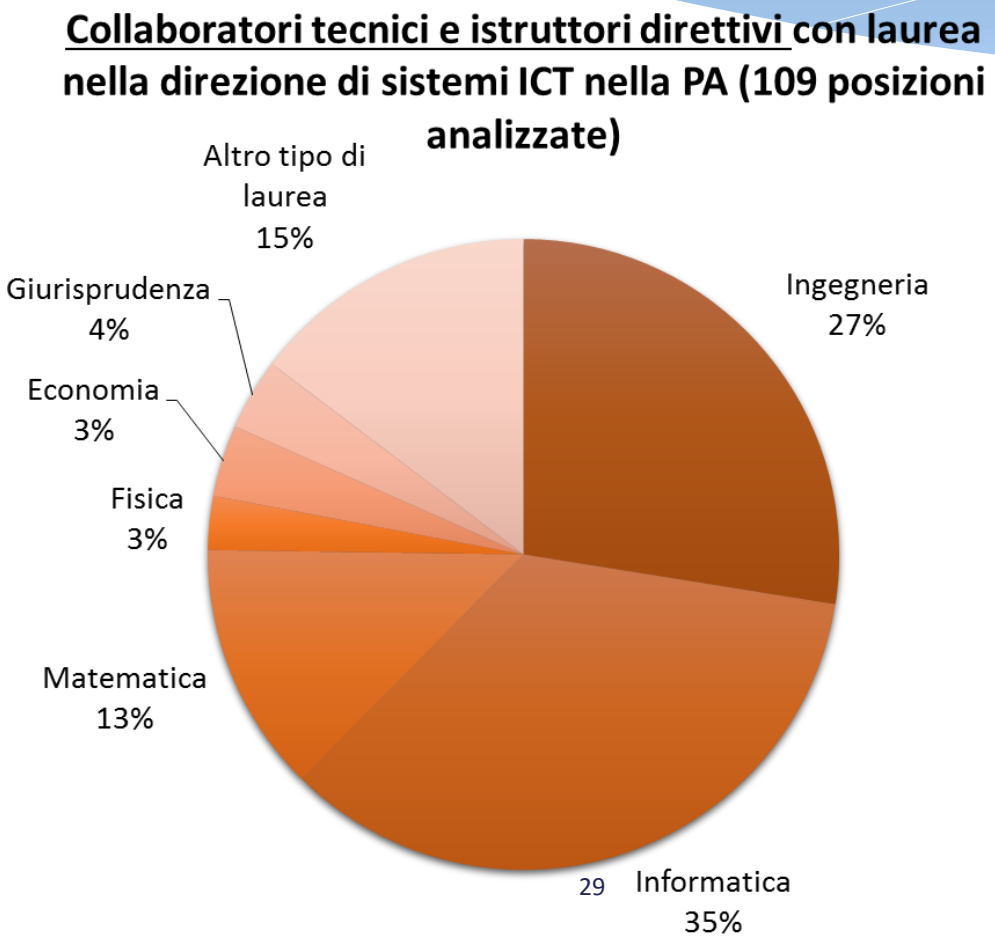


Tra i funzionari l'incidenza dei laureati in ingegneria aumenta al 45% ma si abbassa la presenza dei laureati in informatica: la soglia di accesso a posizioni apicali complesse, per lauree non tecniche, si abbassa quindi ancora di più

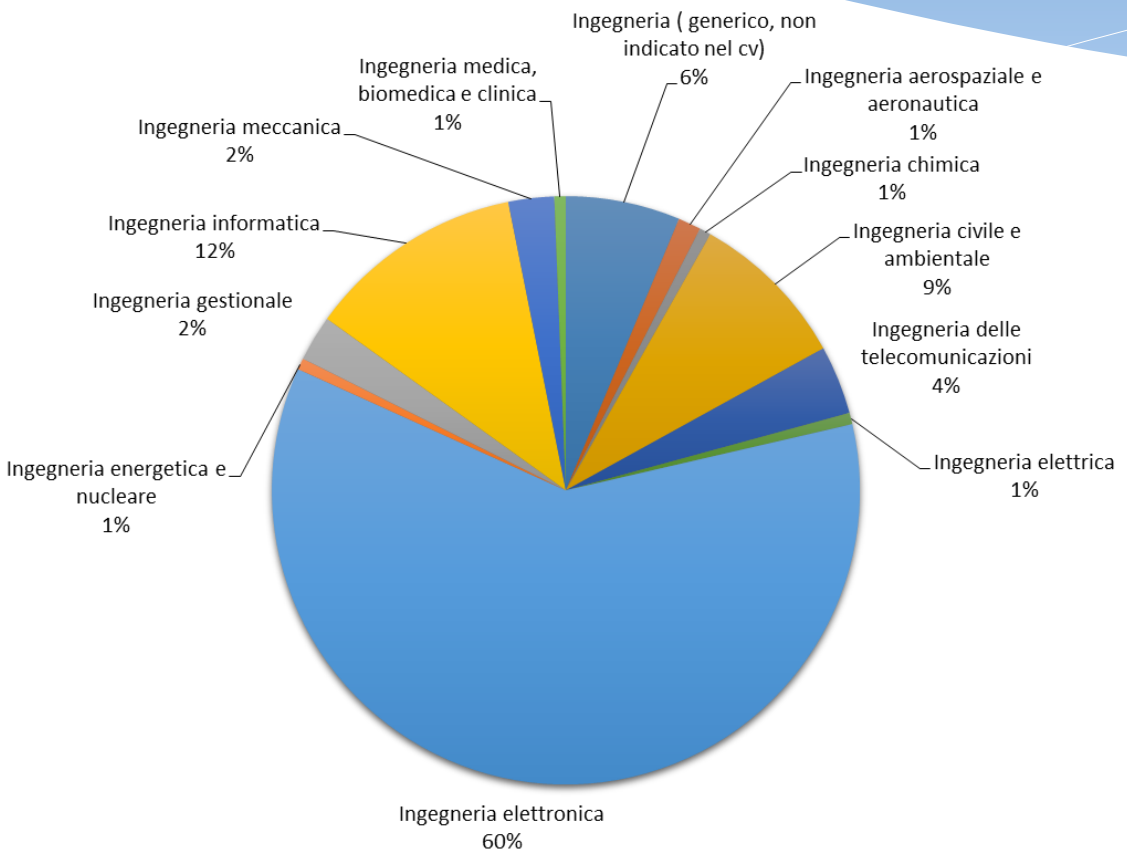
Totale laureati funzionari in posizioni apicali in ambito ICT nella PA (60 funzionari con laurea), per laurea conseguita



Posizioni poco al di sotto di quella di funzionario (collaboratore tecnico e istruttore direttivo)



Distribuzione % dei laureati in ingegneria nelle posizioni apicali dei sistemi di gestione ICT della PA (159 laureati in ingegneria su 495 curricula di laureati analizzati e su 573 curricula complessivamente analizzati)



Solo 19 laureati in ingegneria informatica tra tutte le figure analizzate.

Ingegneria elettronica sembra offrire, nei fatti, le maggiori possibilità di accesso a posizioni apicali legate alle ICT. La seconda posizione (12%) ma a grande distanza dalla prima, è rappresentata da ingegneria informatica

L'ICT e l'Impiego intelligente dell'Energia

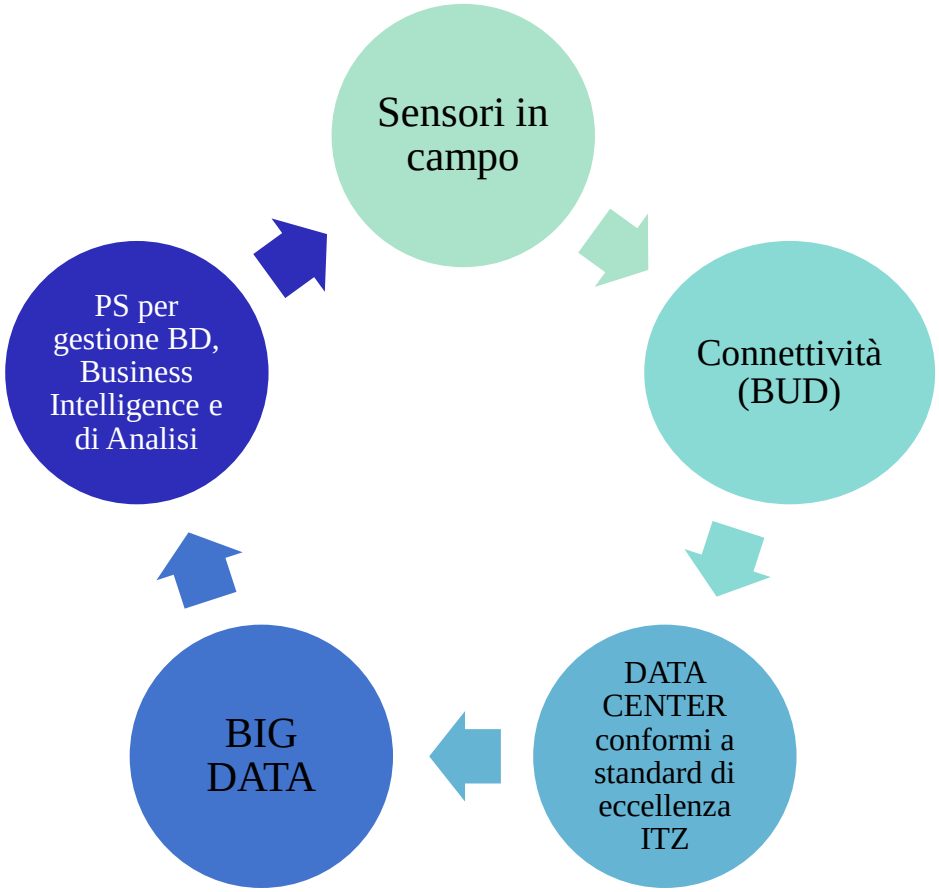
CENTRO STUDI
CONSIGLIO NAZIONALE INGEGNERI

RED 2016
Riviera Engineering Days

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

Smart Grid – Smart City- IoT- IoE (si accettano suggerimenti)



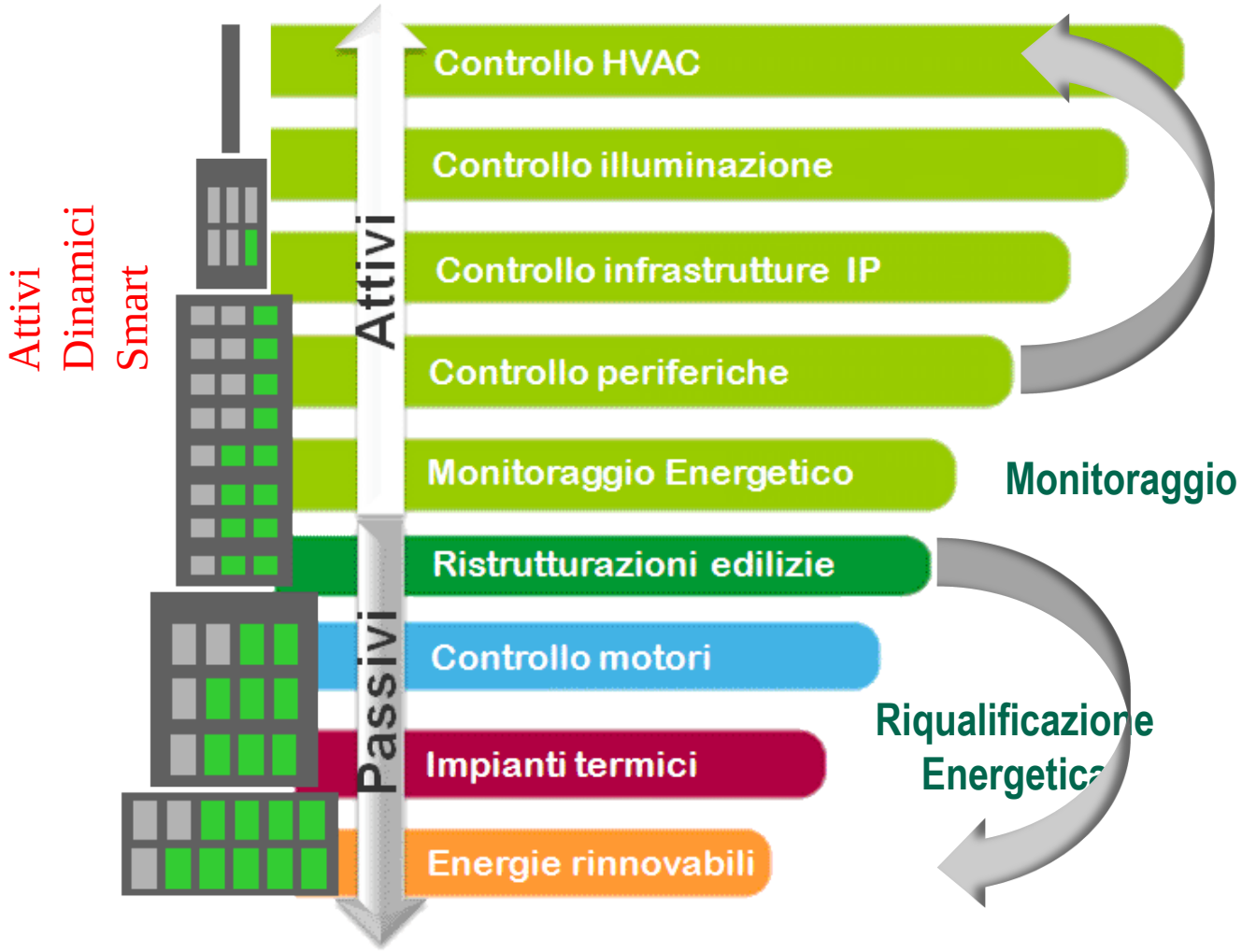
Ingegneria Elettronica, Gestionale ed ICT sono il collante e gli elementi abilitanti

Ma anche l'Ingegneria Civile ed Impiantistica in Generale per i Data Center è pesantemente coinvolta

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

Smart Grid

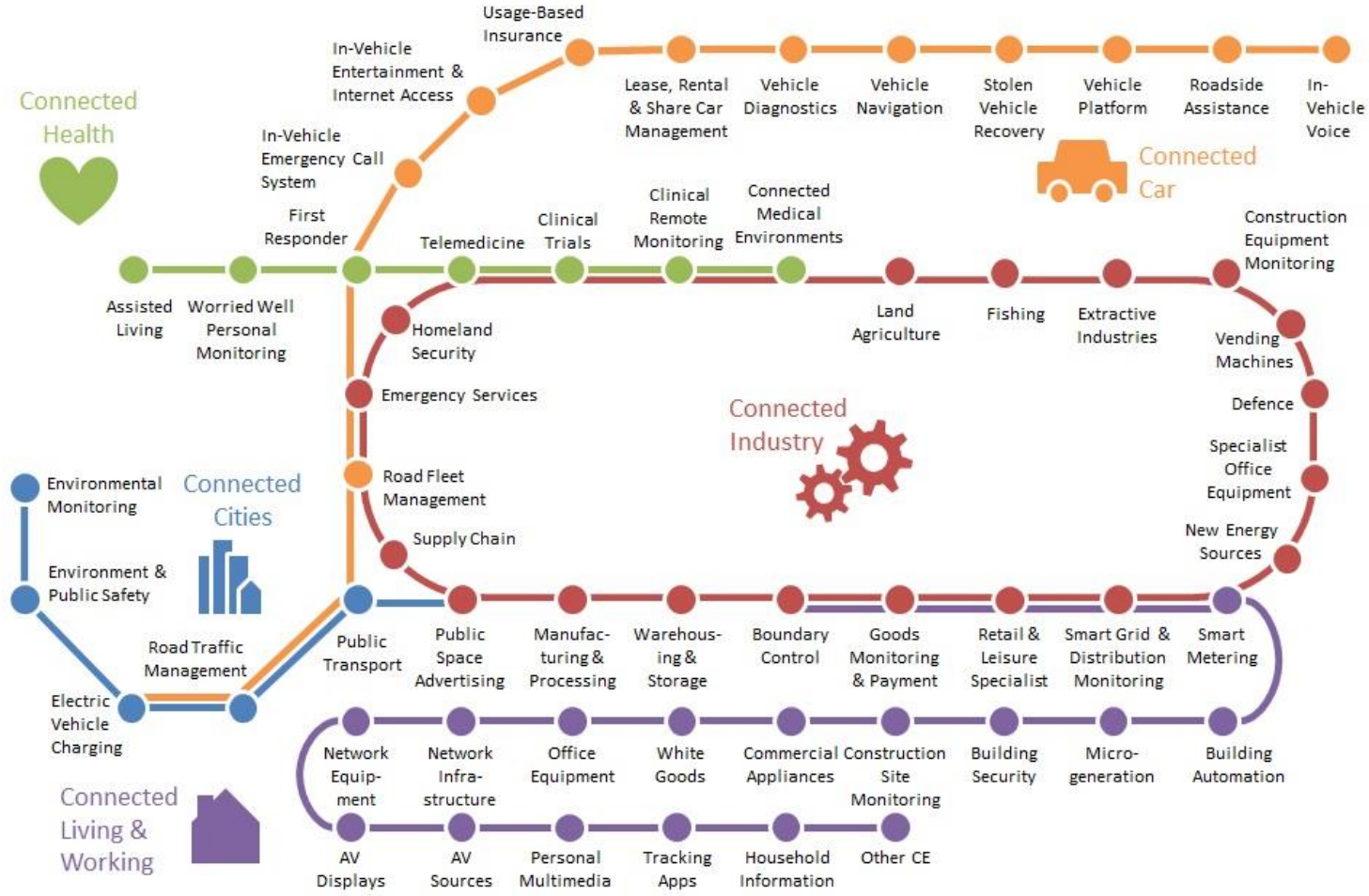


Punto di attenzione: Sensori a fibra ottica per le ristrutturazioni

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

TERZA SUGGESTIONE
I Cluster applicativi per l'IT



L'IoT è stato nel 2014 l'ambito tecnologico che ha destato il maggior interesse e le maggiori crescite.

Il numero dei sensori consegnati è passato da 4,2 miliardi del 2012 a 23,6 miliardi nel 2014 (Cisco, 2014).

Secondo Machina Research sono almeno 60 i cluster che li raggruppano

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

Una visione unitaria

CENTRO STUDI
CONSIGLIO NAZIONALE INGEGNERI

Open, Multi-channel Context-aware platform

APPLICATIONS		Information Monitoring Commands
DATA ARCHIVES		IoT Data Bases Existing Data Data Fusion
NETWORKS		Traditional Fixed/Mobile Networks Low Power Networks
SENSORS		Widespread meters and sensors Active Citizenship
THINGS		Facilities Infrastructures Environment

CONTEXTUAL COMMUNICATION

- Data Context
- Real-Time Communication
- Virtual Context
- Things Context

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

M2M

- MERITA UNA TRATTAZIONE E FORSE UN CONVEGNO A PARTE …
- Machina Research differenzia Machine-to-Machine (M2M) da IoT. Il M2M riguarda la fornitura di soluzioni connesse alla risoluzione di tutti i problemi associati con il collegamento e la gestione di un dispositivo. La strategia del M2M si concentra quindi sulle migliori pratiche tecniche e commerciali nella consegna dell'elemento connettività che attraversa tutte le applicazioni M2M, in ciò tenendo conto delle tendenze chiave del mercato e delle strategie ottimali che è opportuno vengano seguite dagli operatori che forniscono, o utilizzano, connettività M2M. Esiste anche uno standard ETSI di riferimento
- Quasi ovunque si guarda a M2M come riferimento tecnologico per l'evoluzione dei dispositivi di rete che si stanno evolvendo rapidamente. Il mercato per la fornitura di servizi M2M sta vivendo un significativo shake-up, con diversi competitor in competizione con i produttori dei dispositivi che, verosimilmente devono cambiare i loro modelli di business, lo sviluppo di nuove caratteristiche di servizio, la costruzione di nuove alleanze e di trovare nuovi modi per interagire con i propri clienti.
- E' il nuovo che avanza.

E la Sicurezza ?

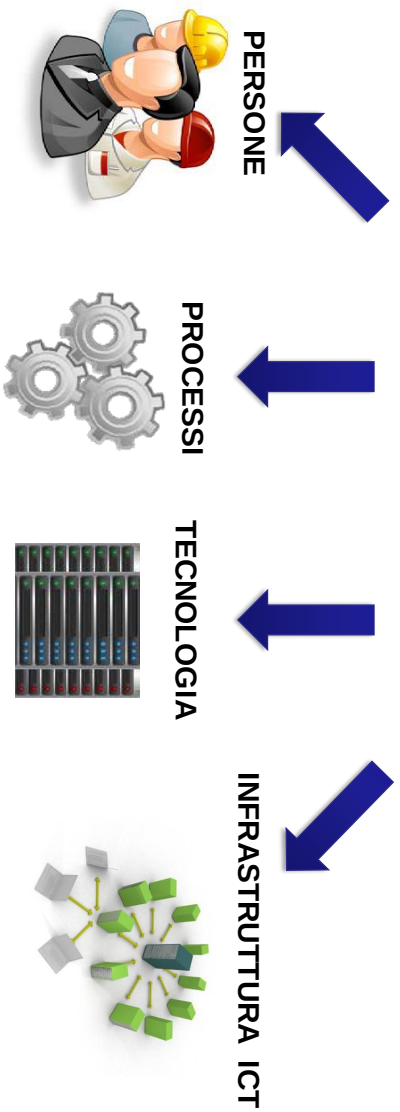
- Quali sono le principali istruzione d'uso per l'ICT nell'ambito dell'IoT e quindi anche dell'impiego intelligente dell'Energia (o per il monitoraggio di strutture o di trasporti, o …) ?
- Devono essere progettate da Professionisti esperti e possibilmente terzi.
- Gestione della connettività:
  - in una soluzione tipicamente client/server devono essere previsti più canali di comunicazione (per superare malfunzionamenti temporanei)
  - tutte le comunicazioni fra client e server devono avvenire tramite protocolli crittografati (ssh).
  - si deve evitare di esporre il client assegnandogli un indirizzo IP di rete pubblica (ad esempio attivando una VPN).
  - il server governa la comunicazione con i client.
- Deve Certificare i valori letti: per ciascuna lettura (gruppo di valori letto dalla medesima fonte/strumento) il sistema di acquisizione, prima di memorizzarlo sulla base dati vi deve associare un checksum tramite il quale è possibile verificare se un qualche valore abbia subito un'alterazione dopo l'acquisizione. Tale processo od un qualunque altro metodo di cifratura serve a garantire che il dato non subisce alterazioni durante il suo trattamento.

E la Sicurezza ?

- Deve Validare i valori letti: per ciascun valore letto il sistema deve verificare che lo stesso ricada nell'ambito di ammissibilità (massimo-minimo) per esso previsto. Qualora un valore non rientri nel range di ammissibilità ad esso associato l'intero gruppo di letture viene ritenuto invalido, in quanto le funzionalità dello strumento/fonte posso essere alterate dall'anomalia che ha inficiato il valore.
- Deve essere fruibile in Cloud ed appoggiarsi a strutture di Data Center con standard di sicurezza elevati tipo TIER III / TIER IV (conviene economicamente ed è difficile che lo si «faccia in casa»).
- Deve essere flessibile ed espandibile perché non c'è nulla di definito in questi ambiti ma «panta rei» e cioè deve essere indipendente dalla tecnologia, ciò attiene alla robustezza e quindi anche sicurezza della soluzione oltre che dell'investimento.
- Dal punto di vista qualitativo e quindi anche di sicurezza deve essere in grado di acquisire dati in formato standard, ad es.:
    - da servizi WEB (XML)
    - da file di testo formattati (CSV)
    - da MIB (Management Information Base) tramite SNMP (Simple Network Management Protocol) … continua …

Conclusioni

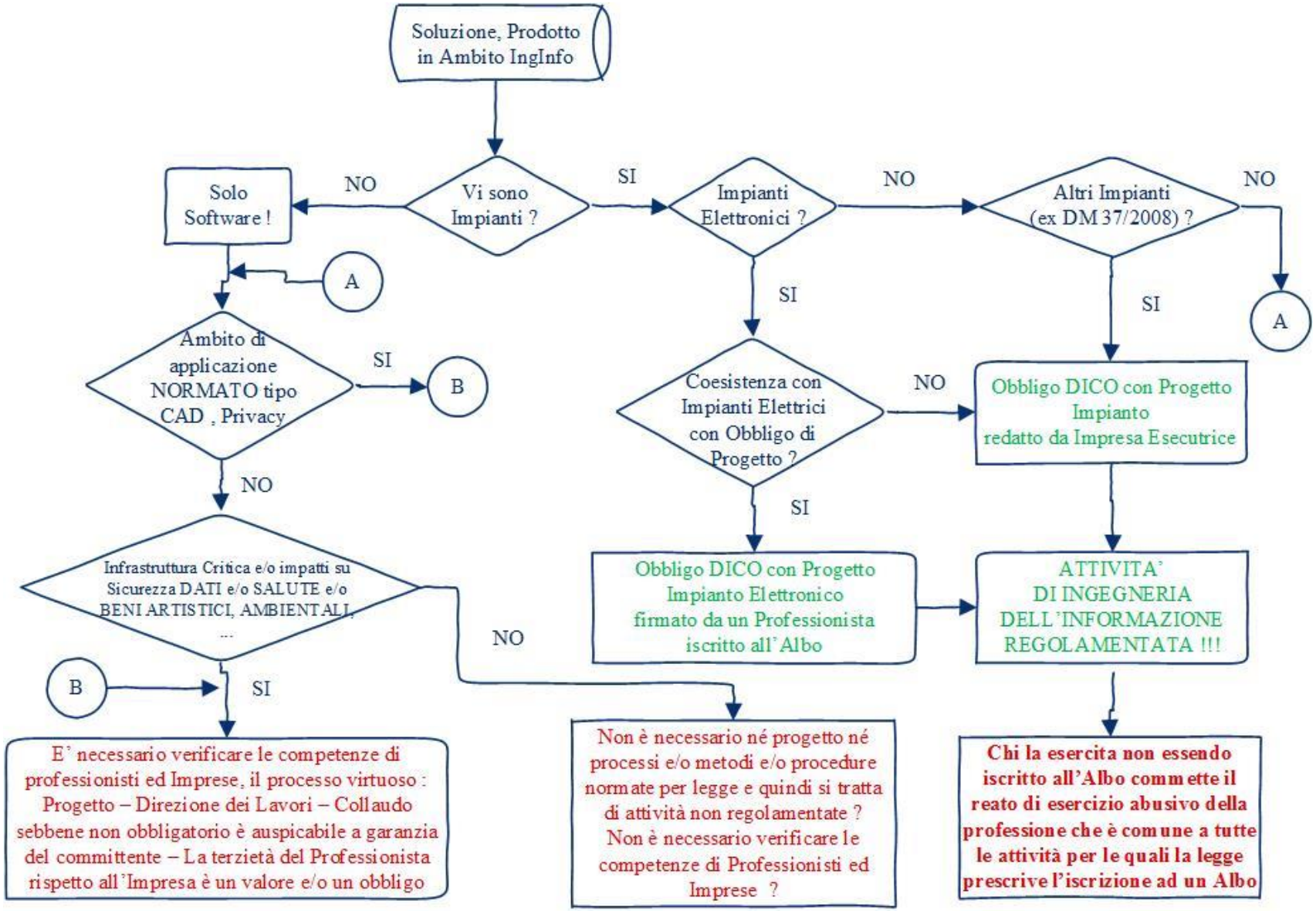
- Ma qual è il valore per l'utente finale della sicurezza ICT
- La sicurezza dipende da tanti elementi che si comprendono nelle categorie qui di fianco.
- La digitalizzazione in atto nel mondo lo rende più sicuro ?
- Il WEF dice che la probabilità non è bassa e l'impatto molto alto paragonabile ad un attacco terroristico o ad una crisi finanziaria.
- Se quindi nella PA non vi sono persone competenti a gestire l'ICT e la rivoluzione 4.0. basata sul Cloud e sull'Iot, qualunque sia il vertical applicativo energetico e non solo
- Se i Processi, le Infrastrutture ICT non utilizzano tecnologie adeguate almeno per le strutture critiche (scuole ospedali presidi militari …) e non vengono progettati da Professionisti che sanno fare … In assenza di un progetto unitario …
- Non si creerà valore ma, al contrario, i progressivi processi di digitalizzazione creeranno disvalore se non adeguatamente accoppiati con idonee misure di sicurezza sia tecnologiche che organizzative



Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

Conclusioni – Un possibile razionale di riferimento.



Conclusioni

L'approccio vincente non è impositivo, corporativistico del tipo: l'attività la deve svolgere quella determinata categoria perché ha una riserva dettata per legge. Questa è una battaglia di retroguardia destinata alla sconfitta.

L'approccio deve essere culturale: le infrastrutture critiche pubbliche devono essere messe in scurezza e progettate nel rispetto dei più altri standard di sicurezza per questo l'Art. 50 bis del CAD va difeso a spada tratta anzi il CAD va migliorato da questo punto di vista. Si deve intervenire !

I professionisti che operano nella PA con responsabilità nel settore ICT devono essere competenti per riconoscere e gestire gli appalti ICT come OO.PP. e non come forniture di beni e servizi e devono essere impegnati professionisti terzi rispetto alle imprese esecutrici a garanzia dell'amministrazione appaltante e quindi della società civile, alla stessa stregua di quanto avviene da decenni per i settori delle OO.PP. Tradizionali (Edili ed Impiantistici).

Poi che con riferimento all'ICT all'interno della PA, o all'estero come professionisti incaricati gli Ingegneri non abbiano le competenze giuste questo è tutto da dimostrare.

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI

CENTRO STUDI
CONSIGLIO NAZIONALE INGEGNERI

George Bernard Shaw ha scritto :

«Se tu hai una mela e io ho una mela e ce le scambiamo, abbiamo sempre una mela per uno, ma se tu hai un'idea e io ho un'idea e ce le scambiamo, allora abbiamo entrambi due idee».

Grazie per l'attenzione.

Ing. Bruno Lo Torto

Consigliere Centro Studi CNI