Report I anno MUSA spoke 4

Cybersecurity
BOZZA

Laser Computer Security Lab, ANCILAB
Prof. Danilo Bruschi
Prof. Alfio Ferrara
Onelia Rivolta
Marzio De Corato
Davide Rusconi
Matteo Zoia
Luca Bramati
Maurizio Piazza

Milano, 13 Febbraio 2024

Rapporto realizzato all'interno del progetto MUSA – Multilayered Urban Sustainability Action, finanziato dall'Unione Europea – NextGenerationE, PNRR Missione 4 Componente 2 Linea di Investimento 1.5: Creazione e rafforzamento degli "ecosistemi dell'innovazione", costruzione di "leader territoriali di R&S"

Hanno partecipato i comuni di: Ricengo, Monticello Brianza, Erve, San Siro, Pognano, Grassobbio, Mulazzano, Rosate, Vailate, Pessano Con Bornago, Moniga Del Garda, Novate Milanese, Corana, Cuggiono, Como, Palazzo Pignano, Laveno-Mombello, Ripalta Arpina, Capralba, Treviolo, Cesana Brianza, Telgate, San Benedetto Po, Sangiano, Piario, Barzana, Vedano Olona, Castellucchio, Padenghe Sul Garda, Montevecchia, Quingentole, Santa Maria Hoè, Bormio, Sarezzo, Asso, Chiari, Musso, Cocquio-Trevisago, Costa Volpino, Nave, Colle Brianza, Zinasco, Marcheno, Rota D'Imagna, Cassinetta Di Lugagnano, Bulciago, Castello Dell'Acqua, Sondrio, Borghetto Lodigiano, Delebio, Curtatone, Zanica, Godiasco Salice Terme, Oggiona Con Santo Stefano, Taino, Cormano, Codogno, Gerola Alta, Borgo San Giovanni, Lierna, Pinarolo Po, Trezzano Sul Naviglio, Bregnano, Galbiate, Pandino, Verolavecchia, Muggiò, Val Brembilla, Lonate Pozzolo, Arsago Seprio, Locate Varesino, Soresina, Treviglio, Casorate Sempione, Renate, Botticino, Verano Brianza, Toscolano-Maderno, Paderno Franciacorta, Fornovo San Giovanni, San Colombano Al Lambro, Gorle, Morimondo, Cervesina, Busto Arsizio, Brescia, Barzio, Gambarana, Bresso, Cassano D'Adda, Buguggiate, Cornate D'Adda, Cozzo, Mandello Del Lario, Rovato, Bressana Bottarone, Albiate, Fiesco, Luino, Albano Sant'Alessandro, Vergiate, Eupilio, Calco, Vimodrone, Chiuduno, Cisano Bergamasco, Baranzate, Pavone Del Mella, Ello, Canegrate, San Gervasio Bresciano, Gardone Riviera, Spino D'Adda, Torre De' Roveri, Romano Di Lombardia, Capriano Del Colle, Marcallo Con Casone, Malegno, Brembio, Luzzana, Cerro Maggiore, Gardone Val Trompia, Cremeno, Fagnano Olona, Voghera, Nerviano, Gussago, Rivanazzano Terme, Sant'Omobono Terme, San Bassano, San Donato Milanese, Filighera, Magnago, Trenzano, Somma Lombardo, Casei Gerola, Sesto Calende, Mello, Tremezzina, Maclodio, Cremona, San Giorgio Su Legnano, Veduggio Con Colzano, Sirone, Valmadrera, Silvano Pietra, Gargnano, Peschiera Borromeo, Arese, Lovere, Castelleone, Venegono Inferiore, Castelnovetto, Castronno, Collio, