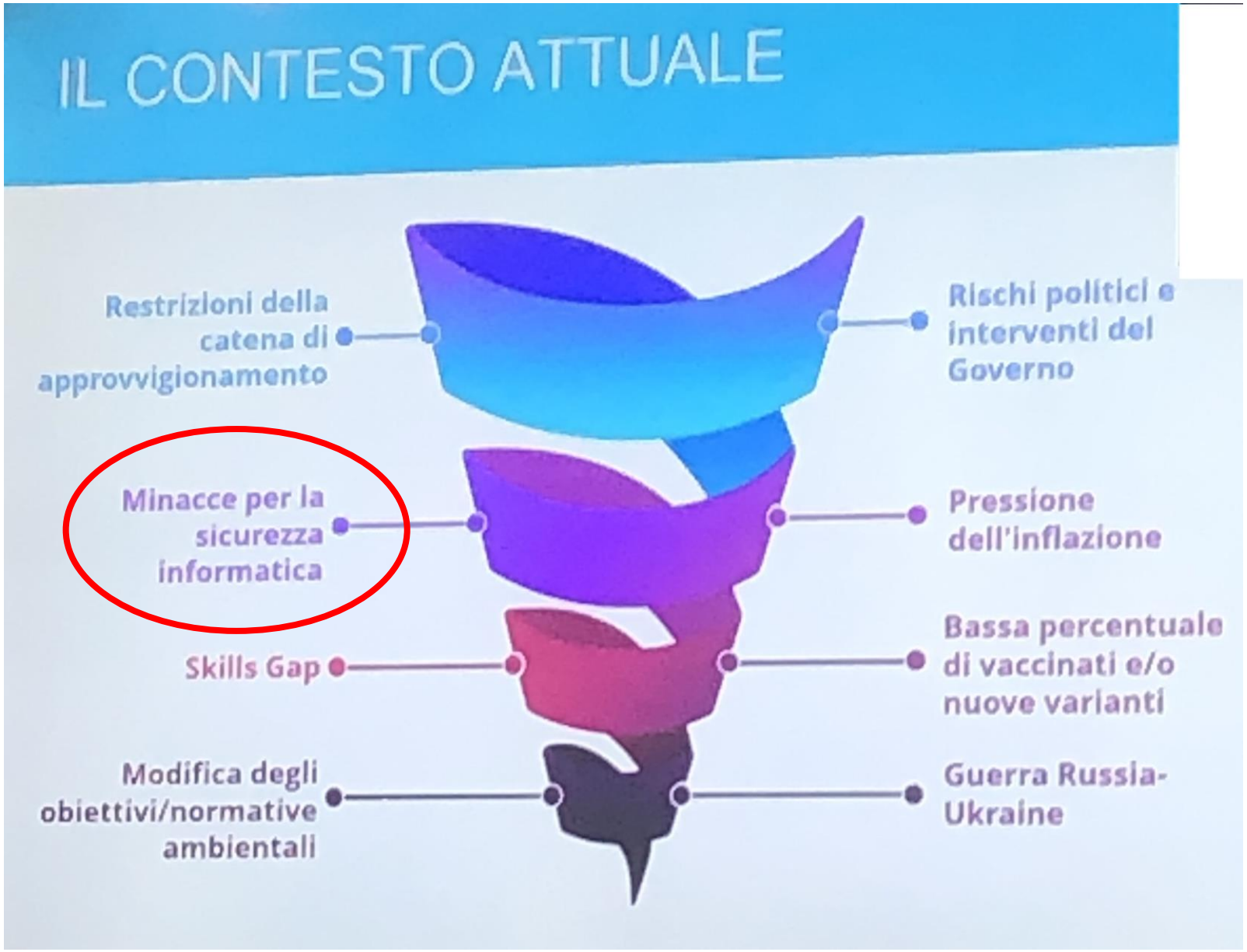
Cybersecurity e Pubblica Amministrazione: un binomio inconciliabile ?

Alessandro Musumeci

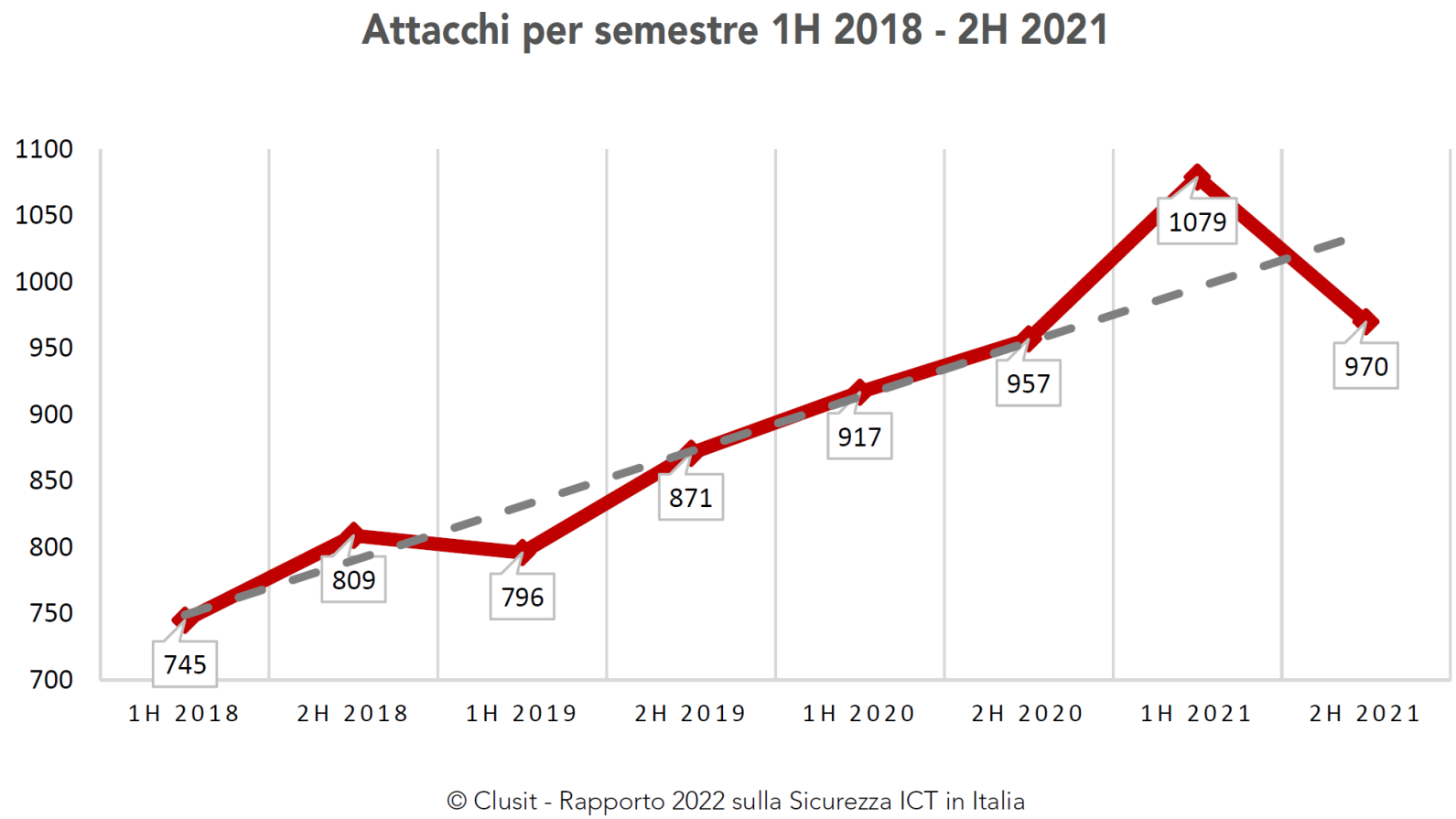
Reggio Calabria, 28 ottobre 2022

- L’evoluzione mondiale degli attacchi di Cybersecurity
- La situazione in Italia
- Lo stato dell’arte della Cybersecurity nella PA italiana
- Alcune esperienze personali
  - Ministero dell’Istruzione, dell’Università e della Ricerca
  - Comune di Milano – Expo 2015
  - Gruppo Ferrovie dello Stato Italiane
- Considerazioni finali



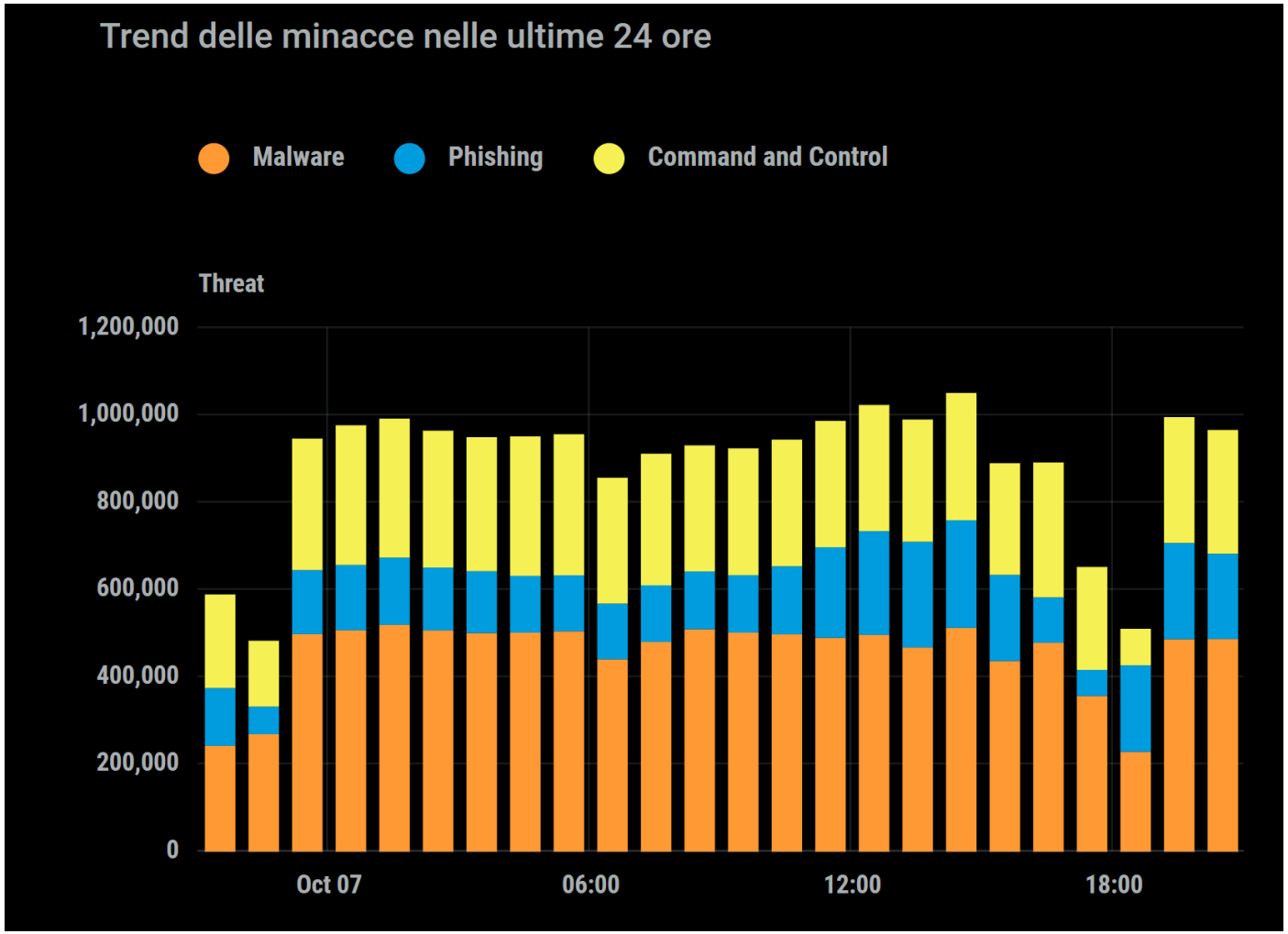
Fonte: IDC 2022

L’evoluzione mondiale degli attacchi di Cybersecurity



Oltre 14.000 attacchi nell’arco di 10 anni con impatto significativo in termini di perdite economiche, di danni alla reputazione, di diffusione di dati sensibili

L’evoluzione mondiale degli attacchi di Cybersecurity



Fonte: Akamai 2022

L’evoluzione mondiale degli attacchi di Cybersecurity

VITTIME PER CATEGORIA	2018	2019	2020	2021	2021 su 2020	TREND 2021
Gov. / Mil. / LE	220	233	225	307	36.4%	↑
ICT	191	233	269	278	3.3%	↗
Multiple Targets	326	406	401	274	-31.7%	↓
Healthcare	161	186	210	262	24.8%	↗
Education	106	140	174	174	0.0%	-
Financial / Insurance	162	107	122	137	12.3%	↗
Professional / Scientific / Technical	18	19	65	82	26.2%	↑
Wholesale / Retail	33	45	54	82	51.9%	↑
Transportation / Storage	33	16	39	75	92.3%	↑
Manufacturing	34	36	65	72	10.8%	↗
News / Multimedia	70	69	43	69	60.5%	↑
Organizations	40	35	46	52	13.0%	↗
Energy / Utilities	24	25	39	43	10.3%	↗
Arts / Entertainment	68	55	40	42	5.0%	↗
Telco	13	19	32	36	12.5%	↗
Hospitability	44	27	22	30	36.4%	↑
Other Services	9	14	15	25	66.7%	↑
Agriculture / Forestry / Fishing	0	0	5	6	20.0%	↗

[9] **ISIC** (International Standard Industrial Classification of All Economic Activities) delle Nazioni Unite e **NACE** della Commissione Europea (Nomenclature statistique des activités économiques dans la Communauté Européenne)

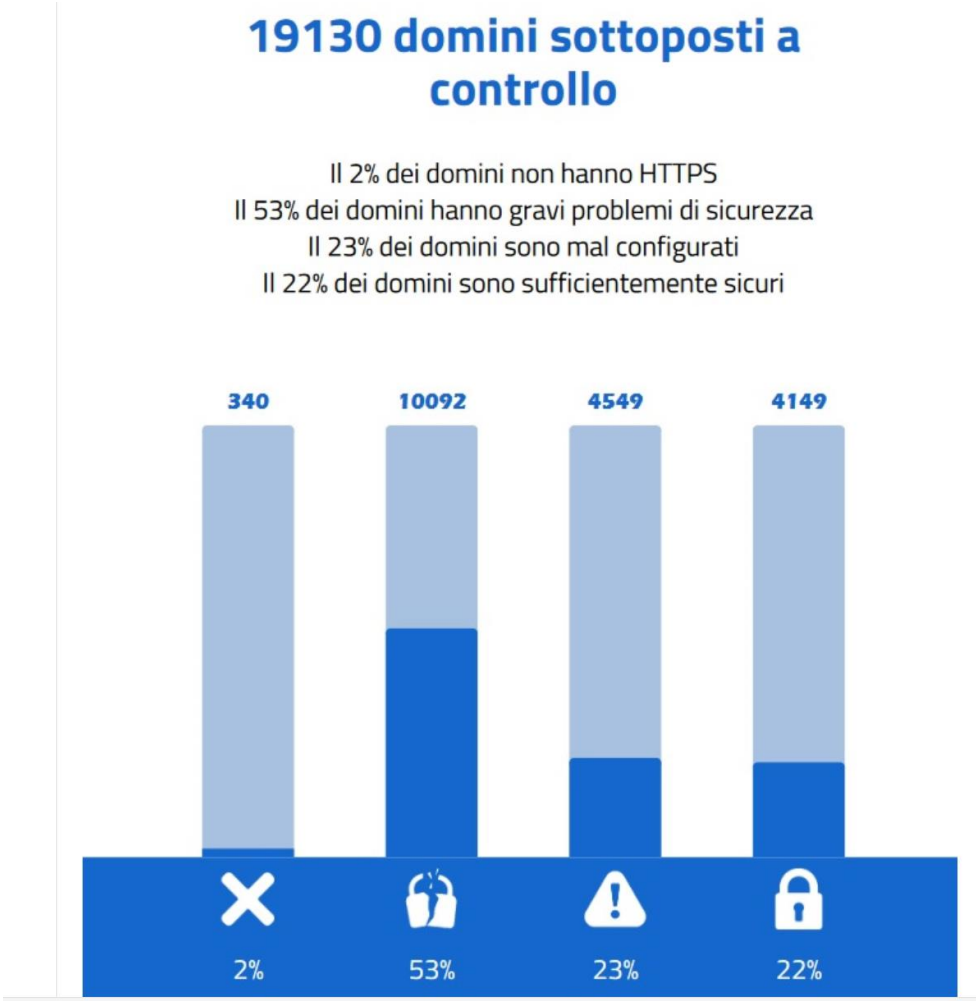
Alcuni attacchi nella PA italiana nel periodo 2020-21

- **Marzo 2020**: tentativo di accesso all'infrastruttura ICT dell'**Istituto Ospedaliero Spallanzani**, in particolare ai file sulle ricerche sul Covid-19.
- **Luglio 2020**: attacco all'**ENAC**, **Ente Nazionale per l'Aviazione Civile** con un ransomware che ha portato al blocco della posta elettronica, distrutto degli archivi digitali e reso inaccessibile il sito web.
- **Giugno 2020**: attacco all'**Enel** con il ransomware Skake/Ekans, che ha portato al furto di 5 TB di dati ed alla richiesta di un riscatto di circa 14 milioni di bitcoin, che la società dichiara di non aver pagato. Sul dark web sono stati pubblicati dati anche tecnici.
- **Settembre 2020**: attacco all' **Università Tor Vergata** con ransomware attivato da spear phishing, che ha bloccato l'intera infrastruttura ICT e colpito in particolare documenti su ricerche in ambito Covid19.
- L'attacco ai SI della **Regione Lazio,** iniziato il **30 luglio 2021**, che ha causato l'interruzione di servizi molto importanti per circa un mese: il sistema sanitario online, il servizio per la vaccinazione Covid-19 e il rilascio dei green pass, oltre al blocco di molte macchine in forza agli uffici tecnici dell'ente pubblico. Gli effetti nefasti del ransomware che ha messo in ginocchio il CED e i servizi informatici della Regione Lazio sono con buona probabilità dovuti all'incredibile ingenuità di un dipendente di una partecipata, a cui sarebbero stati rubati i dati di accesso al sistema, utilizzati per caricare il ransomware, prendere il controllo delle macchine e cifrare i dati.
- Un nuovo attacco ai SI **Enel** il **19 ottobre 2021** mediante il ransomware Netwalker, per il quale sono stati chiesti 14 milioni € in Bitcoin di riscatto e che ha causato il furto di 5 Tera Byte di dati, alcuni dei quali pubblicati nel darkweb.
- L'attacco ransomware a **settembre 2021** all' **Ospedale San Giovanni di Roma**, che ha posto fuori uso per parecchi giorni tutti i server e i pc utilizzati dalla struttura medica, bloccando completamente i vari servizi, dalle prenotazioni online via web alle cartelle cliniche e agli esami radiologici. Il personale medico è stato costretto a gestire i dati in maniera totalmente cartacea.
- L'attacco ai SI della **SIAE,** Società Italiana degli Autori ed Editori, avvenuto nell'**ottobre 2021**, che ha portato all'esfiltrazione di circa 60 terabyte di dati, comprendenti documenti di identità, dichiarazione di paternità di alcune opere e variazione dei recapiti domiciliari forniti dagli artisti alla società nel corso degli anni. L'attacco è iniziato con un phishing, rivendicato dal gruppo Everest, che ha richiesto il riscatto di tre milioni di euro in bitcoin per la restituzione dei dati, che la SIAE, dopo aver informato la Polizia Postale e il Garante della privacy, ha affermato di non aver pagato. Questo attacco è interessante poiché rappresenta un caso significativo della "multiple extortion": si induce la vittima a pagare il riscatto prima per la decifratura dei dati, poi a pagarne un secondo per impedire che i dati sottratti vengano pubblicati o messi in vendita sul dark web. L'attaccante sovente non rispetta totalmente la seconda estorsione, o non viene pagato: contatta quindi direttamente le persone di cui ha ottenuto illegalmente informazioni per ricattarle direttamente, soprattutto se sono personaggi noti al pubblico.

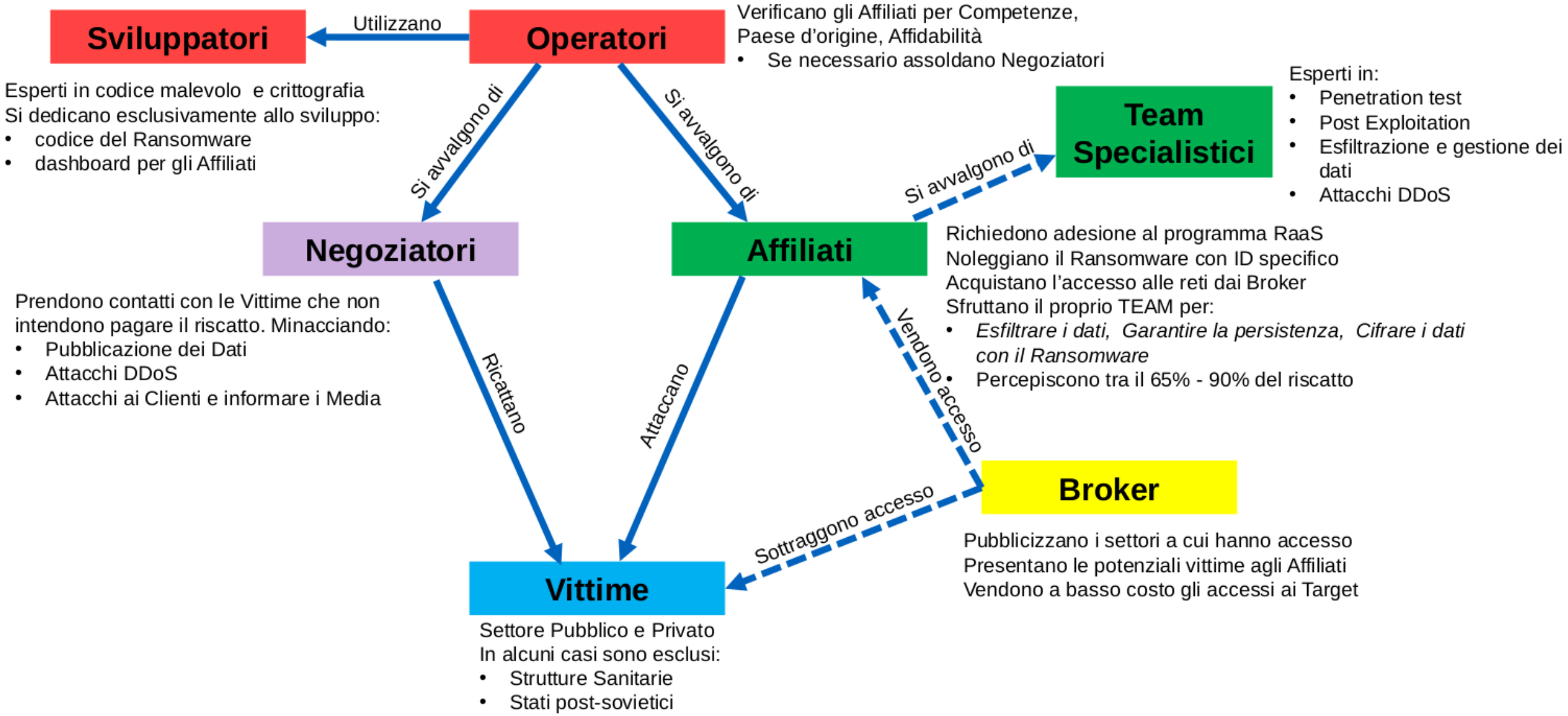
Fonte: rapporto OAD 2021

Dal secondo monitoraggio del protocollo HTTPS e dei CMS sui sistemi della PA-22/10/21

