2014 Italian Cyber Security Report

Consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione Italiana

Research Center of Cyber Intelligence and Information Security
"Sapienza" Università di Roma

Dicembre 2014

A cura di: Roberto Baldoni, Luca Montanari

Autori in ordine alfabetico:

Leonardo Aniello
Stefano Armenia
Roberto Baldoni
Fabrizio D'Amore
Annachiara Di Paolo
Luisa Franchina
Luca Montanari
Ida Claudia Panetta
Leonardo Querzoni
Giovanni Rellini Lerz
Nino Vincenzo Verde

Con il supporto di:

Paolo Agati
Gabriella Caramagno
Mario Cilla
Guglielmo Galasso
Leandro Gelasi
Alessandro Masolin
Diego Mezzina

L'Italian Cyber Security Report 2014 è realizzato da:

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

con il supporto del Dipartimento delle Informazioni per la Sicurezza della Presidenza del Consiglio dei Ministri

e con il generoso contributo di:

Microsoft
hp
Finmeccanica
FireEye

Il Cyber Intelligence and Information Security Center è parte del:

cini Cyber Security National Lab

Stampato in Italia

Dicembre 2014

Via Ariosto 25 00185, Roma, Italy

Prefazione

Da qui a dieci anni la correlazione tra prosperità economica di una nazione ed il fatto che questa Nazione possegga capacità cyber avanzate sarà molto stretta. Quindi per rimanere nel gruppo delle Nazioni sviluppate si dovranno migliorare queste capacità nella società, nel tessuto industriale, nella pubblica amministrazione di un Paese. Per questo ogni Nazione si sta attrezzando attraverso l'implementazione di un piano strategico Nazionale multidimensionale che coinvolge pubblico, privato e ricerca. Alzare le difese del cyber space di un Paese significa, tra l'altro, rendere più appetibile investimenti da parte di operatori internazionali che potrebbero vedere come pericoloso costruire realtà imprenditoriali, come ad esempio nuove aziende sul territorio, in un paese dove non c'è organizzazione e capacità difensiva cyber. Queste aziende potrebbero infatti rivelarsi un punto debole del sistema informativo dell'organizzazione investitrice. Nel terzo millennio, rendere sicuro il cyber space di un Paese significa gettare le basi per l'indipendenza e la prosperità economica di una Nazione.

Ad un anno dalla pubblicazione del Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico, il Cyber Security Report 2014 si concentra sulle problematiche legate alla consapevolezza della minaccia e alla capacità difensiva della pubblica amministrazione italiana. Un questionario è stato inviato a circa 300 pubbliche amministrazioni a livello nazionale, regionale e locale. Lo studio ha consentito di individuare i principali problemi e quindi i punti cruciali, su cui agire per ottenere un miglioramento rapido e sostanziale della nostra protezione. Ha anche purtroppo evidenziato come ci siano lacune importanti e radicate sia in termini di cultura della sicurezza che di organizzazione. Ne consegue una situazione in cui solo pochissime amministrazioni si possono ritenere consapevoli dei rischio cibernetico mentre gli errori e la quantità di best practices ignorate sottolineano la profonda arretratezza culturale, in particolare, rispetto al valore strategico (ed economico) delle informazioni che potrebbero essere trafugate dai sistemi informativi di una pubblica amministrazione.

Porre in sicurezza il cyber space nazionale rappresenta quindi un dovere rispetto alle giovani generazioni di fronte al rischio che ogni minuto si corre in un mondo digitale dove le minacce sono continue ed in costante aumento. Ma questo pericolo può rappresentare un'imperdibile e gigante opportunità economica per il Paese in particolare per la crescita della nostra capacità industriale. Infatti nel dominio cyber l'Italia vanta competenze che il mondo ci invidia (e sempre più spesso purtroppo ci compra), quindi definire una appropriata strategia industriale a livello governativo per sorreggere l'ecosistema cyber italiano può rappresentare un doppio vantaggio economico, di sicurezza ed indipendenza Nazionale. Ad oggi pero' l'Italia investe zero in questo settore, dove altre nazioni, per dimensioni simili alla nostra, hanno budget quadriennali ormai nell'ordine del bilione di euro. D'altra parte le buone pratiche di altre Nazioni mostrano che per implementare strategie nazionali ed industriali adeguate, ci vogliono attori nazionali sparsi sul territorio. Per questo la comunità accademica italiana, ha iniziato a fare la sua parte creando nel corso del 2014 il Laboratorio Nazionale di Cyber Security dove professori e ricercatori di 33 Università Italiane offrono la loro collaborazione per rendere la nostra vita digitale più sicura. Noi speriamo che questa opportunità che abbiamo creato come accademici venga colta e supportata dalle autorità governative.

Lasciatemi infine ringraziare tutti gli autori di questo rapporto, AgID e la Presidenza del Consiglio e i Ministri per la collaborazione alla realizzazione di questo cyber security report. Un grazie particolare va alle tre amministrazioni, segnatamente INPS, Corte dei Conti e Regione Friuli Venezia Giulia, che si sono prestate ad essere casi di studio e a fornire dettagli sulla loro politica di gestione della sicurezza. Grazie anche a tutte le amministrazioni che hanno risposto al questionario. L'aiuto di Claudio Ciccotelli, Federico Lombardi, Antonella Del Pozzo e Daniele Ucci è stato strumentale per il miglioramento del contenuto del testo. Infine è importante rimarcare che la realizzazione del rapporto è stata possibile grazie al generoso contributo di MICROSOFT, HP, FireEye e Finmeccanica.

Questo lavoro rientra nelle attività di ricerca finanziate dal progetto Italiano MIUR TENACE e dai progetti EU Panoptesec, Cockpit-CI e T-NOVA. Tutti nel contesto cyber security.

Roberto Baldoni
Cyber Intelligence and Information Security
Università degli Studi di Roma La Sapienza

Roma, 22 Dicembre 2014

Indice

Indice raccomandazioni

CAPITOLO

1 Introduzione

Il governo italiano ha avviato, sin dagli anni 90, un importante programma volto ad introdurre nella pubblica amministrazione (PA) strumenti informatici ad ogni livello. Questo programma vuole introdurre l'informatica come elemento di base per l'esecuzione di ogni processo dell'amministrazione con il triplice obiettivo di i) favorire lo snellimento delle procedure, ridurne i tempi di esecuzione e, di conseguenza, migliorare la qualità stessa dei servizi e come questa è percepita dai cittadini, ii) rendere più economico lo svolgimento degli stessi servizi al fine di ridurre l'impatto che la macchina amministrativa ha sul bilancio dello Stato e, infine, iii) raggiungere più facilmente i cittadini stessi favorendo l'interazione anche attraverso i mezzi di comunicazione più moderni che la cittadinanza è in grado di abbracciare con una velocità ben maggiore di quanto l'amministrazione stessa riesca a fare.

Lo sforzo di trasformare processi basati sull'uso di documenti cartacei e interazioni dirette tra il personale in processi altamente informatizzati con una completa dematerializzazione dei documenti richiede tempo. I risultati, seppur apprezzabili, sono ancora oggi estremamente eterogenei nella PA. La fatturazione elettronica è un esempio di buona pratica a livello nazionale, mentre a livello di pubblica amministrazione locale, la penetrazione dell'informatica (e dell'informatizzazione dei processi) è avvenuta in modo eterogeneo e con risultati in larga parte dipendenti dalla lungimiranza dei dirigenti locali o dalla intraprendenza di singoli con un background informatico avanzato.

Questo progressivo ammodernamento, che noi auspichiamo abbia un cambio di passo in velocità e scala, porterà ad una sempre maggiore interazione attraverso i canali informatici tra i cittadini e le loro istituzioni. Già oggi questa visione è in parte realtà. Processi come la fatturazione elettronica, il controllo dello stato contributivo di un cittadino, il processo civile telematico sono esempi rilevanti di questo ammodernamento. Questa evoluzione porta con se innumerevoli vantaggi, ma sicuramente renderà i cittadini ancora più dipendenti dal mezzo informatico per poter vivere la loro vita quotidiana facendo diventare l'infrastruttura informatica della PA sempre più una infrastruttura critica per il Paese.

Le grandi opportunità offerte da questa evoluzione si accompagnano quindi ai rischi di una sempre maggiore esposizione ad attacchi di tipo cibernetico. Questo tipo di attività illegali, già oggi colpiscono il cittadino nella sua normale attività *on-line*, ma ancora di più in futuro saranno in grado di impattarne negativamente la quotidianità andando a colpire il collegamento preferenziale e di fiducia tra il cittadino stesso e la PA. In particolare, la PA paga, da questo punto di vista, la propria identità e si configura come obiettivo di preferenza per tutti gli attacchi di tipo dimostrativi (hacktivismo). Tali attacchi hanno come fine principale proprio quello di ridurre la capacità di uno Stato di interagire in modo diretto con la sua popolazione, impedendo questa interazione o sovvertendola o, ancora, intercettandola e modificandone i contenuti in modo da veicolare attraverso una canale considerato "affidabile" contenuti propagandistici. Oltre all'hacktivismo però la PA si configura anche come obiettivo prediletto di attività di ricognizione e spionaggio svolte direttamente o indirettamente da agenzie di paesi esteri interessati ad entrare in possesso di informazioni confidenziali che la nostra PA dovrebbe proteggere. È importante infatti considerare che, così come un paese protegge i propri confini geografici da intrusioni non desiderate di elementi

estranei, allo stesso modo dovrebbero essere definiti e protetti dei confini cibernetici sui quali sia possibile esercitare un controllo diretto e capillare. Questi confini dovrebbero includere e proteggere tutte le informazioni e i servizi importanti per il paese, e dovrebbero quindi comprendere tutti i sistemi informatici della PA.

La recente pubblicazione del *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* ha chiarito questo aspetto, ma la sua implementazione richiederà notevoli sforzi nei prossimi anni. Nel frattempo le minacce non interrompono le loro attività e, ad oggi, lo stato della protezione della PA da questo tipo di attacchi è molto frammentato. Tale protezione, infatti, è rimasta demandata, soprattutto per la PA di più piccola dimensione, alla buona volontà degli amministratori locali che per propria capacità, o perché ben consigliati, si sono resi conto in tempo dei pericoli a cui i loro cittadini erano esposti da una non accurata protezione dei loro servizi e dati. Solo le PA di maggiore dimensione e importanza, avendo a disposizione mezzi e budget adeguati sono state in grado di affrontare il problema in modo sistematico, ma anche in questo caso gli approcci sono stati disuniti portando, nella migliore delle ipotesi, ad un dispendio di risorse non proporzionato o quantomeno evitabile.

La PA italiana, vivendo in questa situazione di estrema frammentazione, senza un punto di riferimento istituzionale, se non le tradizionali autorità di polizia, ha vissuto negli ultimi anni una situazione in cui la cultura della sicurezza è dipesa non tanto dallo Stato, quanto dalla capacità dei singoli amministratori. E' ovvio quindi che, non essendoci leggi o regolamenti che operino a questo livello, solo le amministrazioni consapevoli ed economicamente più forti, sono state in grado di sviluppare un'adeguata consapevolezza del problema. Tutte le amministrazioni di più piccole dimensioni come Comuni, province, ASL, Aziende Ospedaliere vivono tutt'oggi una situazione critica. Eppure, spesso sono proprio queste amministrazione che gestiscono direttamente i dati dei cittadini a cui forniscono i servizi fondamentali.

Il tutto si pone in anni in cui il crimine informatico è cambiato radicalmente, essendo cambiato radicalmente il tipo di attaccante. Si è passati, in meno di 10 anni, da un grande numero di singoli attaccanti, disorganizzati, costituiti da gruppi di fanatici in cerca di qualche ora di facile gloria, a grandi gruppi organizzati di hacker di professione, talvolta finanziati dai governi, talvolta finanziati con l'emergente meccanismo del crowdfunding, altre volte foraggiati dalla malavita organizzata. Anonymous è un esempio più valido, operante con grandi numeri sul territorio italiano. L'aumento di disponibilità di hardware capace e di *malware* più complessi del passato che, installando apparentemente inermi demoni nei singoli dispositivi (siano questi pc domestici, smartphone, ma anche server, NAS ecc) possono agire contemporaneamente a livello addirittura mondiale, fa si che anche piccoli gruppi di attaccanti possano condurre attacchi di grande mole. Se il target di questo tipo di attacco prendesse la forma di qualche amministrazione centrale sarebbe un problema.

È infatti idea consolidata nella comunità di cyber security che gli effetti di un attacco informatico, condotto accuratamente e verso target specifici, avrebbe gli stessi effetti in termini economici di un attacco militare. Non è possibile stimare con certezza i danni di attacchi di grandi dimensioni, così come non è possibile stimare i danni di attacchi bellici. Si pensi, ad esempio, alle conseguenze di una settimana di blocco totale della borsa italiana, oppure una settimana in cui i comuni di grandi città come Roma o Milano rimangano senza servizi anagrafici. Oppure una grande ASL, servente migliaia di persone, senza la possibilità di fornire i propri servizi. I ritardi si accumulerebbero, le persone sarebbero costrette ad usufruire delle ferie per tornare di nuovo a chiedere i servizi con tutte le conseguenze che questo comporta, gli affollamenti successivi avrebbero ripercussioni sul traffico e così via. Un altro esempio è l'INPS: si pensi agli effetti di un attacco perpetrato per due settimane a tale amministrazione, con milioni di persone inabili a ricevere la propria previdenza sociale per tale tempo. Sarebbe il caos.

Ad oggi non sono stati ancora documentati casi di attacchi di questa dimensione in Italia, tuttavia sarebbe ingenuo pensare che la PA non sia un obiettivo di spionaggio o di attacco da parte di azioni sponsorizzate da altri stati. Anzi, gli ultimi eventi legati al malware Regin[1] portano a pensare che le pubbliche amministrazioni siano già fonte di attenzione per attività di spionaggio. Tutto ciò ci porta a pensare che in termini di sicurezza si dovrebbe già ragionare considerando che il nemico è al nostro interno. Non di meno altri rapporti, segnatamente il CLUSIT 2014[2], riportano un lungo elenco di attacchi svoltisi tra il 2013 e l'inizio del 2014 contro le pubbliche amministrazioni.

[1] Regin è un malware sofisticato scoperto da Kaspersky Lab nel novembre del 2014 in grado di trafugare e collezionare dati di diverso tipo: file, voce, dati etc. Si sospetta sia stato sviluppato da Regno Unito e Stati Uniti d'America per controllare i palazzi della Commissione Europea attraverso Belgacom, telco provider di molte strutture della Commissione.

[2] `https://www.clusit.it/`

In questo contesto, il Centro di Ricerca in Cyber Intelligence e Information Security dell'Università degli Studi di Roma "La Sapienza", in collaborazione con AgID e la Presidenza del Consiglio dei Ministri, ha svolto una ricerca volta a capire più in profondità la consapevolezza della minaccia cibernetica e l'attuale capacità difensiva della PA Italiana. A questo scopo, tra Giugno e Agosto 2014 sono stati distribuiti *441* questionari presso altrettante amministrazioni a diversi livelli, incluse PA centrali, regioni, province, comuni capoluoghi di provincia con più di 10000 cittadini, Aziende Sanitarie Locali, Aziende Ospedaliere. Il questionario, strutturato in 61 domande sugli argomenti legati alla consapevolezza, difesa e organizzazione della PA, è stato distribuito, con l'aiuto fondamentale di AgID ai più alti livelli dirigenziali. Le risposte raccolte sono quindi state analizzate per provare a ricreare un quadro realistico a livello nazionale.

Da questa analisi sono emerse luci e ombre di un quadro che non abbiamo esitato, già nelle precedenti righe, a definire quantomai eterogeneo. Risulta sicuramente evidente la maggiore preparazione di alcune PA centrali rispetto alle amministrazioni locali. In queste ultime la situazione è estremamente frammentata con poche eccellenze e molti casi critici. *È fondamentale comunque sottolineare che i risultati riportati in questo documento non devono essere letti come una garanzia che le PA con alto punteggio siano al sicuro*; tutt'altro: tali PA essendo esposte a rischi maggiori hanno intrapreso da più tempo quel percorso che, inevitabilmente, anche le amministrazioni più piccole dovranno intraprendere. Prima questo passo sarà fatto, minori saranno i rischi per il cittadino e per il Paese. Il Capitolo 3 mostra i risultati dello studio utilizzando tre *key performance indicators (KPI)*, segnatamente *awareness*, *organization* e *defense*. Il primo tende a valutare la consapevolezza dell'amministrazione rispetto alla problematica cyber, la seconda come l'organizzazione si è predisposta in termini di policy e organizzativi, mentre la terza valuta le difese tecnologiche adottate rispetto alla minaccia cyber. Il tutto considerando le seguenti categorie: comuni, regioni, pubblica amministrazione centrale, aziende sanitarie locali e aziende ospedaliere. Vengono presentati, oltre ai valori assoluti per categoria, i risultati in base alla dimensione dell'amministrazione, alla posizione geografica e al numero di attacchi subiti. Infine viene fatta una analisi su base statistica delle risposte che porta ad evidenziare quali sono le caratteristiche che uniscono gruppi di amministrazioni che hanno ottenuto punteggi simili nella valutazione secondo i tre KPI. Da questi risultati vengono tratte delle conclusioni, messe in termini di lista di raccomandazioni. Oltre alle raccomandazioni tecniche verso le pubbliche amministrazioni per migliorare i loro livelli di sicurezza, si evincono altri concetti particolarmente rilevanti tra cui:

- il processo di razionalizzazione del patrimonio informativo della pubblica amministrazione in termini di dati, processi e infrastrutture e la loro messa in sicurezza sono un binomio inscindibile. Solo riducendo la superficie di attacco si può pensare di gestire in modo efficace la sicurezza di una infrastruttura nazionale. Questo oggi si può fare attraverso appropriati data center, per esempio dislocati su base regionale, che possono portare anche ingenti risparmi all'erario pubblico;
- il quadro di competenze e responsabilità che esce dal piano strategico di sicurezza cibernetica nazionale nella prevenzione, gestione e risposta ad attacchi cyber è distribuito e frastagliato. E' quindi consigliabile andare verso una centralizzazione di tali competenze e responsabilità in modo da rendere più veloce e coordinata la catena di comando.

Infine, la presente edizione del Italian Cyber Security Report, include anche la descrizione dettagliata di alcuni casi di studio: Corte dei Conti, INPS, e Regione Friuli Venezia Giulia. Ognuno di queste casi di studio mostra alcune best practices che possono essere di interesse per altre pubbliche amministrazioni. I processi di integrazione di Corte dei Conti, l'esperienza del CERT della Regione Friuli Venezia Giulia e l'organizzazione della sicurezza in INPS sono esempi di tali best practices.

Il documento è strutturato come segue: nel Capitolo 2 viene presentata la metodologia della ricerca e nel Capitolo 3 i risultati. Il Capitolo 4 include i tre casi di studio, segnatamente Corte dei Conti, INPS e Regione Friuli Venezia Giulia. Il Capitolo 5 conclude il rapporto presentando e motivando una serie di raccomandazioni. In Appendice, si riportano grafici rappresentanti le risposte alle singole domande del questionario.

CAPITOLO

2 Metodologia di valutazione dei questionari

Al fine di fornire un valore oggettivo che descriva in maniera sintetica il livello di preparazione in termini di cyber security delle pubbliche amministrazioni sono stati individuati tre Key Performance Indicators (KPI). Le risposte alle domande poste nel questionario influenzano, tramite un meccanismo basato su pesi, il punteggio da assegnare ad ognuno di questi KPI. Di seguito è riportata una descrizione dei KPI, una descrizione del questionario, l'associazione tra domande del questionario e KPI influenzati, come pure alcuni dettagli sul calcolo dei punteggi.

2.1 Key Performance Indicator

Un Key Performance Indicator è un indice che viene utilizzato per monitorare l'andamento di un processo aziendale. Nel nostro caso, sono stati individuati tre KPI che misurano tre diversi aspetti della preparazione delle amministrazioni ad affrontare eventi di cyber security: KPI *Organization*, KPI *Defense* e KPI *Awareness*.

Il KPI *Organization* cattura tutti quegli aspetti organizzativi della pubblica amministrazione che hanno una ricaduta diretta sulla capacità di risposta ad eventuali attacchi informatici. Come noto, avere un'organizzazione attenta alle tematiche di sicurezza ha una serie di conseguenze positive sulle capacità di risposta proattive e/o reattive.

Il KPI *Defense* cattura, invece, tutti gli aspetti tecnici legati alla capacità delle organizzazioni di difendersi da attacchi informatici. All'interno di questo KPI viene catturata quindi la presenza o l'assenza di opportune misure tecniche di sicurezza quali per esempio firewall, intrusion detection systems, antivirus e protocolli di comunicazione sicura per i servizi offerti, come pure l'utilizzo di tecnologie obsolete ed ormai notoriamente vulnerabili.

Infine, il KPI *Awareness* cattura il livello di consapevolezza dell'organizzazione rispetto a tematiche di cyber security. Si noti che, in generale, la consapevolezza è uno degli aspetti più importanti per garantire ad un'organizzazione la possibilità di riuscire a migliorare la propria posizione. Ciò è ancor più vero quando si parla di cyber security. Infatti, non essere consapevoli delle minacce a cui si è sottoposti porta spesso a situazioni paradossali in cui si pensa di essere al sicuro e di non subire attacchi, non accorgendosi di essere *perennemente* sotto attacco.

2.2 Il questionario e le domande

Il questionario sottomesso alle PA consta di 61 domande strutturate come segue:

- le prime 15 domande individuano il ruolo del rispondente all'interno della pubblica amministrazione, il tipo di PA, la dimensione della stessa (in termini di numero di sedi, numero di utenti serviti, numero di dipendenti, numero di Centri di Elaborazione) e il tipo di dati trattati, l'eventuale livello di criticità dei servizi offerti;

- le domande dalla 16 alla 28 sono relative alle tecniche utilizzate dalla PA per la protezione dei dati, alle tecnologie utilizzate per l'autenticazione e per l'accesso remoto, alle tecnologie web;
- le domande dalla 29 alla 42 sono relative agli attacchi cibernetici e alla loro prevenzione, alle misure di protezione dei dati, al training degli impiegati;
- le domande dalla 43 alla 47 sono dedicate ai software e al loro aggiornamento;
- le domande dalla 48 alla 61 sono dedicate all'organizzazione e alla politica di sicurezza.

Tutte le domande sono riportate in appendice, ognuna con i relativi risultati divisi per categoria.

2.3 Associazione Domande-KPI

In Tabella 2.1 è riportata l'associazione tra domande e i KPI. Per associazione si intende che la domanda influenza il calcolo del punteggio per un dato KPI. Si noti che la dimensione della pubblica amministrazione, desunta da alcune domande (in particolare dalle domande n. 4, 5 e 14, evidenziate nella colonna *Dim.* in tabella) ed intesa come numero di dipendenti, numero di sedi, numero di utenti registrati, è presa in considerazione nella valutazione dei KPI *Organization* e *Defense*. Il dimensionamento è importante per catturare alcuni aspetti critici delle infrastrutture: riteniamo infatti che in caso di pratiche scorrette è giusto penalizzare meno amministrazioni di piccole dimensioni rispetto alle più grandi. Allo stesso modo, si è più esigenti verso quelle amministrazioni che sono chiamate a gestire una mole di dati e asset sicuramente maggiore. Al fine di considerare l'aspetto dimensionale all'interno dei KPI individuati, sono stati definiti due fattori moltiplicativi fm e fp (maggiori dettagli di seguito) che influenzano rispettivamente i KPI *Defense* e *Organization*.

Tabella 2.1: Associazione tra domande e KPI.

Domande		KPI		Dim
	Organization	Defense	Awareness	
4,5,14	✓	✓		✓
16,20,25,30,31,34-37,43,45		✓		
12,21,23,26,28,29,32,33,44		✓	✓	
22,27,38,40	✓	✓		
15,39,42,46,47	✓	✓	✓	
48,50,52,56-60	✓		✓	
13,49,51,53-55	✓			

2.4 Calcolo dei punteggi

Il processo di calcolo dei punteggi inizia con la raccolta delle risposte alle singole domande da ogni amministrazione e termina con la produzione di tre valori: $< O_i, D_i, A_i >$ compresi nell'intervallo $[0,100]$. I valori rappresentano, rispettivamente, il punteggio ottenuto dall'amministrazione i per i KPI *Organization, Defense, Awareness*. In accordo con le associazioni presentate in Tabella 2.1 e con la valutazione della risposta data, ogni domanda del questionario può contribuire in maniera positiva o negativa alla costruzione di un punteggio associato ad ogni KPI. I contributi delle singole domande vengono sommati e normalizzati per consentire un confronto più immediato tra i vari KPI. Di seguito viene riportata più in dettaglio la procedura di calcolo dei KPI.

Si consideri il KPI *Defense* ed una generica amministrazione a. Sia:

- S_P la somma dei soli punteggi positivi ottenuti dell'amministrazione a per le domande che influenzano il KPI in oggetto;
- S_N la somma dei soli punteggi negativi ottenuti dell'amministrazione a per le domande che influenzano il KPI in oggetto;

Sia inoltre:

- fm un fattore moltiplicativo calcolato a partire dalle risposte date dall'amministrazione a utilizzando un sottoinsieme di domande.

La somma dei pesi negativi S_N sarà moltiplicata per tale fattore ottenendo la somma dei pesi negativi penalizzata:

$$S_{Np} = S_N \times fm.$$

Una volta calcolata S_{Np} questa si somma a S_P ottenendo così la somma totale dei pesi per il KPI *Defense*:

$$S_D = S_{Np} + S_P,$$

si noti che $S_N \leq 0$. Siano

- Max_D e min_D rispettivamente il massimo ed il minimo ottenibile nella somma dei pesi di tutte le domande che influenzano il KPI *Defense*.

In particolare Max_D è la somma di tutti i pesi positivi ottenibili e min_D la somma dei pesi negativi. Max_D e min_D sono calcolati a priori ed quindi indipendenti dalla risposta della singola amministrazione. Il voto D_a relativo alla *Defense* dell'amministrazione a è calcolato come segue:

$$D_a = \left(\frac{(S_D - min_D)}{(Max_D - min_D)} \right) \times 100,$$

ovvero utilizzando la nota formula della *normalizzazione min-max* a S_D. Il discorso è facilmente generalizzabile agli altri KPI seguendo la medesima procedura. Si noti che i valori massimi e minimi sono propri del singolo KPI e che il fattore fm esiste solo per il KPI *Defense*. Per quanto riguarda il KPI *Organization* un fattore moltiplicativo differente, fp, viene applicato alla somma dei pesi positivi. Si ha che la somma totale dei pesi per il KPI *Organization* è:

$$S_O = S_N + S_{Pp},$$

dove $S_{Pp} = S_P \times fp$. Tale fattore moltiplicativo serve a catturare la maggiore complessità che si ha nell'organizzazione di amministrazioni più grandi, quindi premia maggiormente amministrazioni più grandi nel caso siano utilizzate pratiche corrette. Per gli altri KPI, le amministrazioni grandi sono penalizzate di più in caso di pratiche scorrette.

2.5 Punteggi, soglia di idoneità e interpretazione dei grafici

Per interpretare più facilmente i risultati ottenuti dalle elaborazioni dei questionari è stata definita una soglia oltre la quale un'amministrazione può essere ritenuta sufficientemente attenta ai problemi derivanti da minacce informatiche. Tale soglia è da intendersi come una soglia di idoneità, nel senso che le amministrazioni che raggiungono un punteggio oltre tale soglia risultano aver implementato accorgimenti di base, sia tecnologici che organizzativi, adeguati allo stato dell'arte. Aver ottenuto un punteggio oltre tale soglia non si traduce con la certezza di avere un'organizzazione esente da attacchi che possano avere successo. Piuttosto, l'ottenimento di un punteggio oltre la soglia, si traduce nell'essere in grado di rilevare, ad esempio, data leak o altri tipi di attacco con probabilità molto alta, ed avere le capacità di risolvere tali problemi nel minor tempo possibile.

La soglia di idoneità è stata calcolata considerando le singole domande del questionario, l'influenza che le possibili diverse risposte hanno sui singoli KPI, e la presenza o assenza all'interno dell'organizzazione delle misure minime che un'organizzazione dovrebbe prevedere per ritenersi ragionevolmente al sicuro da minacce generiche. E' bene sottolineare ancora una volta che un'amministrazione che si posiziona al di sopra di tale soglia non può ritenersi al sicuro, ma se non altro può essere certa di essere sulla buona strada. E' anche bene sottolineare ulteriormente che un'amministrazione che si posiziona al di sopra di tale soglia non può ritenersi al sicuro da minacce confezionate specificatamente contro l'organizzazione stessa (per esempio attacchi di tipo APT). Al contrario, un'organizzazione che si posiziona al di sotto della soglia di idoneità deve ritenersi ad alto rischio.

Nei grafici che verranno riportati nei capitoli successivi, le aree evidenziate in verde indicano le aree al di sopra della soglia individuata. Le aree con sfondo giallo rappresentano invece aree limite, con margini di miglioramento molto alti, ma da considerarsi a rischio medio/alto. Le aree con sfondo bianco sono invece da considerarsi come zone di grave insufficienza.

CAPITOLO

3 Analisi dei dati raccolti

In questo capitolo saranno presentati, in forma aggregata e in modo da assicurare l'anonimato dei rispondenti, i risultati ottenuti dalle pubbliche amministrazioni che hanno compilato il questionario.

3.1 Campione analizzato e modalità di raccolta dei dati

Il campione oggetto dell'indagine è stato individuato in collaborazione con l'Agenzia per l'Italia Digitale (AgID) ed è composto da 5 categorie di pubbliche amministrazioni:

- Pubbliche Amministrazioni Centrali (PAC): amministrazioni operanti a livello nazionale, compresi ministeri[1];
- Comuni: solo i 117 capoluoghi di provincia;
- Regioni ed Enti Regionali (di seguito "Regioni");
- Aziende Ospedaliere (AO);
- Aziende Sanitarie Locali (ASL).

AgID ha svolto principalmente il ruolo di tramite delle pubbliche amministrazioni per l'iniziativa, e ha contribuito insieme al CIS alla predisposizione del questionario per la raccolta dei dati necessari al rapporto. Di seguito si riportano le modalità con cui il campione oggetto dell'indagine è stato contattato e invitato a rispondere al questionario. Nel periodo maggio-giugno 2014, AgID ha inviato Comunicazioni a:

- 42 Pubbliche Amministrazioni Centrali (tra Ministeri ed Enti);
- 117 Comuni (tutti i Comuni capoluogo di provincia);
- 19 Regioni e le Province Autonome di Bolzano e di Trento (per semplicità indicate nel seguito come Regioni), richiedendo a tali enti di diffondere le richiesta di partecipazione al questionario alle strutture sanitarie dei propri territori (ASL e AO) e agli Enti Regionali;

Le Comunicazioni iniziali contenevano il dettaglio della procedura seguita per la raccolta dei dati. In particolare:

[1] Per la definizione formale di "pubbliche amministrazioni" si rimanda al comma 2 dell'articolo 1 ("Finalità e ambito di applicazione") del DLgs. 165/2001, "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche". I dipartimenti interni ai Ministeri sono stati esaminati come PAC distinte.

1. è stato richiesto di indicare un referente per la compilazione (nome, cognome e un indirizzo di posta elettronica), e di restituire tale informazione via posta elettronica ad una casella e-mail dell'Agenzia; nel caso di Ministeri particolarmente complessi, e con funzioni sensibilmente diversificate nelle proprie strutture, le richieste sono state indirizzate ai vari Dipartimenti dei Ministeri;
2. l'Agenzia ha inoltrato i dati dei referenti al CIS;
3. il CIS ha provveduto ad inviare ai referenti un link personalizzato per la compilazione del questionario;
4. il CIS ha monitorato lo stato di avanzamento delle compilazioni;
5. il CIS e AgID hanno dato supporto alla compilazione quando richiesto.

Come primo risultato di questa indagine, si consideri che:

- dei 117 Comuni contattati dall'Agenzia per l'Italia Digitale, 83 hanno fornito un referente per la compilazione del questionario. Di questi 79 hanno riempito il questionario. Quindi circa il 71% dei comuni contattati da AgID;
- tutte le 42 PAC contattate da AgID hanno fornito un referente e riempito il questionario;
- tutte le 19 Regioni italiane (non enti regionali) contattate da AgID hanno fornito un referente e riempito il questionario.

Non è possibile stabilire con certezza il numero di Aziende Ospedaliere e ASL che hanno ricevuto la richiesta di fornire un referente in quanto tale richiesta è stata inoltrata dalle Regioni alle rispettive Aziende Ospedaliere e ASL e non dall'AgID. Tuttavia si possono fare le seguenti considerazioni sulla rappresentatività del campione a livello nazionale:

- delle 140 ASL presenti sul territorio italiano, 43 hanno fornito un referente per la compilazione del questionario, 34 lo hanno riempito. Ciò corrisponde a circa il 25% delle ASL;
- delle 645 aziende ospedaliere pubbliche presenti sul territorio italiano[2], 34 hanno fornito un referente per la compilazione del questionario, 29 lo hanno riempito. Ciò corrisponde a circa il 4,5% delle aziende ospedaliere pubbliche;

Tutti i referenti comunicati al CIS da AgID hanno ricevuto il questionario. La Tabella 3.1 riporta in dettaglio, divisi per categoria, il numero di questionari inviati, il numero di questionari ricevuti e la percentuale di ricezione.

Tabella 3.1: Numero di questionari inviati e ricevuti per categoria

	PAC	Comuni	Regioni	Aziende Ospedaliere	ASL	Tot.
Inviati	42	83	30	34	43	232
Ricevuti	42	79	25	29	34	209
Percentuale Ric.	100 %	95,2 %	83,3 %	85,3 %	74,4 %	90,1%

Le amministrazioni sono distribuite sul territorio nazionale in accordo a quanto mostrato in Figura 3.1. Le PAC sono escluse da questa rappresentazione in quanto sono tutte localizzate nella regione Lazio. Non risultano pervenuti referenti dalla regione Molise.

[2] fonte `www.saluteinternazionale.info`.

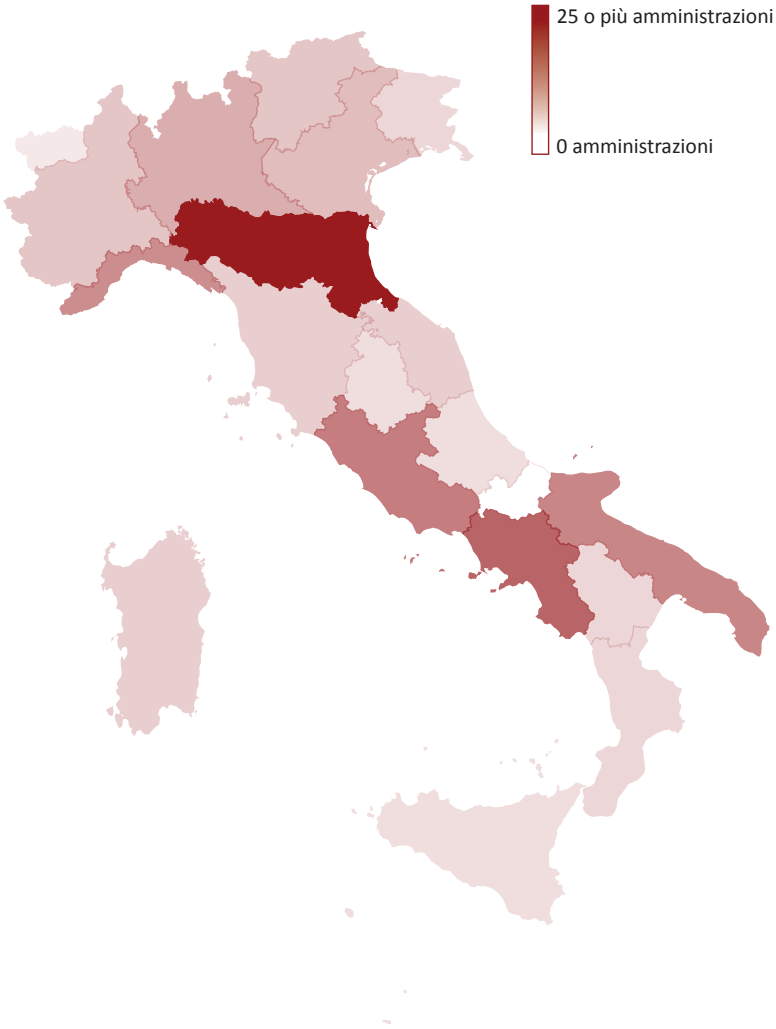


Figura 3.1: Distribuzione delle amministrazioni sul territorio nazionale.

3.2 Confronto tra i valor medi di tutte le categorie

Il primo risultato presentato confronta le cinque diverse categorie esaminate. In Figura 3.2 è presentato il valor medio dei KPI di ogni categoria. Si può notare come il valor medio non sia prossimo alla soglia di idoneità per nessuna categoria. La figura mostra comunque che le PAC e le Regioni si comportano meglio rispetto a Comuni, ASL e aziende ospedaliere, e che queste ultime tre categorie hanno ottenuto risultati molto simili tra di loro. In Figura 3.2, le barre di errore rappresentano la deviazione standard degli insiemi considerati. Si noti come questa raramente superi le 10 unità.

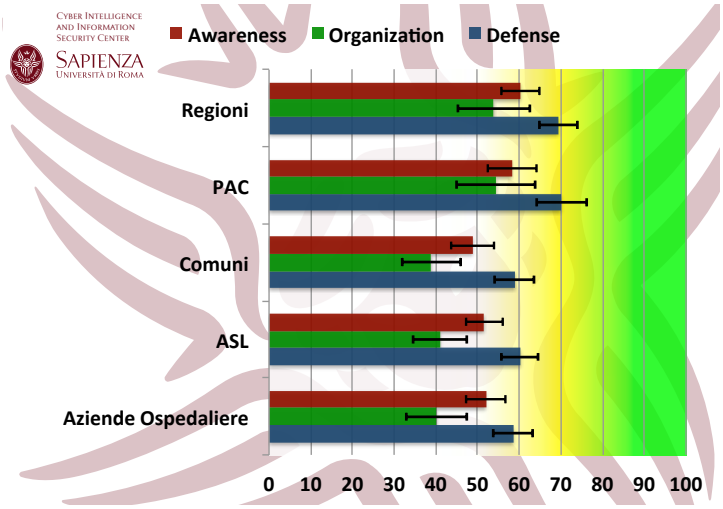


Figura 3.2: Risultati medi per categoria, le barre di errore rappresentano la deviazione standard.

3.3 Confronto tra i valori assoluti di tutte le amministrazioni

Le Figure 3.3, 3.4 e 3.5 mostrano il posizionamento di tutte le amministrazioni analizzate in termini di *Defense*, *Organization* e *Awareness*. In particolare, le figure mostrano la situazione considerando sui due assi tutte le possibili coppie di KPI: rispettivamente *Defense-Organization*, *Defense-Awareness* e *Organization-Awareness* . Ogni punto in figura rappresenta un'amministrazione, e il colore ne indica la rispettiva categoria. Si può apprezzare un alto livello di correlazione tra i vari KPI (l'insieme dei punti è raggruppato nel piano) la quale consente di supporre che alti livelli di *Organization* implichino alti livelli di *Awareness* e *Defense*. Si noti come pochissime amministrazioni

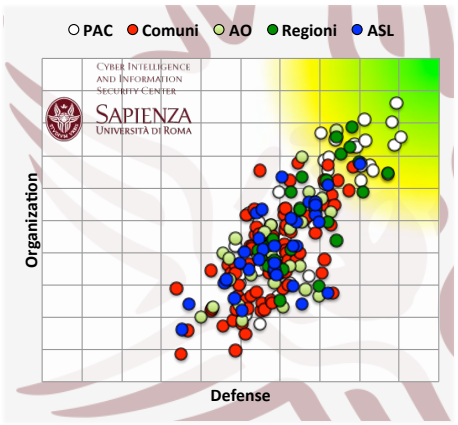


Figura 3.3: Confronto Defense-Organization per tutte le categorie.

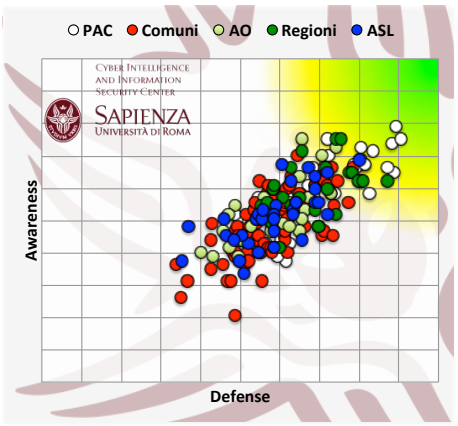


Figura 3.4: Confronto Defense-Awareness per tutte le categorie.

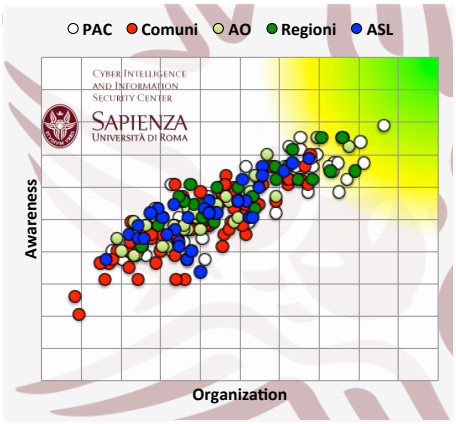


Figura 3.5: Confronto Organization-Awareness per tutte le categorie.

sono nella zona verde (superano cioè la soglia di idoneità), tutte appartenenti alla categoria PAC, mentre la gran parte delle amministrazioni sono nella zona bianca, ovvero mostrano grave impreparazione in termini di cyber security.

3.4 Risultati per le singole categorie

In questa sezione vengono mostrati i risultati ottenuti da ogni categoria di pubblica amministrazione, in termini di confronto *Defense-Organization*, *Defense-Awareness* e *Organization-Awareness*.

3.4.1 Pubbliche Amministrazioni Centrali

I risultati delle Pubbliche Amministrazioni Centrali spaziano nell'intervallo [50,90] per quanto riguarda il KPI Defense, [40,80] per il KPI Organization, [50,75] per il KPI Awareness.

Nonostante la situazione delle PAC è tendenzialmente migliore rispetto alle altre categorie, sono poche le amministrazioni che superano il punteggio 80, in particolare 12 su 42, per il KPI defense. Per quanto riguarda il KPI Organization, solo 3 amministrazioni raggiungono il punteggio 80 e la maggior parte delle altre è ben lontana da tale soglia. Simile, ma leggermente peggiore, è la situazione per quanto riguarda l'*Awareness*. In generale si può riscontrare una situazione molto grave per 22 amministrazioni (vale a dire il 50% del campione), con livelli di *Organization* e *Awareness* entrambi molto bassi e *Defense* inferiori a 70.
Tali risultati sono riportati in Figura 3.6, che mostra i valori di *Defense* in relazione ai valori di *Organization*, in Figura 3.7 che mostra i valori di *Defense* in relazione al KPI *Awareness*, e infine in Figura 3.8 che mostra i valori di *Organization* in relazione al KPI *Awareness*. Analizzando la Figura 3.6, si può notare che i punti sono clusterizzabili in due gruppi ben distinti, uno in cui si ha Organization maggiore di e contemporaneamente Defense maggiore di 70, e l'altro in cui i valori di Organization e Defense al di sotto di tali intervalli. Nella Sezione 3.8 tale situazione verrà indagata in maniera più approfondita e verranno mostrate le motivazioni che causano la divisione in due dell'insieme (Figura 3.42).

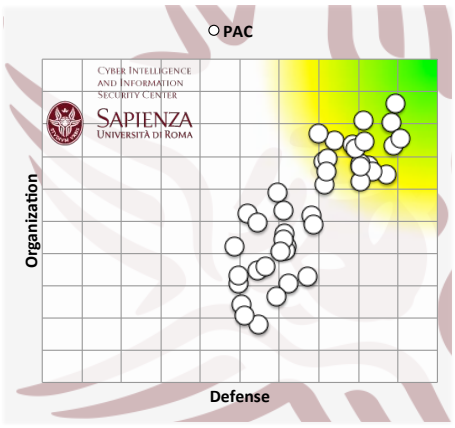


Figura 3.6: Confronto Defense-Organization per le PAC.

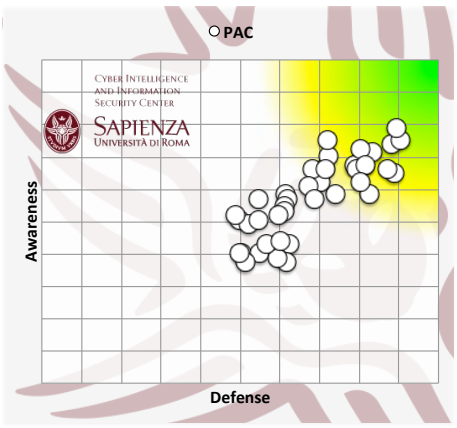


Figura 3.7: Confronto Defense-Awareness per le PAC.

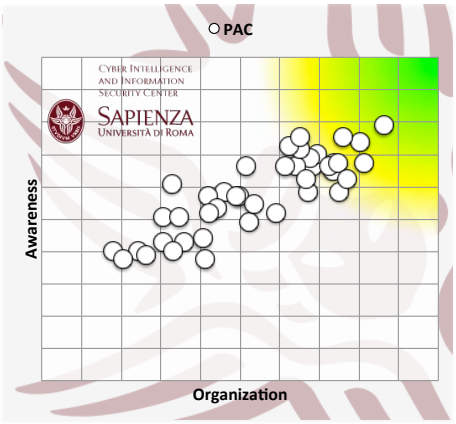


Figura 3.8: Confronto Organization-Awareness per le PAC.

3.4.2 Regioni

I risultati delle Regioni ed Enti Regionali spaziano nell'intervallo [54,87] per quanto riguarda il KPI Defense, [40,64] per il KPI Organization, [50,62] per il KPI Awareness. Le Figure 3.9, 3.10 e 3.11 mostrano rispettivamente l'andamento delle coppie di KPI *Defense-Organization*, *Defense-Awareness* e *Organization-Awareness*, per le Regioni e per gli Enti Regionali. Si può notare che i risultati ottenuti sono inferiori rispetto a quelli ottenuti dalle PAC, in particolare per quanto riguarda i valori massimi di tutti e tre i KPI. In questo caso, solo 3 amministrazioni superano il punteggio 80 per il KPI *Defense*, 2 amministrazioni per il KPI *Organization* e 2 per l'*Awareness*. E' evidente come nessuna amministrazione è nella zona verde e una buona porzione di amministrazioni (14 amministrazioni su 25) non supera contemporaneamente il punteggio 50 in *Organization* e 70 in Defense.

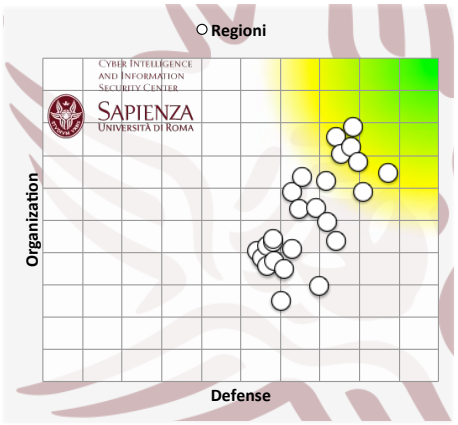


Figura 3.9: Correlazione Defense-Organization per le Regioni.

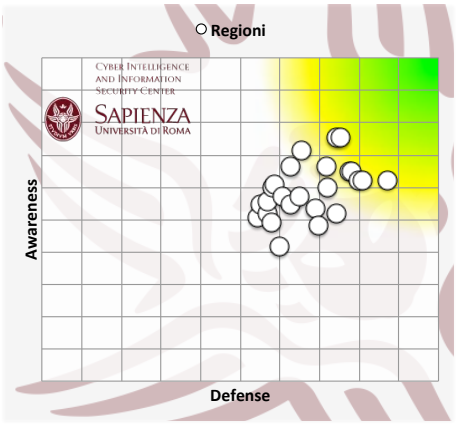


Figura 3.10: Correlazione Defense-Awareness per le Regioni.

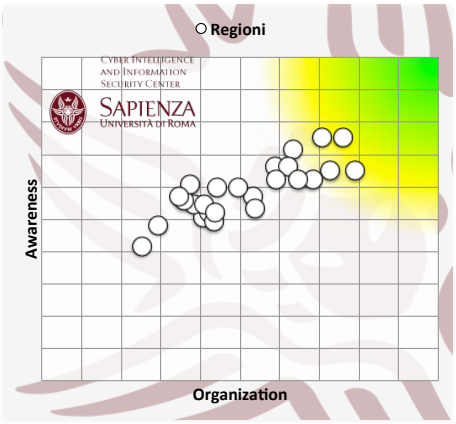


Figura 3.11: Correlazione Organization-Awareness per le Regioni.

Singole Regioni ed Enti Regionali

Come esempio si riporta in Figure 3.12, 3.13, 3.14, la situazione di tutte le categorie appartenenti a tre singole Regioni. Si nota come ci sia sempre un'amministrazione, tipicamente una regione o ente regionale, il cui comportamento generale è migliore delle altre amministrazioni. Questo testimonia come la frammentazione dell'IT delle amministrazioni porta a risultati contrastanti. Le stesse tre Regioni sono esaminate nella Sezione 3.8 al fine di capire cosa accomuna le amministrazioni che mostrano risultati migliori in ambito regionale.

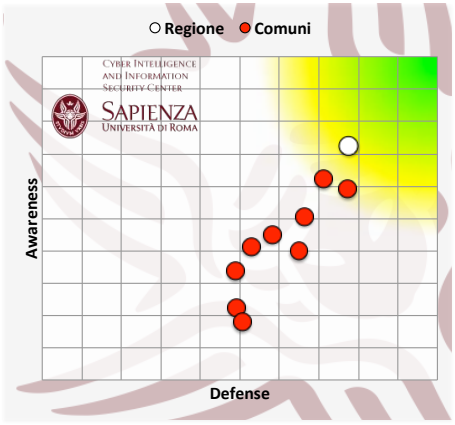


Figura 3.12: Situazione di una singola regione (regione 1).

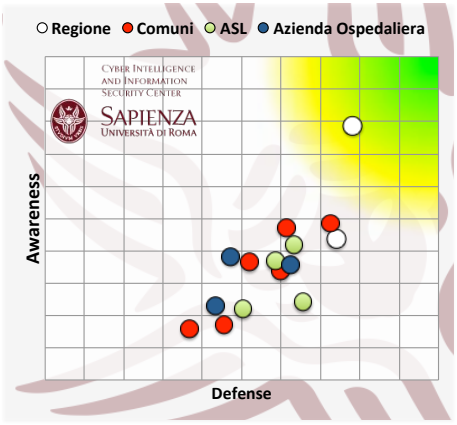


Figura 3.13: Situazione di una singola regione (regione 2).

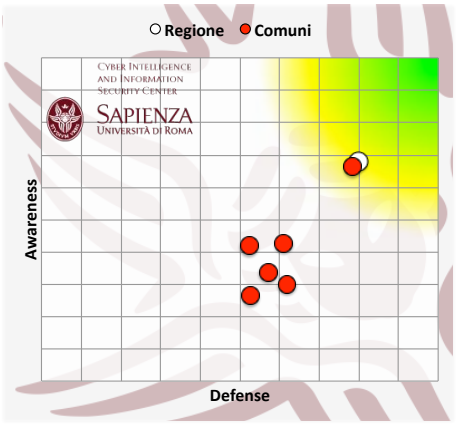


Figura 3.14: Situazione di una singola regione (regione 3).

3.4.3 Comuni

I risultati dei Comuni spaziano nell'intervallo [33,78] per quanto riguarda il KPI Defense, [28,68] per il KPI Organization, [36,70] per il KPI Awareness. Nessuno dei Comuni esaminati ha raggiunto, per il KPI *Defense*, il punteggio di 80 e sono solo 11, su un totale di 79, i Comuni che hanno ottenuto un punteggio superiore a 70. Per gli altri KPI la situazione è anche peggiore. In generale, i Comuni sono la categoria che mediamente si comporta peggio delle altre (si ricorda anche quanto mostrato in Figura 3.2) per quanto riguarda i KPI *Awareness* e *Organization*, pur avendo mediamente un comportamento simile ad ASL e Aziende Ospedaliere per quanto riguarda il KPI *Defense*. Le Figure 3.15, 3.16 e 3.17 riportano questi risultati.

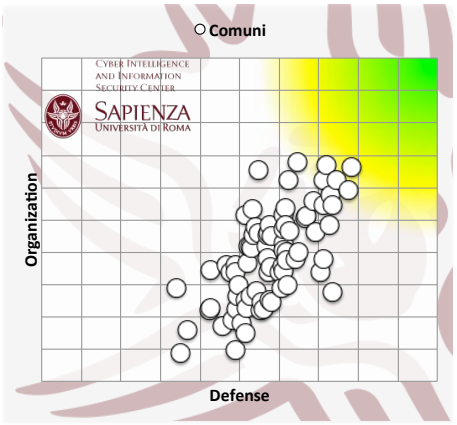


Figura 3.15: Correlazione Defense-Organization per i Comuni.

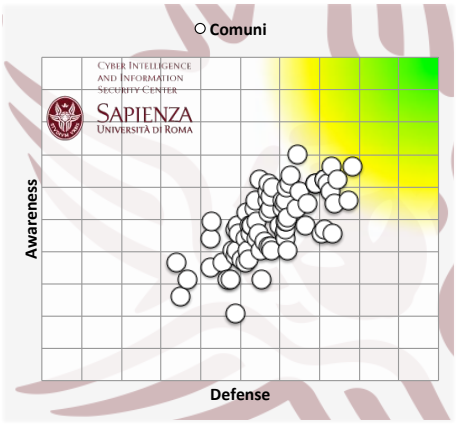


Figura 3.16: Correlazione Defense-Awareness per i Comuni.

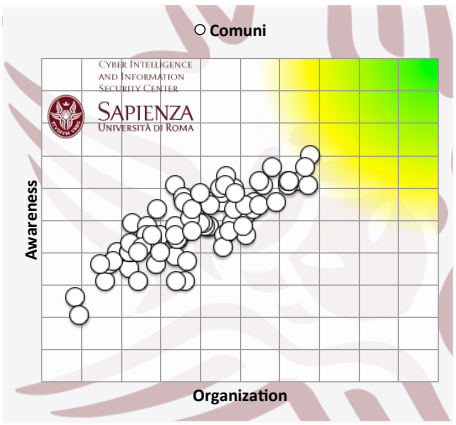


Figura 3.17: Correlazione Organization-Awareness per i Comuni.

3.4.4 ASL

Le ASL spaziano nell'intervallo [35,80] per quanto riguarda il KPI Defense, [16,67] per il KPI Organization, [37,68] per il KPI Awareness, mostrando un comportamento molto simile ai Comuni. Tali risultati sono mostrati nelle Figure 3.18, 3.19 e 3.20.

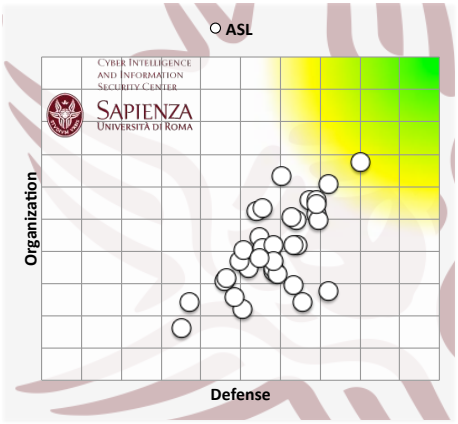


Figura 3.18: Confronto Defense-Organization per le ASL.

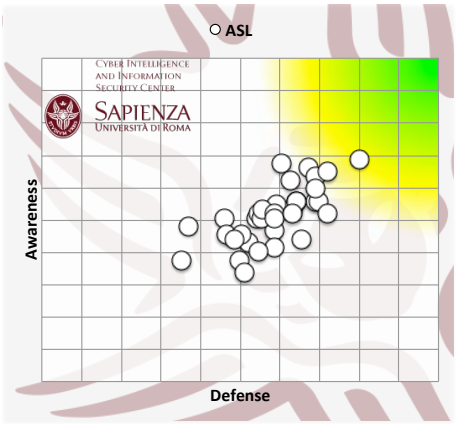


Figura 3.19: Confronto Defense-Awareness per le ASL.

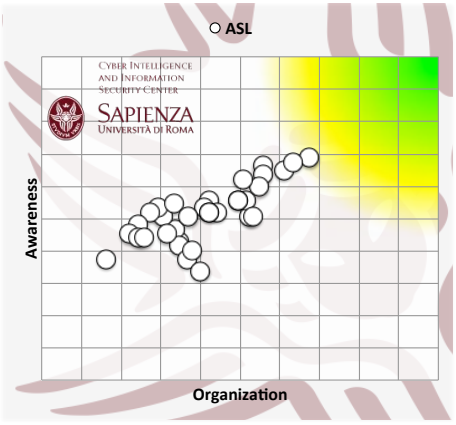


Figura 3.20: Confronto Organization-Awareness per le ASL.

3.4.5 Aziende Ospedaliere

Le aziende ospedaliere spaziano nell'intervallo [40,74] per quanto riguarda il KPI Defense, [20,77] per il KPI Organization, [40,72] per il KPI Awareness, mostrando un risultato leggermente migliore rispetto a Comuni e ASL. Anche in questo caso, come per le ASL, ci sono casi in cui l'*Organization* è distante dal valore ottenuto nel KPI *Defense*. Le Figure 3.21, 3.22 e 3.23 confrontano i KPI e mostrano questi casi. Si può anche apprezzare come mediamente aziende ospedaliere, così come i Comuni, sono distanti dalla soglia di idoneità. In questo caso, il valore di correlazione è leggermente minore.

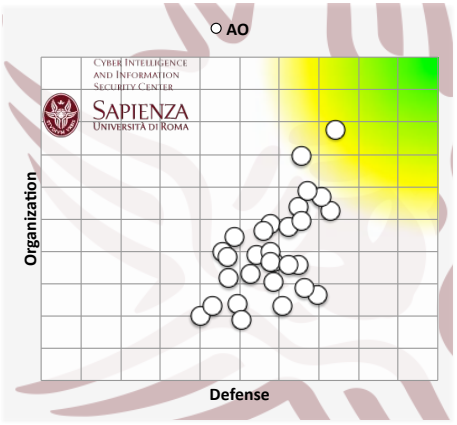


Figura 3.21: Confronto Defense-Organization per le Aziende Ospedaliere.

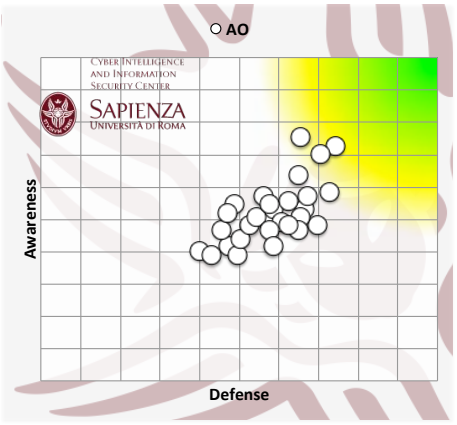


Figura 3.22: Confronto Defense-Awareness per le Aziende Ospedaliere.

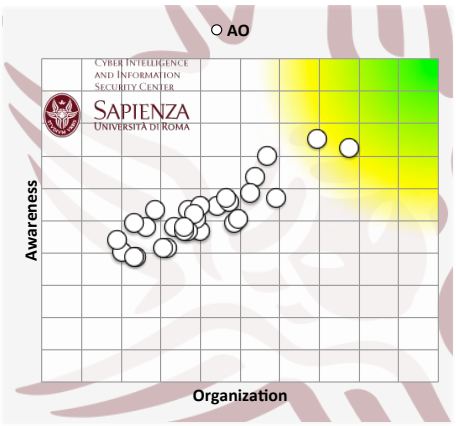


Figura 3.23: Confronto Organization-Awareness per le Aziende Ospedaliere.

3.5 Risultati in base alla dimensione dell'amministrazione

Di seguito sono riportati i risultati medi in relazione ad uno dei parametri dimensionali delle amministrazioni analizzate, vale a dire il numero di utenti serviti dalla amministrazione. In Figura 3.24 si può apprezzare un ordinamento dei risultati: amministrazioni che servono un numero maggiore di cittadini ottengono, mediamente, valori più alti per i tre KPI.

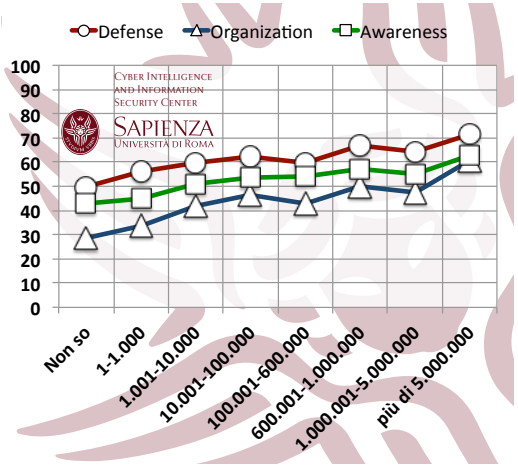


Figura 3.24: Confronto delle amministrazioni in base al numero di utenti servito.

Se si filtrano i risultati, analizzando i risultati ottenuti dalle sole PAC in relazione al numero di utenti servito, si ottiene il risultato riportato in Figura 3.25. Nonostante un risultato leggermente peggiore delle PAC che servono fino a 1000 utenti, non si nota una vera e propria correlazione tra dimensioni e risultati. La medesima situazione si ripete per le ASL (Figura 3.27) e per le Regioni (Figura 3.28). Comuni e Aziende Ospedaliere (Figure 3.26 e 3.29 rispettivamente) presentano una correlazione dimensione-risultati. C'è da notare che le amministrazioni che hanno risposto "non so" alla domanda relativa al numero di utenti servito hanno poi mediamente ottenuto risultati peggiori.

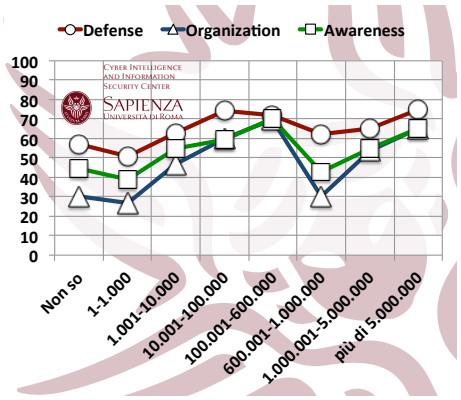


Figura 3.25: Risultati PAC in base al numero di utenti servito.

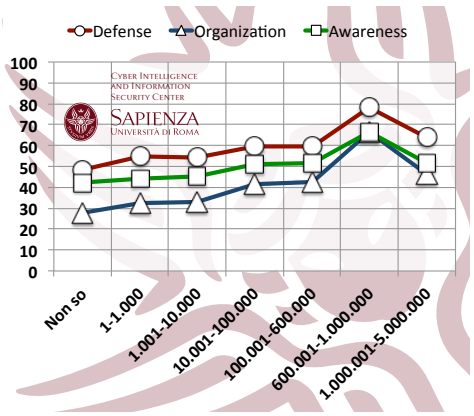


Figura 3.26: Risultati Comuni in base al numero di utenti servito.

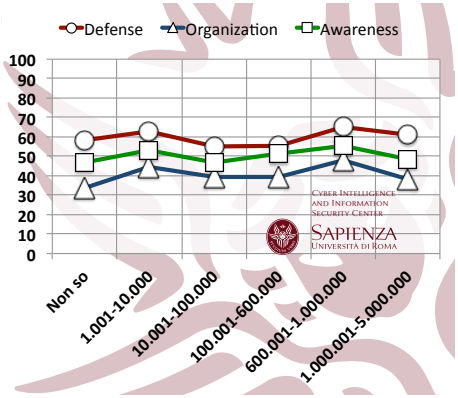


Figura 3.27: Risultati ASL in base al numero di utenti servito.

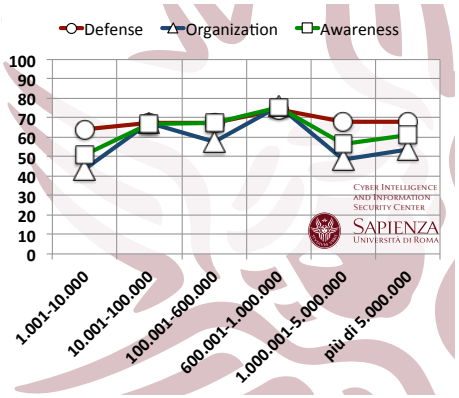


Figura 3.28: Risultati Regioni in base al numero di utenti servito.

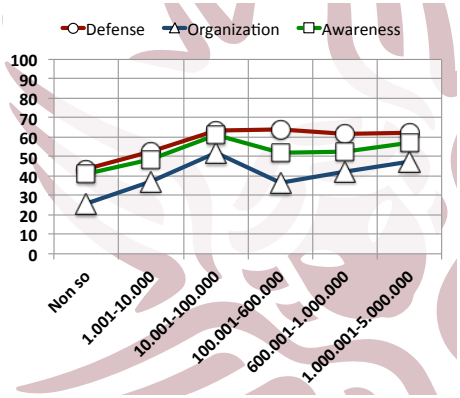


Figura 3.29: Risultati Aziende Ospedaliere in base al numero di utenti servito.

3.6 Risultati in base alla posizione geografica dell'amministrazione

E' utile confrontare i risultati in base alla posizione geografica delle amministrazioni. A tal proposito si è proceduto a classificare Comuni, Regioni, ASL e Aziende Ospedaliere in base alla Tabella 3.2, in accordo con la classificazione ISTAT. La categoria PAC non è presa in considerazione in quanto, per definizione, ogni PAC offre servizi all'intera popolazione.

Tabella 3.2: Associazione Aree geografiche - Regioni

Nord	Emilia-Romagna; Friuli-Venezia Giulia; Liguria; Lombardia; Piemonte; Trentino-Alto Adige; Valle d'Aosta; Veneto
Centro	Lazio; Marche; Toscana; Umbria;
Sud	Abruzzo; Basilicata; Calabria; Campania; Molise; Sardegna; Puglia; Sicilia

Le categorie Comuni e Aziende Ospedaliere mostrano una forte correlazione tra posizionamento geografico e risultati: i Comuni e le AO siti nelle Regioni del nord hanno mediamente risultati migliori delle amministrazioni del centro, quelle del centro risultati migliori delle amministrazioni del sud. Tali valori sono riportati in Figure 3.31 e 3.33; Le categorie ASL e Regioni presentano risultati discordanti: non c'è un ordinamento ben definito per i vari KPI in base al posizionamento geografico. Si ha che per le ASL (Figura 3.32) il KPI *Defense* sia migliore al sud rispetto al centro e al nord, cosa che non accade per il KPI *Organization* che risulta ordinato. Il KPI *Awareness* ha risultati peggiori al centro rispetto al nord e al sud. Per quanto riguarda le Regioni, il centro si comporta mediamente peggio rispetto al sud mentre il Nord meglio del sud (Figura 3.30).

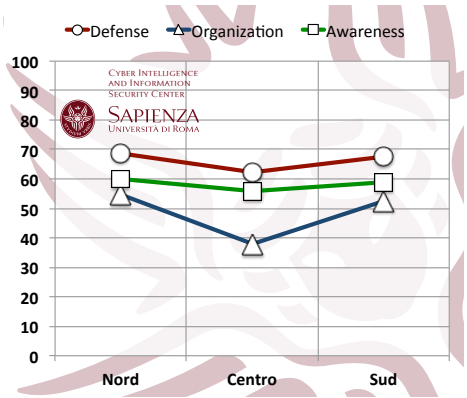


Figura 3.30: Risultati in base alla posizione geografica per le Regioni.

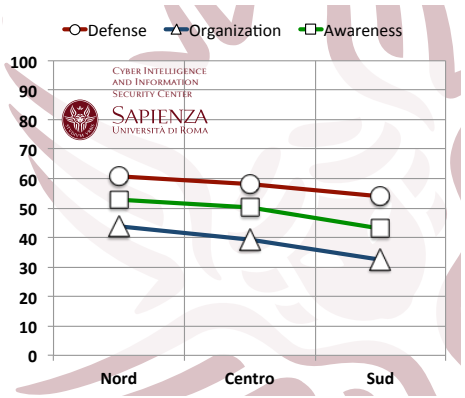


Figura 3.31: Risultati in base alla posizione geografica per i Comuni.

In Figura 3.31 è mostrato il valor medio dei KPI relativi ai Comuni in accordo all'area geografica di appartenenza. Si può notare un graduale peggioramento da nord a sud per tutti i KPI.

La Figura 3.33 riporta i valori medi per i tre KPI in base alla posizione geografica delle Aziende Ospedaliere. Anche in questo caso, così come per i Comuni, si ottiene un un peggioramento dei KPI in accordo alla posizione geografica.

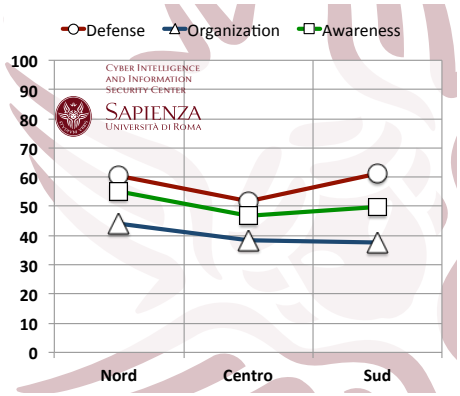


Figura 3.32: Risultati in base alla posizione geografica per le ASL.

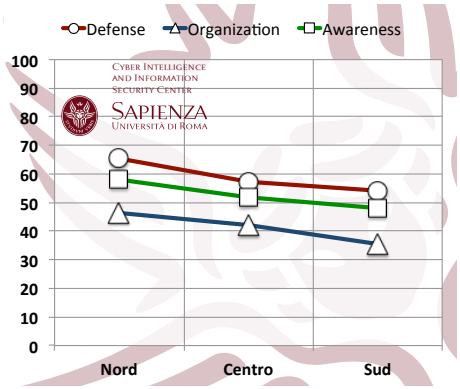


Figura 3.33: Risultati in base alla posizione geografica per le Aziende Ospedaliere.

3.7 Risultati in base ai tentativi di attacco subiti dall'amministrazione

E' importante relazionare il numero di tentativi di attacco subito dalle amministrazioni nel 2013 ai risultati complessivi ottenuti per i 3 KPI. La Figura 3.34 riporta il numero di tentativi di attacco dichiarato sull'asse delle ascisse e il valore medio dei 3 KPI sulle ordinate. E' importante notare come, mediamente, le amministrazioni che di-

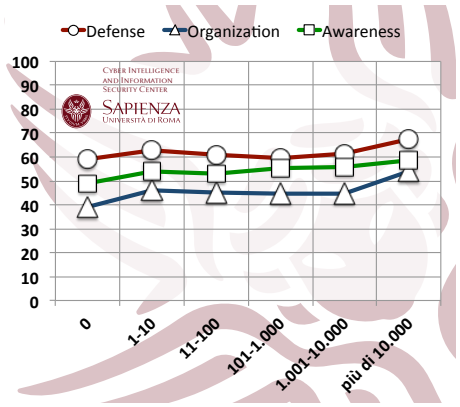


Figura 3.34: Andamento dei KPI in relazione al numero di tentativi di attacco subiti nel 2013.

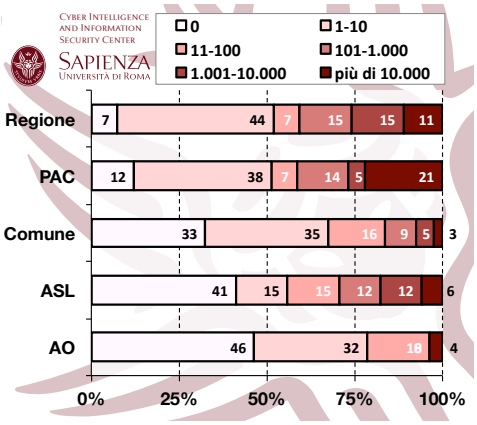


Figura 3.35: Numero di tentativi di attacco subiti nel 2013 a seconda della categoria di amministrazione.

chiarano di aver subito 0 tentativi di attacchi sono quelle che ottengono risultati peggiori per tutti i KPI. Questo è anche evidenziato dalla Figura 3.35 che mostra come Aziende Ospedaliere e ASL dichiarino di aver rilevato un numero esiguo di attacchi: oltre il 40% di loro (41% delle ASL e 46% delle AO), infatti, dichiara di non aver subito affatto tentativi di attacco. Pochissime sono le PAC e le Regioni che dichiarano di non aver subito tentativi di attacco (rispettivamente il 12% e il 7%) così come il 33% dei Comuni. La categoria che maggiormente rileva il maggior numero di tentativi (il 21% dichiara un numero superiore a 10000 in un anno) è quella delle PAC.

3.8 Analisi statistica dei dati ricavati dai questionari

Utilizzando algoritmi appartenenti alle discipline di apprendimento automatico e information retrieval, è stato possibile studiare le caratteristiche che accomunano le amministrazioni che hanno ottenuto un punteggio simile nei tre KPI. Ciò ha consentito di individuare le migliori pratiche volte all'aumento della sicurezza informatica nel suo complesso, e mettere in evidenza gli aspetti più importanti da considerare qualora si voglia aumentare sensibilmente la propria preparazione.

E' importante sottolineare che le oltre 50 domande poste alle pubbliche amministrazioni contribuiscono ad aumentare/diminuire il singolo KPI in modo molto limitato, e tale contributo è limitato superiormente ed inferiormente in maniera indipendente dalla domanda. Tale indipendenza ha consentito di ottenere risultati non influenzati in alcun modo dal meccanismo di pesi assegnato, ma dettati dalle sole risposte date dalle oltre 200 amministrazioni.

In particolare si è studiato cosa accomuna le amministrazioni che hanno ottenuto per tutti i KPI un punteggio maggiore di 50, al fine di individuare le caratteristiche Comuni alle amministrazioni maggiormente attente alle tematiche proposte. Si sono in questo modo ottenute le seguenti regole:

1. Se l'amministrazione non esegue Risk Assessment e contemporaneamente non definisce un piano di risposta ad un attacco informatico allora è con ottima probabilità in una grave condizione.
2. Se l'amministrazione esegue Risk Assessment ma non definisce un piano di risposta ad un attacco informatico, non necessariamente è in una buona condizione.
3. Se l'amministrazione definisce un piano di risposta ad un attacco informatico, ma non esegue Risk Assessment, non necessariamente è in una buona condizione.
4. Se l'amministrazione manifesta la presenza contemporanea di un ISMS, Risk Assessment e piano di risposta ad un attacco informatico allora è con ottima probabilità in una buona condizione.

Grazie all'identificazione delle domande e alla definizione di queste regole è stato possibile rappresentare graficamente le amministrazioni che soddisfino le regole e metterle in relazione al punteggio da loro ottenuto. In particolare nelle Figure 3.36, 3.37 e 3.38 sono riportati i confronti *Defense-Organization*, *Defense-Awareness* e *Organization-Awareness* per tutte le amministrazioni, evidenziando quali regole sono soddisfatte. In tutti e tre le figure si può notare come le amministrazioni nella zona verde siano accomunate (i) da una fase di Risk Assessment eseguita regolarmente, (ii) dalla definizione di un piano di risposta ad un attacco informatico e (iii) dall'adozione di un Information Security Management System (ISMS). Allo stesso tempo si può notare, in tutte e tre le figure, come chi non effettua nessuna delle tre pratiche sia molto distante dall'area verde o soglia di idoneità (punti rappresentati in rosso nelle figure). La presenza di Risk assessment e della definizione di un piano di risposta collocano le amministrazioni nella zona medio alta (rappresentate in verde nelle figure), le amministrazioni che abbiano solo una delle 3 condizioni si collocano nella zona intermedia (rappresentate in bianco nelle figure).

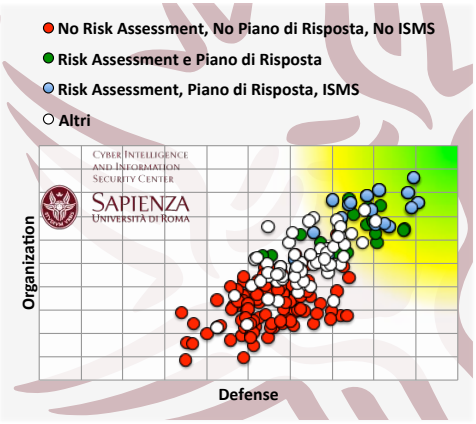


Figura 3.36: Confronto Defense-Organization.

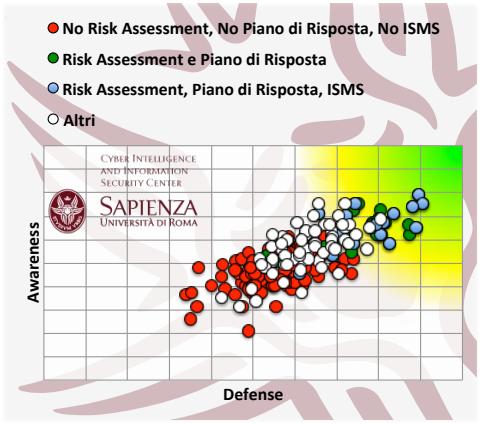


Figura 3.37: Confronto Defense-Awareness.

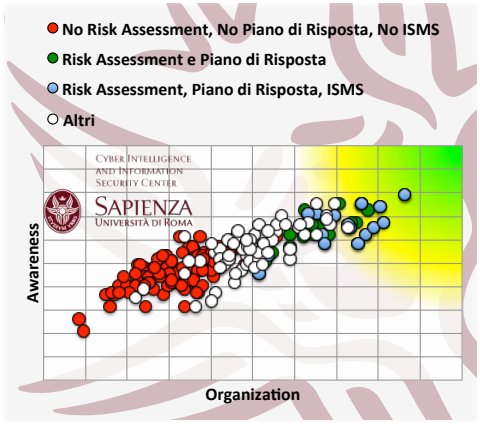


Figura 3.38: Confronto Organization-Awareness.

3.8.1 Singole Regioni ed Enti Regionali

In sezione 3.4.2 si è riportata, come esempio, la situazione di tutte le categorie appartenenti a tre singole regioni (Figure 3.12, 3.13, 3.14). In particolare si è fatto notare come ci sia sempre un'amministrazione il cui comportamento generale è migliore delle altre amministrazioni della medesima Regione. Gli algoritmi utilizzati hanno permesso di stabilire cosa accomuna le amministrazioni con risultati migliori ottenendo i risultati in Figure 3.39, 3.40, 3.41. Si può notare che, per quanto riguarda la Regione 2 (Figura 3.39), l'amministrazione che ottiene punteggio migliore è l'unica di quella Regione ad attuare un piano di Risk Assessment, ad aver definito un piano di risposta ad attacchi informatici e ad avere un ISMS operativo. Nel caso della Regione 3 (Figura 3.40), si hanno due amministrazioni che ottengono punteggio molto maggiore rispetto agli altri enti regionali. In questo caso entrambe non hanno un ISMS, ma sono le uniche della Regione ad avere definito un piano di risposta ad attacchi informatici e che facciano regolarmente Risk Assessment. La Regione 1 mostra una situazione meno chiara. Si ha infatti che le due amministrazioni con punteggio migliore effettuano Risk Assessment o in alternativa abbiano definito un piano di risposta ad attacchi informatici, ma non contemporaneamente. Altre 2 amministrazioni con risultati peggiori presentano tale caratteristica.

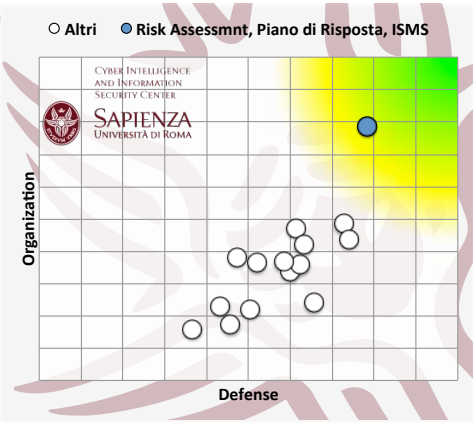


Figura 3.39: Situazione di una singola Regione (Regione 2).

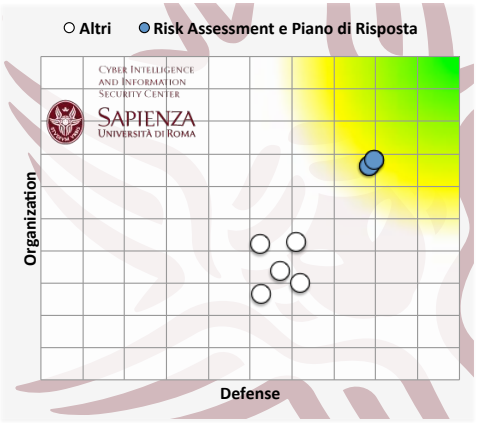


Figura 3.40: Situazione di una singola Regione (Regione 3).

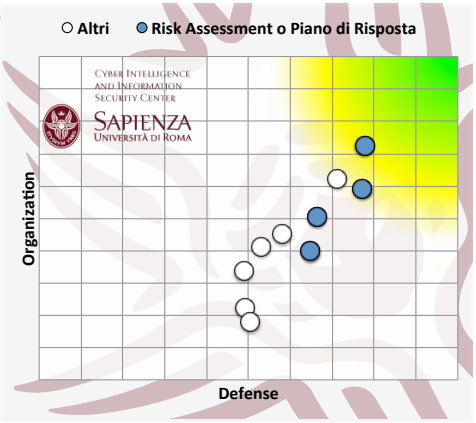


Figura 3.41: Situazione di una singola Regione (Regione 1).

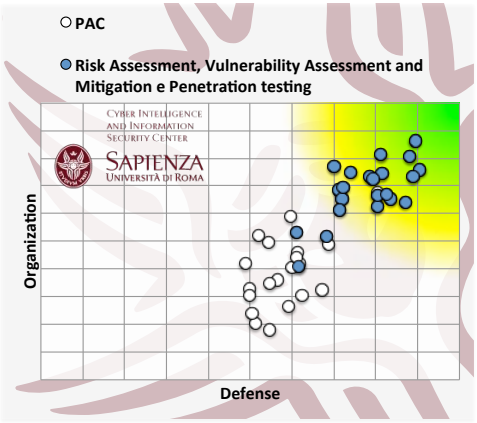


Figura 3.42: Confronto Defense-Organization per le PAC con classificazione.

3.8.2 Pubbliche Amministrazioni Centrali

Come si è mostrato in precedenza, in Figura 3.6, per quanto riguarda il confronto *Defense-Organization* per le Pubbliche Amministrazioni Centrali, si è individuato un gruppo ben definito di amministrazioni con risultati migliori, ed un gruppo ben definito con risultati peggiori. E' utile capire quali siano le pratiche che definiscono questi gruppi e le ragioni che hanno portato le PAC ad avere risultati discordanti. Isolando i risultati di tali amministrazioni è stato possibile classificarle, in particolare si ha che le amministrazioni che svolgono periodicamente Risk Assessment, che effettuano regolarmente Penetration Testing e che seguono la metodologia Vulnerability Assessment and Mitigation rappresentano la totalità del gruppo con risultati migliori. Di contro chi non segue queste pratiche costituisce il gruppo con risultati peggiori, con un errore di sole 3 amministrazioni su 42. La Figura 3.42 rappresenta questa situazione, evidenziando con colori diversi i due gruppi di PAC.

3.8.3 Considerazioni sulla classificazione

Le regole sopra descritte sono state ottenute analizzando l'insieme dei dati raccolti, e definisce un piccolo insieme di domande caratterizzanti alcune situazioni, ma non deve essere mal interpretato. Si noti infatti che:

- nella compilazione dei questionari una risposta affermativa alle sole 3 domande identificate influisce sui singoli KPI non più del 20%;
- il corretto posizionamento di una amministrazione è definito, con certezza, solo dalle risposte all'intero questionario e le domande influenzano il calcolo dei KPI, in accordo con la Tabella 2.1, secondo la metodologia presentata nel Capitolo 2;
- le tre domande riportate sono quelle più influenti per la classificazione delle amministrazioni che hanno ottenuto per tutti i KPI un punteggio maggiore di 50, tale risultato è confermato dalle Figure 3.36, 3.37 e 3.38. Tuttavia, il modello di classificazione ottenuto è più complesso e le varie situazioni intermedie vengono caratterizzate da un insieme molto più ampio di domande. Una lista più ampia delle domande che maggiormente influenzano la classificazione è riportata di seguito.

3.8.4 Le domande più influenti

Di seguito è riportato un elenco delle domande (con numero e breve descrizione) che maggiormente influenzano la classificazione delle amministrazioni che hanno ottenuto per tutti i KPI un punteggio maggiore di 50. Si noti che tale elenco rappresenta una porzione pari al 18% della totalità delle domande e che non sono ordinate per influenza.

- Domanda n. 2: Regione di appartenenza della PA;
- Domanda n.6: numero di utenti che possono usufruire dei servizi della PA;
- Domanda n. 10: numero di addetti/dipendenti IT della PA;
- Domanda n.14: numero di utenti registrati che fruiscono dei servizi della PA;
- Domanda n. 21: controllo di accesso fisico ai locali della PA;
- Domanda n.38: definizione di un piano di risposta ad un attacco informatico;
- Domanda n. 48: Risk Assessment regolarmente effettuato;
- Domanda n.49: Risk Assessment certificato da organizzazioni esterne;
- Domanda n.52: presenza di un ISMS;
- Domanda n. 53: presenza di un gruppo/comitato per la gestione degli incidenti;
- Domanda n. 57: verifiche periodiche dell'organizzazione e del funzionamento della sicurezza ICT.

L'interpretazione di tali domande fornisce una serie di best practices che le amministrazioni dovrebbero seguire per portare il proprio livello di preparazione contro minaccia cibernetica a valori accettabili. In particolare le domande n. 6, 14 e 10 suggeriscono che un adeguato dimensionamento delle risorse umane alle esigenze delle amministrazioni è molto importante. Le domande 48, 49, 52, 53, 57 testimoniano come un'organizzazione ben strutturata sia fondamentale per avere una buona preparazione. Il Risk Assessment permette di aumentare la consapevolezza dei rischi e di prendere delle contromisure, ancora meglio se certificato. La presenza di un gruppo per la gestione degli incidenti, oltre alla ovvia utilità in caso di crisi, testimonia una alta consapevolezza ed attenzione alla cyber security. La verifica periodica dell'organizzazione e del funzionamento della sicurezza IT permette di reagire tempestivamente al comparire di nuove minacce e vulnerabilità. Inoltre, la presenza di un controllo di accesso fisico ai locali è fondamentale per prevenire intrusioni di personale non autorizzato e malintenzionato ai locali preposti alle attività informatiche. Infine, si noti come nell'elenco sia presente solo la domanda n.38 relativa alla *Defense*, nonostante (come dimostrano le Figure 3.36 e 3.37 nell'asse delle x) la classificazione ottenuta pone correttamente i valori di tale KPI. Questo vuol dire che il KPI *Defense* è implicato dall'*Awareness* e dall'*Organization*: il fatto che si è risposto in un determinato modo alle domande nell'elenco implica che si seguano oppure no una serie di pratiche proprie della *Defense*.

3.9 Pratiche più comunemente ignorate dalle amministrazioni

E' utile identificare quali caratteristiche accomunano le amministrazioni con risultati inferiori a 50 per ogni KPI. Questo permette di capire quali sono le pratiche che tipicamente vengono ignorate dalle amministrazioni meno attente alle tematiche di cyber security.

Da quanto detto e mostrato in Figure 3.36, 3.37, 3.38, è chiaro che tutte queste amministrazioni siano accomunate da:

1. mancanza di Risk Assessment o Risk Assessment non effettuato regolarmente;
2. mancanza di piano di risposta ad attacchi informatici;
3. mancanza di ISMS;

tuttavia, la metodologia applicata permette di individuare altre caratteristiche che accomunano le amministrazioni che hanno ottenuto i peggiori risultati. In particolare si ha, oltre ai punti 1-3,

4. mancanza di sistemi di controllo degli accessi fisici ai locali IT;
5. mancanza di attività di Penetration Testing o Vulnerability Assessment and Mitigation;
6. mancanza di gruppo/comitato per la gestione degli incidenti;
7. mancanza di verifiche periodiche dell'organizzazione e del funzionamento della sicurezza ICT;
8. mancata definizione e/o approvazione del Piano della Sicurezza ICT;
9. mancata richiesta di parere ad AgID sullo studio di fattibilità tecnica per i piani di disaster recovery e business continuity.

CAPITOLO

4 Casi di studio

In questo capitolo analizziamo tre casi di studio, ognuno dei quali, per le loro caratteristiche, ha dovuto sviluppare una certa cultura della sicurezza. Per ognuna delle tre amministrazioni analizzate in questo capitolo si riporta il contesto in cui si pone, una breve storia dell'evoluzione dei propri servizi IT e la propria visione di gestione della sicurezza. Le tre amministrazioni sono la Corte dei Conti, l'Istituto Nazionale della Previdenza Sociale (INPS), la regione Friuli Venezia Giulia.

4.1 Corte dei Conti

La Corte dei conti ha sempre posto grandissima attenzione alle tematiche dell'ICT come supporto all'attività istituzionale. Nel corso degli anni la gestione dell'Informatica della Corte è diventata un punto di riferimento per tutta la PA italiana, grazie soprattutto ad un processo continuo di riorganizzazione orientato dalle migliori best practice di riferimento. La gestione della sicurezza ICT è considerata strategica nell'ambito IT di Corte dei conti ed è quindi stato naturale che anch'essa evolvesse in termini organizzativi e tecnologici. La recente adozione delle best practice ITIL v3 all'interno della Direzione Generale per I Sistemi Informativi Automatizzati (DGSIA) ha guidato l'ultima ristrutturazione del comparto Sicurezza che è ora adeguato alle nuove sfide poste dall'aumentato livello delle minacce. L'esperienza di Corte dei conti viene oggi "esportata" presso altre Pubbliche Amministrazioni, tramite accordi di collaborazione che porteranno a consolidare l'erogazione dei servizi presso i data center di Corte. Questo case study descrive le recenti esperienze dell'ICT di Corte dei conti (e nello specifico della sua struttura per l'ICT Security) in termini di riorganizzazione funzionale e di ridefinizione dei processi di gestione. Verrà esposta la realtà tecnologica di Corte dei conti, descritta la struttura organizzativa a supporto dell'ICT e i progetti che, negli ultimi quattro anni, hanno portato ad una complessiva rivisitazione di come si offrono servizi all'utenza e si garantisce continuità e sicurezza di dati ed infrastruttura.

4.1.1 Contesto

La Corte dei conti è un organo di rilievo costituzionale, autonomo ed indipendente da altri poteri dello Stato cui la Costituzione affida importanti funzioni di controllo (art. 100 Costituzione) e giurisdizionali (art. 103 Costituzione). La Corte dei conti è definita dalla Costituzione "organo ausiliario" nel senso che coadiuva gli organi titolari di funzioni legislative, di controllo ed indirizzo politico, esecutive e di amministrazione attiva. La Corte ha un totale di circa 3.500 utenti, di cui 500 magistrati, distribuiti in 25 sedi sul territorio nazionale. Da oltre quindici anni il ruolo del settore ICT di Corte dei conti sta evolvendo in termini di servizio offerto all'utenza e sempre maggior supporto alle funzioni istituzionali. Grazie ad un attento indirizzo da parte degli organi di governo, al supporto continuo dei Magistrati addetti ai Sistemi Informativi e ad una gestione illuminata dei Dirigenti tecnici ed amministrativi, la struttura ICT di Corte si è affermata come una best practice assoluta all'interno della Pubblica Amministrazione

italiana, testimoniata da numerosi premi e riconoscimenti sia per i singoli che per la struttura nel suo complesso. Ovviamente negli anni la Corte ha fatto continuamente evolvere la sua infrastruttura tecnologica e i processi che sottendono all'attività ICT, ponendo inoltre un focus sempre maggiore sulle tematiche della sicurezza di dati e sistemi.

4.1.2 Breve storia dell'evoluzione dei servizi IT in Cdc

All'interno di Corte dei conti, l'ICT è storicamente uno dei settori di vitale importanza per lo sviluppo delle funzioni istituzionali. Fin dai primi anni '90 i vari uffici di Corte dei conti avevano infatti compreso il ruolo strutturale dell'Informatica a supporto dell'attività istituzionale. Negli anni immediatamente successivi è emersa chiaramente la necessità di centralizzare e strutturare meglio la gestione ICT, unificandola sotto un'unica Unità Organizzativa (URSIA, Ufficio del Responsabile dei Sistemi Informativi Automatizzati). Il modello utilizzato per "popolare" l'URSIA è stato al contempo semplice ma estremamente efficace:

- sono state "prelevate" dagli uffici di Corte più avanzati in campo ICT le migliori risorse umane che al tempo avevano a che fare con l'Informatica e con i principali applicativi informatici in essere;
- è stata avviata una vera e propria campagna di recruitment interno ed esterno all'amministrazione, realizzata con specifici concorsi pubblici o procedure di comando/trasferimento da altre Amministrazioni di figure tecniche di alto livello;
- le risorse interne a Corte che mostravano interesse al settore ICT pur non avendo titoli e/o esperienza al riguardo sono state oggetto di formazione specialistica mirata ed incorporate in URSIA.

Non va in ogni caso dimenticato il ruolo della componente magistratuale nella gestione dell'ICT. Fino al 2010 la figura del "Responsabile dei Sistemi Informativi Automatizzati" era appunto un Magistrato, con ruolo di coordinamento e garanzia delle attività IT, portate avanti da personale tecnico/amministrativo. Ancora oggi, pur nell'ambito della nuova organizzazione, in cui il Responsabile è il Direttore Generale di DGSIA, esiste una figura di Magistrato Addetto ai Sistemi Informativi, che funge da collegamento fra le necessità dell'area magistratuale (e quindi delle funzioni istituzionali di Corte) e le strutture tecniche.

Fondamentale è stata inoltre la definizione di un modello di outsourcing "sano": le attività tecniche sono state sempre più demandate a Società esterne (in alcuni casi con la collaborazione di Consip prima e Sogei oggi), ma ne è stata mantenuta in house la governance tecnica, affidata a specifiche professionalità di alto livello presenti nei ruoli di Corte (o formate in modo opportuno).

Nei primi anni Duemila sono state poste le basi per la totale informatizzazione dell'attività istituzionale: i sistemi SICR (Referto e Controllo), SISP (Sezioni e Procure) e le Banche Dati delle Sentenze (Giurisdizione), rappresentano le pietre miliari del percorso di informatizzazione dell'Istituto. Il parco applicativo e di conseguenza le infrastrutture si sono evolute con grande velocità, non tralasciando l'adeguamento tecnologico di tutte le sedi periferiche della Corte e la gestione avanzata delle postazioni di lavoro degli utenti. Nel contempo sono state sperimentate le prime esperienze nell'ambito del riuso, in particolare nel campo della gestione del personale (progetto Siap*Cdc). Il contesto di trasformazione del ruolo istituzionale di Corte dei conti, sempre più chiamata a controllare l'attività di Regioni ed Enti Locali, ha portato, a partire dal 2005, un forte sviluppo di specifici sistemi informativi (SIRTEL, SIQUEL ed altri) fortemente orientati ad essere fruiti da utenza esterna alla Corte.

Negli ultimi dieci anni, grazie all'opera di razionalizzazione e centralizzazione dei servizi operata dalla DGSIA (erede di URSIA, come si vedrà nel seguito) ed in particolare dal Servizio per la gestione del Centro Unico Servizi (CUS), sono state prodotte significative trasformazioni del contesto IT, secondo i principi di modernizzazione e selezione oculata delle tecnologie leader di mercato. La strategia d'innovazione ha sempre perseguito l'obiettivo di razionalizzare i servizi per la definizione di un'offerta completa in grado di soddisfare ed addirittura anticipare le esigenze di tutte le funzioni istituzionali.

In quest'ottica, si inquadra la predisposizione di servizi per lo sviluppo della comunicazione e collaborazione tra uffici (posta elettronica, messaggistica istantanea, videoconferenza, condivisione e distribuzione file, ecc..). A tali strumenti, di fondamentale importanza, si affiancano in modo complementare i Sistemi Informativi tradizionali. A partire dal 2010, l'impulso innovatore prodotto all'interno della DGSIA dal CUS ha inoltre determinato la definizione del modello di continuità dei servizi, la distribuzione dei sistemi su due CED in area metropolitana, la

capacità di offrire servizi ad altre Amministrazioni (CNEL, Avvocatura dello Stato) e la sperimentazione di servizi Cloud ibridi.

L'infrastruttura ICT

La Corte dei conti (Cdc, nel seguito) dispone a Roma di due CED: il primo è dislocato presso i locali del Centro Unico Servizi (CUS) di via Baiamonti ed il secondo presso il sito del Ministero dell'Economia e delle Finanze (MEF) de La Rustica. L'interconnessione fra i due data center è realizzata tramite tecnologia a "fibra spenta" e garantisce prestazioni tali da poter considerare il data center secondario una mera estensione del primario. Il CED "Baiamonti" (primario) eroga il complesso dei servizi Cdc mentre quello di La Rustica (secondario) è in grado di erogare solo una parte degli stessi. La Cdc ha tuttavia già avviato una serie di iniziative volte a garantire la distribuzione oppure il ripristino dei propri servizi sul sito secondario ed ha in piano la progressiva estensione, a tutti i servizi critici, della possibilità di essere erogati "indifferentemente" dai due CED. L'infrastruttura operativa del CED primario è caratterizzata da 3 farm di server, collegate alle infrastrutture di Storage Area Network e di Rete Locale (LAN), dedicate rispettivamente alla piattaforma di virtualizzazione VMware VSphere, agli ambienti Microsoft HyperV ed ai database relazionali (DB Farm). Presso il CED è inoltre presente una Tape Area Network, oltre ad un'infrastruttura per la connettività geografica (servizi esterni, con le altre Amministrazioni e con le sedi periferiche) e Metropolitana (per il collegamento al sito secondario dove è presente, in forma ridotta, un'analoga infrastruttura realizzata con le medesime tecnologie abilitanti presenti nel CED primario).

L'infrastruttura IT della Cdc oggi ospitata presso il CED Baiamonti è composta da:

- 84 server (rackable e blade) per circa 800 core e 8.6 TB di RAM complessivi;
- 200 TB di spazio storage;
- 30 apparati di rete;
- 12 apparati di sicurezza perimetrale (firewall, sonde IPS, IDS, Web Application Firewall), il tutto distribuito in 16 rack.

Come detto in precedenza, il CED secondario ospita in versione ridotta le stesse infrastrutture: sono al momento in corso acquisizioni di hardware allo scopo di espanderne la capacità per far fronte ai nuovi rilasci previsti nei prossimi mesi. L'obiettivo finale di massima è infatti quello di realizzare due data center "gemelli", sia in termini di disegno, sia in termini di infrastrutture (comprese quelle di sicurezza). A tal proposito sono state avviate una serie di iniziative a breve e medio termine (conclusione prevista entro il primo semestre 2015) con i seguenti obiettivi:

- potenziamento dell'infrastruttura IT attraverso la distribuzione di sistemi e servizi nel data center secondario;
- attività di adeguamento dell'infrastruttura hardware e network;
- configurazione definitiva delle modalità di recovery dei servizi;
- definizione delle procedure operative e perfezionamento dei piani di disaster recovery.

Le infrastrutture di virtualizzazione, database e application server sono considerate e gestite come trasversali ai vari silos applicativi ospitati e hanno i corrispettivi ambienti di collaudo e manutenzione. La conduzione dei sistemi è affidata in outsourcing tramite una gara europea multi-lotto, con la Direzione Generale dei Sistemi Informativi Automatizzati (DGSIA) della Corte dei conti che mantiene (con il supporto di SOGEI) la governance tecnica e alcune funzioni ritenute particolarmente strategiche (come l'Identity Management). Complessivamente, i processi di gestione delle infrastrutture tecnologiche coinvolgono oltre 50 persone, fra consulenti esterni e personale tecnico/amministrativo di Corte.

Il cambiamento organizzativo e la scelta ITIL v3

La costante crescita dei servizi IT forniti da Corte dei conti alla propria utenza ha evidenziato, negli ultimi anni, la necessità di una profonda riorganizzazione sia in termini di struttura aziendale che di reingegnerizzazione dei processi. È stata infatti riscontrata un'insufficiente strutturazione dei processi intesi come attività trasversali, cosa che portava ad un livello di efficienza (soprattutto in termini di tempi di risposta alla richiesta di nuovi servizi da parte degli utenti) non più adeguato. A ciò si è aggiunta l'eccessiva dimensione in termini di risorse umane (come singolo ufficio) della Direzione ICT di Corte dei conti che rendeva assai complesso il lavoro delle singole Unità Organizzative.

Fondamentale, in questo ambito di ridefinizione del nuovo regolamento di funzionamento di Cdc, è stato il fortissimo commitment da parte delle massime cariche istituzionali e della dirigenza, le quali, grazie alla loro sponsorship, hanno consentito di procedere in modo organico su entrambi i fronti. Per quanto riguarda la struttura aziendale, l'Amministrazione ha dunque optato per una maggiore articolazione del settore ICT: da un ufficio monolitico (URSIA) si è passati ad una struttura di Direzione Generale (Direzione Generale dei Sistemi Informativi Automatizzati, DGSIA) composta da tre direzioni tecniche ed una direzione amministrativa (quest'ultima con competenza su acquisti, gare e contratti).

L'organizzazione della DGSIA è così strutturata:

- Servizio per la Gestione del Centro Unico Servizi - CUS;
- Servizio per la Gestione dei Progetti Applicativi - SPA;
- Servizio per la Gestione ed il coordinamento dei Servizi Informatici e telematici presso le sedi regionali - SIR;
- Servizio per la Gestione di Gare, Acquisti e Contratti - AGC.

Il Dirigente Generale è affiancato da una Segreteria direzionale con compiti estesi alla pianificazione strategica. Per quanto riguarda i processi, è stata presa la decisione di seguire un ben definito processo evolutivo con il principale obiettivo di integrare le best practice relative all'ITSM (IT Service Management) nell'intera gestione dell'ICT di Corte dei conti, partendo dallo specifico contesto operativo del Servizio per la Gestione del Centro Unico Servizi (CUS) ed allargandosi alle altre direzioni. Si è deciso di adottare il Service Life Cycle usando come framework le best practice ITIL v.3 (2011), adattate (dove si è ritenuto opportuno farlo) alle peculiarità tecniche, organizzative e amministrative del contesto funzionale della Corte dei conti. In termini concettuali l'intera attività della DGSIA è stata rivista nell'ottica del concetto di "servizio", inteso (secondo ITIL) come *valore fornito in modo misurabile all'utenza* e di "processo" *trasversale* rispetto alle singole Direzioni. Dal punto di vista operativo, è stato avviato un progetto con risorse umane e materiali dedicate, che si è focalizzato sull'implementazione di alcuni dei processi delle fasi *Transition* ed *Operation* proprie del framework ITIL [1]. Nel corso dei mesi, il progetto ha prodotto quanto segue:

- Per la fase *Transition*, sono stati definiti i processi di:
  - Asset management;
  - Configuration management;
  - Change management;
  - Release and Deploy management.
- Per la fase *Operation*, sono stati definiti i processi di:
  - Incident management;
  - Problem management.

[1] per i dettagli si veda ad esempio `http://www.itil-italia.com/itilv3.htm`.

Va assolutamente chiarito che il "rilascio in esercizio" dei processi suddetti non è stato un atto puramente formale, ma ha portato alla revisione reale delle modalità di lavoro, (in termini di avvio, gestione e rendicontazione delle attività) e che esso ha riguardato l'intera catena dei fornitori ICT di Corte dei conti. Il cambiamento organizzativo è stato "epocale" e, come tale, ha avuto bisogno di alcuni mesi per essere accettato ed interiorizzato (sia dalle risorse umane di Corte dei conti che da quelle dei fornitori). Tuttavia, una volta terminato l'inevitabile periodo di adattamento, sono stati percepiti nettissimi miglioramenti in termini di qualità del lavoro, soddisfazione del personale, efficacia ed efficienza nel fornire i servizi all'utenza. Ovviamente l'introduzione di nuovi processi lavorativi ha richiesto a Cdc di dotarsi di un'opportuna piattaforma software a supporto. L'attività progettuale interna, relativa alla reingegnerizzazione dei processi interni attraverso ITIL, è tuttora in corso e si sta attualmente focalizzando su:

- Revisione del processo di Problem Management (in ottica di miglioramento continuo);
- Rilascio del processo di Service Level Management;
- Rilascio del processo di Request Fullfillment.

4.1.3 La gestione della sicurezza e della robustezza dei servizi IT

Riorganizzazione dell'ICT Security

La ristrutturazione dei processi in ottica ITIL ha portato necessariamente ad una riorganizzazione del settore ICT Security di DGSIA (facente capo al CUS), per adeguarlo alla nuova metodologia, che, fra l'altro, suggerisce fortemente una separazione netta fra gli ambiti di Service Operations (la conduzione dei sistemi) e quella di Service Design (la fase progettuale) in tutti i comparti, compreso quello della sicurezza.

Storicamente la gestione della sicurezza ICT, pur essendo sempre stata considerata fra le attività maggiormente "critiche", non aveva mai goduto di una propria "dignità" di specifico settore all'interno della conduzione dei sistemi. In particolare, i contratti che governavano la conduzione medesima non prevedevano espressamente la fornitura di competenze progettuali in tale settore, che ricadeva nel più generale ambito del networking. L'aumento del numero dei servizi esposti e delle minacce ai servizi stessi, le criticità riscontrate nel corso degli ultimi 3 anni e l'evidente necessità di dotarsi di maggiori competenze settoriali hanno portato, nel 2012, alla decisione di scorporare l'ambito ICT Security da quello della conduzione per migliorarne la qualità e l'efficacia. Per garantire la migliore flessibilità ed efficacia possibili, è stato quindi progettato il seguente scenario:

- è stata indetta una gara specifica per la fornitura di servizi di gestione della Sicurezza ICT, organizzata in due lotti di gara indipendenti (quindi le aziende vincitrici sono diverse);
- Il "Lotto 1" copre oggi la gestione day-by-day della sicurezza (Service Operation) e dei relativi apparati (implementazione di policy, definizione del routing, gestione ed analisi dei log di sicurezza, ecc.), operando principalmente da remoto tramite risorse localizzate presso un SOC (Security Operation Center);
- Il "Lotto 2" si occupa di tutti gli aspetti di progettazione e reingegnerizzazione delle infrastrutture di network e sicurezza, della produzione di policy e linee guida (Service Design), nonché delle verifiche preventive/successive sui silos applicativi (in particolare, "penetration testing" di pre- e post-passaggio in produzione).

Strategicamente la suddivisione in due sotto-forniture distinte ha consentito di ottenere il meglio possibile in termini di risorse umane e tecnologiche; il personale e le strutture dei due gruppi di lavoro collaborano attivamente, con il coordinamento del personale di Cdc e di Sogei, per la gestione degli incidenti di sicurezza (è presente una specifica procedura di analisi, contrasto ed escalation) e per la relativa remediation.

Ridisegno del modello IT Security di Cdc

La riorganizzazione dell'ICT Security ha consentito di poter dedicare risorse umane e materiali alle attività di Service Design (condotte come detto in precedenza dal personale del "Lotto 2"). Qui vengono riassunti i principali obiettivi raggiunti negli ultimi due anni.

Disegno nuova architettura "TO-BE" Da tempo era stata riscontrata la progressiva inadeguatezza dell'infrastruttura di network, bilanciamento e firewalling del CED primario, anche in termini di eccessiva complessità. Nel contempo andava definita correttamente l'architettura per il CED secondario. E' stata quindi avviata un'attività di analisi e ridisegno complessivo. Tale attività è stata in primo luogo focalizzata sull'analisi AS-IS dell'architettura di sicurezza dell'infrastruttura, in termini di servizi di sicurezza perimetrali e sistemi di protezione interna. L'analisi, effettuata solo a livello infrastrutturale (e non applicativo, poichè oggetto di un diverso processo di assessment), era tesa ad individuare il gap tecnologico rispetto alle migliori soluzioni di sicurezza sul mercato per il contesto di esercizio di Corte dei conti. La metodologia adottata durante le attività di Audit Infrastrutturale per il progetto "Audit dell'attuale Modello di Protezione Infrastrutturale" è descritta nel dettaglio in Figura 4.1, nella quale sono indicate le fasi dell'attività.

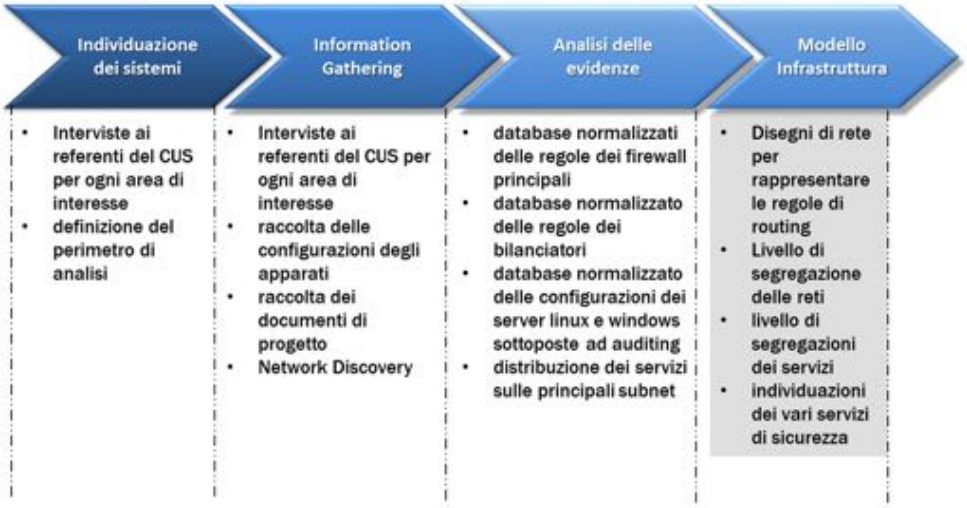


Figura 4.1: Metodologia adottata.

Il risultato di tale attività ha evidenziato numerose debolezze ed incongruenze ed ha permesso la riprogettazione dell'area di server farm e delle logiche di funzionamento di tutta la rete della Corte dei conti. Dall'analisi della situazione (AS-IS) si è quindi passati ad una definizione di uno scenario TO-BE, che consentisse di ottenere i seguenti risultati:

- Razionalizzazione dei firewall esterni e interni dei data center della Corte dei Conti;
- Separazione strutturata dei layer applicativi tra servizi di front-end (es. sistemi di accesso alla posta elettronica, servizi web, ecc.) e sistemi di gestione dei dati (es. banche dati, storage di mail, ecc.);
- Segregazione completa tra le diverse aree di sicurezza;
- Architetture gemelle in termini logici e funzionali fra data center primario e secondario.

Sono stati inoltre definiti una serie di requisiti di sicurezza ai quali qualsiasi infrastruttura, sia hardware che software, presente nella rete della Corte dei conti, deve adeguarsi. Tale progetto ha dunque permesso la realizzazione di una nuova infrastruttura di rete in grado di assicurare l'aderenza a tutti i requisiti di sicurezza, garantendo la funzionalità di tutte le componenti necessarie ed aumentando, in alcuni casi, la semplicità e la linearità delle soluzioni implementate.

Il processo di "Change e Release" specifico per le architetture di sicurezza in Cdc Nell'ambito del generale processo di Change & Release introdotto con la metodologia ITIL, si è deciso di "specializzare" il processo di

valutazione delle nuove architetture e di validazione dei requisiti di sicurezza minimi da applicare all'infrastruttura di rete di Corte dei Conti. Gli obiettivi specifici del processo sono i seguenti:

- Separazione;
- Segregazione;
- Monitoraggio;
- Sicurezza Passiva;
- Evitare la presenza di routing asimmetrico.

Il processo di valutazione delle nuove architetture prevede una serie di fasi da attivare secondo necessità, le cui principali sono:

- L'analisi della nuova architettura;
- La definizione eventuale di un tavolo tecnico;
- La definizione eventuale di una nuova Isola Applicativa.

Il processo di Change per regole di firewalling in Cdc Il processo di Change specifico per le modifiche di regole sui firewall è stato pensato nell'ottica di rendere più semplice la fase decisionale in carico al personale di Corte dei Conti/SOGEI e più rapida la fase di implementazione, a carico del personale del SOC. Nell'ambito di un Change complessivo, l'implementazione di una nuova policy sui firewall, e più in generale la modifica e/o cancellazione di una policy, è sempre prima richiesta da un "Richiedente" (personale di Corte dei conti, fornitore applicativo, conduzione sistemistica), poi validata da un "Referente di Area" (in casi complessi anche da una "Commissione di Approvazione"), ed infine attuata dal SOC (che ha in carico la gestione operativa dei firewall).

La metodologia per l'analisi e test di prodotti di ICT Security in Cdc Data la continua attenzione all'evoluzione tecnologica, il CUS è frequentemente coinvolto nell'analisi di nuove soluzioni tecnologiche nei vari ambiti di competenza, compresa la sicurezza ICT. Nel corso degli anni è stato definito un framework operativo per lo scouting tecnologico, che viene normalmente condotto con il supporto di SOGEI ed il coordinamento di un responsabile di Corte dei conti. Partendo da una definizione puntuale dei requisiti richiesti al nuovo "prodotto" oggetto di valutazione, per ognuno dei requisiti vengono individuati uno o più test raggruppati in due macro categorie:

- Valutazioni tecniche: definite e condivise da tutto il gruppo di lavoro, contribuiscono per il 70% al giudizio complessivo;
- Valutazione del gruppo di lavoro: definite e condivise dal gruppo di lavoro e contribuiscono per il 20% al giudizio complessivo.

Viene quindi stilata una "checklist" sul rispetto dei requisiti (che hanno ciascuno un valore pesato). Il punteggio massimo complessivo che una soluzione può totalizzare è 90 punti con scala a 0.5 punti. Per ognuna delle valutazioni sono utilizzati i seguenti metodi di controllo:

- *Intervista*: quando non è possibile/conveniente eseguire dei test sullo specifico requisito ci si attiene alle dichiarazioni del vendor;
- *Documentale*: al pari del precedente o in situazioni in cui si ritiene utile integrare i test è stato deciso affiancare documentazione ufficiale del vendor che attesta la rispondenza o meno a determinati requisiti.
- *Strumentale*: il metodo strumentale prevede la verifica del test mediante prova operativa eseguita alla presenza del team di valutazione nell'ambiente di test predisposto.
- *Qualitativo*: In alcuni casi non sarà possibile misurare il livello di validità della realizzazione di una funzionalità o gruppo di esse. In tali casi verranno riportate delle considerazioni (in modo descrittivo) che riassumano i risultati del test in base all'esperienza dell'analista ed alle best practice diffuse.

L'output complessivo del processo è un documento di valutazione delle varie soluzioni tecnologiche sotto esame, che servirà da riferimento per il successivo processo di acquisizione.

4.1.4 IT security presso Cdc

Presidi di sicurezza La configurazione degli apparati di sicurezza perimetrale ed interna, segue delle precise linee guida che, oltre ad adeguarsi ai fondamentali criteri di sicurezza validi nel campo dell'IT, sono state redatte proprio in base allo specifico contesto di Corte dei conti.

Tale organizzazione dell'intera infrastruttura della Corte dei conti è finalizzata ad assicurare la massima resilienza ad attacchi provenienti dall'esterno (internet) e minimizzare l'impatto sulle aree non attaccate direttamente. Inoltre assicura la corretta segregazione tra aree a diverso grado di sicurezza. La suddivisione in tre aree logiche separate, client, Esterna e Server Farm, è realizzata attraverso l'utilizzo di istanze virtualizzate dei firewall UTM. In particolare i firewall sono configurati in maniera differenziata per sopperire al meglio alle esigenze dei diversi ambienti. Esempio di tale diversificazione sono:

- l'applicazione di regole IPS sul Firewall perimetrale;
- terminazione di VPN site-to-site, con porzioni di data center in cloud è effettuata direttamente sul firewall interno;
- Terminazione delle VPN client-to-site per l'accesso alle reti di management è realizzata sul firewall client.

Sulla catena di navigazione, notoriamente critica sotto l'aspetto della sicurezza, sono presenti due presidi di sicurezza distinti che in parallelo analizzano e filtrano il traffico in ingresso ed uscita. Tali presidi si declinano tramite le seguenti architetture:

- Web Proxy;
- Piattaforma di AntiAPT.

A protezione delle piattaforme che rendono disponibili servizi erogati direttamente dalla Corte dei conti vi sono due presidi di sicurezza specifici:

- WAF (Web Application Firewall);
- Anti DDoS (network/applicativo).

Il Web Application Firewall è posto a protezione di tutti i servizi web indipendentemente che questi siano acceduti da rete interna o da rete pubblica. Le piattaforme di Anti-DDoS network e applicativo sono servizi esterni alla Corte dei conti che presidiano gli accessi pubblici.

Strategie per la definizione di policy di sicurezza La strategia utilizzata per la definizione delle politiche di sicurezza è basata sull'applicazione di opportuni requisiti definiti dalla Corte dei conti. Tali requisiti regolamentano tutti gli aspetti riguardanti le architetture presenti sulla rete. In particolare danno precise indicazioni in merito ai seguenti ambiti:

- posizionamento delle architetture in rete;
- definizione modalità di accesso;
- gestione del ciclo di vita delle utenze;
- definizione delle misure minime per l'aderenza al cogente;
- gestione corretta dei log;
- gestione del Ciclo di vita sicuro delle applicazioni.

Alcuni punti fondamentali della strategia adottata dalla Corte dei conti per la definizione di politiche di sicurezza architetturale sono di seguito declinate:

- Tutte le architetture proposte prima della loro validazione sono soggette ad un'analisi di dettagli finalizzata all'individuazione di tutti i flussi di comunicazione end-to-end coinvolti nell'erogazione del servizio verso l'utente finale;
- Va assicurata la segregazione tra gli ambienti di esercizio e collaudo, al fine di evitare qualsiasi tipo di commistione tra flussi applicativi che hanno SLA differenti e che afferiscono a basi di dati rispondenti a livelli di sicurezza diversi;
- Va assicurata la segregazione tra ambiente "client" e "server farm" al fine di assicurare un adeguato livello di sicurezza commisurato alla criticità degli ambienti garantendo, inoltre, la capacità di intercettare il traffico malevolo da e verso i client;
- nell'ambito Datacenter, per quanto concerne la componente Server, viene definita ed attuata una netta separazione tra il traffico di management e il traffico di erogazione del servizio;
- sono espressamente vietate condizioni di configurazione che consentano al traffico di "saltare" di tra zone contigue di protezione;
- è prevista la comunicazione tra host solo su protocolli opportunamente documentati a livello progettuale;
- sono espressamente vietate regole che abilitino la comunicazione subnet-to-subnet tranne casi particolari;
- sono espresamente vietate regole che abilitino la comunicazione da un'intera subnet verso un singolo IP (fatta eccezione per subnet client).

A completamento delle politiche di sicurezza sono state declinate in uno specifico sistema di black list e white list tutte le possibili configurazioni degli apparati di sicurezza.

Processo di gestione macchine infette Il processo può essere innescato o a fronte di un warning generato dalla piattaforma antivirus a valle delle regolari operazioni di scansione e monitoraggio, oppure da una segnalazione esterna lato utente. La fase successiva coinvolge la struttura del SOC che, tramite tool specifici, analizza i files sospetti ed investiga approfonditamente sulla natura della possibile infezione, al fine di delinearne sia il grado di profondità sul sistema impattato sia la potenziale capacità dello stesso di propagarsi verso altre risorse di rete. Qualora non si trattasse di un falso positivo, il SOC individuerà la più appropriata strategia di intervento e di comunicazione verso le opportune strutture di riferimento. Il SOC elaborerà la corretta procedura di rimozione dell'infezione. Tale procedura verrà consegnata al comparto di Service Operation al fine di applicarla sull'asset interessato. La procedura verrà conservata in un knowledge database come traccia di lesson learned per il futuro. Al contrario, qualora si trattasse di un falso positivo, il SOC produrrà un report relativo agli asset che presentano l'antivirus non funzionante. A fine attività viene comunque rilasciato un report finale. Tali fasi sono rappresentate in Figura 4.2.

Application Security L'application security consta di proxy di navigazione, AntiAPT, Web Application Firewall e Secure Software Development Life Cycle. Seguono dettagli su tali applicazioni.

Proxy di navigazione L'architettura proxy di Corte dei conti, prevede l'applicazione di due presidi di sicurezza che, lavorando in parallelo, garantiscono un adeguato livello di sicurezza. Tali componenti effettuano analisi statica (Antivirus) e dinamica (Anti APT) del traffico individuando la presenza di qualsiasi tipo di minaccia veicolata attraverso la navigazione.

AntiAPT La soluzione anti APT consiste in una componente web ed una componente mail che, lavorando in sinergia ed in maniera "quasi sincrona", riescono ad intercettare ed analizzare tutti i contenuti attivi sia sul flusso di navigazione che all'interno delle mail generando dinamicamente delle policy di blocco impedendo il download di contenuti malevoli.

WAF (Web Application Firewall) La soluzione di Web Application Firewall adottata in Corte dei conti intercetta ed analizza tutto il traffico da internet e dalle reti interne indirizzato verso le web application della Corte dei conti. Tale traffico è analizzato alla ricerca di eventuali attacchi presenti nelle richieste e bloccato o segnalato a seconda delle policy implementate. Tale protezione è presente sia sui front-end Internet sia su quelli interni al fine di intercettare attacchi provenienti dai client.

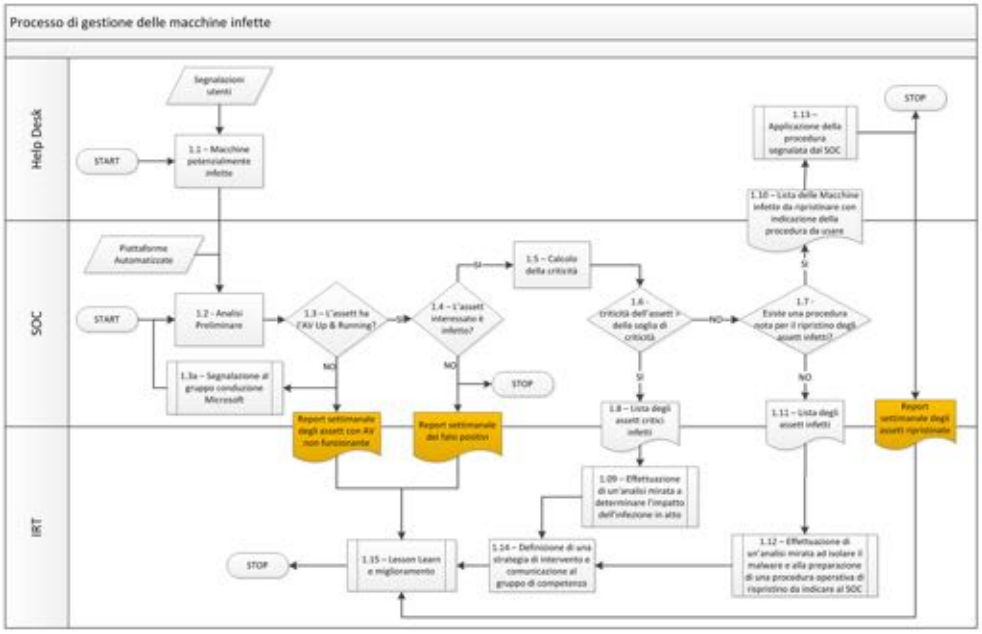


Figura 4.2: Processo di gestione macchine infette.

SSDLC (Secure Software Development Life Cycle) La Corte dei conti ha recentemente implementato ed adottato un processo di Secure Software Development Life Cycle, ossia un ciclo di vita sicuro del software atto a considerare ed implementare opportune attività di sicurezza nel corso nelle varie fasi di definizione dei requisiti, progettazione, sviluppo, test e manutenzione. Tale metodologia ha l'obiettivo di migliorare l'efficacia nella prevenzione del rilascio di software affetto da vulnerabilità di sicurezza, e si basa sul perfezionamento del proprio SDLC (Software Development Life Cycle) tramite l'introduzione della sicurezza come requisito cardine in ogni sua fase, come peraltro previsto da numerose best pratices (ISO/IEC 25000, PCI/DSS, ecc.).

4.1.5 Continuità operativa

Di concerto con le linee guida dettate dal nuovo Codice dell'Amministrazione Digitale (CAD), Corte dei Conti ha avviato le fasi necessarie ad implementarne le direttive in materia di Continuità Operativa, ossia Business Continuity (BC), e di Disaster Recovery (DR), con particolare riferimento all'assolvimento degli obblighi di cui all'art. 50-bis.

In Figura 4.3, è rappresentato il perimetro di riferimento per:

- La continuità operativa generale;
- La continuità operativa ICT.

Tali elementi sono da considerarsi indispensabili per la produzione dei documenti relativi al Piano di Continuità Operativa (PCO) e al Piano di Disaster Recovery (PDR). I piani sopra descritti sono adottati sulla base di uno studio di fattibilità tecnica, cui seguono le fasi di:

- Valutazione e Classificazione;
- Soluzione tecnica;
- Implementazione e verifica.

Figura 4.3: Continuità Operativa.

Lo studio di fattibilità prodotto da Corte dei conti ha ricevuto il parere positivo e di approvazione da parte di AgID (ex DigitPA). Nello studio sono state in particolare identificate le applicazioni "mission critical" alle quali deve essere garantita la più alta protezione in caso di disastro. I servizi che Corte dei Conti ha dichiarato "Mission Critical" sono sostanzialmente quelli legati all'immagine della Corte (quali il sito web), alla collaborazione (servizio di posta elettronica e documentale) e alle funzioni istituzionali (giurisdizione e controllo enti locali).

Gli scenari tecnologici adottati, a seconda delle diverse applicazioni da proteggere, fanno riferimento ad alcune metodologie di BC/DR definite come:

- *shared systems*, ovvero active-active;
- *hot standby*, ovvero il sito secondario è sempre allineato al primario, pronto ad essere attivato;
- *cold standby*, ovvero il sito secondario viene allineato al primario (restore di dati) in caso di disastro.

Perciò la strategia per replicare i dati, i sistemi e le applicazioni non è unica, ma varia a seconda del sito applicativo.

Negli scenari di Hot/Cold Standby, in caso di disastro sul sito primario potrà essere deciso di attivare il sito secondario. L'attivazione scelta è di tipo "Manuale", ovvero frutto di una decisione umana e di operazioni manuali o semi-automatiche. Negli scenari di Hot/Cold Standby, quando viene effettuata la ripartenza dei servizi sul sito secondario (failover) è poi possibile, in caso di ripristino del sito primario, la riattivazione (failback) dei servizi stessi sul sito primario.

Vediamo alcuni esempi di quanto realizzato. Il servizio di *posta elettronica* è stato dispiegato in modalità "shared system", ovvero active-active sui due siti. L'architettura dell'ambiente Exchange 2013 (che è totalmente virtualizzata su piattaforma MS Hyper-V) si basa su un *site service model* generale chiamato *unbounded*, realizzabile quando sono soddisfatti i seguenti prerequisiti:

- L'infrastruttura può essere realizzata usando due data center;
- I due data center sono connessi con un link con opportune caratteristiche di banda disponibile e latenza (DWDM);
- Ogni sede con utenti del servizio di posta elettronica dispone di un collegamento *ridondato* ad *entrambi* i data center;
- Ogni sede è in grado di contattare ognuno dei due data center, anche in caso di indisponibilità del link tra i due CED.

La soluzione Microsoft prevede di avere un DAG (Database Availability Group), distribuito sui server di via Baiamonti e La Rustica, contenente 5 copie di ogni database:

- Due copie residenti nel data center primario;
- Due copie nel data center secondario;
- Un'ulteriore copia *lagged* , sempre sul secondario.

Il *sito istituzionale* ed altri servizi critici sono stati invece implementati in modalità Hot Standby. La replica dei dati viene effettuata in modo sincrono lato Storage-array verso il sito secondario, dove è presente tutto lo "stack infrastrutturale IT" necessario al restart dei servizi. A fronte di un disastro nel senso letterale del termine, dal punto di vista della consistenza del dato, una soluzione del genere è capace di garantire "Crash Consistency" ma non "Application Consistency".

La *Crash Consistency* in una replica è l'equivalente della ripartenza dopo uno spegnimento dei server non pianificato. In particolare, la soluzione di replica, in questo caso ha una conoscenza limitata, o nulla, delle applicazioni sovrastanti. In seguito ad un failover, non ci sarà consistenza transazionale per quelle transazioni in corso durante il guasto. La *Application Consistency* assicura in una replica che tutte le transazioni siano complete e le informazioni in cache siano scritte su disco per garantire la consistenza.

Al contrario, per far fronte alle molteplici esigenze di interruzione programmata dovute ad interventi di manutenzione straordinaria sulle facility del CED primario (energia elettrica, condizionamento, ecc.) che possono perdurare anche oltre le 8 ore, una soluzione "hot standby" consente di ridurre il downtime dei servizi a livelli accettabili.

In modalità Cold Standby è stata implementata una soluzione di backup remoto, che utilizza una replica dei dati di backup deduplicati tra un sito e l'altro.

4.1.6 La cultura organizzativa come elemento abilitante alla replicabilità del modello organizzativo

La cultura organizzativa della Corte dei conti, l'esperienza condotta nello sviluppo del proprio settore IT, il costante confronto con le esigenze istituzionali e le offerte del mercato, costituiscono un patrimonio di competenze che pongono la Direzione Generale dei Sistemi Informativi Automatizzati (DGSIA) al centro del dibattito sulla razionalizzazione dei servizi IT della PA.

In questo contesto, la Corte dei conti si è fatta promotrice di un'iniziativa (IDEA@PA) volta ad individuare sinergie nell'ambito delle PA Centrali ed ha recentemente stipulato protocolli di intesa con alcune Amministrazioni per l'erogazione di servizi informatici utilizzando i propri Data Center, compatibilmente a quanto stabilito dalle linee guida DigitPA in materia di razionalizzazione dei Data Center della Pubblica Amministrazione.

Modello generale di integrazione Il CUS (Centro Unico Servizi), basandosi su best practice disponibili sul mercato, ha predisposto un modello, applicabile in qualsiasi contesto di integrazione, che prevede un processo di integrazione organizzativa, ripetibile per ogni iniziativa e composto delle seguenti fasi, ognuna delle quali con i propri obiettivi:

- *Accoglienza/Coesistenza*: minimizzare l'impatto del cambiamento e garantire la continuità delle esigenze primarie;
- *Adeguamento/Integrazione*: introduzione graduale delle modifiche in base alle esigenze degli ospiti e delle politiche dell'organizzazione ospitante;
- *Sviluppo/Consolidamento*: cooperazione totale e sfruttamento comune delle risorse. Risparmio e produttività.

Nella definizione delle singole fasi va considerato quanto segue:

- Cdc già dispone, presso i propri CED, di moderne infrastrutture che sono il frutto di recenti investimenti, e che sono in corso di razionalizzazione per l'uso condiviso (CNEL, Avvocatura di Stato);
- Le Amministrazioni ospitate potranno erogare servizi utilizzando configurazioni di alta affidabilità e, in futuro, con capacità di business continuity tra il CED primario e quello secondario, consentendo dunque il disaster recovery della totalità dei servizi;

- Cdc può assicurare direttamente una serie di servizi legati alla logistica e agli impianti, tra i quali:
  - sicurezza fisica del CED;
  - servizi collegati alla logistica del CED (manutenzione impianti, monitoraggio ambientale, gestione magazzino, ecc.);
  - monitoraggio delle infrastrutture (impiantistiche, logistiche, infrastrutturali);
  - approccio integrato alla sicurezza.

Considerato quanto sopra e allo scopo di minimizzare gli impatti in termini organizzativi e di disponibilità dei servizi, la prima fase del processo di integrazione è sempre focalizzata sulle componenti IT del data center. Le altre fasi progettuali verranno di volta in volta attivate a fronte di una valutazione di impatto ed opportunità, essendo particolarmente eterogeneo (specie in termini di dimensioni) l'insieme dei partner istituzionali coinvolti.

Integrazione con CNEL Corte dei conti e CNEL, con il patrocinio dell'Agenzia per l'Italia Digitale, hanno sottoscritto, in data 2 dicembre 2013, un accordo di collaborazione per la digitalizzazione della PA e la diffusione del cloud computing. Il primo obiettivo dell'accordo consiste nella fusione dei data center dei due Enti, con l'obiettivo di chiudere il data center del CNEL (ospitato presso la sede di Via Lubin, Roma) il prima possibile. Il comitato di gestione dell'accordo, seguendo le indicazioni di massima viste prima ed adottando una gestione progettuale di tipo agile, ha messo in atto tutta una serie di attività che hanno portato ai seguenti risultati:

- Il CNEL è stato interconnesso al data center primario di Corte dei conti tramite il Sistema Pubblico di Connettività(SPC), alla stregua di una sede periferica di Corte;
- Tutti i servizi destinati all'utenza del CNEL sono oggi forniti tramite le infrastrutture tecnologiche di Corte dei conti;
- A breve sarà possibile dismettere completamente il data center del CNEL, ottenendo il primo risultato reale della politica di riduzione del numero dei data center della PA italiana voluta da AgID.

Nei prossimi mesi, compatibilmente con i tempi della riforma costituzionale in via di approvazione in Parlamento (che prevede la cancellazione del CNEL), verranno avviate le successive fasi del modello di integrazione, partendo dalla fusione dei servizi di collaborazione (posta elettronica e documentale).

Integrazione con Avvocatura Generale dello Stato È stato recentemente firmato un accordo istituzionale fra Cdc e Avvocatura Generale dello Stato (AGS) per l'unificazione dei data center. Date le dimensioni (1.500 utenti, 26 sedi) di AGS, pari circa alla metà di Cdc, si è scelto un approccio progettuale più classico e graduale rispetto a quanto fatto con il CNEL. In questi giorni è in avanzata fase di redazione (a cura di SOGEI) lo studio di fattibilità per la fusione, che sarà presentato ai vertici istituzionali di entrambi gli enti nelle prossime settimane. Nello studio vengono in particolare definite le linee guida tecniche ed organizzative per l'integrazione dell'erogazione dei servizi. I primi risultati del progetto sono previsti per la seconda metà del 2015.

4.2 INPS

L'Istituto ha fatto della tecnologia informatica il suo elemento trainante ed abilitante per lo svolgimento dei suoi compiti istituzionali, prestando particolare attenzione alla cura dei rapporti con i suoi utenti finali. A tal fine, negli ultimi anni, l'Istituto ha completato un processo di completa telematizzazione della sua azione amministrativa giungendo a rendere esclusivo l'utilizzo degli strumenti telematici per l'inoltro di qualsiasi istanza. Al fine di venire incontro alle esigenze di tutti i cittadini ha creato una rete di servizi di tipo multicanale (internet, contact center, intermediari, mobile, PEC, fax, ..) per consentire a chiunque l'individuazione delle modalità più idonee alle proprie capacità e conoscenze informatiche. Un tale forte processo di telematizzazione non può prescindere da una infrastruttura di sicurezza IT capace di garantire la riservatezza, l'integrità e la disponibilità dell'enorme mole di informazioni che tratta. A tal fine si è dotata di una struttura organizzativa e tecnologica dedicata ai servizi di sicurezza IT che viene illustrata in questa breve sintesi.

Questo Case Study descrive le esperienze nel campo ICT condotte da INPS (e nello specifico della sua struttura per l'ICT Security) in termini di riorganizzazione funzionale e di ridefinizione dei processi di gestione. Verrà esposta la realtà tecnologica di INPS, descritta la struttura organizzativa a supporto dell'ICT e i progetti che, negli ultimi anni, hanno portato ad una complessiva rivisitazione dell'offerta di servizi all'utenza, garantendo continuità e sicurezza di dati ed infrastrutture.

4.2.1 Contesto

L'INPS è tra i più grandi e complessi enti previdenziali d'Europa, gestisce la quasi totalità della previdenza italiana ed ha un bilancio che per entità è secondo solo a quello dello Stato. Sono assicurati all'INPS la maggior parte dei lavoratori dipendenti del settore pubblico e privato e dei lavoratori autonomi. Nato oltre cento anni fa, allo scopo di garantire i lavoratori dai rischi di invalidità, vecchiaia e morte, l'Istituto ha assunto nel tempo un ruolo di crescente importanza, fino a diventare il pilastro del sistema nazionale del welfare.

Le principali tappe

L'Istituto nasce all'inizio del secolo scorso e negli anni ha assunto sempre maggiori funzioni incorporando, fino alla fine dello scorso secolo, diversi altri enti tra cui l'INAM (Istituto Nazionale per l'Assicurazione contro le Malattie), l'ENAOLI (Ente Nazionale Assistenza Orfani Lavoratori Italiani), lo SCAU (Servizio per i Contributi Agricoli Unificati). Nel 2003 l'INPDAI (Istituto Nazionale Previdenza per i Dirigenti di Aziende Industriali) confluisce nell'INPS con il conseguente trasferimento all' Istituto di tutte le sue funzioni. Nel 2004 è stata approvata la legge delega sulla riforma delle pensioni. La maggior parte delle novità introdotte dalla riforma sono operative dal 2008. Nel 2007 viene approvata una legge che modifica nuovamente i requisiti richiesti per l'accesso al trattamento pensionistico e le finestre di uscita dal lavoro. Tra i punti salienti della riforma la revisione automatica dei coefficienti di trasformazione che incidono sul calcolo della pensione. Nel 2007 viene aggregata la Cassa di Previdenza per l'Assicurazione degli Sportivi SPORTASS. Nel 2009 una nuova legge di riforma dispone che i requisiti di età per ottenere la pensione vengano adeguati all'incremento della speranza di vita accertato dall'Istat. La diffusione del nuovo strumento dei buoni lavoro per il pagamento del lavoro occasionale accessorio, nuove norme e sinergie istituzionali rafforzano il ruolo dell'Istituto nel contrasto al lavoro nero e nel recupero dei crediti contributivi. Nel 2010, dal 31 maggio, l'IPOST (Istituto Postelegrafonici) viene soppresso e tutte le sue funzioni vengono trasferite all'INPS. Nel 2011 vengono soppressi INPDAP (Istituto nazionale di previdenza per i dipendenti dell'amministrazione pubblica) ed ENPALS (Ente Nazionale di Previdenza e di Assistenza per i Lavoratori dello Spettacolo) e viene disposto, al 31 marzo 2012, il trasferimento all'IINPS di tutte le competenze dei due Enti al fine di rendere più efficiente ed efficace il servizio pubblico, assicurando cosi ai cittadini un unico soggetto interlocutore per i servizi di assistenza e previdenza.

Le principali attività dell'Istituto

L'attività principale consiste nella liquidazione e nel pagamento delle pensioni e indennità di natura previdenziale e assistenziale.

Prestazioni previdenziali: Le pensioni sono prestazioni previdenziali, determinate sulla base di rapporti assicurativi e finanziate con i contributi di lavoratori e aziende pubbliche e private.

Prestazioni a sostegno del reddito: L'INPS gestisce anche le prestazioni assistenziali - interventi propri dello "stato sociale" - volte a tutelare i lavoratori che si trovano in particolari momenti di difficoltà della loro vita lavorativa e provvede al pagamento di somme destinate a coloro che hanno redditi modesti e famiglie numerose. Per alcune di queste prestazioni l'INPS è coinvolto solo nella fase di erogazione; per altre svolge tutto il procedimento di assegnazione. Gestisce anche la banca dati relativa al calcolo dell'ISE (indicatore della situazione economica) utilizzato dai Comuni per concedere gli assegni per il nucleo familiare e per la maternità, e dell'ISEE (Indicatore della Situazione Economica Equivalente), che permette di usufruire di alcune prestazioni sociali agevolate.

Il Pubblico Impiego: Con l'acquisizione delle funzioni della gestione ex INPDAP, l'INPS eroga trattamenti pensionistici di fine servizio e rapporto e le prestazioni di carattere creditizio e sociale per dipendenti e pensionati pubblici. Tali prestazioni includono prestiti e mutui; borse di studio per la frequenza di scuole medie e superiori, università, master post universitari e dottorati di ricerca; vacanze sport in Italia e vacanze studio all'estero; accoglienza di studenti in convitti di proprietà o in convenzione; stage all'estero; soggiorni in Italia e ospitalità in case albergo per anziani e in strutture residenziali convenzionate per malati di Alzheimer.

La Vigilanza: L'INPS ha anche compiti di vigilanza svolti dagli ispettori dotati di strumentazione telematica, che consentono l'interrogazione di banche dati interne ed esterne all'INPS. L'obiettivo è l'affermazione del rispetto dei diritti previdenziali ed assicurativi e la garanzia di eque condizioni di concorrenza tra le imprese sul mercato.

L'INPS: i numeri dello stato sociale

Il gran numero di attività svolte dall'Istituto è testimoniato anche dalle cifre:

- oltre 40,7 milioni di utenti;
- 23,4 milioni di lavoratori (l'82% della popolazione occupata in Italia);
- 1,4 milioni di imprese;
- 16 milioni di pensionati;
- 21 milioni di pensioni erogate ogni mese, compresi i trattamenti agli invalidi civili;
- 4,4 milioni di persone che ricevono prestazioni a sostegno del reddito;
- 10,4 miliardi di euro spesi ogni anno per il sostegno alla famiglia;
- 22,7 miliardi di euro spesi ogni anno per il sostegno del reddito.

Gli organi istituzionali

La governance dell'Istituto è assicurata dai seguenti organi:

- il Presidente che ha la legale rappresentanza dell'ente, predispone il bilancio e i piani di spesa e investimento e attua le linee di indirizzo strategico dell'Istituto;
- il Consiglio di Indirizzo e Vigilanza, attualmente composto da 24 membri rappresentanti tutte le forze sociali, che ha il compito di fissare gli obiettivi strategici e di approvare i bilanci;
- il Direttore Generale che è il responsabile del conseguimento degli obiettivi e coordinatore della tecnostruttura;
- il Collegio dei sindaci che vigila sull'osservanza della legge e sulla regolarità contabile dell'Istituto;
- il Magistrato della Corte dei Conti che esercita un controllo continuativo sulla gestione dell'Istituto;
- i Comitati Regionali e Provinciali che stabiliscono regole, decidono sui ricorsi e formulano proposte normative in materia di prestazioni e contributi.

4.2.2 Evoluzione dei servizi IT in INPS

L'Istituto, essendo chiamato sempre più a rispondere ad obiettivi sfidanti per far fronte alla continua evoluzione degli strumenti di aiuto allo stato sociale, ha fatto della leva tecnologica il suo fattore abilitante e trainante. L'uso sempre più pervasivo degli strumenti ICT ha consentito di far fronte ad un perimetro di azione sempre più ampio nonostante i seguenti fattori:

- calo progressivo del numero di dipendenti determinato dalle norme di blocco del turnover;
- continuo arricchimento dei compiti e delle attività determinate dalla continua evoluzione del contesto sociale e dell'arricchimento delle proprie funzioni determinato dall'incorporazione degli enti disciolti.

Il seguente grafico illustra chiaramente l'aumento della produzione equivalente a fronte di una continua riduzione del personale.

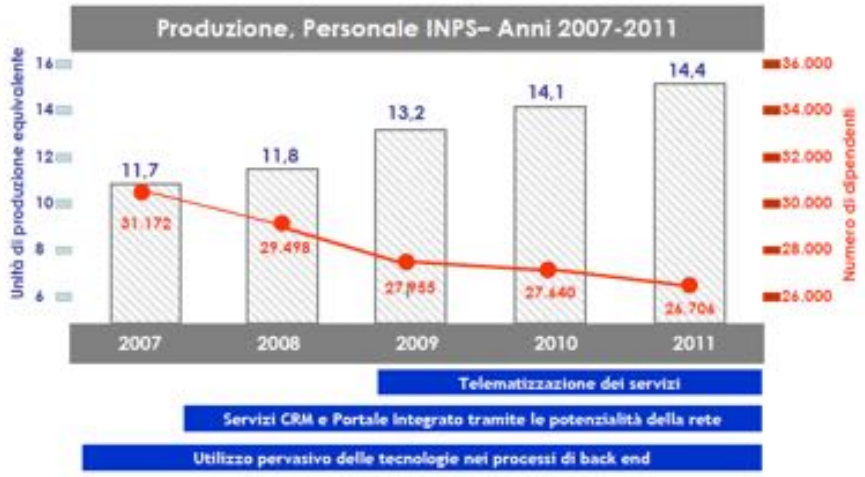


Figura 4.4: Riduzione del personale vs aumento dei servizi

La trasformazione dell'Ente ha sfruttato in modo intelligente le potenzialità dell'informatica e delle tecnologie della comunicazione in modo da:

- cogliere l'opportunità di miglioramento offerta dall'efficientamento dei costi attraverso l'adozione di tecnologie innovative finalizzate alla qualità dei servizi e all'adozione di una rete di servizi di tipo multicanale;
- ridurre i costi per tutti gli utenti dell'Istituto, legati alla burocrazia, mettendo a frutto le potenzialità offerte dall'uso pervasivo dell'ICT.

Al fine di garantire la qualità dei servizi e i benefici forniti dalla tecnologia l'INPS ha adottato anche tecniche di Customer Experience Management (CEM) per migliorare i processi di servizio verso il cliente, innescando un processo virtuoso di miglioramento della qualità del servizio

Principali fasi evolutive del Sistema Informativo

Il sistema informativo INPS moderno ha avuto inizio alla fine degli anni'60 e ha visto ed integrato i diversi cicli di riorganizzazione, adeguamenti strutturali e innovazioni tecnologiche che si sono succeduti fino ad oggi:

- Fine anni '60 adottano il primo sistema centrale IBM 360;

- Metà anni ’70 si adottano i primi sistemi dipartimentali IBM 3790 / 8100 presso le sedi provinciali interconnessi con il centro nazionale;
- Fine anni ’80 introduzione dei sistemi dipartimentali IBM AS/400;
- Fine anni ’90 adozione dei primi server open e pubblicazione del primo sito internet;
- 2001 pubblicazione del servizio estratto conto online con PIN (primi servizi online autenticati);
- 2003 attivazione del centro di Disaster Recovery;
- 2004 Sportello Virtuale Unico INPS-INAIL 803.164;
- 2006 accesso alla rete SPC della pubblica amministrazione;
- 2006 attivazione dei servizi di Business Continuity;
- 2010 introduzione dell’architettura SOA;
- 2010 avvio processo di completa telematizzazione dei servizi: tutte le istanze possono essere presentate all’INPS esclusivamente attraverso strumenti telematici, direttamente dai cittadini o per il tramite degli intermediari autorizzati (patronati, CAF, consulenti, associazioni di categoria, ecc.).

Figura 4.5: Crescita dei servizi al crescere della maturità tecnologica

La rete dei servizi

L’INPS offre un’ampia e complessa gamma di servizi e prestazioni accessibili direttamente dal portale internet dell’Istituto (www.INPS.it). Il portale web rappresenta sempre più il canale fondamentale nel rapporto con l’utenza, offrendo la possibilità di usufruire dei servizi in modo diretto e connotandosi come un caso d’eccellenza rispetto ai portali puramente informativi. Le informazioni e i servizi, che si avvalgono di circa 21.000 pagine web, sono fruibili 24 ore al giorno, 7 giorni alla settimana. Il portale web è il canale preferenziale ma, per venire incontro alle esigenze tutte le categorie di utenti, è stata creata una rete multicanale di accesso costituita da:

- Portale internet;
- Applicazione mobile per Android e iOS;
- Contact Center;
- Fax;

- SMS;
- Email / PEC;
- Intermediari (patronati, CAF, consulenti, altre P.A., ecc.).

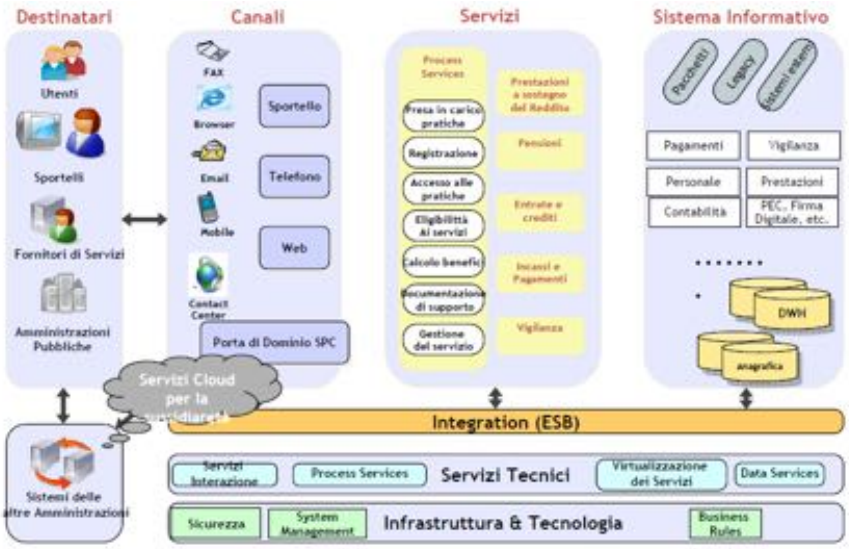


Figura 4.6: Schema generale della rete INPS

Dimensioni del sistema informativo

Il sistema informativo dell'INPS nasce con un'architettura host centrica ed evolve ad oggi verso standard di architettura open. Alcune cifre:

- Mainframe: 28.000 Mips;
- Server Risc (IBM + SUN): 10 (oltre 500 processori);
- Server logici (fisici e virtuali) su piattaforma Intel: 2.000 (oltre 11.500 core);
- Dimensioni Storage: oltre 2 PetaByte (incluso Disaster Recovery e business Continuity);
- Patrimonio applicativo: circa 5,5 milioni di punti funzione;
- Postazioni di lavoro (fisse e mobili): circa 38.000.

Architettura del sistema informativo

Il sistema informativo è fondato su una architettura a 3 siti a garanzia della Business Continuity e del Disaster Recovery: due siti in campus per la continuità operativa e un sito di disaster recovery a protezione da eventi disastrosi.

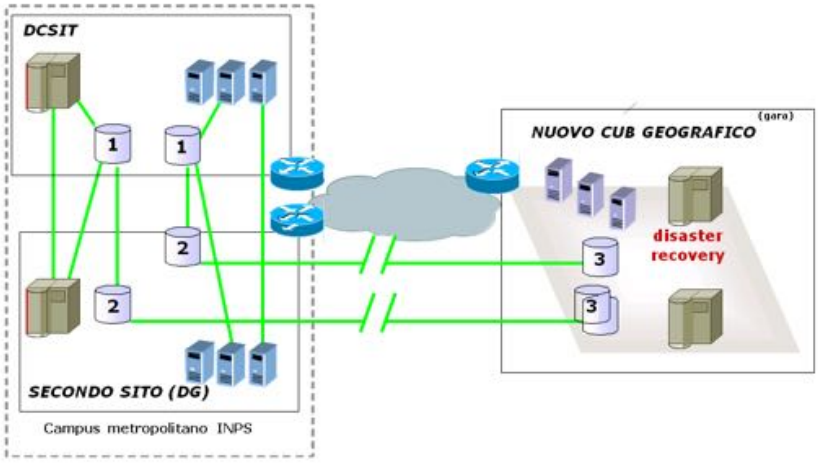


Figura 4.7: Architettura del sistema informativo INPS

4.2.3 La Gestione della sicurezza dei servizi IT in INPS

La necessità di garantire la conformità dei servizi istituzionali rispetto alle direttive ed alle disposizioni normative del settore in cui INPS opera, richiede un impegno costante nell'armonizzazione e nel governo della sicurezza tra i diversi ambiti aziendali.

Organizzazione della sicurezza ICT

Il governo della sicurezza informatica è affidato all'area dirigenziale Sicurezza ICT della Direzione Centrale Sistemi Informativi e Tecnologici che opera principalmente in sinergia con la Direzione Centrale Audit e l'Ufficio Centrale di Monitoraggio e Coordinamento in materia di protezione dei dati personali e accesso alle banche dati.

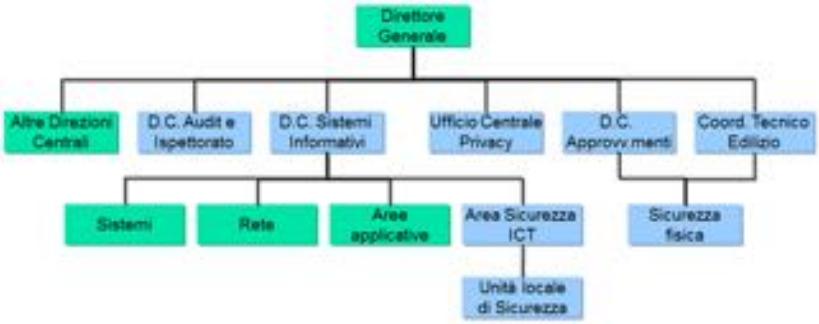


Figura 4.8: Organigramma per la gestione della sicurezza

All'interno della Direzione Centrale Sistemi Informativi e Tecnologici è stata costituita l'ULS (Unità Locale di Sicurezza) che è composta da personale interno coadiuvato da un team di consulenti che costituiscono l'IRT (Incident Response Team). Tutto ciò al fine di disporre di una migliore capacità nella gestione della sicurezza informatica e degli incidenti di tipo informatico. L'obiettivo è di poter fornire all'Amministrazione servizi allineati con le migliori pratiche di sicurezza ed in linea con le linee guida e le normative di riferimento. L'ULS risponde di-

rettamente al Responsabile dell'Area Sicurezza ICT e si avvale di referenti delle seguenti Aree interne alla Direzione Centrale Sistemi Informativi e Tecnologici (DCSIT)

- Area sicurezza ICT;
- Area Architetture e TLC;
- Area Gestione del Ciclo di Vita del Software;
- Area Portale (Internet/Intranet/Extranet) e Comunicazione;
- Area Esercizio Applicazioni;
- Staff del Direttore DCSIT.

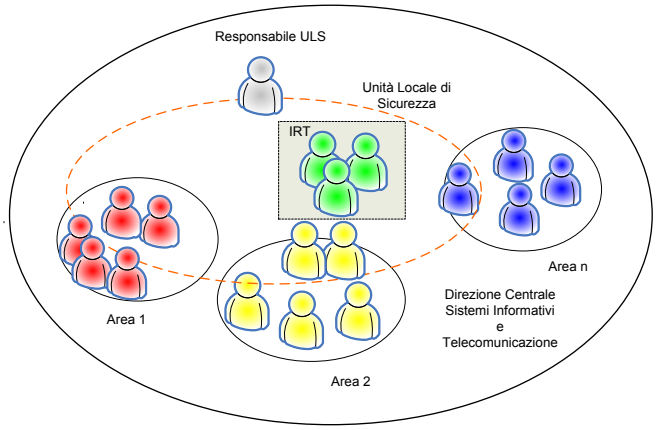


Figura 4.9: Schema Unità Locale di Sicurezza (ULS)

Le aree coinvolte nell'ULS sono tutte quelle con competenza in ambito infrastrutturale e di conduzione del sistema informativo. I referenti di tali aree, all'interno dell'ULS, garantiscono il loro supporto per le attività relative al proprio ambito di competenza. Al fine di garantire all'ULS il pieno supporto nelle fasi di identificazione e mitigazione degli incidenti di sicurezza sono stati individuati alcuni referenti per le seguenti aree funzionali:

- Database;
- Sistemi operativi Microsoft;
- Sistemi operativi UNIX (AIX, Linux, SUN Solaris, etc);
- Sistema centrale mainframe;
- Network;
- Sicurezza perimetrale IDS/IPS/Firewall/proxy (SOC interno);
- Gestione della continuità operativa, backup e monitoraggio;
- Identity Management;
- Conduzione applicazioni intranet;
- Conduzione applicazioni internet;
- Posta elettronica e PECs;
- Active Directory;
- Gestione delle postazioni di lavoro.

Gestione degli incidenti La gestione degli incidenti viene condotta attraverso un processo strutturato che prevede le seguenti fasi: identificazione, classificazione, notifica, risposta, ripristino e analisi post-mortem. Ogni fase prevede un workflow strutturato che guida nello svolgimento delle varie fasi e che consente di standardizzare il flusso delle decisioni e delle valutazioni in modo da garantire processi di gestione più reattivi. Il workflow guida nell'attribuire del corretto livello di rischio dell'incidente e di decidere le eventuali azioni di comunicazione ed escalation da compiere. Sulla base della gravità dell'incidente possono essere innescati processi di escalation, di tipo informativo o decisionale, verso il Dirigente dell'Area Sicurezza ICT e verso i Direttori sovraordinati. Tutte le fasi di gestione di un incidente sono registrate attraverso un sistema di tracking al fine di:

- tenere traccia di tutte le azioni, le comunicazioni e le evidenze raccolte durante tutto il processo di gestione di un incidente;
- costituire una knowledge base a cui fare riferimento per la gestione di incidenti futuri;
- produrre report sugli incidenti.

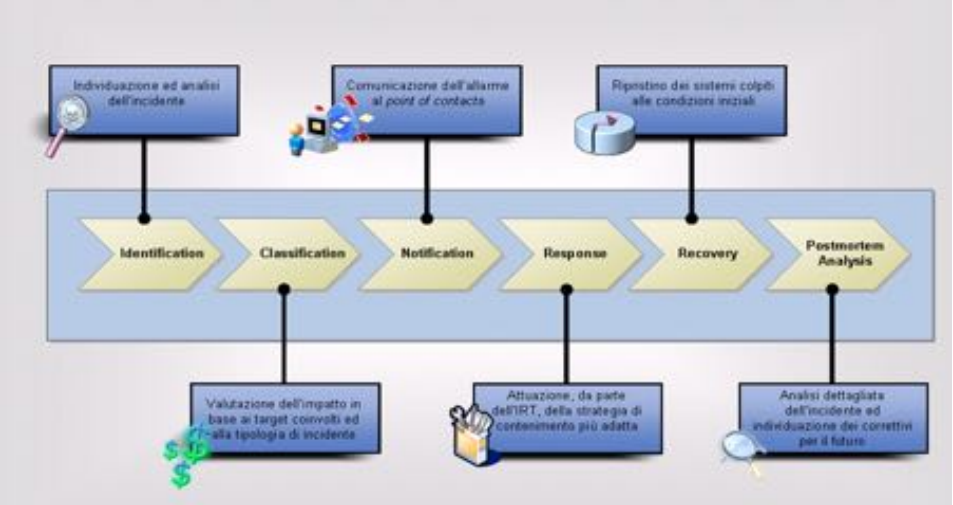


Figura 4.10: Gestione Incidenti

L'Incident Response Team (IRT) All'interno dell'attuale struttura organizzativa dell'ULS, l'IRT è l'Unità Operativa che, attraverso un processo strutturato, svolge i seguenti compiti:

- contribuire al coordinamento del processo di gestione degli incidenti garantendo:
  - una appropriata analisi degli incidenti;
  - il supporto consulenziale per assicurare una risposta efficace, il ripristino del normale livello e/o qualità di servizio nel minor tempo possibile, la salvaguardia del bene informativo aziendale, la minimizzazione o eliminazione dell'impatto sul business, la centralizzazione e non duplicazione degli sforzi;
- aggiornarsi costantemente sulle minacce, sugli attacchi e sulle evoluzioni tecnologiche collocandosi come centro di competenza e riferimento autorevole per l'ULS e per l'Istituto;
- analizzare e approfondire eventuali vulnerabilità sui sistemi e sulle infrastrutture IT fornendo suggerimenti per la prevenzione (Early Warning);

- contribuire, supportando il Responsabile dell'ULS, ad incrementare la consapevolezza degli utenti rispetto alle minacce ed alle vulnerabilità in materia di sicurezza IT;
- gestire, tramite procedure e flussi formalizzati, il processo di notifica dell'incidente ed il coinvolgimento delle entità interne all'Istituto;
- coordinare e monitorare le attività operative di risposta agli incidenti informatici;
- predisporre e comunicare con cadenza periodica rapporti e indicatori sulla gestione degli incidenti;
- essere il soggetto preposto alla raccolta ed all'analisi degli indicatori, forniti dai sistemi di gestione della sicurezza in essere presso l'Istituto, volti alla misurazione dell'efficacia e dell'efficienza dei processi di sicurezza implementati;
- contribuire al miglioramento/adeguamento delle misure di sicurezza implementate, con particolare riferimento alla sicurezza logica perimetrale;
- fornire, sulla base degli strumenti e dei dati a disposizione dell'IRT della conoscenza degli incidenti, informazioni e consigli utili volti a migliorare la qualità del sistema di gestione della sicurezza delle informazioni;

Modalità di ingaggio dell'IRT L'IRT dispone dell'accesso a molteplici strumenti di monitoraggio e analisi delle informazioni di sicurezza attraverso i quali effettua autonome attività di analisi. Attraverso l'esperienza continua acquisita durante la gestione di incidenti realizza autonomi strumenti di controllo e di alerting al fine di identificare segnali di rischio che richiedono approfondimenti. Attraverso tali strumenti l'IRT è in grado di rilevare autonomamente eventuali minacce ed innescare i processi di gestione di un incidente. Le fonti di informazioni sono essenziali per una efficace azione di prevenzione e reazione a possibili incidenti ma è altrettanto importante avere una rete di segnalazione che consente di innescare tempestivamente un processo di gestione di un incidente. Per tale motivo, all'interno del contesto tecnologico e organizzativo dell'INPS, l'IRT rappresenta un punto di contatto unico per tutte le segnalazioni che possono avere un impatto sulla sicurezza. Rappresentano fonti di identificazione e di segnalazione all'IRT di un potenziale incidente le seguenti entità:

- ***Presidi di sicurezza***: i diversi presidi di gestione dei sistemi di sicurezza (FW, AV, NIDS, VA, policy compliance, sicurezza DB, CLOG, IAM, ecc..) hanno un accesso diretto alla piattaforma di tracking degli incidenti attraverso la quale posso comunicare all'IRT potenziali incidenti allegando eventuali evidenze.
- ***Membri ULS***: per gli ambiti di propria competenza ogni membro dell'ULS è tenuto a comunicare all'IRT ogni evento sospetto o allarme generato dai sistemi di controllo e monitoraggio in dotazione.
- ***Responsabili per l'assistenza informatica periferica***: presso ogni sede regionale è costituito un Gruppo per l'Assistenza Informatica (GAI) con il compito di fornire assistenza agli utenti interni nella gestione delle postazioni di lavoro nell'utilizzo delle procedure informatiche; il GAI fornisce anche supporto all'utenza esterna nell'uso delle procedure web. è compito di tali responsabili segnalare all'IRT ogni evento che possa costituire un rischio di sicurezza con particolare riferimento al rispetto delle politiche sull'utilizzo degli strumenti informatici.
- ***Qualsiasi utente interno***: contattando direttamente l'IRT o per il tramite dell'Help Desk.
- ***CERT-PA.***

4.2.4 Principali servizi di Sicurezza

Governo della Sicurezza L'Istituto si è dotato di un insieme di politiche di sicurezza orientate a regolamentare i processi di progettazione, gestione e utilizzo delle componenti del sistema informativo oltre che regolamentare l'utilizzo degli strumenti informatici da parte degli operatori, in conformità alle normative ed ai regolamenti vigenti nonché alle principali best practices in tema di data privacy e sicurezza IT. Particolare rilevanza ha la "Politica per l'utilizzo degli strumenti informatici", divulgata a tutti i dipendenti, che regolamenta i comportamenti consentiti nell'utilizzo delle postazioni di lavoro, della navigazione internet, della posta elettronica e degli altri strumenti

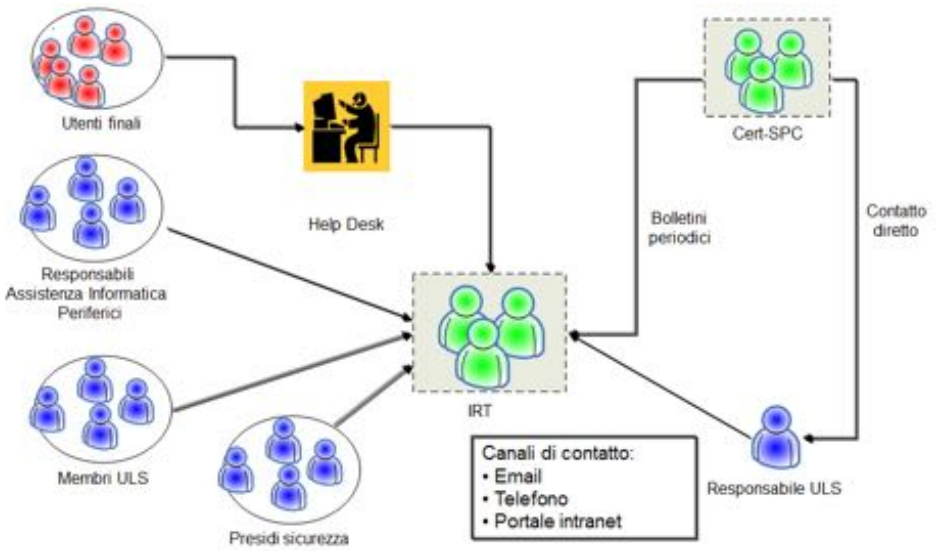


Figura 4.11: Modalità di ingaggio dell'Incident Response team (IRT)

di comunicazione. Sono anche definite le politiche di tracciamento delle operazioni effettuate e le modalità di trattamento e i tempi di conservazione dei log prodotti. Oltre alla divulgazione della "Politica per l'utilizzo degli strumenti informatici", al fine di sviluppare una consapevolezza diffusa delle tematiche di sicurezza (Security Awareness) e dunque incidere con misure preventive sul fattore umano, sono stati realizzate alcune semplici guide interattive in autoapprendimento su alcune tematiche quali: lo spam, il phishing, il social engineering, il malware, la firma digitale, Data Privacy, ecc. Nell'ambito delle attività di governo della sicurezza rientrano le attività di verifica della compliance attuata attraverso la rilevazione, con l'ausilio di strumenti automatici di Vulnerability Assessment, della configurazione dei sistemi che viene confrontata con le baseline e i controlli definiti dal sistema di sicurezza. Le non conformità e le vulnerabilità rilevate sono comunicate, attraverso un sistema di gestione del workflow, agli amministratori di sistema per le opportune attività di remediation. è inoltre assicurata la conformità alle disposizione del Garante per la protezione dei dati personali in merito alle misure di trattamento dei dati personali e agli specifici provvedimenti.

Identity e Access Management per utenti internet Per la numerosità delle funzioni svolte e dei servizi web offerti, l'INPS consente l'accesso ai servizi online ad una grande varietà di categorie di soggetti esterni, contando oggi circa 15,8 milioni di utenti registrati. Considerate le peculiarità, la varietà di soggetti e la loro numerosità, l'INPS ha sviluppato un proprio sistema di Identity e Access Management che, partito nel 2001, si è sempre più evoluto in un sistema capace di gestire l'accesso di una così grande platea di utenti attraverso un sistema di profilazione multiprofilo che adotta schemi di user provisioning molto flessibili.

Il sistema di accesso consente l'accesso con diversi schemi di autenticazione:

- codice fiscale e PIN (attribuito online);
- codice fiscale e PIN (di tipo dispositivo);
- codice fiscale e PIN con OTP (One Time Password);
- codice fiscale e 4 caratteri casuali del PIN per gli accessi tramite Contact Center;
- Carta Nazione dei Servizi (CNS);
- Attraverso credenziali di altri Identity Provider SAML 2.0 compliant.

L'evoluzione delle reti di servizi online delle pubbliche amministrazioni richiede sempre più il ricorso a nuove credenziali di autenticazione. Considerata la complessità di gestione di un sistema di Identity e Access management è sempre più frequente il ricorso a schemi di Identità Federata per favorire l'accesso ai servizi online di altre pubbliche amministrazioni. A tal fine l'INPS, in qualità di Identity Provider, per accelerare il processo di digitalizzazione della pubblica amministrazione ha reso disponibile l'utilizzo del proprio sistema di accesso, e dunque delle relative credenziali gestite, anche ad altre amministrazioni pubbliche, rendendo immediatamente disponibile una così vasta platea di utenti registrati. L'iniziativa consente ad altre amministrazioni di rendere subito fruibili i propri servizi online senza affrontare un processo complesso e dispendiOSo di provisioning e gestione di proprie credenziali. Sotto questi presupposti attraverso le credenziali INPS è possibile accedere:

- Dal 2010 ai servizi di Equitalia;
- da fine 2014 ai servizi INAIL per i cittadini;
- da marzo 2015 al servizio di dichiarazione 730 precompilata sul sito dell'Agenzia delle Entrate (in fase di definizione).

Alcuni dati dimensionali aggiornati al 31/10/2014:

- Numero di credenziali rilasciate: 15.811.514;
- Numero di credenziali con profilo di intermediario o ente pubblico: 435.086;
- Numero di servizi profilati: oltre 200.

Si riporta in Tabella 4.1, per tipologia di accesso, il numero degli accessi (intesi come autenticazioni), nel periodo gennaio - ottobre 2014:

Tabella 4.1: Numero di accessi per modalità di accesso

Modalità di accesso	Totale accessi	Media accessi giornalieri	Picco di accessi giornalieri
Web con PIN	105934897	348470	845014
Web con CNS	566499	1875	6173
App mobile con PIN	727936	2394	4790
Contact center con sub-PIN	449862	1691	6409

Infine, si riportano nel seguito i servizi di identità federata, nel periodo gennaio - ottobre 2014:

- Numero di accessi in qualità di Identity Provider verso altri enti: 19.608.944;
- Numero di utenti che hanno acceduto a servizi di altri enti con le credenziali INPS: 2.060.434;
- Numero di accessi in qualità di Service Provider per altri Enti: 375.194;
- Numero di utenti che hanno acceduto a servizi INPS con le credenziali di altri Enti: 37.842;

Servizi di sicurezza perimetrale e delle postazioni di lavoro La sicurezza perimetrale è affidata alle seguenti misure:

- Firewall, IDS, IPS;
- Web Application Firewall;
- Proxy con funzioni di content filtering e antimalware;
- Protezione contro APT e zero day attack.

I servizi di firewalling garantiscono la segmentazione e l'isolamento delle subnet che identificano zone a sicurezza differenziata.

La sicurezza delle postazioni di lavoro è affidata alle seguenti misure:

- Agli utenti non sono assegnati permessi privilegiati per prevenire modifiche alle configurazioni di sicurezza, l'installazione arbitraria di software, esecuzione di codice malevolo con diritti amministrativi. L'installazione di software è consentito solo agli amministratori di sistema che potranno provvedere solo dopo un iter approvativo. Alternativamente, attraverso la piattaforma di software distribution, è possibile installare in self service i pacchetti software opzionali pre-autorizzati;
- Sistema centralizzato di gestione continuo degli aggiornamenti (patch management) del sistema operativo e del software più diffuso (MS Office suite, Adobe, Java, ecc..);
- Protezione antivirus e antimalware con sistema centralizzato di gestione degli aggiornamenti e delle policy;
- Personal firewall con sistema centralizzato di gestione;
- Funzionalità di host integrity per la quarantena della postazione in assenza dei requisiti minimi di sicurezza; attraverso la funzionalità di host integrity sono implementate anche misure di prevenzione personalizzate su malware zero day rilevati attraverso le analisi dell'IRT;
- Verifica della conformità alle politiche di sicurezza dell'Istituto.

Al fine di assicurare una più efficace protezione antivirus vengono impiegate tecnologie di analisi multi-fornitore sui diversi livelli di controllo. Nel seguito, alcuni dati dimensionali relativi ad un mese di osservazione:

- Sicurezza delle Postazioni di lavoro
  - malware bloccato (virus, worm, trojan, greyware, spyware, ecc.): circa 41.000 / mese
  - malware distinti individuati: circa 200 / mese
  - numero di postazioni su cui è stato rilevato almeno un malware: circa 1.200 / mese
- Servizio Proxy
  - URL richieste: 900.000.000 / mese
  - URL bloccate attraverso il motore standard di URL e Content filtering: 35.000.000 / mese
  - URL bloccate attraverso regole personalizzate sulla base delle analisi dell'IRT: 600.000 / mese
  - Virus e codici malevoli bloccati: 2.200 / mese

Sicurezza applicativa Il patrimonio informativo dell'Istituto è acceduto da diversi canali ma, con l'attuazione del processo di completa telematizzazione dei servizi, il canale web è divenuto quello prevalente. Come detto, il patrimonio applicativo è costituito da una imponente quantità di applicazioni. In questo contesto, la sicurezza delle applicazioni riveste una importanza primaria, per evitare abusi o accessi non autorizzati. Per questo motivo, l'Istituto si è dotato di un insieme di strumenti e processi atti a verificare la conformità e l'assenza di vulnerabilità del software prodotto, prima della messa in produzione. L'Istituto ha definito delle linea guida, sulla base della Developer Guide OWASP, che sono state adattate ed integrate alle specifiche architetture applicative e di sistema dell'Istituto. All'interno del processo di release management, è attivo un task di verifica della sicurezza applicativa

svolto anche con l'ausilio di strumenti automatici ma principalmente eseguita da esperti della materia. Le attività di verifica producono un report delle eventuali vulnerabilità e i suggerimenti per la loro risoluzione. Alcuni dati dimensionali relativi al periodo gennaio-ottobre 2014:

- Numero di applicazioni distinte verificate: circa 210;
- Numero di collaudi effettuati: circa 900;
- Numero di collaudi che hanno rilevato almeno una vulnerabilità: circa 115.

Logging delle Applicazioni Considerato il ruolo cruciale delle transazioni telematiche all'interno dei processi istituzionali, al fine di acquisire idonee evidenze per la tracciabilità delle transazioni, l'Istituto si è dotato, fin dai primi servizi online, di un sistema di logging applicativo attraverso il quale sono registrati gli eventi applicativi corrispondenti alle funzioni di business. Gli eventi da riportare nei log sono identificati nella fase di progettazione delle applicazioni e la compliance delle registrazioni effettuate costituiscono un requisito essenziale per la messa in produzione di una applicazione. Tale sistema costituisce un essenziale strumento per:

- la rilevazione delle operazioni di trattamento delle informazioni;
- fornire riscontro alle richieste dell'autorità giudiziaria e ai processi di audit interno;
- le analisi sull'utilizzo dei servizi da parte degli utenti;
- l'identificazione di potenziali abusi nell'accesso alle informazioni o nell'identificazione di potenziali furti di identità.

Alcuni dati dimensionali relativi al periodo gennaio-ottobre 2014:

- numero di log prodotti: 1,7 miliardi;
- numero di applicazioni che effettuano logging: 770;
- numero di eventi applicativi distinti catalogati: 6.200.

Logging dei Sistemi I log di sicurezza prodotti dai sistemi sono centralizzati su un SIEM (Security Information and Event Management) per la loro raccolta, filtro, archiviazione e correlazione. Numerose sono le tipologie di apparati che generano eventi per il SIEM dell'Istituto e che vanno dai sistemi z/OS ai sistemi Unix, dagli apparati di rete ai DataBase, dalle sonde di Intrusion Detection/Prevention ai sistemi di autenticazione e autorizzazione.

L'infrastruttura di raccolta e correlazione dei log, per ogni sua specifica componente, processa gli eventi di sicurezza che, analizzati dagli specialisti consentono di determinare eventuali violazioni di sicurezza, abusi, accessi non autorizzati, attività di software malevolo o anche più semplicemente criticità operative delle infrastrutture. Eventuali anomalie rilevate sono gestite dall'IRT che, identificate le possibili azioni di contenimento, coordina i gruppi sistemistici e di sicurezza per le attività di rientro. Il sistema di aggregazione e correlazione degli eventi di sicurezza è continuamente implementato con specifiche regole di correlazione al fine di identificare comportamenti di malware di tipo zero day (vd. Zbot/Zeus) non ancora identificati dai sistemi di protezione perimetrale o altre violazioni di sicurezza.

Un altro approccio è l'analisi di metriche quantitative rispetto alle baseline, valutate sulla base di scale temporali medie e lunghe, al fine di evidenziare fenomeni ed anomalie che possono nascondere l'azione di agenti malevoli.

Alcuni dati dimensionali:

- numero di eventi elaborati: 1,3 miliardi / mese;
- picchi di 9.000 eventi/sec.

4.3 Regione Friuli Venezia Giulia

Il sistema ICT della Regione Friuli Venezia Giulia e del suo territorio ha subito una lunga e complessa evoluzione che, partendo da una realtà scarsamente informatizzata e dominata dai sistemi centralizzati quale quella dei primi anni '70, ha portato alla situazione attuale in cui possiamo dire di disporre di un Sistema Informativo Integrato Regionale (SIIR) che comprende, oltre all'Ente Regione stesso, la maggior parte delle PA del territorio (enti locali, enti del sistema socio sanitario, enti pubblici economici) e mette a fattor comune infrastrutture di comunicazione di rete, infrastrutture applicative, nonché un'ampia gamma di servizi, a vantaggio non solo delle PA in senso stretto ma di tutta la popolazione e delle imprese che agiscono sul territorio. Parlando di un sistema integrato, uno degli aspetti chiave dell'integrazione è la gestione dell'IT Security, che ha subito anch'essa un'analoga e fondamentale evoluzione, partendo dal mondo monolitico dei mainframe anni '70 sino a giungere alla realtà complessa e multiforme del Cloud in tutte le sue declinazioni odierne. Scopo di questo documento è dunque illustrare, per quanto sinteticamente, l'approccio all'IT Security da parte della Regione Friuli Venezia Giulia, dando conto sia degli aspetti organizzativi e culturali che di quelli più eminentemente tecnici andando a toccare alcuni degli aspetti più rilevanti quale ad esempio la realizzazione del CERT - raFVG (regione autonoma Friuli Venezia Giulia).

In questo caso di studio si illustrerà come vengono affrontate le problematiche relative alla sicurezza ICT nell'ambito del Sistema Informativo Integrato Regionale (SIIR) della Regione Autonoma Friuli Venezia Giulia, partendo dal quadro normativo di riferimento e da una breve descrizione del contesto attuale e degli sviluppi a breve e medio termine. Il documento prosegue poi descrivendo gli elementi caratteristici del modello di IT Security del SIIR e la suddivisione delle competenze nella gestione della sicurezza ICT tra Ente Regione e società in-house (Insiel S.p.a.). Vengono inoltre riassunti gli aspetti più tecnici dell'IT Security regionale, partendo dai Presidi di sicurezza, nel cui contesto sono descritte più estesamente le tipologie di attività del CERT - raFVG, e passando per le strategie utilizzate nella definizione delle politiche di sicurezza e per la valutazione della sicurezza delle applicazioni. Ampio spazio viene dedicato alla gestione della Continuità Operativa, con particolare riguardo alle problematiche del Disaster Recovery, per poi affrontare gli aspetti relativi alla Cultura organizzativa della Sicurezza, nel cui ambito si introducono le attività del CERT - raFVG, che svolge importanti funzioni di consulenza e disseminazione di conoscenza in campo IT Security.

4.3.1 Contesto

La Regione Autonoma Friuli Venezia Giulia è stata istituita con la legge costituzionale n.1 del 31 gennaio 1963. È una Regione a statuto speciale e come tale dispone di forme e condizioni particolari di autonomia sotto il profilo politico, legislativo, amministrativo e finanziario all'interno di uno Stato che per la sua Costituzione "riconosce e promuove le autonomie locali". In virtù della "specialità", lo Stato ha affidato alla Regione una gamma di compiti o, come si dice, di funzioni pubbliche più ampia rispetto a quella attribuita alle Regioni a statuto ordinario. La Regione Friuli Venezia Giulia è così responsabile del sistema sanitario regionale (degli ospedali e delle aziende sanitarie, della spesa farmaceutica, dell'assistenza domiciliare, ecc.), delle politiche di sostegno del diritto allo studio, dell'industria, del commercio, dell'artigianato, dell'agricoltura e del turismo, della caccia e della pesca, delle funzioni di assistenza sociale, del finanziamento dei comuni, delle province e delle comunità montane, delle strade regionali, delle politiche di sostegno delle zone svantaggiate di confine, delle misure di tutela delle minoranze linguistiche, di alcune politiche dell'ambiente, del demanio marittimo, degli interventi di protezione civile. L'impegno primario dell'Ente Regione nel settore ICT nasce proprio da quanto sopra enunciato ed è funzionale all'attuazione del dettato legislativo di autonomia: la realizzazione di un Sistema Informativo Integrato Regionale, previsto dalla L.R. n. 9 del 14/7/2011 (di cui si dirà in seguito) è la chiave di volta per poter garantire una gestione integrata e trasversale delle realtà e dei fenomeni che insistono sul proprio territorio, senza la quale sarebbe impossibile ottenere gli obiettivi di efficacia, efficienza, coordinamento, consolidamento, razionalizzazione della spesa e sviluppo omogeneo che la Regione si è prefissa.

4.3.2 Breve storia dell'evoluzione dei servizi IT in Regione FVG

L'attenzione verso il mondo dell'ICT in Friuli Venezia Giulia nasce da lontano: già nel 1972 venne promulgata la prima legge organica sull'informatica (Legge regionale 27 aprile 1972, n. 22 "Istituzione di un sistema informa-

tivo elettronico di interesse regionale ed intervento a favore del Centro di calcolo dell'Università di Trieste") e, in maniera sorprendente per i tempi, il focus era rivolto non solo all'Ente Regione e alle sue "dipendenze" strette ma veniva esteso a tutte le PPAA del territorio regionale anticipando i concetti di trasversalità ed integrazione. A seguito della promulgazione della Legge n. 22 nasce Insiel S.p.a. (all'epoca Informatica Friuli Venezia Giulia), inizialmente partecipata tra Italsiel e l'Azienda Ospedaliera Udinese: la società evolve nel tempo, venendo acquisita al 100% da raFVG nel 2005 per assumere l'assetto definitivo nel 2009 con lo scorporo delle attività non in-house e il reintegro del ramo d'azienda finalizzato alla realizzazione della rete regionale in banda larga. Si arriva così all'impianto legislativo attuale, definito dalla Legge regionale 14 luglio 2011, n. 9 "Disciplina del sistema informativo integrato regionale del Friuli Venezia Giulia" in cui non a caso si parla di sistema informativo integrato, inteso come l'insieme degli asset ICT (basi dati, software, servizi, infrastrutture) delle PPAA che operano sul territorio regionale. La Regione assume in questo contesto un ruolo di indirizzo, coordinamento e controllo del Sistema Informativo Integrato Regionale (con apposito rilievo per ciò che riguarda gli aspetti della sicurezza) ponendosi gli obiettivi di aumento dell'efficacia e dell'efficienza complessiva del sistema, razionalizzazione complessiva degli oneri nel settore ICT, sviluppo dell'interoperabilità ICT tra i vari soggetti facenti parte del SIIR, sviluppo uniforme e omogeneo delle funzionalità attinenti al SIIR ed infine di promozione della trasparenza (open data). La gestione operativa del sistema viene poi affidata, mediante apposito disciplinare, ad Insiel che assume a sua volta il ruolo di attuatore e gestore del SIIR.

Ruolo e funzioni attuali dell'IT in Regione FVG

Riprendendo quanto detto nei paragrafi precedenti, il risultato complessivo dello sforzo normativo ed organizzativo messo in atto sinora è una infrastruttura che è nata, sin dal 1972, come un sistema integrato all'interno del quale le PPAA del territorio regionale beneficiano di una serie di servizi e infrastrutture messe a fattor comune dall'Ente Regione, ed in particolare:

- Portfolio di soluzioni applicative comuni messo a disposizione di Enti Locali e Aziende Socio Sanitarie ed Ospedaliere;
- Data center regionale, dal quale vengono erogati servizi applicativi ed infrastrutturali in modalità "Cloud" verso l'Ente Regione, gli Enti Locali e le Aziende Sanitarie ed Ospedaliere;
- Rete unitaria della PA regionale, che potrà avvalersi entro la fine 2015 del completamento del progetto "Ermes" (realizzazione Rete Pubblica Regionale in fibra ottica) collegando tutte le PPAA del territorio;
- Infrastruttura centralizzata di cyber security, che garantisce il monitoraggio e la sicurezza di quanto indicato nei punti precedenti facendo rientrare nel perimetro di sicurezza regionale tutte le realtà che usufruiscono di detti servizi.

Il processo di consolidamento ed evoluzione prosegue con molteplici ed importanti attività: per la Sanità sono stati avviati progetti quali il Fascicolo Sanitario Elettronico, la Prescrizione e la Dematerializzazione delle ricette, il collegamento in rete dei Medici di Medicina Generale e i Pediatri di Libera Scelta, il Progetto PACS. Nell'ambito degli Enti Locali invece è ormai disponibile un repertorio applicativo che copre la quasi totalità delle esigenze di informatizzazione degli enti. A questo si è aggiunto nel corso del 2014 un servizio Cloud in modalità IaaS rivolto specificamente agli EELL (Enti Locali) e sarà attivato tra breve un servizio VoIP a favore delle amministrazioni territoriali.

Nel Piano Strategico Regionale 2014-2018, approvato con deliberazione della Giunta regionale n. 1332 dell'11 luglio 2014, sono anche indicate le linee di azione secondo cui si muoverà lo sviluppo della ICT regionale nel prossimo quadriennio. Come detto più volte, assumono particolare importanza le azioni che hanno una valenza trasversale e sono rivolte all'integrazione. Tra queste ricordiamo in breve le più significative, alcune delle quali già menzionate in precedenza:

- Sviluppo di un Data Center a beneficio del territorio;
- Completamento del programma Ermes per la costruzione della Rete Pubblica Regionale tramite il collegamento con infrastrutture a banda larga di tutti i comuni della regione e le strutture sanitarie;

- Coordinamento dello sviluppo da parte di Insiel di un sistema di gestione informatizzata delle procedure di acquisizione di beni e servizi finalizzato alla realizzazione di una Centrale di Acquisto al servizio delle PPAA regionali;

- Coordinamento dello sviluppo dei sistemi informativi a livello locale e, in questo ambito, introduzione del nuovo sistema finanziario-contabile derivante dall'armonizzazione dei bilanci pubblici (a regime dal 2015), accompagnando gli enti locali al fine di costruire un sistema consolidato;

- Garanzia di accesso in banda larga a tutte le scuole per lo sviluppo della cultura digitale.

4.3.3 La gestione della sicurezza IT in Regione FVG

Breve cronistoria

Il sistema informatico regionale, nato e sviluppatosi a partire dagli anni '70, è stato da sempre utilizzato per il trattamento di informazioni legate alle attività della pubblica amministrazione, sia interne sia ovviamente inerenti ai cittadini. E in tale contesto la sicurezza informatica è sempre stato argomento rilevante. Nei primi anni dello sviluppo del sistema, sostanzialmente basato su un modello centrale con architettura mainframe con una rete ad estensione limitata e perimetro ben definito e controllato, il concetto di sicurezza era per lo più legato alla protezione del dato in termini di disponibilità e integrità. Trovavano quindi spazio contromisure legate a controlli sull'elaborazione, salvataggio dei dati oltre a controlli stringenti sull'accesso alle risorse di elaborazione centrali. Il tutto completato da procedure specifiche di controllo degli accessi fisici e di gestione dell'emergenza e dell'operatività in caso di indisponibilità del sistema informatico. Con la progressiva transizione tecnologica verso sistemi dipartimentali e la contestuale migliore connettività disponibile agli Enti sono emerse ulteriori esigenze: l'introduzione della normativa sulla protezione dei dati personali ha ribadito la necessità di far evolvere il sistema di sicurezza per coprire maggiormente gli aspetti legati alla riservatezza delle informazioni e il controllo degli accessi, per minimizzare il rischio di accessi non autorizzati ai dati personali. Sono quindi progressivamente state introdotte contromisure quali i sistemi di accesso centralizzati, sistemi di controllo dei flussi di traffico, sistemi di protezione a più livelli, ma anche misure di formazione e sensibilizzazione, accompagnate da atti di responsabilizzazione degli operatori, il tutto nell'ottica di indirizzare in maniera coerente i rischi connessi con il trattamento delle informazioni stesse.

Organizzazione attuale

Attualmente il sistema informativo integrato regionale (SIIR) del Friuli Venezia Giulia è disciplinato secondo quanto disposto dalla Legge Regionale 14 luglio 2011, n.9. Il dettato legislativo prevede che l'Ente Regione promuova lo sviluppo, la diffusione e l'utilizzo integrato delle tecnologie dell'informazione e della comunicazione (ICT) nelle pubbliche amministrazioni del proprio territorio e nella società regionale al fine di favorire:

- lo sviluppo organico e integrato sul territorio regionale della società dell'informazione in coerenza con il contesto normativo comunitario e nazionale;

- il miglioramento della qualità della vita dei cittadini nel rapporto con le pubbliche amministrazioni del territorio regionale e la promozione dello sviluppo economico del territorio favorendone la competitività;

- lo sviluppo di infrastrutture e servizi innovativi idonei a potenziare la cooperazione, l'efficienza e la capacità di servizio delle amministrazioni pubbliche del territorio regionale.

In tale contesto i soggetti che contribuiscono alla erogazione del SIIR, anche in termini di sicurezza informatica, sono la Regione e la società informatica in-house Insiel. Il dettaglio dei ruoli assunti dai due attori principali (raFVG e Insiel) è definito di seguito.

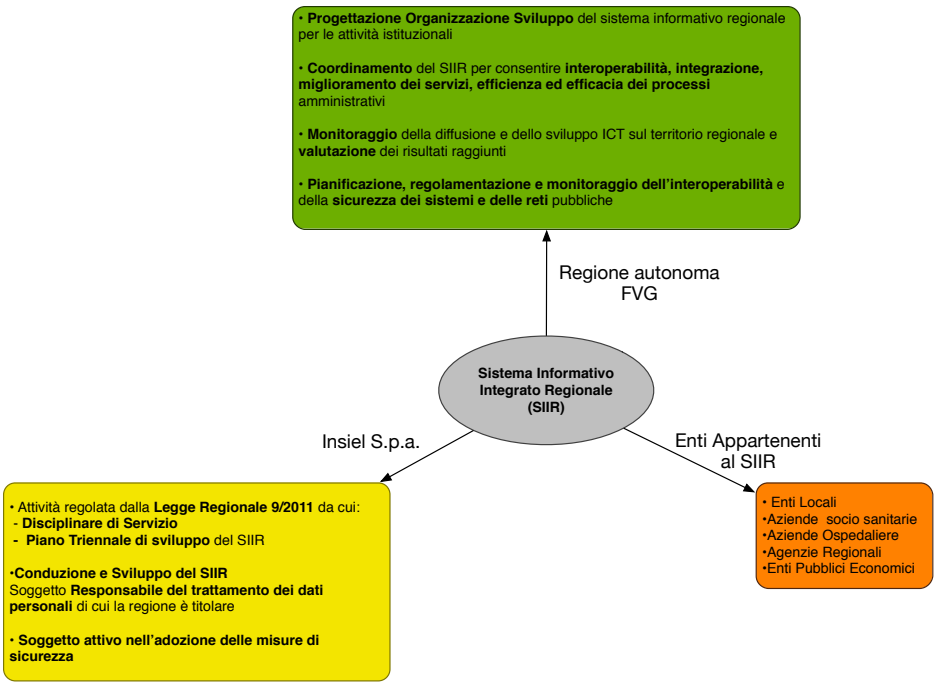


Figura 4.12: Schema organizzativo generale del SIIR FVG

Identificazione elementi caratteristici del modello IT Security della Regione

Gli elementi caratteristici del modello del sistema informativo integrato regionale (SIIR) sono quelli evidenziati nei punti precedenti e mirano a premiare il concetto di integrazione tra i soggetti presenti sul territorio. Quindi pur operando in presenza di realtà (enti e aziende) che possiedono e fanno valere la propria autonomia, il sistema informativo integrato regionale è la chiave di volta per garantire un'unitarietà di paradigmi nei servizi ICT in genere ed in quelli relativi alla sicurezza nello specifico. Pertanto, anche l'IT Security deve tener conto di tale linea di indirizzo in tutte le sue manifestazioni; grazie al sistema integrato tutti gli enti che rientrano nel suo ambito godono di un meccanismo complessivo di sicurezza e in forza di tale meccanismo devono sottostare ad un insieme di regole quali la previsione di misure di separazione tra la rete dell'ente e la rete RUPAR-FVG, l'individuazione di un soggetto di riferimento, e l'impegno a implementare nel contesto di riferimento tutte le misure di sicurezza previste dalla normativa, in modo da non costituire una minaccia per la rete regionale e gli altri Enti connessi. L'adesione di un Ente al sistema regionale non comporta tuttavia solamente un impegno da parte di quest'ultimo a rispettare tali misure di sicurezza, ma offre anche la possibilità di fruire di alcuni servizi specifici per la sicurezza IT [2]. In sintesi le misure di sicurezza di cui un Ente connesso può beneficiare sono:

- Protezione antimalware, anche "cloud";
- Canale di navigazione Internet protetto;
- Posta elettronica protetta.

[2] Tali servizi di sicurezza completano un contesto di "repertorio applicativo" per gli Enti composto da decine di applicazioni il cui dettaglio è reperibile a questo link: goo.gl/zj4cnR

4.3.4 IT security presso la Regione Friuli Venezia Giulia

Presidi di sicurezza

I presidi di sicurezza a disposizione del Sistema Informativo Integrato Regionale (SIIR) sono composti sia da controlli tecnologici implementati per ridurre i rischi insistenti sul patrimonio informativo sia da presidi operativi necessari alla loro corretta gestione. Di seguito un quadro di sintesi a titolo esemplificativo ma non esaustivo:

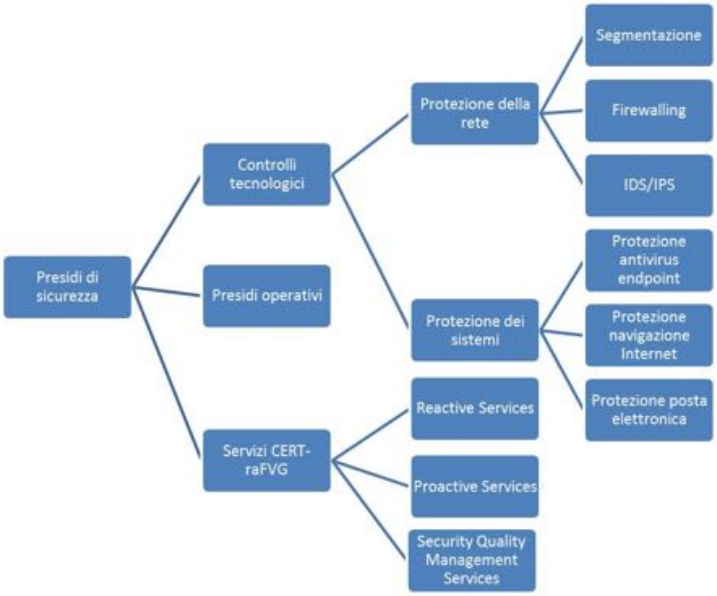


Figura 4.13: Presidi di sicurezza presso Regione FVG

Controlli Tecnologici

Per quanto riguarda i controlli tecnologici, essi comprendono vari elementi come di seguito indicato.

Protezione della rete L'architettura delle reti gestite prevede l'isolamento dei singoli segmenti in sintonia con i servizi offerti ed i contratti esistenti. Tale segmentazione corrisponde dal punto di vista tecnico alla suddivisione della rete tra i vari Enti connessi alla rete regionale. La protezione delle reti interne si basa sulla presenza di una struttura di accesso ad Internet a più livelli, separati dai dispositivi firewall. Inoltre, sono implementate politiche di segmentazione delle reti in contesti logici diversi a seconda delle caratteristiche dei servizi erogati. Da tale punto di partenza, relativamente all'incremento delle capacità di prevenzione e reazione ai tentativi di violazioni esterne, sono in uso sistemi IDS (Intrusion Detection System) e IPS (Intrusion Prevention System).

Protezione antivirus, della navigazione Internet e dalla posta elettronica Il sistema di protezione antivirus attualmente in uso ha la prerogativa di avere una gestione centralizzata e di provvedere alla distribuzione automatica di tutti gli aggiornamenti. La soluzione adottata è di tipo multi-piattaforma e provvede alla protezione dai malware a più livelli. Una console dedicata provvede al completo monitoraggio delle apparecchiature aventi installato il prodotto antivirus. La stessa rileva la presenza di virus, evidenzia gli elaboratori contagiati, permette la creazione di report sui virus più intercettati, le postazioni interessate e statistiche da cui può essere rilevato il servizio erogato. Per il controllo antivirus della navigazione via Web viene utilizzato un prodotto specifico, che opera associato logicamente ai server proxy mentre il controllo antivirus della posta elettronica viene effettuato sia a livello di gateway

Internet, per la verifica della posta proveniente da Internet, sia a livello dei server di posta Intranet, controllando i messaggi inviati da e verso tali server.

Presidi operativi Data Center Regionale

Il Data Center Regionale viene presidiato 24 ore al giorno da personale Insiel che provvede alle attività necessarie a garantire la regolare operatività dei servizi. Tra le varie attività possiamo individuare:

CERT raFVG

Come già anticipato, il contesto CERT-raFVG raccoglie specifiche attività sulla sicurezza che sono state erogate nel tempo nel contesto dell'amministrazione regionale; esse si possono dividere in tre macrocategorie (reactive services, proactive services, security quality management services). Per ognuna di esse, di seguito dettagliate, nel contesto della regione sono stati erogati un sottoinsieme di servizi, che sono evidenziati in Figura 4.14 e di seguito descritti.

Figura 4.14: Tipologie di servizi del CERT raFVG

Reactive Services - Alerts and Warnings Questo servizio consiste nel fornire informazioni che descrivano vulnerabilità di sicurezza, intrusioni informatiche, virus o altre minacce e fornire delle indicazioni sulle modalità di comportamento per la gestione del potenziale problema segnalato. Nel contesto del CERT-raFVG questo servizio viene erogato inviando periodicamente alert relativi a vulnerabilità che superino una soglia di criticità concordata a priori con l'utenza.

Reactive Services - Incident handling Questo servizio consiste nel:

- Identificare le situazioni di potenziale violazione della sicurezza informatica;
- Raccogliere le informazioni relative ed analizzarle;
- Intraprendere azioni di risposta per mitigarne l'impatto, eliminarne le cause e ripristinare le condizioni di regolare servizio.

Le fasi che si possono identificare nell'attività di gestione di un incidente sono riportate in Figura 4.15.

Le fonti di informazione tramite le quali il CERT-raFVG viene a conoscenza di un avvenuto o presunto incidente informatico sono per lo più le seguenti:

- Segnalazioni dai gruppi tecnici deputati all'erogazione del servizio (gestione dei sistemi regionali);
- Infrastrutture di protezione implementate nel contesto regionale (a livello host, web, mail);
- Sistemi di monitoraggio delle infrastrutture regionali;

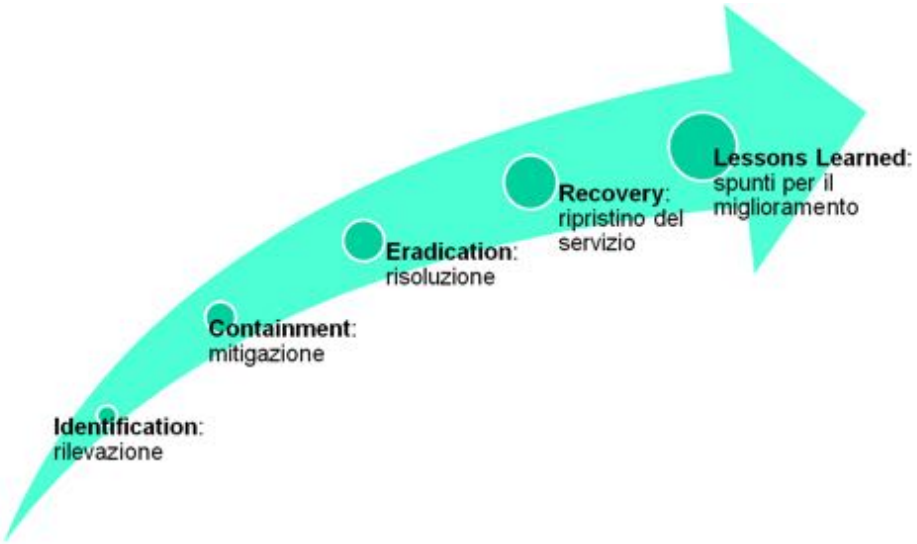


Figura 4.15: Fasi nell'attività di gestione di un "incident"

- Sistemi IDS o IPS.

Per avere un dato numerico indicativo sugli attacchi rilevati, intesi come eventi significativi per la sicurezza, si hanno i seguenti parametri:

- 600.000 eventi gestiti ogni mese dal sistema IPS;
- 3 milioni di blocchi effettuati ogni mese dal sistema di navigazione web su circa 25.000 utenti;
- 30.000 malware bloccati ogni mese su circa 20.000 postazioni di lavoro;
- 30.000 malware bloccati ogni mese su oltre 26.000 caselle di posta;
- 800.000 mail di spam bloccate ogni mese su oltre 26.000 caselle di posta;
- 15 milioni di connessioni rifiutate ogni mese dal sistema antispam in quanto provenienti da spammers.

Proactive Services - Technology Watch Questo servizio consiste nel monitorare costantemente sia il trend di evoluzione delle minacce alla sicurezza sia l'evoluzione delle tecnologie di protezione. Il personale che opera nel contesto del CERT-raFVG si mantiene aggiornato su queste tematiche attraverso:

- Aggiornamento on-line;
- Confronto con i vendor di tecnologie e servizi di sicurezza;
- Partecipazione a seminari e convegni specifici.

Proactive Services - Security Audits or Assessments Questo servizio ha l'obiettivo di aumentare la consapevolezza dello stato di sicurezza delle infrastrutture gestite come punto di partenza per azioni correttive/migliorative e per una corretta gestione. Questo servizio è stato erogato sostanzialmente attraverso attività di Vulnerability Assessment volte ad identificare vulnerabilità esportate sulla rete dalle infrastrutture gestite:

- Scansione;
- Analisi risultati;
- Identificazione interventi correttivi.

Proactive Services - Intrusion Detection Services Questo servizio ha l'obiettivo di raccogliere informazioni circa la possibile presenza di attacchi o intrusioni informatiche sui sistemi in esercizio per indirizzare più efficacemente la risposta. Questo servizio è stato erogato tramite:

- l'introduzione di sonde con funzione di Network Intrusion Detection System (NIDS) in particolari punti della rete regionale;
- l'introduzione di Host Intrusion Detection System (HIDS) sui sistemi della server farm regionale.

Security Quality Management Services - Security Consulting Questo servizio ha l'obiettivo di fornire linee guida per la realizzazione e l'erogazione dei servizi con adeguati livelli di sicurezza, nell'ambito di riferimento. Questo servizio è stato erogato tramite il supporto a:

- stesura di linee guida per l'implementazione delle soluzioni;
- stesura di linee guida per lo sviluppo sicuro del software;
- problematiche relative al contesto di sicurezza e protezione.

Security Quality Management Services - Awareness Building e Education Training L'obiettivo dell'Awareness Building è la sensibilizzazione dell'utenza sulle criticità in essere, mentre l'obiettivo dell'Education/Training è quello di fornire gli elementi per indirizzare le problematiche di sicurezza, coerentemente con il target di riferimento. Per erogare questo servizio, nel contesto del CERT-raFVG fino ad ora sono state svolte le seguenti attività:

- Partecipazione alla realizzazione di Corsi e-learning su tematiche di sicurezza/privacy;
- Istituzione sessioni di sensibilizzazione su tematiche e trend di sicurezza;
- Erogazione di sessioni di formazione specifiche su tematiche di sicurezza/privacy.

Le attività nel contesto dei Security Quality Management Services sono attivate a richiesta da parte dell'Amministrazione.

I servizi che si possono annoverare nel contesto delle attività del CERT-raFVG sono erogati da personale esperto e certificato sulle tematiche di security e privacy. In particolare le competenze specifiche sono:

- Certificazioni CISSP, Lead Auditor ISO 27001, CISM e altre (Security in SDLC, ...);
- Certificazioni di prodotto sulle tecnologie di protezione gestite;
- Conoscenze di tecniche e tool di sicurezza.

Strategie per la definizione di policy di sicurezza

Accesso utente ai sistemi L'accesso ai sistemi è previsto, per gli utenti dell'amministrazione regionale, solo attraverso il superamento di una procedura di autenticazione/autorizzazione, attuata attraverso un sistema centrale. La gestione delle credenziali è svolta con dei criteri volti a ridurre al minimo la possibilità di violazioni o sottrazioni di identità quali, ad esempio, la lunghezza e la "complessità" della password ed un tempo massimo di validità della stessa.

Accesso ad Internet Oggi è indispensabile non solo predisporre opportune barriere che filtrino il traffico proveniente dall'esterno, bloccando sul nascere l'ingresso nella rete di contenuti potenzialmente dannosi, ma è necessario anche proteggere le risorse regionali e alle postazioni di lavoro dei dipendenti durante l'accesso a contenuti Internet. In tal senso è stata predisposta una *politica di protezione della navigazione Internet* che prevede:

- *Autenticazione*: l'accesso a Internet avviene solo dopo che è stata eseguita una autenticazione dell'utente/risorsa interna verso un dominio di autenticazione;
- *Autorizzazione*: solo l'utente autenticato ed abilitato alla navigazione Internet potrà effettivamente accedere al servizio di navigazione;

- *Controllo sui contenuti in base a categorizzazione*: la pagina web richiesta verrà effettivamente acceduta solo se tale pagina non appartiene ad una categoria ritenuta non correlata alla attività lavorativa e quindi messa in modalità di blocco;
- *Controllo su contenuti malevoli in base a categorizzazione*: l'accesso alla pagina web richiesta verrà bloccata se appartiene ad una categoria ritenuta pericolosa dal punto di vista della sicurezza informatica (Es.: siti riconosciuti come potenzialmente pericolosi ossia "Malicious Websites ", siti di phishing, di Spam, ecc.);
- *Controllo antivirus sulle pagine e sugli allegati scaricati*: ogni pagina web e ogni allegato viene controllato per evidenziare e bloccare eventuali script malevoli e file infetti.

La peculiarità del sistema di accesso, nel contesto regionale, sta nella possibilità di essere configurato secondo le esigenze e le policy del singolo Ente, pur essendo erogato in maniera centralizzata e con tecnologia uniforme.

Accesso ospiti Per consentire la disponibilità di accesso alla rete anche a persone che occasionalmente hanno necessità di operare nel contesto dell'Amministrazione regionale (ospiti) viene garantito un servizio di connettività Internet attraverso una rete wireless. Essa è di tipo aperto (senza protocollo di sicurezza e cifratura). Chiunque può collegarsi alla rete e ricevere un indirizzo IP. Gli IP appartengono ad una rete chiusa (segregata) che ha come default gateway un firewall che accede direttamente ad Internet. Un ospite, prima di poter navigare su Internet deve "superare" un portale di autenticazione. Non ci sono filtri né sui contenuti della navigazione né sui protocolli IP di comunicazione. Le credenziali di accesso vengono fornite da personale regione, abilitato alla creazione di utenti sul server di autenticazione, tramite una pagina web. Le informazioni inserite sono nome, cognome, numero di telefono della SIM card italiana (per certi aspetti equivalente alla carta di identità in quanto il provider che ha rilasciato la SIM ha copia della carta di identità dell'utilizzatore della SIM). Le credenziali vengono inviate via sms e restano invisibili al personale che ha creato l'account. L'utente creato può avere validità 1 giorno, 1 settimana, 1 mese e 3 mesi.

Application Security

Nell'ottica di perseguire un livello di protezione adeguato nel contesto delle applicazioni che sono alla base del sistema informativo integrato regionale, sono state intraprese diverse iniziative specifiche, ulteriori rispetto alle iniziative per la sicurezza generali descritte nelle sezioni precedenti, secondo le seguenti direttrici:

- Redazione di specifiche linee guida rivolte al personale addetto allo sviluppo di applicazioni, con focalizzazione sulle applicazioni web, inerenti lo sviluppo sicuro: in particolare, in maniera coerente con la metodologia OWASP, sono presenti specifiche indicazioni circa le modalità di individuazione e gestione delle principali vulnerabilità riscontrabili in quel contesto;
- Previsione di specifici interventi formativi indirizzati allo sviluppo sicuro delle applicazioni web;
- Previsione di verifiche di sicurezza, con tool automatici ma anche con l'ausilio di soggetti terzi qualificati, relativamente alle applicazioni componenti il sistema regionale, compatibilmente con le disponibilità.

Information Security (confidenzialità, integrità, autenticazione e non ripudio)

Di seguito vengono elencati alcuni processi relativi ai temi in oggetto.

Gestione dei cambiamenti HW e SW Ogni infrastruttura tecnologica presente presso la server farm della amministrazione regionale ha un suo ciclo di vita che passa attraverso le seguenti fasi:

- **Progettazione**: fase che prende in considerazione tutti i requisiti e formalizza in un documento tutte le componenti hw, sw e i relativi flussi rete/dati necessari all'infrastruttura;
- **Attivazione**: fase che consiste nella predisposizione dei sistemi come da progetto;
- **Passaggio in esercizio**: fase che consiste nell'avvio delle attività propedeutiche al corretto funzionamento del servizio e a garantirne i livelli di servizio previsti quali, ad esempio, le attività di monitoraggio e di backup. Viene innescata a seguito della configurazione della infrastruttura tecnologica e dei test di funzionamento e collaudo;

- **Richiesta di revisione**: fase in cui viene riesaminato il progetto, vengono formalizzate le modifiche generando una nuova versione del documento di progetto e viene richiesta la effettiva modifica dell'infrastruttura; viene innescata nel caso in cui una infrastruttura tecnologica già in esercizio abbia bisogno di essere modificata o aggiornata;

- **Dismissione**: Fase che consiste nel liberare tutte le risorse allocate ad un infrastruttura e cessare le attività introdotte nella fase di passaggio in esercizio a garanzia del corretto funzionamento e dell'integrità dei dati; tale fase viene attivata formalmente quando un'infrastruttura deve cessare la sua funzione.

Politica di Backup Come detto precedentemente, all'interno del ciclo di vita delle infrastrutture tecnologiche è presente la fase di passaggio in esercizio che, di fatto, rappresenta il momento in cui l'infrastruttura tecnologica diventa operativa. In questa fase vengono innescate anche alcune attività tra cui quella di backup. Ogni infrastruttura tecnologica prevede una procedura di backup standard con verifica giornaliera degli esiti. In caso una procedura di backup non abbia dato esito positivo, gli operatori della server farm effettuano una verifica sulle relative cause ed innescano, se necessario, l'intervento dei sistemisti di riferimento.

Regole per l'installazione del software sulle postazioni di lavoro Nel contesto dell'amministrazione regionale, i PC dei dipendenti prevedono una installazione standard che comprende, oltre al sistema operativo, varie applicazioni di produttività personale secondo quanto concordato con il servizio preposto. L'accesso al PC del dipendente avviene con un utente senza abilitazioni di tipo privilegiato e che non permette l'installazione di nuovo software o la disinstallazione di quello presente. Tale disposizione ha vantaggi sia gestionali sia di sicurezza in quanto da una parte permette di mantenere un parco di software installato standard e dall'altra impedisce l'installazione o l'esecuzione di software malevolo (malware) con diritti amministrativi. In caso l'utente abbia bisogno di utilizzare un particolare software per il proprio lavoro che non è presente tra quelli preinstallati sul PC, dovrà seguire una procedura amministrativa che prevede una richiesta che dovrà essere approvata. In seguito il personale tecnico provvederà all'installazione richiesta.

4.3.5 Continuità Operativa

Insiel eroga oltre 2000 servizi alle aziende socio-sanitarie e ospedaliere, alle direzioni e agli enti locali della regione Friuli Venezia-Giulia. Un simile contesto ben rappresenta un portfolio completo delle soluzioni che le pubbliche amministrazioni offrono quotidianamente agli operatori, ai cittadini e ai pazienti. Appare perciò evidente come la necessità di assicurare la continuità del servizio, oltre ad un obbligo normato dalle vigenti leggi, diventi una priorità inderogabile. Allo stato attuale è attivo un progetto regionale inerente la revisione di tutte le infrastrutture tecnologiche che, aderendo alle indicazioni di AgID e alle più comuni Best Practices in materia di ICT, si prefigge l'obiettivo di assicurare la continuità operativa di tutti i servizi erogati. Tale progetto prevede delle tempistiche sfidanti che includono una fase di testing da concludersi entro dicembre 2014, l'applicazione della protezione di DR ad un primo nucleo di applicazioni entro dicembre 2015, per concludersi nel corso del 2016. Il progetto rientra nell'ambito del Piano Triennale Regionale per il consolidamento e la razionalizzazione dei CED di tutte le pubbliche amministrazioni che contribuiscono a formare il Sistema Informativo Integrato Regionale (SIIR). I punti cardine del progetto sono sintetizzabili negli obiettivi seguenti :

- adeguare il Data Center primario alle Linee Guida AgID;

- utilizzare infrastrutture già esistenti di altre PA regionali per garantire il Disaster Recovery e la continuità operativa.

Nel prosieguo, non ci si soffermerà sul dettaglio delle fasi di analisi, di disegno e di realizzazione del progetto, che descrivono un percorso molto specifico ed ampiamente conosciuto e consolidato per gli specialisti di settore. Ci si soffermerà invece sulle esperienze fino ad ora maturate, utilizzate nella definizione dei requisiti di progetto, e sul significato che viene attribuito al concetto di continuità operativa, applicato ad ogni "categoria" di servizi erogati.

Affidabilità dei sistemi e gestione ordinaria

Affinchè i servizi informatici possano essere erogati con continuità e piena rispondenza alle esigenze degli utilizzatori finali, è essenziale ben operare sin dalla fase relativa alla loro *gestione ordinaria*: ci si deve quindi dotare di dispositivi informatici affidabili e gestiti da personale competente, che operi sulla base di processi conosciuti e ben documentati. In rispondenza a questa affermazione di base, Insiel applica gli accorgimenti di seguito descritti:

- Robustezza, resilienza ed affidabilità dei dispositivi utilizzati;
- Eliminazione di ogni "single point of failure" per tutti i servizi erogati. Requisito di base di ogni architettura ospite del Data Center regionale è la duplicazione delle componenti, l'utilizzo di sistemi di alta affidabilità, l'adozione di sistemi di bilanciamento automatico del carico di lavoro. Il più delle volte queste soluzioni sono sviluppate per assicurare la continuità del servizio anche senza l'ausilio di un presidio operativo o sistemistico. Una tipica architettura di riferimento si compone di:
  - un'infrastruttura di sicurezza finalizzata al controllo del "traffico", dei "contenuti" e degli "accessi" (IDS, IPS, Firewall, Reverse Proxy, ...);
  - un sistema di bilanciamento del carico elaborativo, configurato in modalità ridondata, che distribuisce le transazioni sui server di riferimento;
  - un livello "application server" configurato in modo che ogni "aggregato", cioè ogni gruppo omogeneo identificato dal servizio ospitato, possa crescere in modo "orizzontale" all'aumentare del carico di lavoro;
  - un livello "Data Base", in configurazione High Availability, che utilizza la tecnologia che meglio si adatta alla criticità del servizio reso (active-active; active-standby, real cluster, ...);
  - un sistema di monitoraggio del "servizio";
- Utilizzo della metodologia ITIL quale modello di riferimento nel disegno dei processi ICT. Alcuni processi sono già stati attivati mentre è in corso la progressiva adozione di quelli restanti. Per meglio specificare, in una prima fase ci si è concentrati sui processi che ITIL identifica all'interno del Service Operation: Incident Management, Problem Management, Monitoring and Control. L'adozione di questi processi, che ha consentito di intervenire in modo efficace principalmente durante la fase di erogazione del servizio, si è concretizzato con la definizione di un iter che regola il monitoraggio costante finalizzato alla prevenzione degli incidenti e con la definizione di un iter che regola, con interventi rapidi e strutturati, le operazioni di correzione dei guasti conclamati. Sono in fase di sviluppo i processi che ITIL identifica all'interno del Service Transition quali Planning, Change Management, Deployment Management. Successivamente verranno presi in considerazione i processi inerenti il "Service Design" e il "Service Strategy".

Gestione delle attività di manutenzione programmata

Le attività di manutenzione programmata, soprattutto se in riferimento a sistemi informatici critici (es. sistemi ospedalieri) che operano con continuità (in modalità 24x7), devono essere adeguatamente progettate e supportate da idonei dispositivi, al fine di evitare lunghe interruzioni del servizio. Insiel ha adottato diverse tecnologie che, ognuna applicata alle soluzioni di riferimento, consentono di intervenire senza interruzioni del servizio. In tutto ciò l'utilizzo pervasivo delle tecnologie di virtualizzazione offre un grande aiuto, in quanto rende più flessibili e modulari gli interventi sulle risorse del sistema informatico.

Gestione degli eventi straordinari

In questo ambito ricadono quegli eventi che escono da un contesto ordinario e quindi non gestibili sulla base delle normali procedure operative. Gli eventi "straordinari" rappresentano le situazioni che obbligano all'innesco del "piano di continuità operativa". Il progetto sviluppato da Insiel, che è in fase di realizzazione, prevede diversi livelli di intervento, volti ad assicurare la continuità del servizio a fronte di tali eventi.

LIVELLO-1: "Continuità Operativa con replica sincrona dei dati" In questo contesto vanno considerate le situazioni di "guasto grave", che però non rientrano nelle casistiche assoggettabili ad un piano di disaster recovery

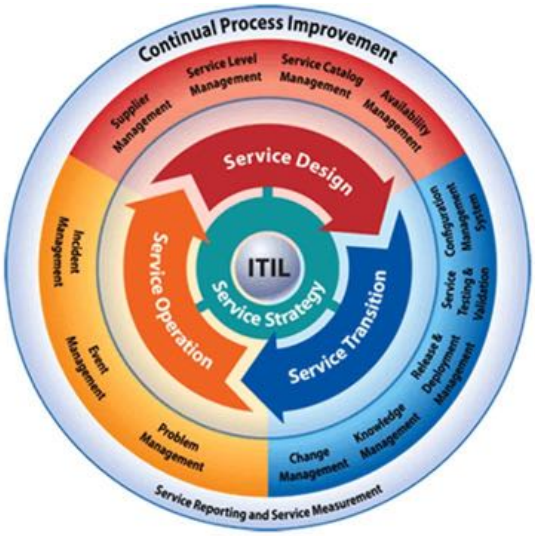


Figura 4.16: Il processo di miglioramento continuo visto secondo l'approccio ITIL

Lo scopo primario di queste procedure è di assicurare la continuità del servizio, garantendo un RPO (Recovery Point Objective, ossia il massimo tempo di perdita di aggiornamento dei dati) pari a 0 (zero data loss). Per raggiungere tale obiettivo verranno utilizzate delle strutture secondarie preesistenti, poste a distanza tale da garantire la replica "sincrona" dei dati gestiti. Tali strutture andranno a formare una "rete di data center" secondari sui quali distribuire i servizi critici, nella logica di protezione degli investimenti già operati dalla PA regionale. I servizi maggiormente interessati a questa tipologia di protezione sono quelli afferenti all'ambito sanitario ospedaliero: a fronte di un possibile guasto gli utenti percepiranno solo una breve interruzione del servizio e continueranno a disporre di una base dati congruente e aggiornata.

LIVELLO-2: "Disaster Recovery" In questo contesto vanno considerate le situazioni di "disastro", che rientrano nelle casistiche assoggettabili ad un piano di disaster recovery. Le tecnologie e le procedure da utilizzarsi sono quelle necessarie ad assicurare una continuità operativa sulla base di accordi relativamente al massimo tempo di indisponibilità del servizio (RTO) ed al massimo tempo di perdita di aggiornamento dei dati (RPO), per ogni singolo servizio normalmente erogato. Il ripristino del sito primario alla sua piena funzionalità implica un'importante attività di riallineamento dati e di approvvigionamento/ripristino delle tecnologie. Attualmente è attivo un piano di DR a protezione di un numero limitato di servizi erogati. Il progetto di DR in fase di attuazione verrà esteso a tutti i servizi ospitati presso il Data Center regionale ed è correlato con l'attività di razionalizzazione delle infrastrutture tecnologiche presenti nel territorio regionale che, coerentemente con le indicazioni di AgID, vede impegnata l'amministrazione regionale nella proposizione di progetti che ne facilitino l'attuazione. In tale contesto è attivo dal mese di Luglio 2014 un servizio denominato "Cloud degli Enti Locali" attraverso il quale viene offerto agli Enti che ne fanno richiesta un "cloud di infrastruttura" (IaaS).

Tecnologie di riferimento

Qualsiasi progetto di DR deve essere accompagnato da un'attività propedeutica di razionalizzazione e consolidamento delle infrastrutture ICT che porti all'adozione di specifiche architetture e tecnologie, tali da semplificare la successiva replica di dati e programmi. Ad oggi oltre il 90% dei servizi attivi presso il Data Center regionale usufruiscono di sistemi virtualizzati. Queste tecnologie hanno facilitato lo svecchiamento del parco hardware installato ed il consolidamento dei sistemi su di un numero limitato di server fisici. Il software di gestione delle infrastrutture virtuali consente inoltre di avere un controllo semplificato dei sistemi installati, del loro effettivo utilizzo e delle risorse necessarie. Inoltre, per ogni tecnologia utilizzata, sono state acquisite le specifiche "featu-

re" che abilitano al trattamento dei dati e dei sistemi all'interno di architetture volte ad assicurare la continuità del servizio. Tra queste vanno citate le feature che consentono la replica dei dati a livello di "storage subsystem" (mirror, copy, snapshot); gli strumenti che facilitano la replica dei dati dei DB a livello logico (es. standby DB); il software di allineamento e gestione della consistenza delle infrastrutture virtuali.

4.3.6 La cultura organizzativa della sicurezza ICT in regione: policy di sicurezza, formazione, sensibilizzazione

Per quanto riguarda gli aspetti inerenti la cultura della sicurezza IT, che vadano anche oltre alla dimensione puramente tecnologica, la Regione Friuli- Venezia Giulia si è attivata sia verso l'ambito interno alla macchina amministrativa regionale, sia in maniera più estesa verso le altre realtà presenti sul territorio. Per dar conto di ciò vengono citate ed espanse due iniziative: la prima, il CERT - raFVG, rappresenta un esempio di valorizzazione del concetto di sicurezza nei confronti dell'amministrazione interna; la seconda, il Security Summit FVG, rappresenta un esempio di valorizzazione specifica dei temi della sicurezza all'esterno della sola amministrazione regionale, interessando gli altri Enti del territorio del Friuli Venezia Giulia. Inoltre, per dare conto ai cittadini delle iniziative inerenti al rispetto e all'armonizzazione con l'agenda digitale italiana, la Regione ha pubblicato nella sezione del proprio portale dedicata all'Agenda Digitale FVG l'elenco delle iniziative intraprese sul fronte della digitalizzazione e della sicurezza. Infine, il concetto di sicurezza trova spazio nel "Programma triennale per lo sviluppo delle ICT dell'e-government e delle infrastrutture telematiche della Regione Friuli Venezia Giulia per gli anni 2014-2016" con un'apposita sezione dove possono trovare spazio le specifiche iniziative che dovessero essere necessarie o richieste.

CERT - raFVG

Il CERT - raFVG nasce nel 2005 come punto di riferimento per le attività di sicurezza informatica in ambito regionale. I servizi rientranti nell'ambito vengono erogati normalmente tramite Insiel S.p.A. e sono una parte di quelli previsti dall' "Handbook for CSIRTs" dove CSIRT sta per Computer Security Incident Response Team. In particolare i servizi erogati nel tempo sono i seguenti:

- **Reactive Services**
  - Alerts and Warnings: fornitura di informazioni che descrivano vulnerabilità di sicurezza, intrusioni informatiche, virus o altre minacce e fornitura di indicazioni sulle modalità di comportamento per la gestione del potenziale problema segnalato;
  - Incident Handling: gestione di situazioni di potenziale violazione alla sicurezza informatica;
- **Proactive Services**
  - TechnologyWatch: monitoraggio e aggiornamento sul trend delle evoluzioni delle minacce alla sicurezza e della tecnologia di protezione;
  - Security Audits or Assessments: verifica periodica dello stato di sicurezza delle infrastrutture gestite per azioni correttive e/o migliorative;
  - Intrusion Detection Services: protezione e monitoraggio da eventuali attacchi o intrusioni informatiche.
- **Security Quality Management Services**
  - Security Consulting: fornitura di linee guida per la realizzazione e l'erogazione dei servizi con adeguati livelli di sicurezza;
  - Awareness Building e Education/Training: attività formative e di sensibilizzazione sui temi della sicurezza informatica.

In ottica evolutiva, le azioni di sviluppo previste per il Sistema Informativo Integrato Regionale volte a favorire l'integrazione e la centralizzazione dei servizi estenderanno naturalmente il perimetro delle attività quali la gestione degli incidenti e la disponibilità di misure tecnologiche da mettere a fattor comune a beneficio dei servizi erogati per gli Enti del territorio.

Organizzazione del Security Summit FVG

Il "Security Summit FVG" è una iniziativa organizzata nel maggio 2013 in collaborazione con CLUSIT (Associazione Italiana per la Sicurezza Informatica) con l'obiettivo di portare nelle amministrazioni locali della Regione Friuli Venezia Giulia competenze e "best practice" per una corretta gestione della sicurezza delle informazioni, mutuando la formula del "Security Summit", principale convegno sulla sicurezza informatica in Italia. Il convegno è stato indirizzato ad un pubblico di utenti, anche non specializzati, costituito principalmente da responsabili di enti ed amministrazioni locali, con l'obiettivo di:

- Aumentare la conoscenza delle delicate problematiche tecnologiche, organizzative, legali e gestionali connesse alla sicurezza delle informazioni e quindi incrementare la cultura della sicurezza;
- Diffondere i concetti di base e le "buone prassi" della ICT Security presso i dipendenti delle Pubbliche Amministrazioni locali, che per il loro ruolo utilizzano computer con applicazioni di tipo "office" e che hanno relazioni con l'interno e l'esterno della Pubblica Amministrazione attraverso email, navigazione siti, scambio file, utilizzo di nuovi dispositivi (smartphone, tablet), ecc.;
- Approfondire, anche a beneficio degli addetti ai sistemi IT e/o alla sicurezza ICT, alcuni temi specialistici di particolare interesse ed attualità.

Inoltre per dare conto ai cittadini delle iniziative inerenti al rispetto e all'armonizzazione con l'agenda digitale italiana, la Regione ha pubblicato nella sezione del proprio portale dedicata all'Agenda Digitale FVG l'elenco delle iniziative intraprese sul fronte della digitalizzazione e della sicurezza.

CAPITOLO

5 Conclusione e raccomandazioni

Google è il perfetto esempio di quanto può valere l'informazione dei cittadini nel mondo di Internet. Nonostante nel 2013 abbia speso 7,3 miliardi di dollari per ammodernare i suoi data centers in termini di reti e hardware e la maggior parte delle sue applicazioni sono gratuite, Google è riuscita ad essere una delle aziende a più alto profitto a livello mondiale. La potenza di Google sta tutta nelle informazioni che gli utenti lasciano al suo interno e che possono essere usate per profilare gli stessi e migliorare le loro applicazioni di punta, traendo profitti con pubblicità mirate. Gli utenti, lato loro, sono contenti in quanto avvertono il miglioramento continuo delle applicazioni. In essenza, questa è la magia di Google.

La pubblica amministrazione italiana deve avere consapevolezza che i dati che posseggono, a livello locale, regionale e nazionale, hanno un grande valore. Il valore di questi dati può essere di tipo commerciale, di tipo strategico e di sicurezza nazionale, o entrambe le cose contemporaneamente. In ogni caso, va sfruttato ove possibile, ma soprattutto difeso dagli attacchi. Tali attacchi possono ledere la privacy del cittadino, rendere i dati indisponibili, far perdere il valore degli stessi diffondendoli e rendendoli accessibili a terzi.

Se questo semplice concetto non verrà recepito dalle pubbliche amministrazioni sarà difficile che migliori il livello di sicurezza. Il rapporto ha purtroppo evidenziato che la maggior parte delle amministrazioni italiane ha delle capacità difensive molto limitate. Certamente un miglioramento di tali capacità deve andare di pari passo con la possibilità di trovare sul mercato esperti di sicurezza e di poterli far lavorare in un'organizzazione e in un contesto nazionale coordinato, dove le responsabilità del chi fa cosa siano chiare. Per questo l'implementazione del piano strategico nazionale gioca un ruolo strategico.

Di seguito riportiamo una serie di raccomandazioni che partono da quelle a livello di strategia di Paese fino a quelle tecniche e organizzative a livello di singola amministrazione:

5.1 Razionalizzazione del patrimonio informativo della pubblica amministrazione e sicurezza

Non si può pensare di mettere in sicurezza il patrimonio informativo della pubblica amministrazione italiana senza ridurne la superficie di attacco. Infatti, come mostra il rapporto, il numero enorme di micro e mini centri di calcolo (o semplici stanze server) non permette di avere un numero adeguato di tecnici con skill in sicurezza informatica in grado di assicurarne le adeguate difese. Si parla di decine di migliaia di centri di spesa a fronte di un numero di esperti di sicurezza informatica in Italia molto ridotto. Da qui il bisogno di portare avanti, in sinergia, il processo di razionalizzazione del patrimonio informativo della pubblica amministrazione e l'innalzamento dei livelli di sicurezza, come descritto nelle seguenti raccomandazioni:

Aggregazione delle amministrazioni su base geografica o di business per innalzare le difese cibernetiche

Come i grafici relativi alle regioni mostrano chiaramente, la razionalizzazione delle infrastrutture della PA va a braccetto con un aumento di sicurezza. Quest'ultimo si può ottenere, infatti, attraverso un processo di aggregazione che faccia ospitare i sistemi informativi delle pubbliche amministrazioni locali in strutture qualificate (data center), probabilmente già presenti nella regione di appartenenza. Le strutture IT di alcune regioni, spesso gestite da società in-house, possono offrire immediatamente delle risposte a diverse esigenze, tra cui: la presenza di controllo di accesso fisico ai locali (domanda 21); la presenza di un ISMS (domanda 52); la presenza di un gruppo/comitato per la gestione degli incidenti (domanda 53). Inoltre, tale aggregazione aumenterebbe il numero di risorse IT con figure adeguate, tipicamente esperte in sicurezza. Questo imporrebbe, ad esempio ai comuni, la migrazione del loro livello interno di organizzazione della sicurezza, gettando così le basi di un circolo virtuoso che porterebbe in pochissimo tempo i comuni ad avere gli stessi livelli di sicurezza delle regioni, rendendo il sistema Paese immediatamente più resistente a minacce cibernetiche. Realtà di questo tipo sono già presenti in Italia, il caso di studio Friuli Venezia Giulia ne è un esempio.

Ciò che è stato sottolineato su base geografica per regioni e comuni potrebbe essere realizzato per enti nazionali e locali che condividono lo stesso "business". Ad esempio, Aziende Ospedaliere, Aziende Sanitarie Locali e Ministero della salute potrebbero essere ospitati da alcuni data center interconnessi sul territorio nazionale condividendo applicazioni, dati e infrastrutture. Quello che ha fatto il CINECA con le università può essere un esempio di tale processo di incorporamento, o più in piccolo, ciò che ha fatto Corte dei Conti con l'avvocatura dello stato.

Infrastruttura di IT come asset strategico nazionale

E' importante rimarcare che una corretta gestione di una infrastruttura che sia basata su cloud regionali, non porrebbe ostacoli alla proprietà, alla riservatezza o alla operatività dei comuni. Ridurrebbe però sensibilmente i costi di gestione attraverso la condivisione di applicazioni e dell'infrastruttura stessa. Quindi razionalizzare l'infrastruttura tecnologica della pubblica amministrazione, passando dalle attuali decine di migliaia di centri spesa, a un numero prossimo ai cinquantina, avrebbe il triplo vantaggio di (i) realizzare risparmi nell'ordine di centinaia di milioni di euro, (ii) aumentare sensibilmente i livelli di sicurezza e di disponibilità dei servizi della PA e (iii) realizzare un vero e proprio asset infrastrutturale tecnologico necessario per lo sviluppo del Paese. Certamente tutto questo non può essere ottenuto a costo zero ma attraverso un investimento adeguato da parte del governo, che renda conveniente questa transizione. Da notare come un'organizzazione così strutturata avrebbe il vantaggio di rendere più semplice la mobilità dei dipendenti, ad esempio tra amministrazioni della stessa regione, che ritroverebbero gli stessi strumenti di lavoro informatico.

Data center della pubblica amministrazione come infrastrutture critiche

Esattamente come avviene nei sistemi informativi delle compagnie che gestiscono infrastrutture critiche (elettricità, gas, acqua, trasporti etc.), i dati mantenuti all'interno delle pubbliche amministrazioni possono essere particolarmente importanti, sia per quanto riguarda la sicurezza, sia per la stabilità di un Paese. Si pensi ad esempio alle ripercussioni che potrebbero avere malfunzionamenti o attacchi ad applicazioni che gestiscono il debito pubblico del Paese, o all'Agenzia delle Entrate, al Catasto, al Servizio Sanitario Nazionale etc. In una visione simile a quella individuata nella precedente raccomandazione, i data center della pubblica amministrazione dovrebbero essere considerati come infrastrutture critiche, imponendo quindi opportuni livelli di sicurezza e di affidabilità alle strutture. Il livello di criticità della struttura dovrebbe essere definito in base alla criticità delle informazioni che immagazzina. Tutto ciò andrebbe appositamente normato a livello nazionale.

Cloud "made in Italy" e volano economico per piccole e medie imprese

Questa rete di data center qualificati potrebbe essere usata anche per ospitare i sistemi informativi di piccole e medie imprese. Questo getterebbe le basi per la creazione di una nuvola "made in Italy", sulla base del modello tedesco, che permetta lo sviluppo di tali imprese, sempre garantendo la riservatezza delle informazioni trattate, in

accordo alle normative vigenti nel nostro Paese. Usando fornitori di servizi cloud americani, come Amazon, per ospitare dati e applicazioni dell'azienda, non si deve dimenticare che questi fornitori sono sottoposti al Patriot Act, quindi per i dati da loro ospitati il governo americano potrebbe avere voce in capitolo.

5.2 Implementazione del piano strategico di sicurezza cibernetica

Questa sezione analizza alcune raccomandazioni in base al piano strategico di sicurezza cibernetica firmato dal Presidente del Consiglio dei Ministri Letta nel Dicembre 2013 e pubblicato in G.U. nel febbraio del 2014.

Centralizzazione delle competenze e responsabilità nel quadro strategico di sicurezza cibernetica

Il quadro che esce fuori dal piano strategico nazionale di sicurezza cibernetica è distribuito e frastagliato in termini di competenze e responsabilità nella prevenzione, gestione e risposta ad attacchi cyber. In Italia, inoltre, abbiamo una mancanza di esperti di sicurezza che non consiglia una ulteriore dispersione di queste competenze tra i tanti attori partecipanti al quadro strategico nazionale. Infine la velocità con cui gli attacchi si dispiegano richiederebbe un forte coordinamento tra rilevazione della minaccia e risposta che non consiglia una distribuzione delle responsabilità. Quindi una revisione del piano strategico allo scopo di centralizzare, ove possibile, competenze e responsabilità sarebbe auspicabile, se non mandatorio. Molti paesi come Francia, Germania, Israele e Olanda hanno già concentrato queste attività in apposite agenzie o enti.

Operatività dei CERT e information sharing

L'Italia rispetto ad altri paesi ha registrato un ritardo significativo nella operatività dei CERT. Rendere operativo il sistema dei CERT nazionali come definito dal Decreto Monti del 24 Gennaio 2013, rimane quindi una priorità assoluta. Per quanto riguarda la pubblica amministrazione, la priorità è l'organizzazione di una rete di CERT regionali con a capo il CERT PA e la creazione di un appropriato sistema di information sharing, in modo da migliorare la prevenzione e la risposta alla minaccia cyber. Inoltre il CERT dovrebbe definire chiare linee guida per la classificazione delle minacce, dei loro livelli di criticità e di sensitività.

Promuovere la cultura della sicurezza: tecnologia vs fattore umano

Dai grafici del report si evince che, per tutte le categorie sotto esame, il valore ottenuto nel KPI *Defense* (che si associa al possesso e uso di tecnologie per la protezione e la difesa) è più alto, in media, dei KPI *Awareness* e *Organization*: questo significa che si spende mediamente di più in tecnologie, anche non frutto di progetti di insieme e di visioni strategiche, mentre si tralasciano aspetti legati al fattore umano (awareness) e all'organizzazione, che stanno alla base dell'uso di tali tecnologie e alla base della loro potenzialità di resa in termini di efficacia. Questo è un ritornello noto, frutto della lontananza dell'utente medio dal lessico e dalle tecniche dell'"esperto", ma è anche il frutto di una patologica pigrizia e di una incapacità di trascinamento intrinseche alle PA. Si pensa sempre più spesso che i "pezzi di ferro" in surplus compensino l'inefficacia del nostro operato. Tutto ciò ricade all'interno del famigerato "fattore umano", che in campo sicurezza è tanto importante quanto il possesso e l'operatività di buona tecnologia. Il fattore umano viene ulteriormente esacerbato dal problema che la sicurezza e le sue "policy" sono percepite come orpelli, atti a ritardare e controllare l'impiegato e il funzionario medio di una PA. In una parola sono percepite come i tornelli per il controllo delle presenze. E la dirigenza non ha strumenti (né motivazione) per cambiare tale percezione.

Migliorare la consapevolezza nella pubblica amministrazione riguardo l'importanza del patrimonio informativo che questa gestisce e la consapevolezza di come il singolo impiegato possa essere obiettivo di un attacco facilitando, suo malgrado, accessi ai sistemi dell'ente senza che le tecnologie preposte siano in grado di rilevarli. Lavorare su questa consapevolezza significa migliorare il fattore umano.

Addestrare sul campo i lavoratori delle PA attraverso formazione ed esercitazione è tanto importante quanto acquisire nuova tecnologia. Sulla stessa linea, assessment organizzativi diventano importanti come, ad esempio, penetration testing e altre pratiche tecnologiche.

Ricerca, sviluppo e investimenti in tecnologia

Poiché la messa in sicurezza del cyber space nazionale è un obiettivo strategico che impatta crescita e prosperità della Nazione e questo obiettivo è in continuo movimento a causa della natura dell'avversario, non possiamo dare in outsourcing queste competenze ad altre Nazioni, anche amiche, ma dobbiamo trovare una soluzione metodologica, di policy, organizzativa e (il più possibile) tecnologica italiana al problema per poi renderla coerente rispetto ad un quadro di alleanze internazionali. Migliorare le competenze domestiche e consolidare il ruolo di primo attore che l'Italia ha in questo settore (in questo momento) a livello internazionale. Bloccare l'emorragia di personale con grandi competenze di sicurezza che sta abbandonando l'Italia.

Per fare questo c'è bisogno di un grande piano di riqualificazione tecnologica delle infrastrutture italiane con una visione chiara e diretta allo sviluppo della Nazione come quello definito nelle prime raccomandazioni. Razionalizzazione e ristrutturazione dell'infrastruttura tecnologica italiana rappresenterebbero un gigantesco volano economico per il Paese. Per fare questo ci vogliono attori di dimensione nazionale. Sul piano ricerca stiamo cercando di fare del nostro meglio per presentare una comunità scientifica italiana organizzata e compatta. La creazione del Laboratorio Nazionale di Cyber Security [1] va in questa direzione. Finanziare ricerca e industria in questo settore all'interno di un progetto strategico è quindi prioritario. Tutto deve essere realizzato per raggiungere, come Italia, il maggior grado di indipendenza possibile nella prevenzione e gestione di rischi relativi al nostro patrimonio informatico.

5.3 Suggerimenti alle pubbliche amministrazioni per migliorare i loro livelli di sicurezza

In questa sezione elenchiamo alcune raccomandazioni per le singole pubbliche amministrazioni che vogliono migliorare i loro livelli di sicurezza basandosi sui risultati ottenuti dai loro questionari. Particolare attenzione è posta al rapporto costi-benefici, rivolgendosi quindi soprattutto a quelle amministrazioni che intendono migliorare il proprio livello di sicurezza in maniera rapida ed economica.

Suggerimenti alle PA: L'importanza del Risk Assessment

La cultura della sicurezza richiede investimenti e tali investimenti non necessariamente portano ad un beneficio tangibile. E' chiaro, quindi, che nel momento stesso in cui ci si pone il problema non si sappia a quale attività dedicare i propri sforzi. Noi crediamo che il punto cruciale da cui partire al fine di ottenere il miglior rapporto costi-benefici sia il Risk Assessment.

Non è un caso infatti che l'analisi statistica dei risultati ottenuti in questo studio ha evidenziato come le amministrazioni che effettuano risk assessment, soprattutto se certificato da organizzazioni esterne, abbiano avuto una valutazione complessiva migliore. Eseguire Risk Assessment significa porsi il problema della sicurezza, andare a scovare le proprie criticità, capire con certezza quali sono i punti sui quali agire; fornisce, quindi, in maniera tempestiva ed economica, le direzioni da prendere.

Suggerimenti alle PA: Accesso fisico ai locali IT e logico a tutte le postazioni

La cyber security parte dal controllo degli accessi fisici ai locali. Non ha senso implementare anche le più innovative misure anti intrusione informatica se poi è possibile entrare fisicamente nei locali ospitanti le risorse e i dati informatici. Purtroppo da questa indagine è emerso che la mancata restrizione degli accessi fisici è tra le pratiche

[1] Cyber Security National Laboratory: `http://www.consorzio-cini.it/lab-cyber-security`.

più comuni. Questo è uno dei punti da cui partire per migliorare il livello di sicurezza della propria amministrazione. Implementare sistemi di restrizione a tutti i locali ospitanti server, ma anche computer che hanno accesso a dati rilevanti è mandatorio. L'ideale sarebbe l'utilizzo di certificati per l'accesso logico a tutte le macchine presenti nell'ambito dell'amministrazione e fisico per tutti i locali ospitanti dati o informazioni rilevanti.

Suggerimenti alle PA: Penetration Testing

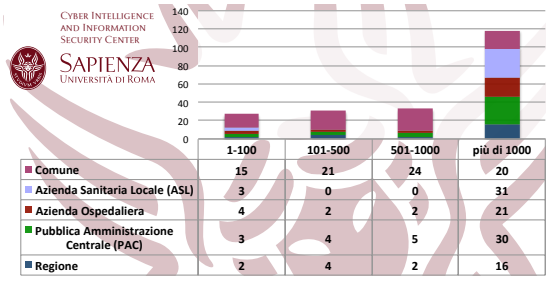
Il principale veicolo di attacchi informatici è il web. Il 100% delle amministrazioni contattate ha confermato di fornire servizi attraverso questo canale. E' ovvio quindi che il più esposto punto di accesso al sistema informativo di ogni amministrazione è il sito web. Il penetration testing consiste nel simulare le azioni di attaccanti al fine di scovare eventuali falle di sicurezza dei punti di accesso del sistema informativo. E' un'attività economica, se paragonata ad una estensiva fase di risk assessment. Chiunque espone servizi via web deve adoperarsi per effettuare penetration test periodici, dato che nuove vulnerabilità su sistemi adoperati tuttora in utilizzo, sono scoperte con cadenza giornaliera.

Suggerimenti alle PA: Esternalizzare i servizi critici in caso di impossibilità nel proteggerli

Esternalizzare alcuni o tutti i servizi in caso ci si renda conto di non essere in grado di proteggerli accuratamente può essere la soluzione più economica per migliorare sensibilmente le proprie capacità in termini di sicurezza. Il budget può essere il principale fattore che fa mettere da parte le pratiche di protezione dei sistemi IT. Questo è naturalmente dovuto al fatto che si paga per un beneficio potenziale piuttosto che tangibile. Una buona cultura della sicurezza, magari a valle di una fase di risk assessment, è in grado di individuare i principali problemi e, se non si è in grado di risolverli, stipulare contratti con provider di sicurezza può migliorare la protezione dei propri servizi e dei propri dati. In alternativa può essere più economico rispetto a soluzioni puramente in-house, appoggiarsi a società terze. Nell'indagine condotta, le regioni e PAC che hanno una società in-house dedita all'IT hanno ottenuto risultati notevolmente migliori.

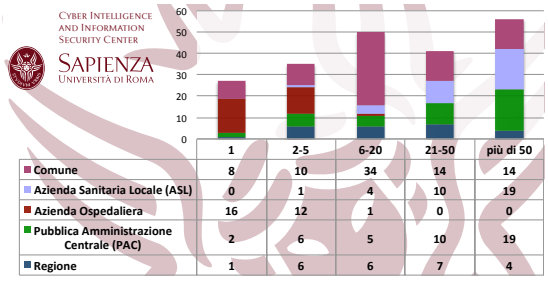
Appendice: Questionario e Risposte alle Domande

Questa appendice riporta le domande del questionario posto alle Pubbliche Amministrazioni e le risposte ottenute aggregate per categoria di amministrazione. Si noti che non sono risultati percentuali e che durante la sottomissione era implementata una logica di salto: alcune domande non sono state poste ai rispondenti in quanto escluse dalla risposta data a domande precedenti.



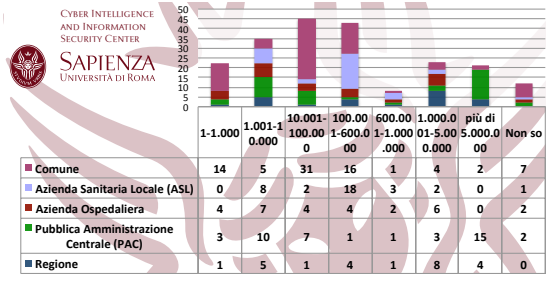
	1-100	101-500	501-1000	più di 1000
Comune	15	21	24	20
Azienda Sanitaria Locale (ASL)	3	0	0	31
Azienda Ospedaliera	4	2	2	21
Pubblica Amministrazione Centrale (PAC)	3	4	5	30
Regione	2	4	2	16

Domanda n.4: Selezionare il numero di dipendenti



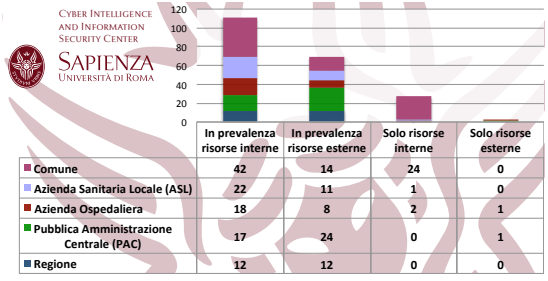
	1	2-5	6-20	21-50	più di 50
Comune	8	10	34	14	14
Azienda Sanitaria Locale (ASL)	0	1	4	10	19
Azienda Ospedaliera	16	12	1	0	0
Pubblica Amministrazione Centrale (PAC)	2	6	5	10	19
Regione	1	6	6	7	4

Domanda n.5: Selezionare il numero di sedi



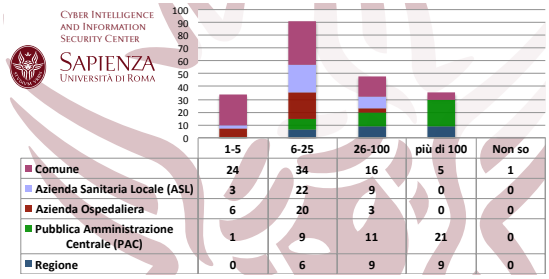
	1-1.000	1.001-10.000	10.001-100.000	100.000-600.000	600.000-1.000.000	1.000.001-5.000.000	più di 5.000.000	Non so
Comune	14	5	31	16	1	4	2	7
Azienda Sanitaria Locale (ASL)	0	8	2	18	3	2	0	1
Azienda Ospedaliera	4	7	4	4	2	6	0	2
Pubblica Amministrazione Centrale (PAC)	3	10	7	1	1	3	15	2
Regione	1	5	1	4	1	8	4	0

Domanda n.6: Inserire il numero degli utenti (sia interni che esterni) che possono usufruire dei servizi forniti dalla PA di riferimento



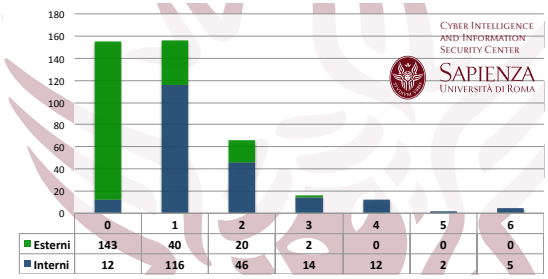
	In prevalenza risorse interne	In prevalenza risorse esterne	Solo risorse interne	Solo risorse esterne
Comune	42	14	24	0
Azienda Sanitaria Locale (ASL)	22	11	1	0
Azienda Ospedaliera	18	8	2	1
Pubblica Amministrazione Centrale (PAC)	17	24	0	1
Regione	12	12	0	0

Domanda n.9: Gli addetti/dipendenti IT sono



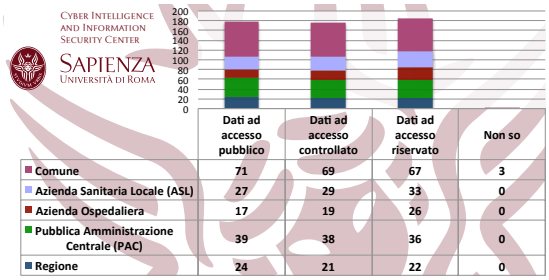
	1-5	6-25	26-100	più di 100	Non so
Comune	24	34	16	5	1
Azienda Sanitaria Locale (ASL)	3	22	9	0	0
Azienda Ospedaliera	6	20	3	0	0
Pubblica Amministrazione Centrale (PAC)	1	9	11	21	0
Regione	0	6	9	9	0

Domanda n.10: Selezionare il numero di addetti/dipendenti IT



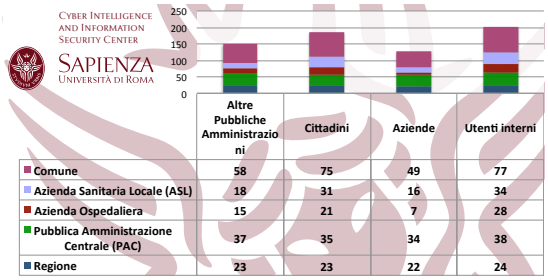
	0	1	2	3	4	5	6
Esterni	143	40	20	2	0	0	0
Interni	12	116	46	14	12	2	5

Domanda n.11: Selezionare il numero di Centri di Elaborazione Dati (CED o data center) della PA di riferimento.



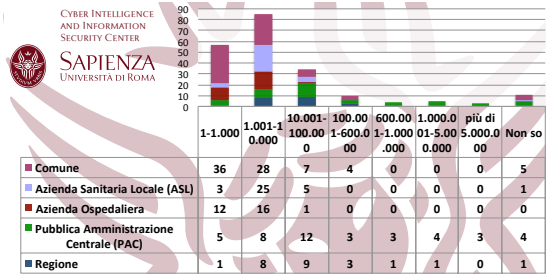
	Dati ad accesso pubblico	Dati ad accesso controllato	Dati ad accesso riservato	Non so
Comune	71	69	67	3
Azienda Sanitaria Locale (ASL)	27	29	33	0
Azienda Ospedaliera	17	19	26	0
Pubblica Amministrazione Centrale (PAC)	39	38	36	0
Regione	24	21	22	0

Domanda n.12: Selezionare il tipo di dati trattati



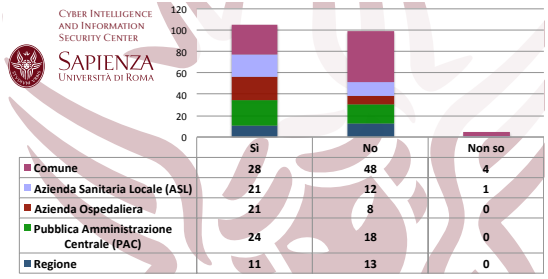
	Altre Pubbliche Amministrazioni	Cittadini	Aziende	Utenti interni
Comune	58	75	49	77
Azienda Sanitaria Locale (ASL)	18	31	16	34
Azienda Ospedaliera	15	21	7	28
Pubblica Amministrazione Centrale (PAC)	37	35	34	38
Regione	23	23	22	24

Domanda n.13: Selezionare le tipologie di utenza che i sistemi IT servono



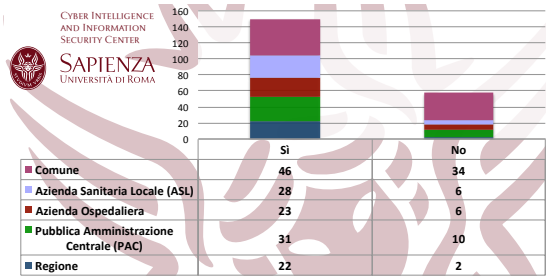
	1-1.000	1.001-10.000	10.001-100.000	100.001-600.000	600.001-1.000.000	1.000.001-5.000.000	più di 5.000.000	Non so
Comune	36	28	7	4	0	0	0	5
Azienda Sanitaria Locale (ASL)	3	25	5	0	0	0	0	1
Azienda Ospedaliera	12	16	1	0	0	0	0	0
Pubblica Amministrazione Centrale (PAC)	5	8	12	3	3	4	3	4
Regione	1	8	9	3	1	1	0	1

Domanda n.14: Selezionare il numero di utenti registrati che fruiscono dei servizi IT



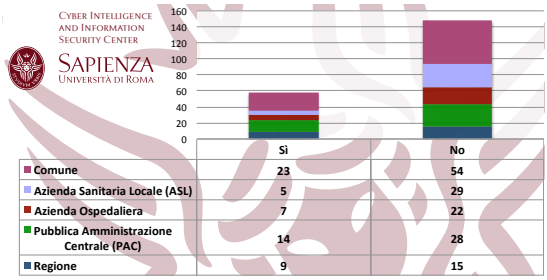
	Sì	No	Non so
Comune	28	48	4
Azienda Sanitaria Locale (ASL)	21	12	1
Azienda Ospedaliera	21	8	0
Pubblica Amministrazione Centrale (PAC)	24	18	0
Regione	11	13	0

Domanda n.15: La PA di riferimento fornisce servizi IT critici per i quali un'indisponibilità anche breve (fino a un'ora) non è tollerabile?



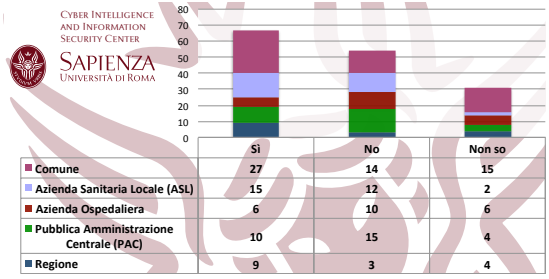
	Sì	No
Comune	46	34
Azienda Sanitaria Locale (ASL)	28	6
Azienda Ospedaliera	23	6
Pubblica Amministrazione Centrale (PAC)	31	10
Regione	22	2

Domanda n.16: I dipendenti possono accedere ai sistemi o ai dati critici dall'esterno, usando login remoto (ad esempio ssh, vpn o similari)?



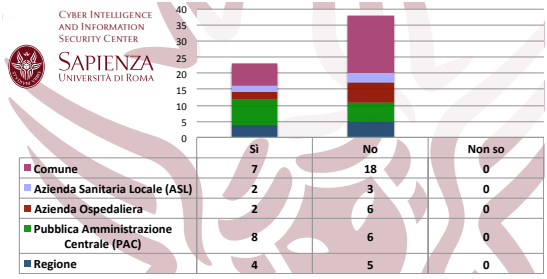
	Sì	No
Comune	23	54
Azienda Sanitaria Locale (ASL)	5	29
Azienda Ospedaliera	7	22
Pubblica Amministrazione Centrale (PAC)	14	28
Regione	9	15

Domanda n.17: La PA di riferimento utilizza servizi basati su Cloud Computing?



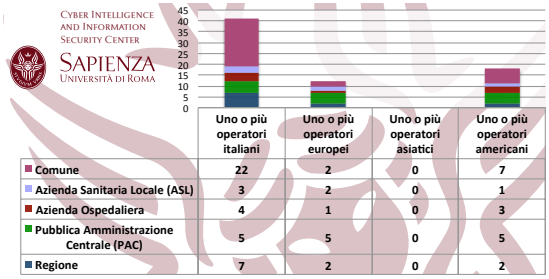
	Sì	No	Non so
Comune	27	14	15
Azienda Sanitaria Locale (ASL)	15	12	2
Azienda Ospedaliera	6	10	6
Pubblica Amministrazione Centrale (PAC)	10	15	4
Regione	9	3	4

Domanda n.18: La PA di riferimento ha intenzione di usare servizi basati su Cloud Computing?



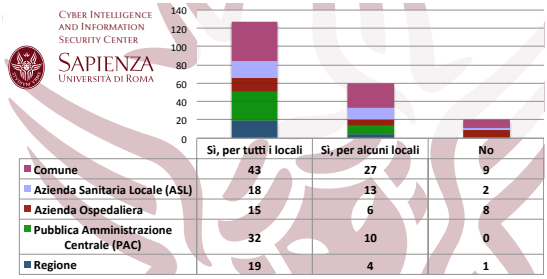
	Sì	No	Non so
Comune	7	18	0
Azienda Sanitaria Locale (ASL)	2	3	0
Azienda Ospedaliera	2	6	0
Pubblica Amministrazione Centrale (PAC)	8	6	0
Regione	4	5	0

Domanda n.19: Esistono servizi critici offerti dalla PA basati su Cloud Computing?



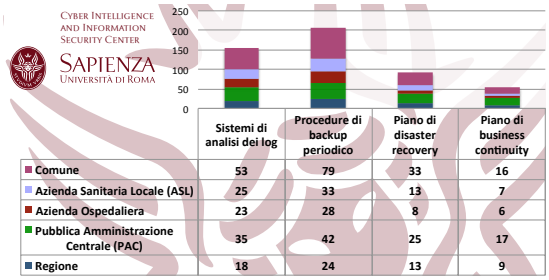
	Uno o più operatori italiani	Uno o più operatori europei	Uno o più operatori asiatici	Uno o più operatori americani
Comune	22	2	0	7
Azienda Sanitaria Locale (ASL)	3	2	0	1
Azienda Ospedaliera	4	1	0	3
Pubblica Amministrazione Centrale (PAC)	5	5	0	5
Regione	7	2	0	2

Domanda n.20: Per il Cloud Computing la PA si avvale di:



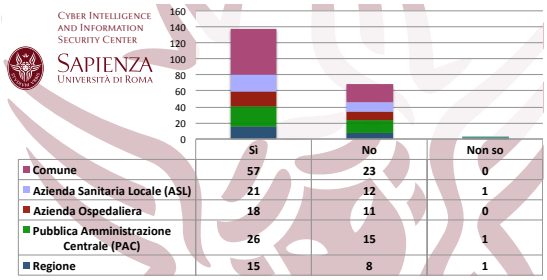
	Sì, per tutti i locali	Sì, per alcuni locali	No
Comune	43	27	9
Azienda Sanitaria Locale (ASL)	18	13	2
Azienda Ospedaliera	15	6	8
Pubblica Amministrazione Centrale (PAC)	32	10	0
Regione	19	4	1

Domanda n.21: Esistono sistemi di controllo degli accessi fisici ai locali che ospitano risorse elaborative, di storage e di rete (escluse postazioni personali)?



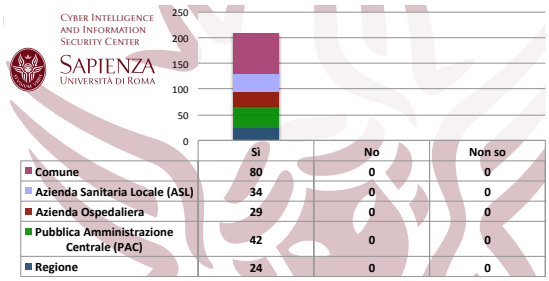
	Sistemi di analisi dei log	Procedure di backup periodico	Piano di disaster recovery	Piano di business continuity
Comune	53	79	33	16
Azienda Sanitaria Locale (ASL)	25	33	13	7
Azienda Ospedaliera	23	28	8	6
Pubblica Amministrazione Centrale (PAC)	35	42	25	17
Regione	18	24	13	9

Domanda n.22: I dati e i documenti informatici custoditi sono controllati e protetti da:



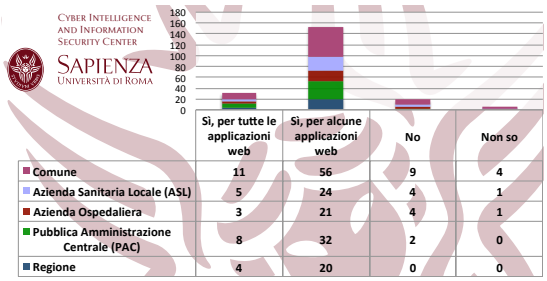
	Sì	No	Non so
Comune	57	23	0
Azienda Sanitaria Locale (ASL)	21	12	1
Azienda Ospedaliera	18	11	0
Pubblica Amministrazione Centrale (PAC)	26	15	1
Regione	15	8	1

Domanda n.23: I supporti contenenti i dati di backup sono conservati materialmente in un altro sito fisico?



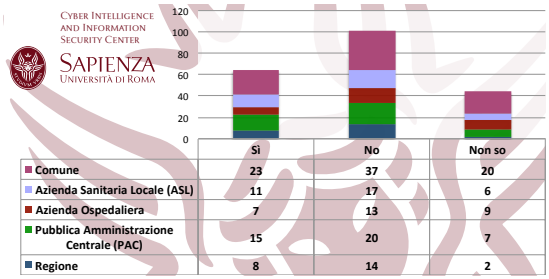
	Sì	No	Non so
Comune	80	0	0
Azienda Sanitaria Locale (ASL)	34	0	0
Azienda Ospedaliera	29	0	0
Pubblica Amministrazione Centrale (PAC)	42	0	0
Regione	24	0	0

Domanda n.24: La PA di riferimento utilizza e/o fornisce servizi basati su tecnologie WEB?



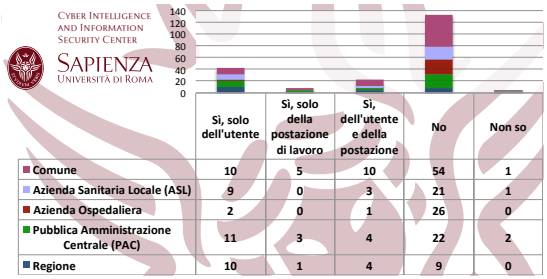
	Sì, per tutte le applicazioni web	Sì, per alcune applicazioni web	No	Non so
Comune	11	56	9	4
Azienda Sanitaria Locale (ASL)	5	24	4	1
Azienda Ospedaliera	3	21	4	1
Pubblica Amministrazione Centrale (PAC)	8	32	2	0
Regione	4	20	0	0

Domanda n.25: Le applicazioni web fornite e/o utilizzate dalla PA di riferimento sono offerte adoperando protocollo SSL/TLS?



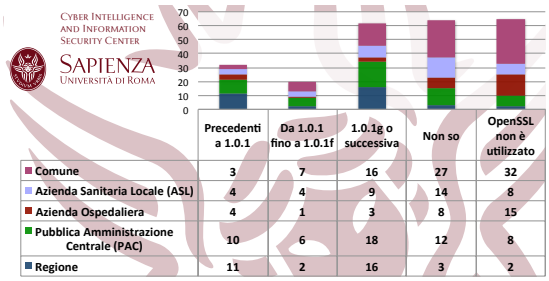
	Sì	No	Non so
Comune	23	37	20
Azienda Sanitaria Locale (ASL)	11	17	6
Azienda Ospedaliera	7	13	9
Pubblica Amministrazione Centrale (PAC)	15	20	7
Regione	8	14	2

Domanda n.26: Nel caso sia utilizzato https, vengono usati certificati digitali Extended Validation (EV)?



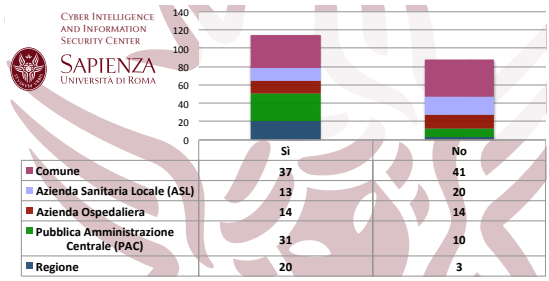
	Sì, solo dell'utente	Sì, solo della postazione di lavoro	Sì, dell'utente e della postazione	No	Non so
Comune	10	5	10	54	1
Azienda Sanitaria Locale (ASL)	9	0	3	21	1
Azienda Ospedaliera	2	0	1	26	0
Pubblica Amministrazione Centrale (PAC)	11	3	4	22	2
Regione	10	1	4	9	0

Domanda n.27: Esiste una procedura di autenticazione con certificato digitale dell'utente e della postazione di lavoro?



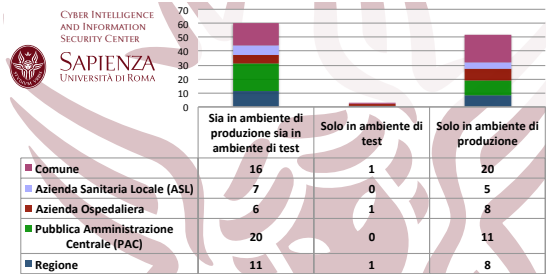
	Precedenti a 1.0.1	Da 1.0.1 fino a 1.0.1f	1.0.1g o successiva	Non so	OpenSSL non è utilizzato
Comune	3	7	16	27	32
Azienda Sanitaria Locale (ASL)	4	4	9	14	8
Azienda Ospedaliera	4	1	3	8	15
Pubblica Amministrazione Centrale (PAC)	10	6	18	12	8
Regione	11	2	16	3	2

Domanda n.28: Se utilizzata la libreria openSSL per SSL/TLS, quale versione?



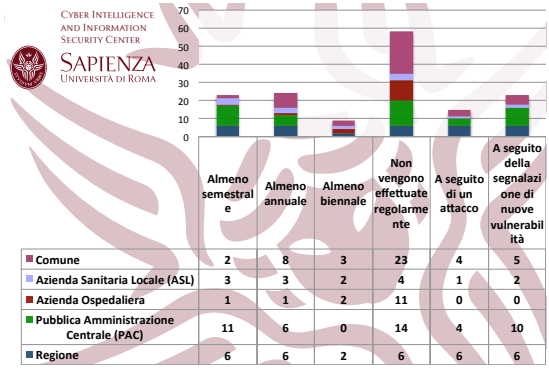
	Sì	No
Comune	37	41
Azienda Sanitaria Locale (ASL)	13	20
Azienda Ospedaliera	14	14
Pubblica Amministrazione Centrale (PAC)	31	10
Regione	20	3

Domanda n.29: Sono state mai effettuate attività di Vulnerability Assessment and Mitigation o Penetration Testing?



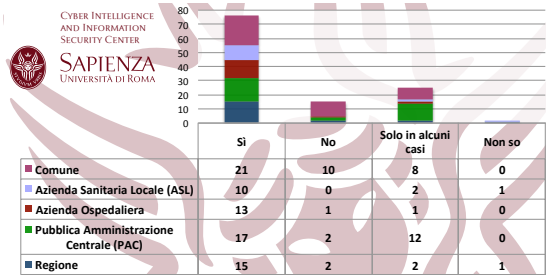
	Sia in ambiente di produzione sia in ambiente di test	Solo in ambiente di test	Solo in ambiente di produzione
Comune	16	1	20
Azienda Sanitaria Locale (ASL)	7	0	5
Azienda Ospedaliera	6	1	8
Pubblica Amministrazione Centrale (PAC)	20	0	11
Regione	11	1	8

Domanda n.30: Rif. Domanda 29, tali test vengono eseguiti:



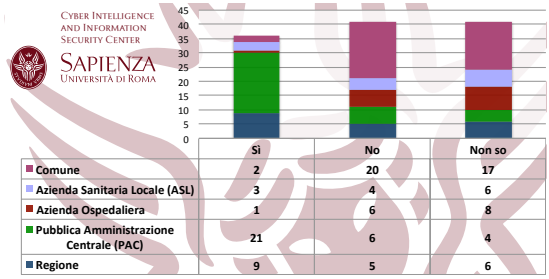
	Almeno semestrale	Almeno annuale	Almeno biennale	Non vengono effettuate regolarmente	A seguito di un attacco	A seguito della segnalazione di nuove vulnerabilità
Comune	2	8	3	23	4	5
Azienda Sanitaria Locale (ASL)	3	3	2	4	1	2
Azienda Ospedaliera	1	1	2	11	0	0
Pubblica Amministrazione Centrale (PAC)	11	6	0	14	4	10
Regione	6	6	2	6	6	6

Domanda n.31: Rif. Domanda 29, con quale cadenza vengono effettuati?



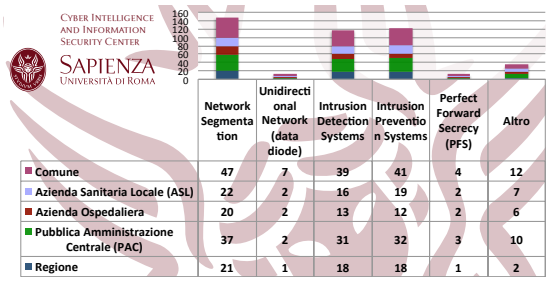
	Sì	No	Solo in alcuni casi	Non so
Comune	21	10	8	0
Azienda Sanitaria Locale (ASL)	10	0	2	1
Azienda Ospedaliera	13	1	1	0
Pubblica Amministrazione Centrale (PAC)	17	2	12	0
Regione	15	2	2	1

Domanda n.32: Rif. Domanda 29, i test vengono eseguiti da fornitori esterni?



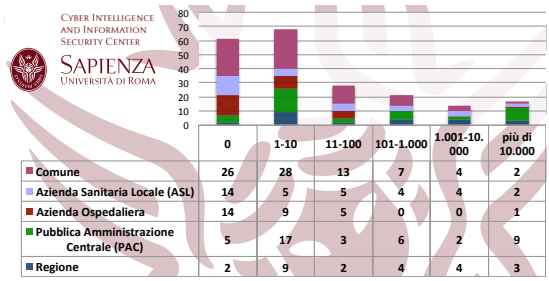
	Sì	No	Non so
Comune	2	20	17
Azienda Sanitaria Locale (ASL)	3	4	6
Azienda Ospedaliera	1	6	8
Pubblica Amministrazione Centrale (PAC)	21	6	4
Regione	9	5	6

Domanda n.33: Rif. Domanda 29, le applicazioni web sono testate seguendo la metodologia OWASP?



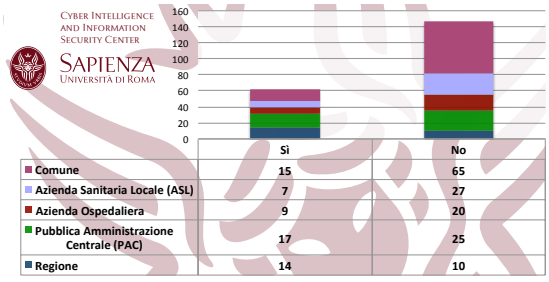
	Network Segmentation	Unidirectional Network (data diode)	Intrusion Detection Systems	Intrusion Prevention Systems	Perfect Forward Secrecy (PFS)	Altro
Comune	47	7	39	41	4	12
Azienda Sanitaria Locale (ASL)	22	2	16	19	2	7
Azienda Ospedaliera	20	2	13	12	2	6
Pubblica Amministrazione Centrale (PAC)	37	2	31	32	3	10
Regione	21	1	18	18	1	2

Domanda n.34: Quali delle seguenti misure sono implementate nei sistemi per prevenire la diffusione di un eventuale attacco cibernetico?



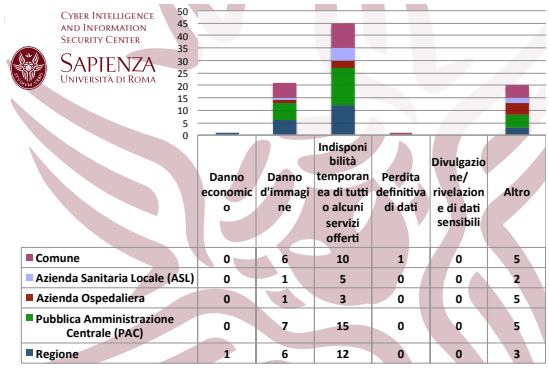
	0	1-10	11-100	101-1.000	1.001-10.000	più di 10.000
Comune	26	28	13	7	4	2
Azienda Sanitaria Locale (ASL)	14	5	5	4	4	2
Azienda Ospedaliera	14	9	5	0	0	1
Pubblica Amministrazione Centrale (PAC)	5	17	3	6	2	9
Regione	2	9	2	4	4	3

Domanda n.35: Quanti tentativi di attacco sono stati rilevati nell'anno 2013?



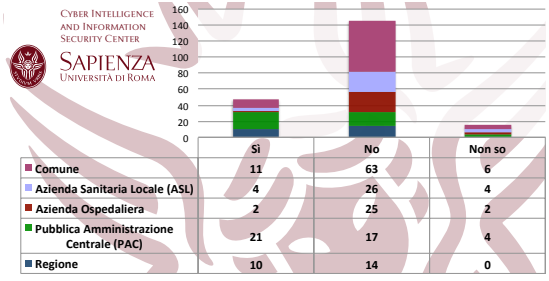
	Si	No
Comune	15	65
Azienda Sanitaria Locale (ASL)	7	27
Azienda Ospedaliera	9	20
Pubblica Amministrazione Centrale (PAC)	17	25
Regione	14	10

Domanda n.36: Si è al corrente di attacchi informatici, di cui la PA di riferimento è stata obiettivo, che hanno avuto successo?



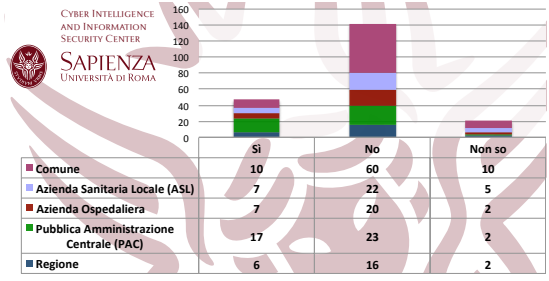
	Danno economico	Danno d'immagine	Indisponibilità temporanea di tutti o alcuni servizi offerti	Perdita definitiva di dati	Divulgazione/ rivelazione di dati sensibili	Altro
Comune	0	6	10	1	0	5
Azienda Sanitaria Locale (ASL)	0	1	5	0	0	2
Azienda Ospedaliera	0	1	3	0	0	5
Pubblica Amministrazione Centrale (PAC)	0	7	15	0	0	5
Regione	1	6	12	0	0	3

Domanda n.37: Quale tipo di danno, causato da attacchi di successo, è stato riscontrato?



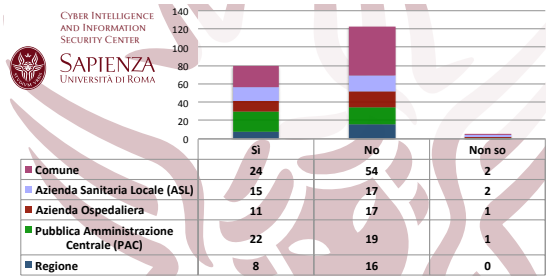
	Si	No	Non so
Comune	11	63	6
Azienda Sanitaria Locale (ASL)	4	26	4
Azienda Ospedaliera	2	25	2
Pubblica Amministrazione Centrale (PAC)	21	17	4
Regione	10	14	0

Domanda n.38: La PA di riferimento ha formalizzato un piano di risposta o una procedura da seguire in caso di rilevazione di un attacco informatico?



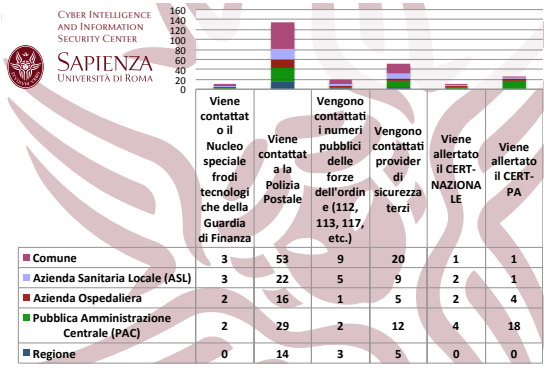
	Si	No	Non so
Comune	10	60	10
Azienda Sanitaria Locale (ASL)	7	22	5
Azienda Ospedaliera	7	20	2
Pubblica Amministrazione Centrale (PAC)	17	23	2
Regione	6	16	2

Domanda n.39: Per la gestione quotidiana degli eventi di sicurezza IT viene adottato un Security Information and Event Management (SIEM)?



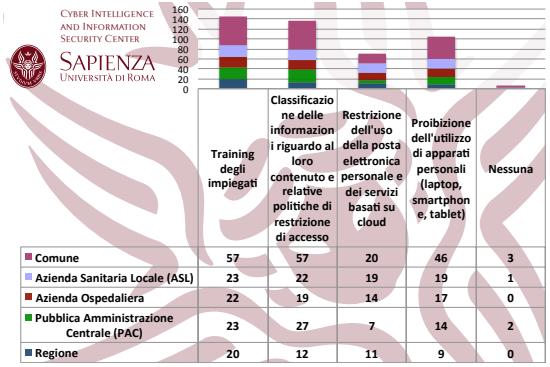
	Si	No	Non so
Comune	24	54	2
Azienda Sanitaria Locale (ASL)	15	17	2
Azienda Ospedaliera	11	17	1
Pubblica Amministrazione Centrale (PAC)	22	19	1
Regione	8	16	0

Domanda n.40: La PA di riferimento ha stipulato contratti con provider di servizi per la sicurezza IT?



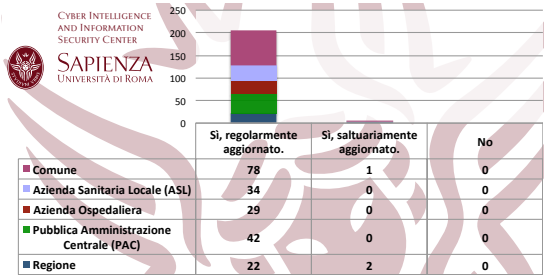
	Viene contattato il Nucleo speciale frodi tecnologiche della Guardia di Finanza	Viene contattata la Polizia Postale	Vengono contattati i numeri pubblici delle forze dell'ordine (112, 113, 117, etc.)	Vengono contattati provider di sicurezza terzi	Viene allertato il CERT-NAZIONALE	Viene allertato il CERT-PA
Comune	3	53	9	20	1	1
Azienda Sanitaria Locale (ASL)	3	22	5	9	2	1
Azienda Ospedaliera	2	16	1	5	2	4
Pubblica Amministrazione Centrale (PAC)	2	29	2	12	4	18
Regione	0	14	3	5	0	0

Domanda n.41: In caso di rilevazione di un attacco nei confronti della PA di riferimento, verso quali enti esterni è prevista una comunicazione?



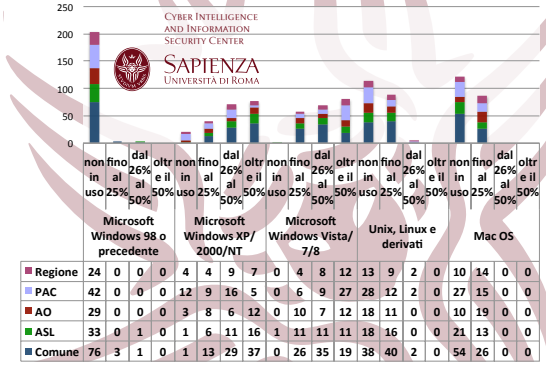
	Training degli impiegati	Classificazione delle informazioni riguardo al loro contenuto e relative politiche di restrizione di accesso	Restrizione dell'uso della posta elettronica personale e dei servizi basati su cloud	Proibizione dell'utilizzo di apparati personali (laptop, smartphone, tablet)	Nessuna
Comune	57	57	20	46	3
Azienda Sanitaria Locale (ASL)	23	22	19	19	1
Azienda Ospedaliera	22	19	14	17	0
Pubblica Amministrazione Centrale (PAC)	23	27	7	14	2
Regione	20	12	11	9	0

Domanda n.42: Quali delle seguenti misure sono implementate per la protezione di dati e sistemi dall'utilizzo scorretto da parte degli impiegati?



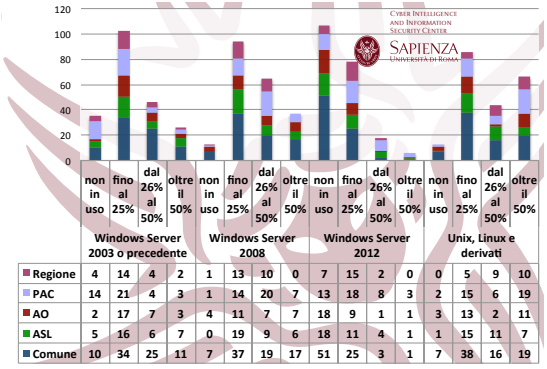
	Si, regolarmente aggiornato.	Si, saltuariamente aggiornato.	No
Comune	78	1	0
Azienda Sanitaria Locale (ASL)	34	0	0
Azienda Ospedaliera	29	0	0
Pubblica Amministrazione Centrale (PAC)	42	0	0
Regione	22	2	0

Domanda n.38: Nella PA di riferimento è prevista l'installazione di software antivirus?



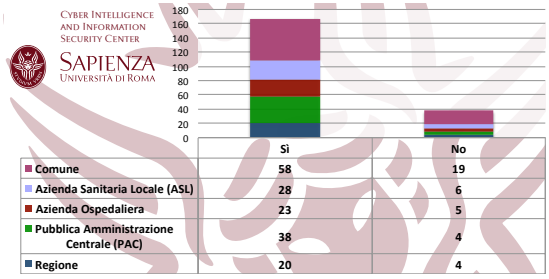
	Microsoft Windows 98 o precedente				Microsoft Windows XP/ 2000/NT				Microsoft Windows Vista/ 7/8				Unix, Linux e derivati				Mac OS			
	non in uso	fino al 25%	dal 26% al 50%	oltre il 50%	non in uso	fino al 25%	dal 26% al 50%	oltre il 50%	non in uso	fino al 25%	dal 26% al 50%	oltre il 50%	non in uso	fino al 25%	dal 26% al 50%	oltre il 50%	non in uso	fino al 25%	dal 26% al 50%	oltre il 50%
Regione	24	0	0	0	4	4	9	7	0	4	8	12	13	9	2	0	10	14	0	0
PAC	42	0	0	0	12	9	16	5	0	6	9	27	28	12	2	0	27	15	0	0
AO	29	0	0	0	3	8	6	12	0	10	7	12	18	11	0	0	10	19	0	0
ASL	33	0	1	0	1	6	11	16	1	11	11	11	18	16	0	0	21	13	0	0
Comune	76	3	1	0	1	13	29	37	0	26	35	19	38	40	2	0	54	26	0	0

Domanda n.44: Selezionare la percentuale di adozione dei sistemi operativi sulle macchine CLIENT operanti nella PA di riferimento



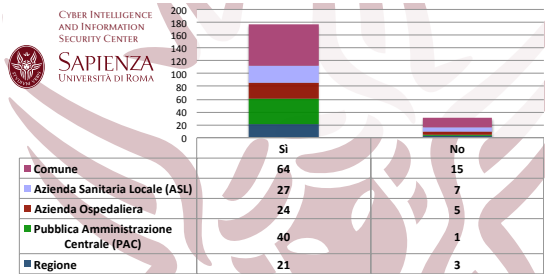
	Windows Server 2003 o precedente				Windows Server 2008				Windows Server 2012				Unix, Linux e derivati			
	non in uso	fino al 25%	dal 26% al 50%	oltre il 50%	non in uso	fino al 25%	dal 26% al 50%	oltre il 50%	non in uso	fino al 25%	dal 26% al 50%	oltre il 50%	non in uso	fino al 25%	dal 26% al 50%	oltre il 50%
Regione	4	14	4	2	1	13	10	0	7	15	2	0	0	5	9	10
PAC	14	21	4	3	1	14	20	7	13	18	8	3	2	15	6	19
AO	2	17	7	3	4	11	7	7	18	9	1	1	3	13	2	11
ASL	5	16	6	7	0	19	9	6	18	11	4	1	1	15	11	7
Comune	10	34	25	11	7	37	19	17	51	25	3	1	7	38	16	19

Domanda n.45: Selezionare la percentuale di adozione dei sistemi operativi sulle macchine SERVER operanti nella PA di riferimento



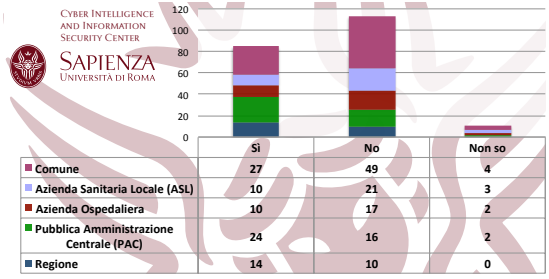
	Sì	No
Comune	58	19
Azienda Sanitaria Locale (ASL)	28	6
Azienda Ospedaliera	23	5
Pubblica Amministrazione Centrale (PAC)	38	4
Regione	20	4

Domanda n.38: Esiste una politica di aggiornamento dei sistemi operativi delle macchine client?



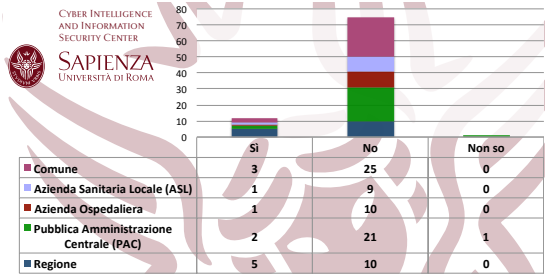
	Sì	No
Comune	64	15
Azienda Sanitaria Locale (ASL)	27	7
Azienda Ospedaliera	24	5
Pubblica Amministrazione Centrale (PAC)	40	1
Regione	21	3

Domanda n.47: Esiste una politica di aggiornamento dei sistemi operativi dei server?



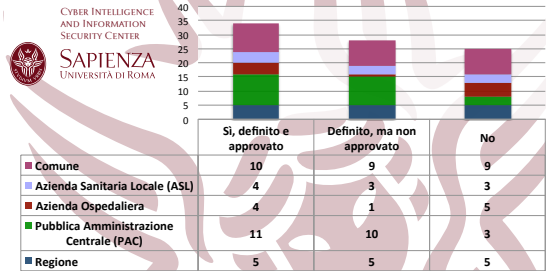
	Sì	No	Non so
Comune	27	49	4
Azienda Sanitaria Locale (ASL)	10	21	3
Azienda Ospedaliera	10	17	2
Pubblica Amministrazione Centrale (PAC)	24	16	2
Regione	14	10	0

Domanda n.48: Viene eseguita periodicamente un'analisi di valutazione del rischio informatico (Risk Assessment)?



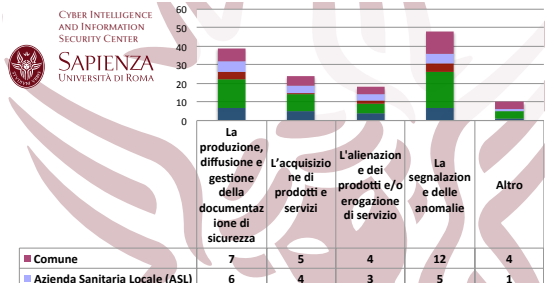
	Sì	No	Non so
Comune	3	25	0
Azienda Sanitaria Locale (ASL)	1	9	0
Azienda Ospedaliera	1	10	0
Pubblica Amministrazione Centrale (PAC)	2	21	1
Regione	5	10	0

Domanda n.49: La valutazione del rischio (risk assessment) è certificata da un'organizzazione esterna?



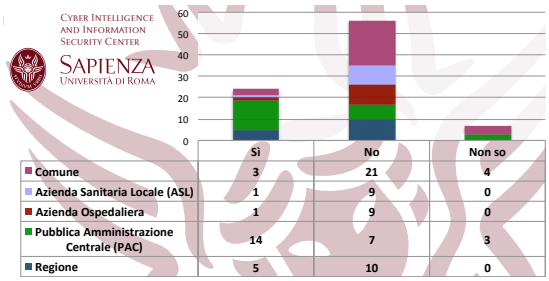
	Sì, definito e approvato	Definito, ma non approvato	No
Comune	10	9	9
Azienda Sanitaria Locale (ASL)	4	3	3
Azienda Ospedaliera	4	1	5
Pubblica Amministrazione Centrale (PAC)	11	10	3
Regione	5	5	5

Domanda n.50: E' stato definito e approvato un documento (Piano della Sicurezza ICT) che descrive l'organizzazione della struttura per la sicurezza informatica, i ruoli e le responsabilità?



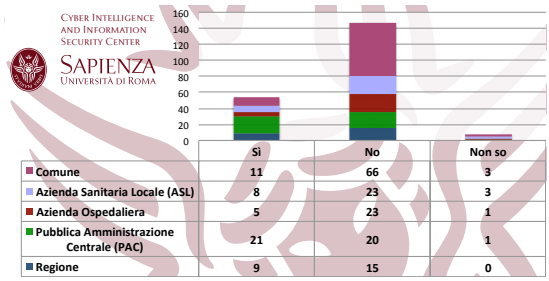
	La produzione, diffusione e gestione della documentazione di sicurezza	L'acquisizione di prodotti e servizi	L'alienazione dei prodotti e/o erogazione di servizio	La segnalazione delle anomalie	Altro
Comune	7	5	4	12	4
Azienda Sanitaria Locale (ASL)	6	4	3	5	1
Azienda Ospedaliera	4	1	2	5	0
Pubblica Amministrazione Centrale (PAC)	15	9	5	19	4
Regione	7	5	4	7	1

Domanda n.51: Il Piano della Sicurezza ICT definisce anche le procedure da seguire per:



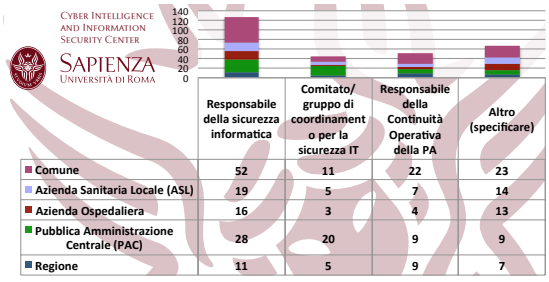
	Sì	No	Non so
Comune	3	21	4
Azienda Sanitaria Locale (ASL)	1	9	0
Azienda Ospedaliera	1	9	0
Pubblica Amministrazione Centrale (PAC)	14	7	3
Regione	5	10	0

Domanda n.52: La PA di riferimento adotta correntemente un Sistema di Gestione per la Sicurezza delle Informazioni (ISMS)?



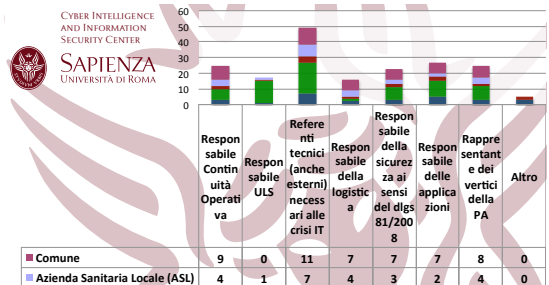
	Sì	No	Non so
Comune	11	66	3
Azienda Sanitaria Locale (ASL)	8	23	3
Azienda Ospedaliera	5	23	1
Pubblica Amministrazione Centrale (PAC)	21	20	1
Regione	9	15	0

Domanda n.53: E' stato creato un gruppo/comitato per la gestione degli incidenti?



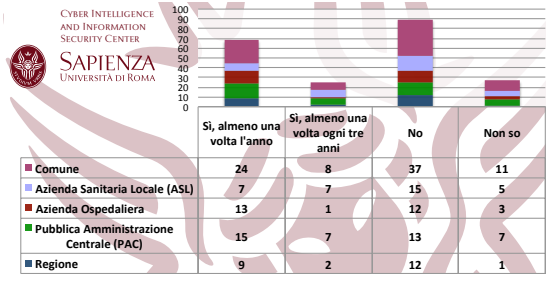
	Responsabile della sicurezza informatica	Comitato/ gruppo di coordinamento per la sicurezza IT	Responsabile della Continuità Operativa della PA	Altro (specificare)
Comune	52	11	22	23
Azienda Sanitaria Locale (ASL)	19	5	7	14
Azienda Ospedaliera	16	3	4	13
Pubblica Amministrazione Centrale (PAC)	28	20	9	9
Regione	11	5	9	7

Domanda n.54: Quali dei seguenti ruoli sono stati individuati (ruoli assegnati a personale) presso la vostra struttura?



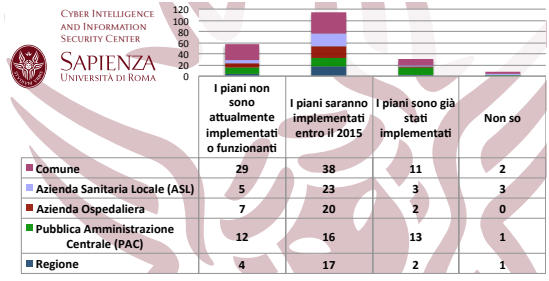
	Responsabile Continuità Operativa	Responsabile ULS	Referenti tecnici (anche esterni) necessari alle crisi IT	Responsabile della logistica	Responsabile della sicurezza ai sensi del dlgs 81/2008	Responsabile delle applicazioni	Rappresentante dei vertici della PA	Altro
Comune	9	0	11	7	7	7	8	0
Azienda Sanitaria Locale (ASL)	4	1	7	4	3	2	4	0
Azienda Ospedaliera	2	1	4	1	2	3	1	2
Pubblica Amministrazione Centrale (PAC)	7	14	20	2	8	10	9	0
Regione	3	1	7	2	3	5	3	3

Domanda n.55: Quali delle seguenti figure sono previste nel Comitato per la gestione degli incidenti?



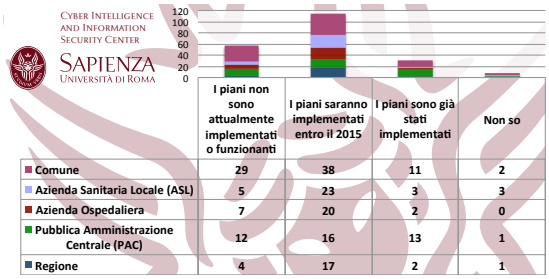
	Sì, almeno una volta l'anno	Sì, almeno una volta ogni tre anni	No	Non so
Comune	24	8	37	11
Azienda Sanitaria Locale (ASL)	7	7	15	5
Azienda Ospedaliera	13	1	12	3
Pubblica Amministrazione Centrale (PAC)	15	7	13	7
Regione	9	2	12	1

Domanda n.57: Sono previste verifiche dell'organizzazione e del funzionamento della sicurezza ICT?



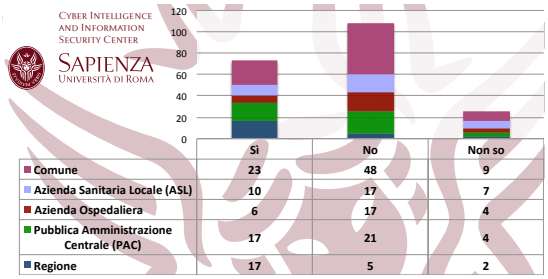
	I piani non sono attualmente implementati o funzionanti	I piani saranno implementati entro il 2015	I piani sono già stati implementati	Non so
Comune	29	38	11	2
Azienda Sanitaria Locale (ASL)	5	23	3	3
Azienda Ospedaliera	7	20	2	0
Pubblica Amministrazione Centrale (PAC)	12	16	13	1
Regione	4	17	2	1

Domanda n.58: Quali delle seguenti iniziative sono state adottate per sensibilizzare il personale alla sicurezza informatica?



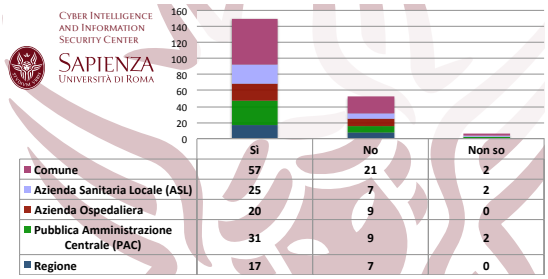
	I piani non sono attualmente implementati o funzionanti	I piani saranno implementati entro il 2015	I piani sono già stati implementati	Non so
Comune	29	38	11	2
Azienda Sanitaria Locale (ASL)	5	23	3	3
Azienda Ospedaliera	7	20	2	0
Pubblica Amministrazione Centrale (PAC)	12	16	13	1
Regione	4	17	2	1

Domanda n.59: In base all'art. 50bis del Codice di Amministrazione Digitale (CAD), avere piani di disaster recovery e continuità operativa è obbligatorio. Nella PA di riferimento:



	Si	No	Non so
Comune	23	48	9
Azienda Sanitaria Locale (ASL)	10	17	7
Azienda Ospedaliera	6	17	4
Pubblica Amministrazione Centrale (PAC)	17	21	4
Regione	17	5	2

Domanda n.60: Il comma 4 art. 50bis del Codice di Amministrazione Digitale (CAD), richiede obbligatoriamente la richiesta di parere ad Agid sullo studio di fattibilità tecnica per quanto riguarda i piani di disaster recovery e business continuity. L'ente ha ottemperato a tale richiesta?



	Si	No	Non so
Comune	57	21	2
Azienda Sanitaria Locale (ASL)	25	7	2
Azienda Ospedaliera	20	9	0
Pubblica Amministrazione Centrale (PAC)	31	9	2
Regione	17	7	0

Domanda n.61: E' possibile che un malfunzionamento di un servizio ICT in una o più società sfornitrici abbia un significativo impatto sulla PA di riferimento?