- Il monitoraggio effettuato mediante una serie di strumenti sviluppati internamente dagli analisti di AgID segnala che solo il 22% dei siti della PA utilizza una corretta configurazione HTTPS, mentre solo l' 8,3% dei CMS utilizza versioni aggiornate dal punto di vista della sicurezza



Galassia e organizzazione del Ransomware as a Service

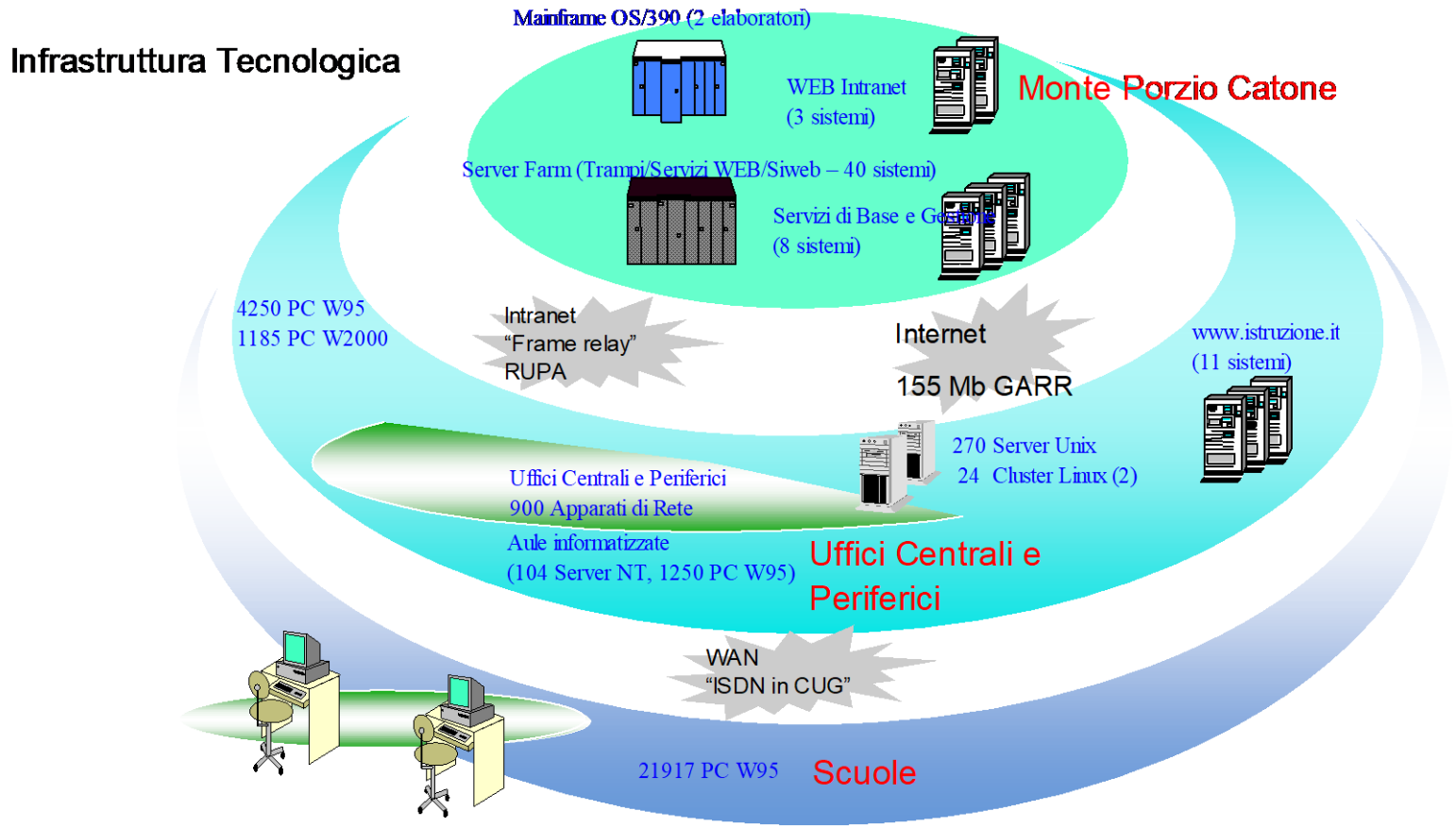


Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) – 2002-2006

Come ho analizzato i problemi di sicurezza nel contesto MIUR

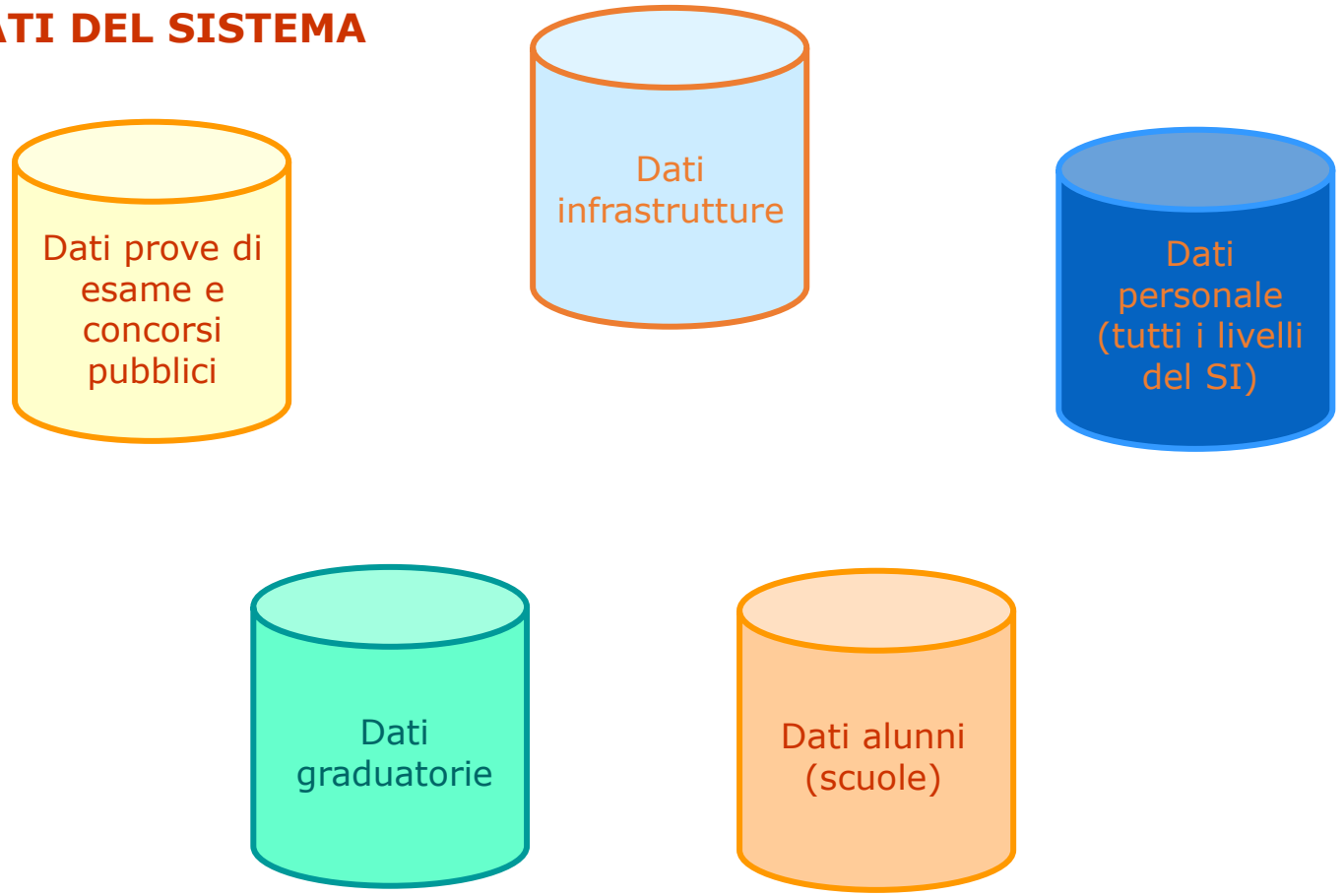
- La dimensione e l'articolazione del Sistema: presenti tutti i fattori della complessità, quali estensione del SI, articolazione, utenza variegata con diverse esigenze, dati critici (dati sul personale, dati sui concorsi pubblici, graduatorie…)
- La presenza delle scuole: implica la criticità legata alla gestione di dati di minori
- La gestione in outsourcing del SI: si pongono complessi problemi per gestire i requisiti di sicurezza nei confronti dei fornitori dei servizi in outsourcing
- L'assenza di una vera e propria politica per la sicurezza: l'approccio seguito nel passato è stato basato sugli interventi necessari e non su una strategia specifica

Il contesto del SI del MIUR



I dati gestiti nel sistema e le criticità

I DATI DEL SISTEMA



Alcune delle possibili minacce

- Accesso ad informazioni riservate (studenti e personale)
- Accesso abusivo ad Internet tramite LAN delle Scuole
- Furto di notebook e/o hard disk
- Interruzione dei servizi (causati da fornitori)
- Denial of Service in conseguenza di attacchi multipli
- Interruzione dei servizi a causa di virus, mal funzionamenti, guasti ed eventi naturali
- Perdita di dati per deterioramento o alterazione dei supporti magnetici
- Rallentamenti dei servizi per congestione della rete
- Accessibilità ai siti da parte di fornitori di servizi vari

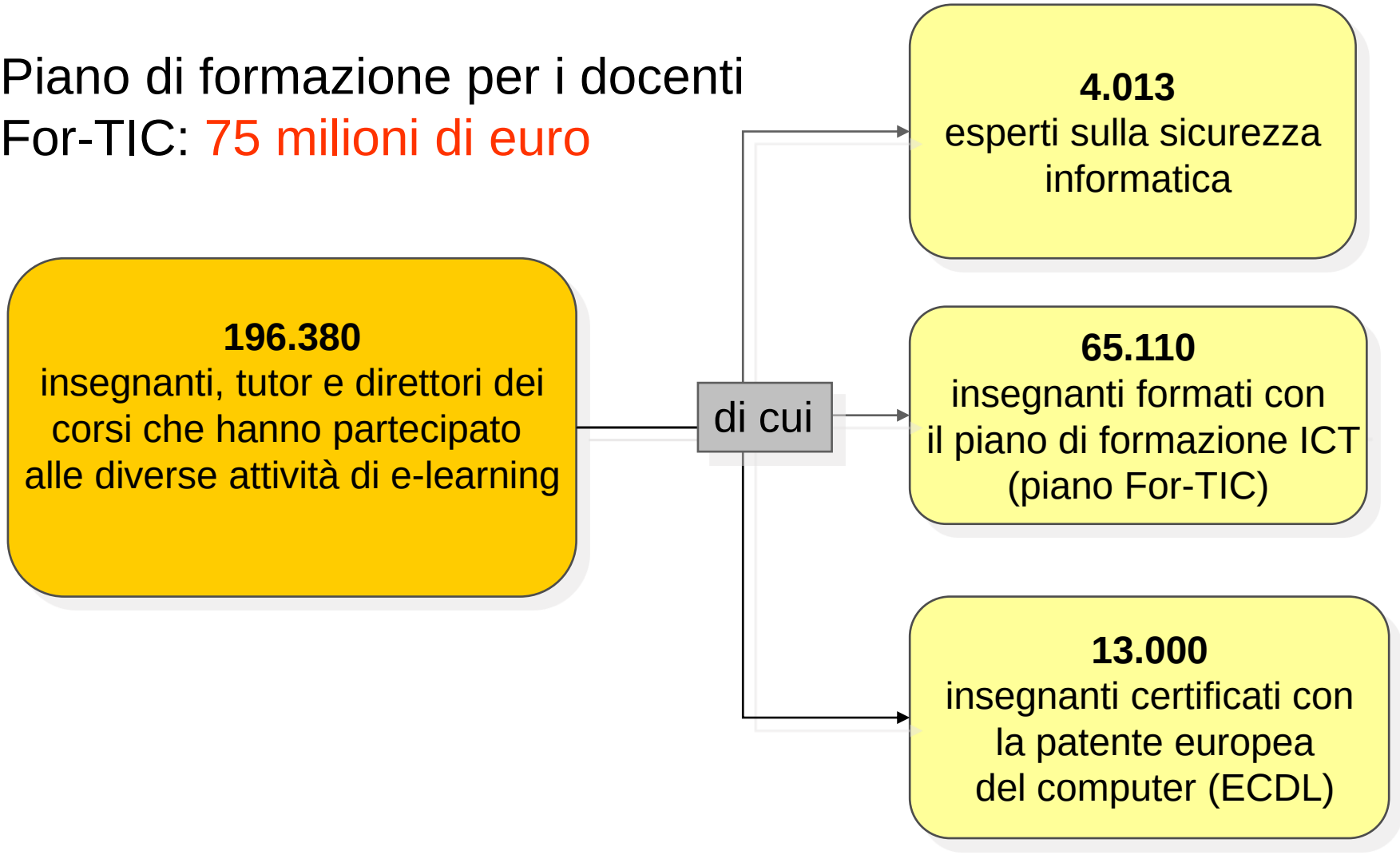
Alcuni esempi di problemi riscontrati

Gli incidenti pur non avendo generato situazioni particolarmente critiche impattano su aspetti variegati della sicurezza (es. fisica, logica, organizzativa)

- Furto di dispositivi hardware (personal computer, portatili, stampanti) e apparati di rete (più rilevante negli istituti scolastici);
- Episodi di attacchi DOS, a seguito di netstrike dichiarati contro il sito dell'amministrazione;
- Aumento di messaggi e-mail fasulli e indesiderati (spamming);
- Cattiva gestione delle credenziali di autenticazione da parte degli utenti (condivisione di password e/o badge fisici di accesso ai servizi);
- Attacchi provenienti da virus e trojan;
- Modifica non autorizzata di basi di dati (situazioni di stato giuridico dei docenti, posizioni in graduatoria permanente);
- Interruzioni temporanee del servizio dovute a malfunzionamenti, guasti ed eventi naturali (es black out elettrico);

Le iniziative messe in campo (1)

Piano di formazione per i docenti
For-TIC: 75 milioni di euro



Le iniziative messe in campo (2)

CHI HA PAURA... DELLA RETE?

per un uso consapevole
-- di Internet --

home | navigatori per caso ...

✓per i Bambini

qui puoi giocare per scoprire molte cose su Internet; alla fine del gioco ti sarà consegnata la patente del "buon navigatore".

✓per i Ragazzi

qui puoi imparare come utilizzare Internet, conoscere le regole da rispettare e i diritti da far valere per essere un "buon navigatore".

✓per i Genitori

qui puoi trovare utili consigli e la possibilità di scaricare un prodotto software per filtrare i contenuti che non ritieni adatti ai tuoi figli.

Per saperne di più

- [x] navigatori per caso
- [ ] acquisti on line
- [ ] chat lines
- [ ] dipendenza da internet
- [ ] peer to peer
- [ ] filtri

CHI HA PAURA... DELLA RETE?

per un uso consapevole
-- di Internet --

home

✓Internet è...

...è una grande e inesauribile enciclopedia. Ogni movimento del mouse apre una nuova pagina che può mostrarti posti lontani e interessanti, fornirti tutte le informazioni che desideri, farti conoscere nuovi amici e compagni di viaggio. Insomma con un solo click puoi davvero visitare tutto il mondo!
Con Internet hai non solo la possibilità di comunicare senza limiti di spazio e di tempo, oltre ogni confine geografico e culturale, ma disponi anche di una gamma vastissima di servizi che vanno dalla posta elettronica alle operazioni finanziarie, dalle attività commerciali fino alle conferenze telematiche.

I benefici e i vantaggi che l'utilizzo di Internet può portare nella vita di tutti i giorni sono immensi, ma è impensabile, se volessimo ricorrere a un'immagine diffusa, che di una medaglia esista solo una facciata.
Anche Internet, come accade nella realtà, può riservare delle brutte sorprese. Per questo appare indispensabile favorire un uso consapevole della rete, un utilizzo delle moderne tecnologie che sia dettato da buon senso e ragionevolezza, ma soprattutto dalla conoscenza delle immense potenzialità della rete.

Per saperne di più

- navigatori per caso
- acquisti on line
- chat lines
- dipendenza da internet
- peer to peer
- filtri

Comitato Regionale per le Comunicazioni
CORECOM
Friuli - Venezia Giulia

CHI HA PAURA... DELLA RETE?

per un uso consapevole
-- di Internet --

✓Bambini

Internet è un mondo meraviglioso che può offrirti molto ma che, come il mondo reale, nasconde delle insidie che lo rendono pericoloso.

Conoscere questo mondo fantastico e le insidie che in esso si nascondono ti aiuterà a navigare tranquillo

Scopriamo insieme....

- **A cosa serve internet**
- **Cosa si può e cosa non si deve fare**
- **I diritti**

Se vuoi conoscere il significato dei termini più utilizzati vai al Glossario

✓Regole

3.In rete puoi trovare molto materiale per la tua tesina.

a. raccolgo tutto il materiale a disposizione, ne faccio un rapido collage e consegno la tesina
b. consegno una tesina che ho trovato in rete già fatta
c. grazie alle informazioni che ho trovato su Internet farò la tesina più originale
d. il materiale che ho trovato in rete è prezioso: decido che metterò on line anche la mia tesina così qualcun altro potrà usufruire del mio lavoro

◂◂ Torna all'elenco

✓Regole

c.grazie alle informazioni che ho trovato su Internet farò la tesina più originale

BRAVO !!!

Grazie a migliaia di persone che ogni giorno decidono, spontaneamente e senza fini di lucro, di **condividere** in rete le loro conoscenze, Internet è una risorsa inesauribile di informazioni per continuare sempre a imparare e a migliorarti.

Il passo successivo è decidere di **condividere** con gli altri le conoscenze che la rete ti ha aiutato ad acquisire.

Continua ▸▸

✓Regole

d.il materiale che hai trovato in rete è prezioso: decidi di mettere on line anche la tua tesina appena l'avrai finita così qualcun altro potrà usufruire del tuo lavoro

BRAVO !!!

Hai colto in pieno lo spirito di **condivisione** che anima le comunità di Internet e tutte le altre importanti inziative che rendono la rete una sterminata risorsa di informazioni che persone generose e lungimiranti decidono ogni giorno di condividere con tutto il mondo.

Continua ▸▸

CHI HA PAURA... DELLA RETE?

per un uso consapevole
-- di Internet --

✓Consigli

1. Non tenere il computer in un ambiente isolato. Internet deve essere considerato come uno strumento di famiglia.

2. Condividi i principi con tuo figlio. Scrivi insieme a lui la carta delle regole di comportamento in internet

3. Dialoga con tuo figlio. Accetta e chiedi che ti mostri quali sono i suoi siti preferiti e ascolta le sue osservazioni.

4. Fai vedere a tuo figlio come internet possa essere utile. Utilizzalo con lui quando devi organizzare per esempio una vacanza.

5. Cerca di navigare insieme a tuo figlio, non lasciarlo da solo per troppo tempo, ricorda che internet non è una babysitter.

6.Se trovi in rete materiale illegale o presumibilmente dannoso per i bambini, puoi segnalarlo al sito della Polizia delle Telecomunicazioni.

7. Fa che il suo rapporto con internet sia equilibrato.

8. Educalo alla prudenza, a non dare notizie personali, ad abbandonare un sito dai contenuti inadatti e a non incontrare persone conosciute in internet senza averne prima parlato con te.

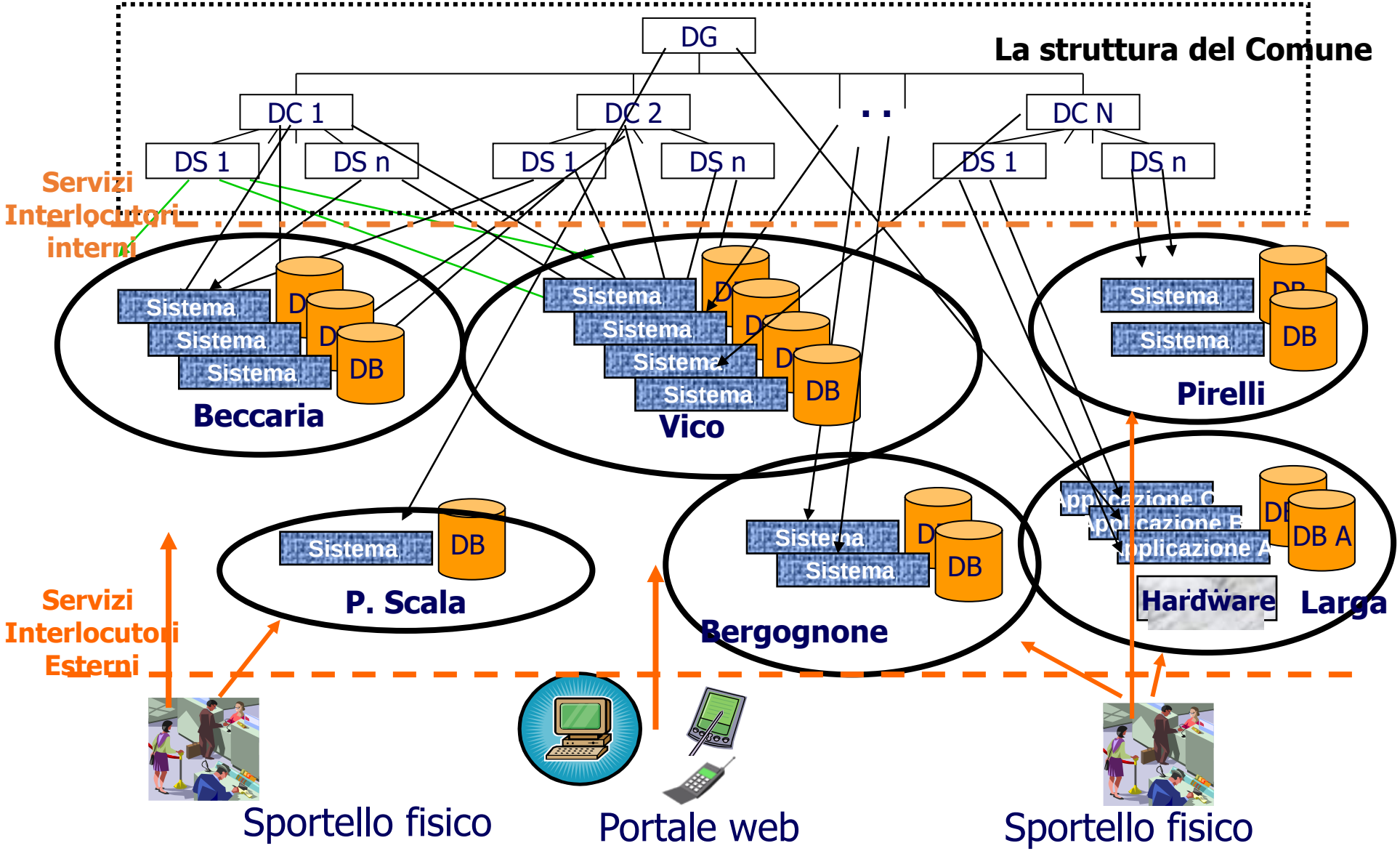
9. Evidenzia l'importanza dell'educazione e del rispetto nelle chat e nella posta elettronica.

10. Insegna a tuo figlio che non deve acquistare nulla in internet senza averne parlato con te.

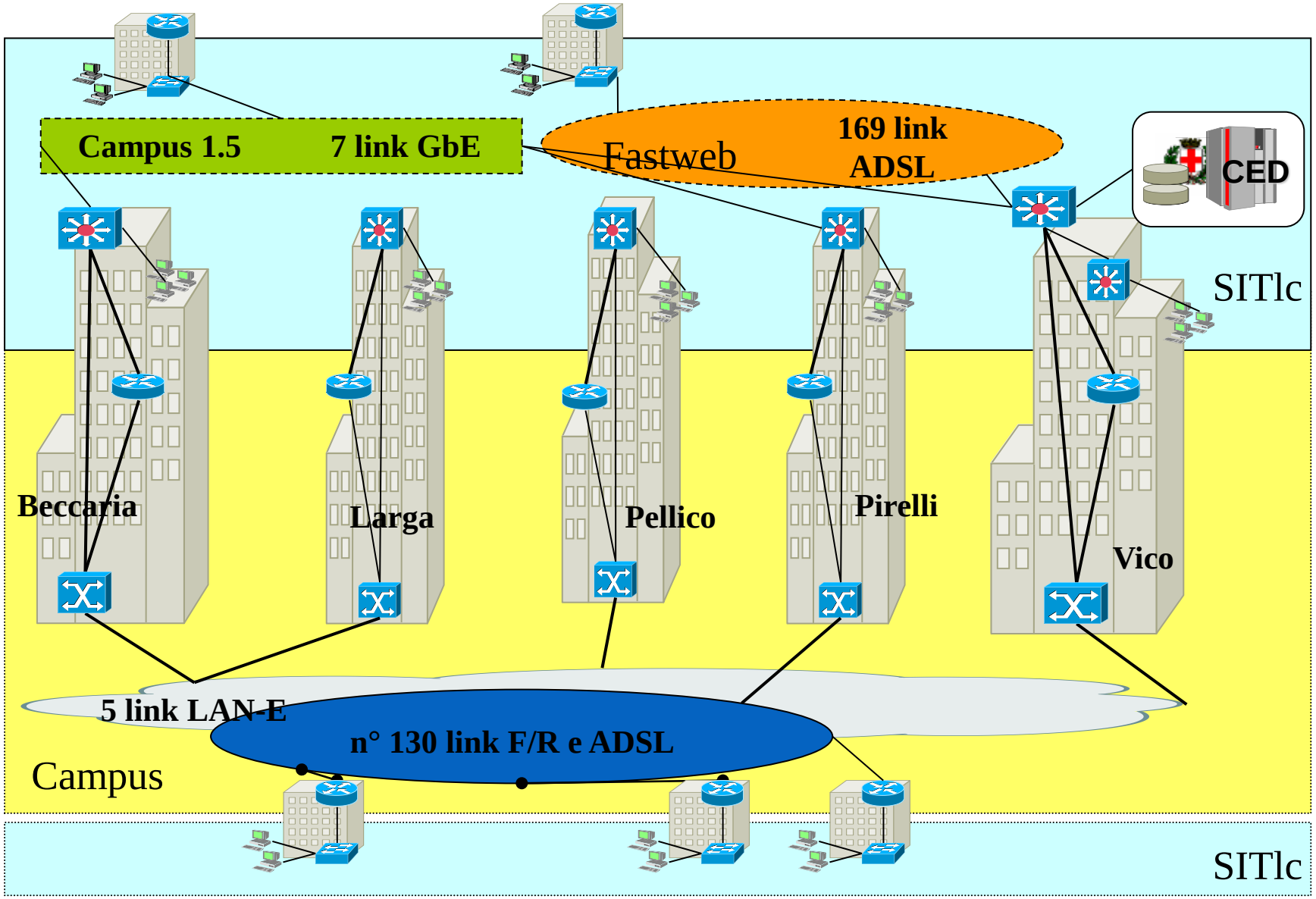
11. Stabilisci contatti con altri genitori nella rete, diventa più esperto nell'utilizzo di internet.

Comune di Milano (2006-2008)

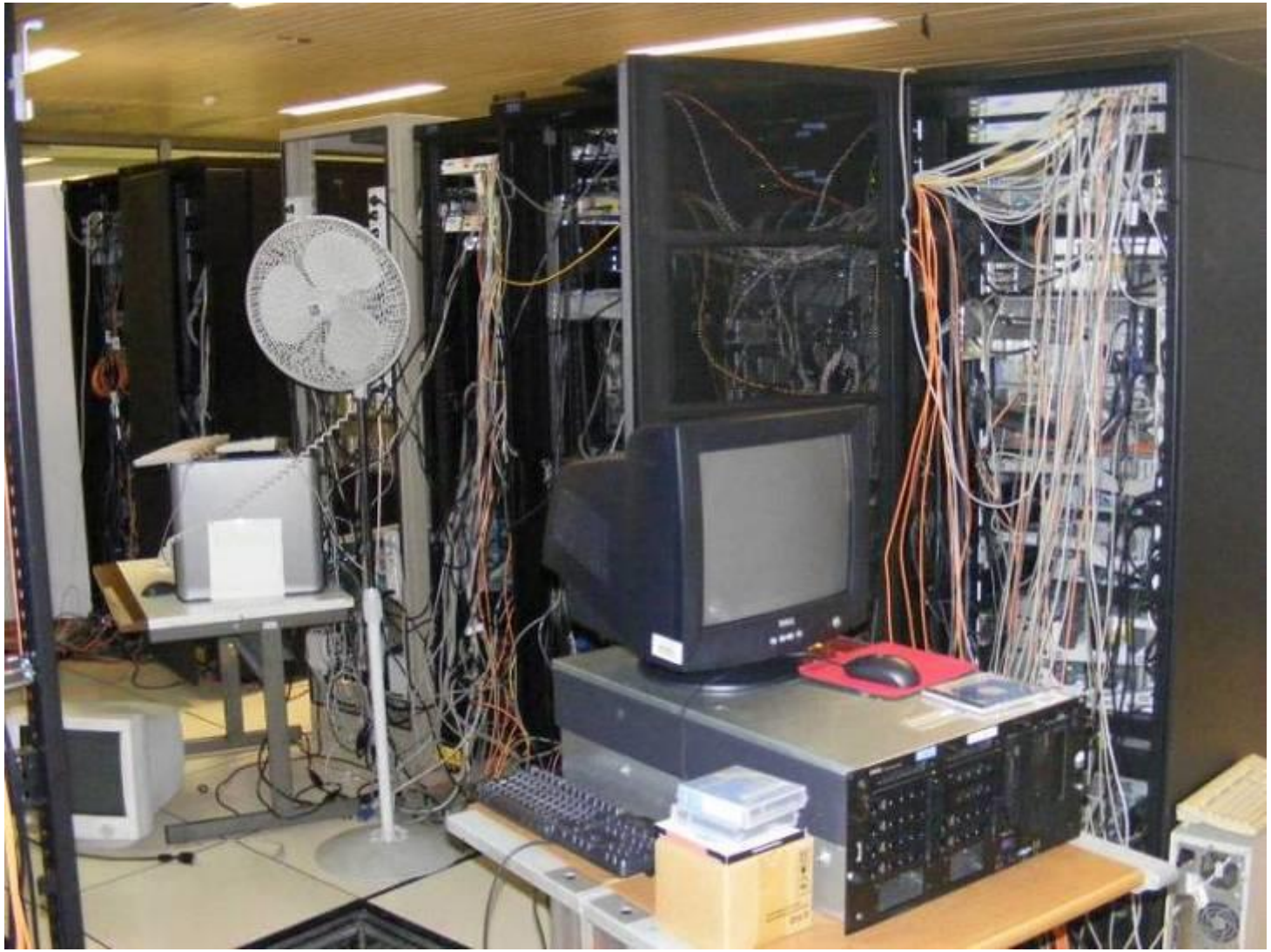
La situazione informatica del 2006



La rete Campus 1 (2006)



Comune di Milano –la vecchia sala CED (2006)



il caso

Virus informatico in Comune, computer spenti fino a lunedì: ma si possono richiedere i certificati

L'anagrafe funziona nonostante Kamasutra

2/2/2006 Corriere della...

Cronaca di Milano

Disagi e proteste per il blocco di certificati e carte d'identità. Paralisi anche agli sportelli dell'Urbanistica e dei vigili urbani

«Virus nei computer, Comune sotto attacco»

L'assessore Martella: un sabotaggio interno, oggi i cittadini si informino prima di andare all' Anagrafe

Blackout all'anagrafe, ai tributi, per i servizi sociali e i vigili urbani. Martella: è un attacco che arriva dall'interno

Comune, 10mila computer in tilt

Caccia al virus. Anche oggi sarà difficile avere un certificato

«Virus kamasutra», fuori uso i computer del Comune

Email sexy paralizza il sistema informatico di uffici e polizia locale. Tutto fermo fino a lunedì

L'ALLARME

Programmato per colpire oggi, a Palazzo Marino diecimila pc in tilt

Virus Kamasutra a Milano ko i computer del Comune

- l’attacco portò ad un DDoS (Distributed Denial of Services) che si replicava su server mal o per nulla protetti a livello di Amministratore di sistema, gestiti da altre Direzioni del Comune e non da quello dei Sistemi Informativi.
- Il Comune non fu pronto a gestire l’emergenza, in particolare la comunicazione coi media, amplificando l’impatto dell’attacco
- Il Comune denunciò alla Polizia delle Telecomunicazioni l’accaduto
- Dopo quasi due anni sono arrivati avvisi di garanzia per 6 funzionari
- I sistemi informativi del Comune possono essere un significativo obiettivo per attacchi
- Il Comune e la DSSI si deve preparare per poter non solo prevenire ma anche gestire l’attacco e le sue conseguenze al meglio, riducendone gli impatti
- La sicurezza ICT non è solo un problema tecnico, è soprattutto un problema organizzativo
- Cruciale il ruolo della gestione della sicurezza ICT nell’ambito della più generale ICT governance

Comune di Milano (2006-2008) definizione di un piano generale di sviluppo 2006-2011 (pagg. 43-44)

- **L'attuale sistema si svilupperà per i prossimi anni:**
  1. **Per le infrastrutture:**
     a) **Implementando una nuova rete comunale**
     b) **Con il nuovo Progetto Informatica Personale Distribuita**
     c) **Con l'implementazione di innovative politiche per la sicurezza informatica**
  2. **Per i sistemi applicativi**
     a) **Con il Nuovo portale del Comune di Milano**
     b) **Implementando progetti di e-government, co-finanziati dallo stato o in partnernship pubblico-privato**
     c) **Con una nuova gestione documentale e del protocollo**
     d) **Con l'accentramento delle macchine in un unico CED**

Comune di Milano – la nuova sala CED (2008)

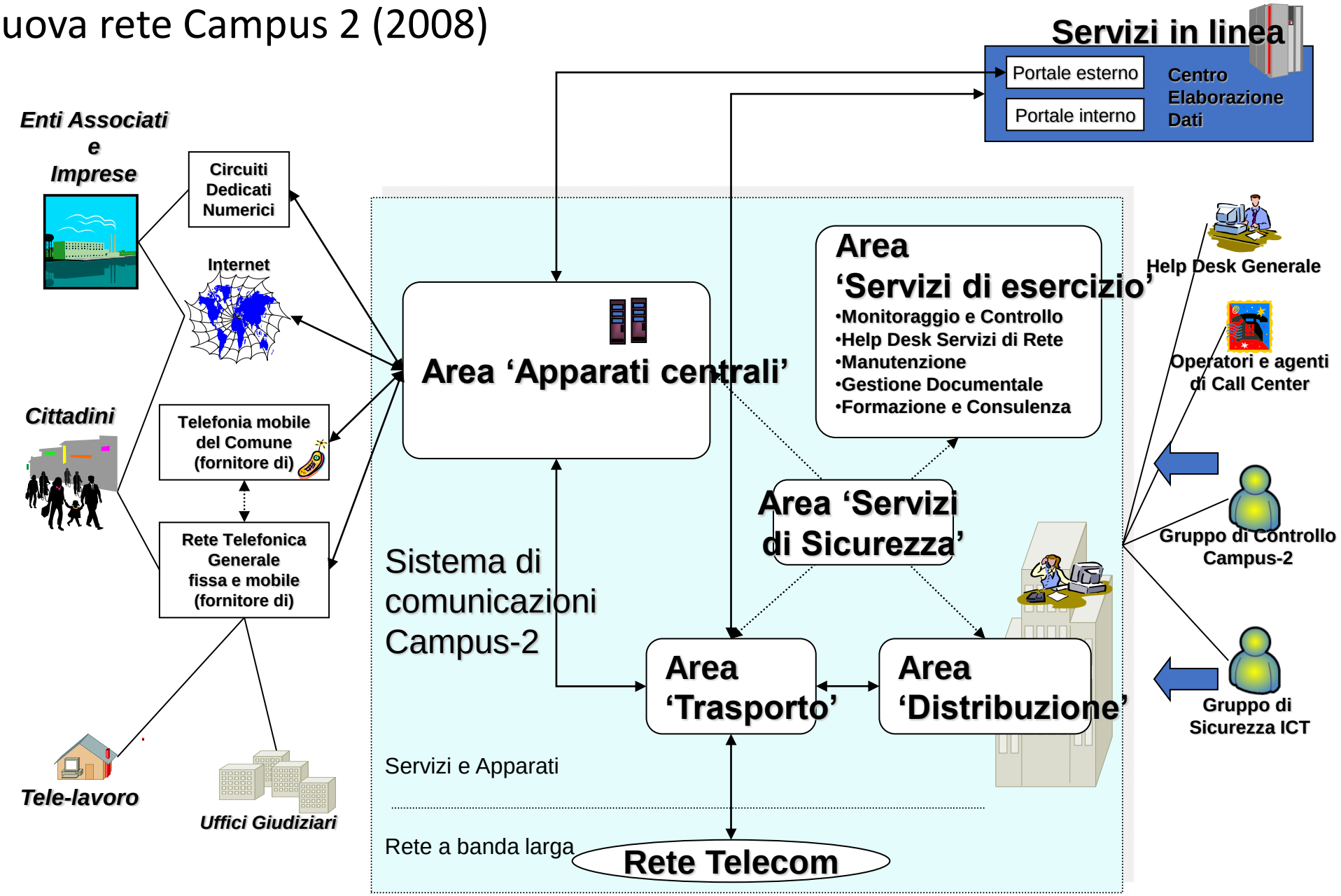
Comune di Milano
Centro di Controllo sulla Sicurezza

PC con utenze sospette

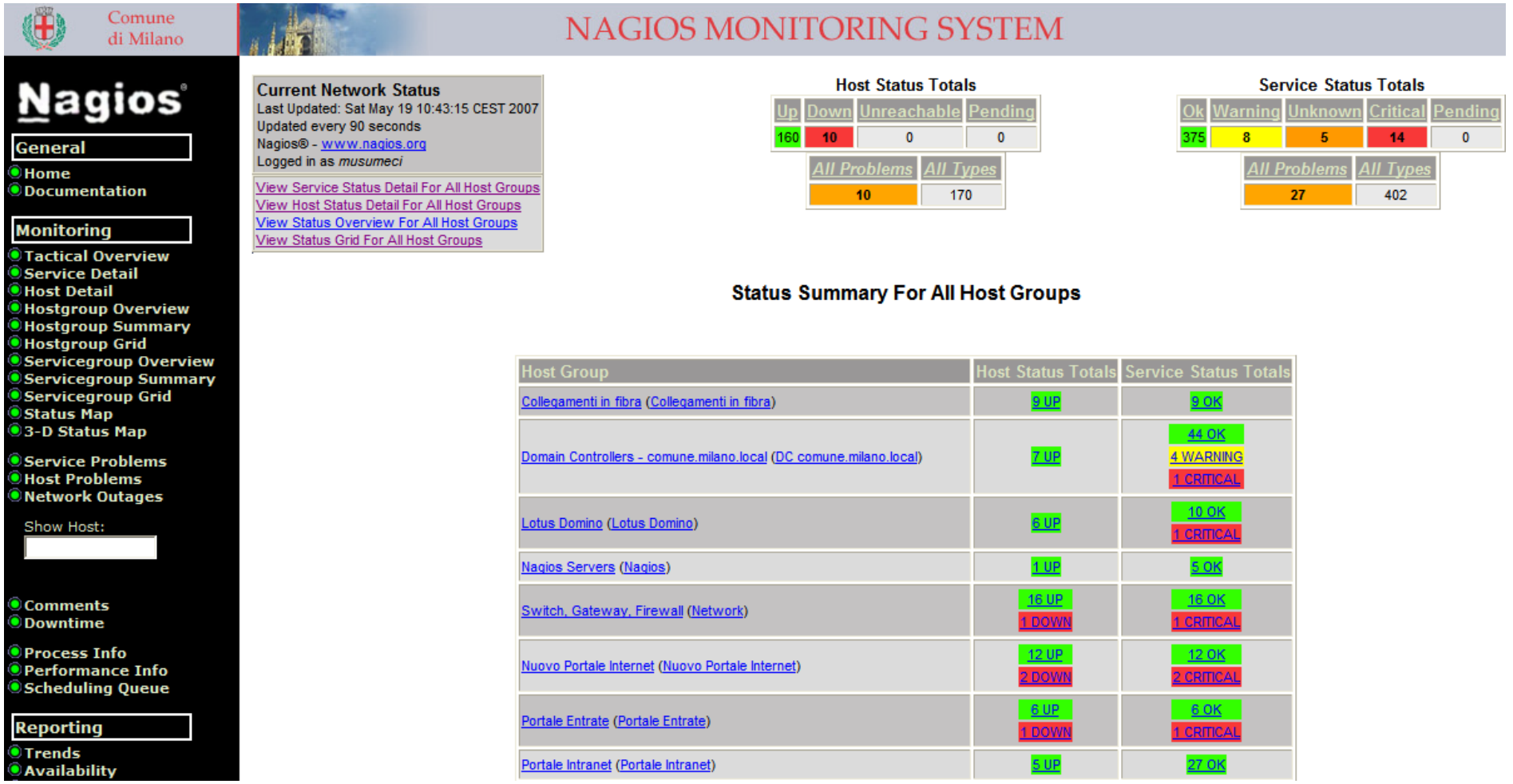
26/02/2007

Data	Ora	Nome PC	Gruppo	Utente
27/02/2007	9.59.30	B1023984	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.00.54	B1024002	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.04.07	B1024059	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.04.12	B1024005	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.05.38	B1024001	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.07.24	B1023971	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.09.13	B1024066	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.11.03	B1024073	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.11.05	B1023459	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.11.48	B1024068	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.13.34	B1024074	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.13.37	B1024070	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.13.42	B1012757	BI User	S-1-5-21-1780879593-1264614178-1435325219-1030
27/02/2007	10.13.42	B1012757	BI User	S-1-5-21-1780879593-1264614178-1435325219-1831
27/02/2007	10.14.21	B1024076	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.15.26	B1023996	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.18.50	B1024078	BI User	S-1-5-21-632241361-372386011-2764512682-1767
27/02/2007	10.19.34	B1024060	BI User	S-1-5-21-632241361-372386011-2764512682-1767

La nuova rete Campus 2 (2008)



Implementazione di un prodotto Open Source (Nagios) per il controllo della rete e dei server

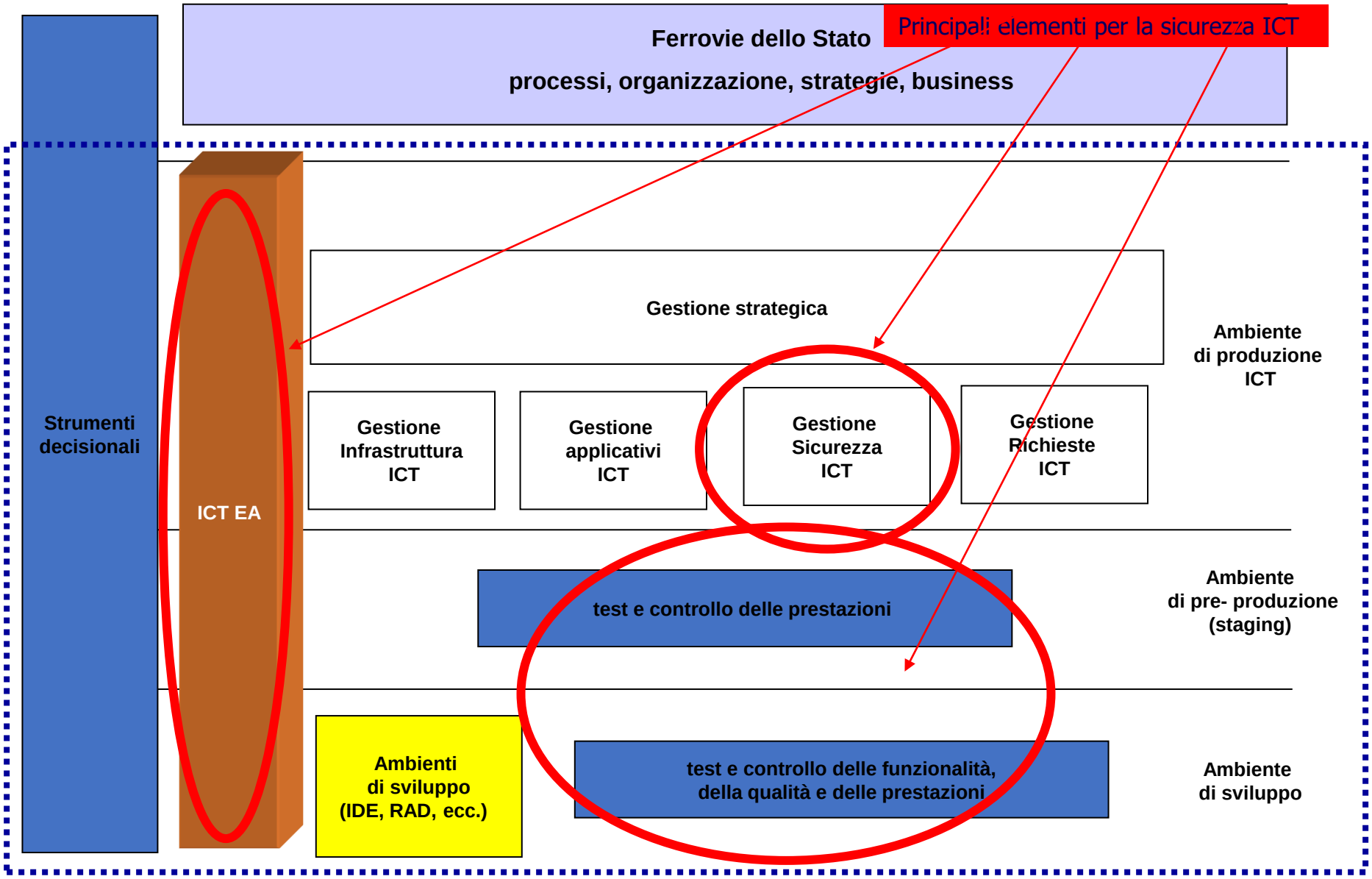


Gruppo Ferrovie dello Stato Italiane (dal 2008 in poi)

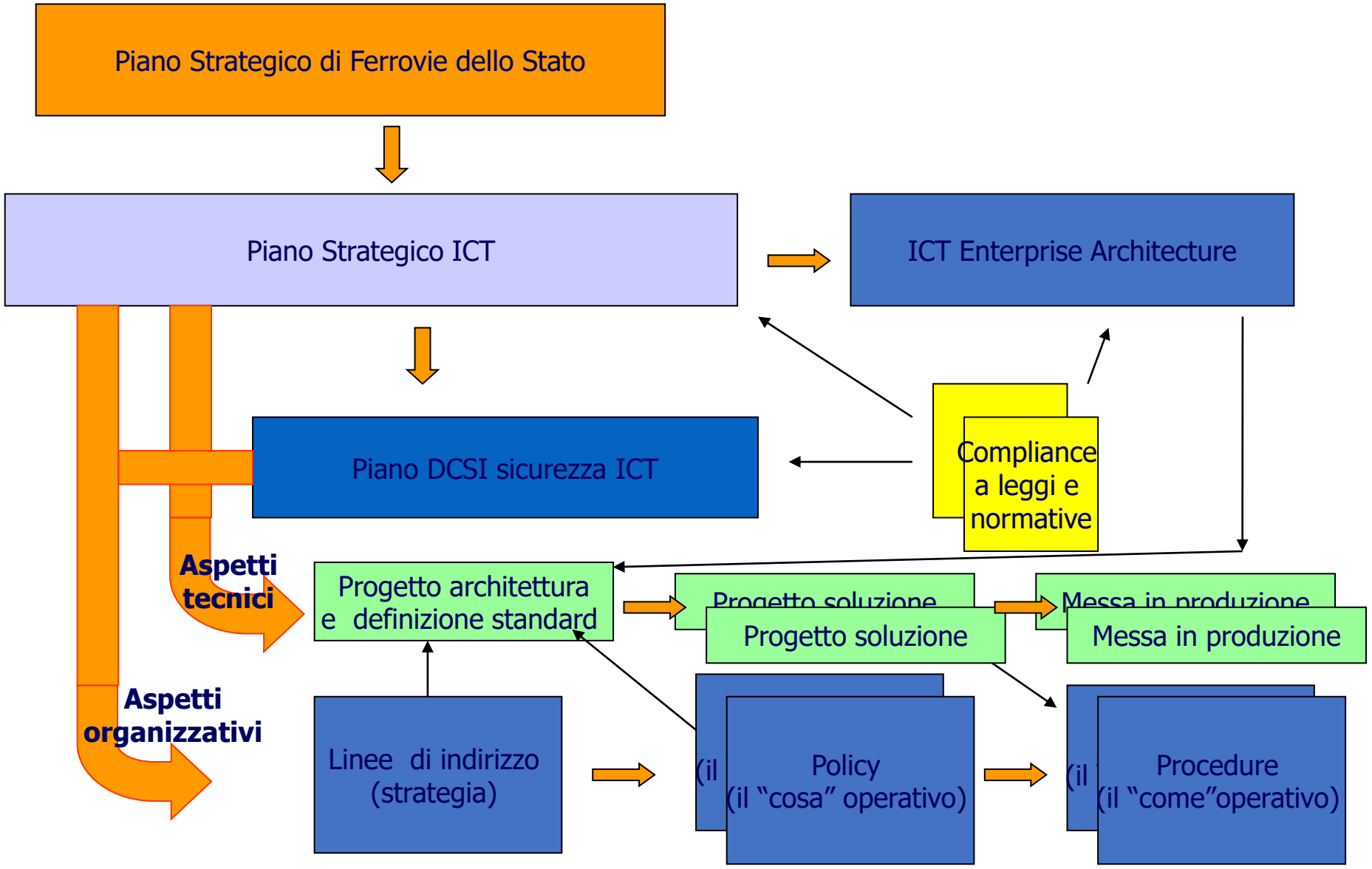
Il ruolo della sicurezza informatica in Ferrovie

- Il sistema ICT di Ferrovie dello Stato è un sistema complesso, eterogeneo, distribuito, con più di 77.000 utenti interni e con, potenzialmente, milioni di utenti esterni
- Il Piano strategico di Ferrovie dello Stato considera l'ICT lo strumento abilitante ai servizi per i diversi interlocutori:
  - Il ruolo dei sistemi ICT e della DCSI richiede quindi una profonda evoluzione nel passaggio da "centro di costo" e da "parziale" gestore dell'ICT di Ferrovie nell'unico "fornitore di servizi ICT" e di "centro di competenze ICT"
- La sicurezza ICT deve essere pervasiva a tutti i livelli ed in tutti i dispositivi, ed essere ben bilanciata
- La sicurezza ICT non è un insieme di prodotti-soluzioni, ma un processo continuo che deve essere gestito day-by day e che deve evolvere in funzione delle nuove esigenze, dell'evoluzione tecnologica e dei nuovi rischi
- L'attuazione della sicurezza ICT dev'essere normata attraverso l'uso di opportune policy (come quella per tutto il personale dell'agosto 2009 o quella per l'uso delle reti Wi-Fi)

La sicurezza ICT nella visione concettuale dell'ICT Governance



Dal piano strategico alle policy ed agli interventi per la sicurezza ICT



Linee di indirizzo, Policy e Procedure

Linee di indirizzo

Descrivono gli indirizzi a più alto livello, con una vista strategica e pluriennale nell'ambito dell'eviluzione dell'EA

Policy di Sicurezza

Indica un insieme di regole e norme che specificano o regolamentano le modalità con cui un sistema o un'organizzazione fornisce servizi di sicurezza per proteggere risorse critiche o riservate.

Cosa

Finalità: far prendere coscienza all'Ente dei propri asset e del loro valore, prescrivendo un livello di sicurezza applicabile, misurabile e verificabile.

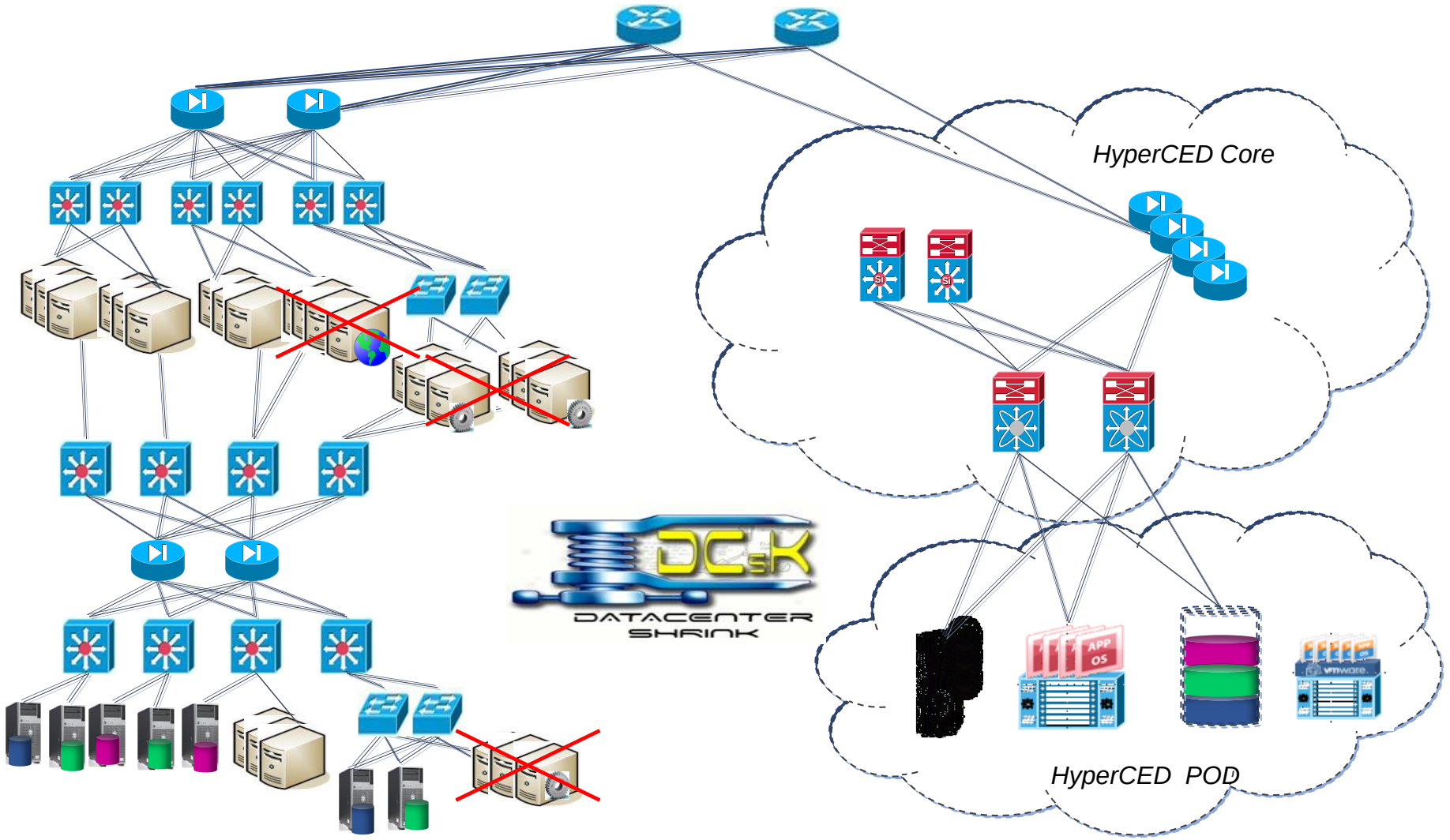
Procedura di Sicurezza

Indica lo scopo di un'attività, ciò che deve essere fatto e chi lo deve fare, quando e/o come deve essere fatto, quali strumenti e attrezzature devono essere utilizzati e come dovranno essere controllati e registrati.

Come

Finalità: documentare con accuratezza le istruzioni e le prassi operative vigenti all'interno dell'Ente.

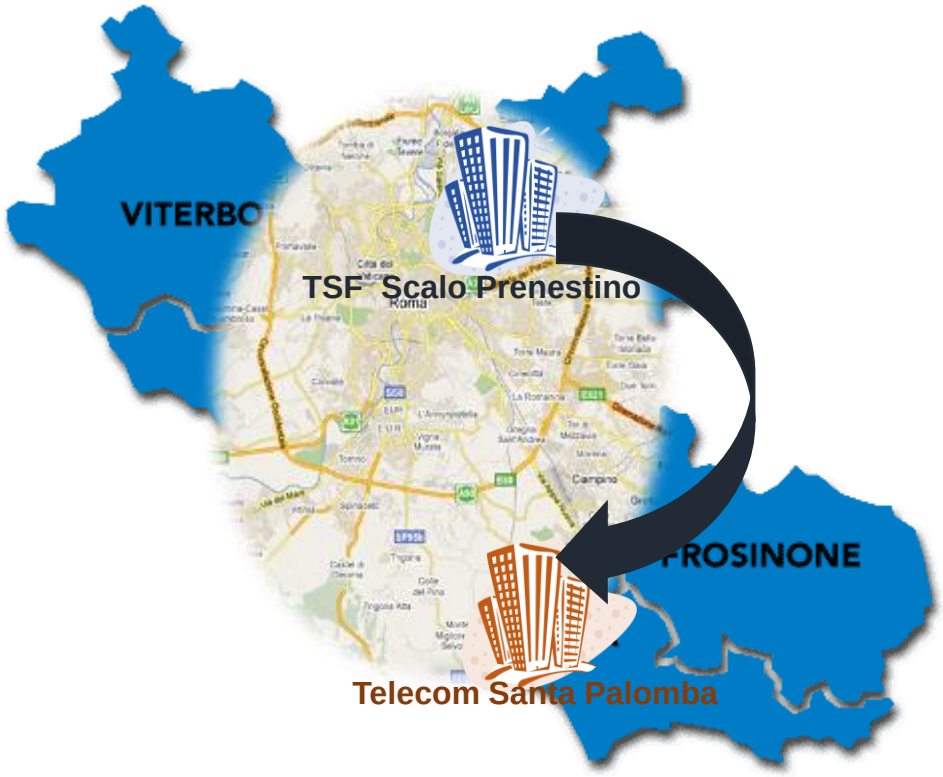
ICT Transformation: dal CED tradizionale al Private Cloud



DCsK – ICT Transformation

Managed Hosts	Managed Applications	Managed storage
4248	>500	4 PB

Affidabilità – Disaster Recovery



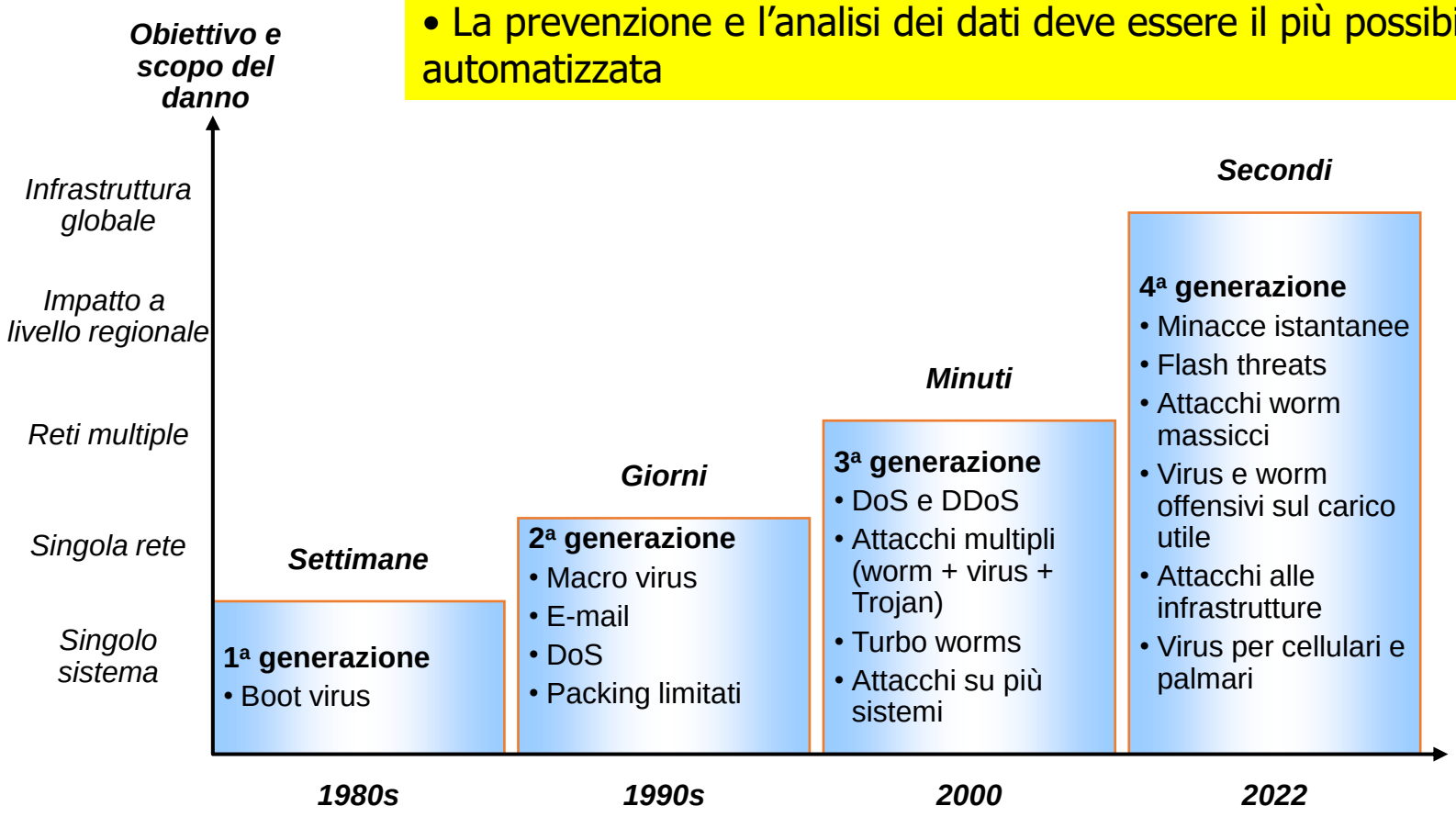
- Sito secondario **sempre pronto ad erogare servizi**, senza necessità di riconfigurare apparati di rete e sicurezza
- Nel sito di DR sono sempre disponibili i dati allineati in modalità semi-sincrona (finestre di replica di 5 minuti) e potenza elaborativa in stand-by a caldo
- Unità organizzativa di **Disaster Recovery Management** della Service Control Room
- *Corporate Private Cloud* dedicato ai servizi FS, che usufruisce anche dell'**infrastruttura Nuvola Italiana** di Telecom

Dal costo della sicurezza ICT al costo della “non sicurezza”

- Il costo della sicurezza deve essere paragonato al costo della “non sicurezza”, ossia ai danni diretti ed indiretti che possono essere causati → Analisi del Rischio
- Nel costo complessivo, la quota maggiore è per gli aspetti organizzativi (chi fa che cosa, chi controlla il controllore, formazione, sensibilizzazione, addestramento, …) più che per gli aspetti tecnici
- I costi assicurativi sul rischio residuo diminuiscono al crescere del livello di sicurezza in atto
- Forte e crescente l’impatto dell’adeguamento per la conformità alle diverse normative e leggi che impattano sulla sicurezza e sulla gestioni dei sistemi informatici
- Se non si ha e non si implementa una idonea policy per la sicurezza ICT:
  - si incorre in sanzioni amministrative e/o penali: Legge 196 sulla privacy, Legge 231 sulla Governance, IAS, …
  - non si possono produrre e vendere prodotti e servizi, oltre a non poter essere quotati in determinate Borse: IAS, SOX, HPPI, ...

Passato, presente e futuro di minacce ICT

- Le velocità di attacco attuali non sono più gestibili a livello "umano"
- La prevenzione e l'analisi dei dati deve essere il più possibile automatizzata



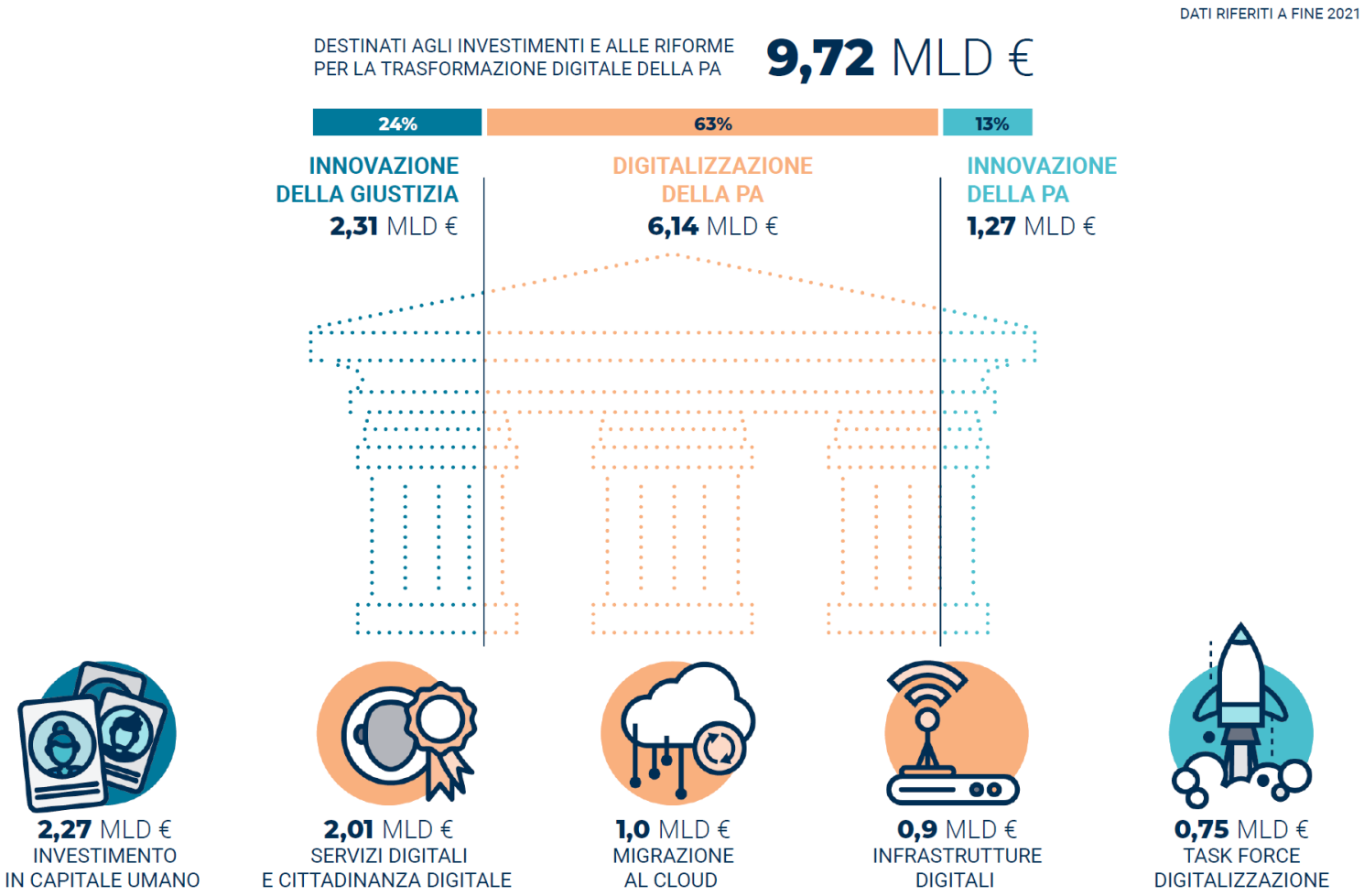
Fonte: "La sicurezza digitale" di M. Bozzetti

La necessità di rendere più sicure le credenziali di accesso

Survey Results Rank	Survey Average Score	Issue Name
1	7.729927	Insufficient ID, Credential, Access and Key Mgt, Privileged Accounts
2	7.592701	Insecure Interfaces and APIs
3	7.424818	Misconfiguration and Inadequate Change Control
4	7.408759	Lack of Cloud Security Architecture and Strategy
5	7.275912	Insecure Software Development
6	7.214493	Unsecure Third Party Resources
7	7.143066	System Vulnerabilities
8	7.114659	Accidental Cloud Data Disclosure/ Disclosure
9	7.097810	Misconfiguration & Exploitation of Serverless & Container Workloads
10	7.088534	Organized Crime/ Hackers/ APT
11	7.085631	Cloud Storage Data Exfiltration

Fonte: rapporto CSA 2022

Le risorse economiche del PNRR per la PA



Fonte: Osservatorio Agenda Digitale-Politecnico di Milano 2022

Considerazioni finali

- Il fattore umano è sempre l'elemento più debole, quindi è necessario investire sulla formazione culturale e ICT degli addetti della PA
- Occorre investire, ad esempio con le risorse del PNRR, sulla riorganizzazione dei Data Center della PA (attualmente 11.000, il 95% dei quali con carenze nei requisiti minimi in materia di sicurezza) per realizzare una serie di Poli Strategici Nazionali dove concentrare le applicazioni in ambiente cloud
- E' necessario intensificare la collaborazione con l'Autority per la Cybersecurity nazionale, che può fornire supporto alle PA circa linee guida e software open source per verificare i requisiti minimi di sicurezza

Grazie per l’attenzione

musumeci@cdti.org alessandro.musumeci@unint.eu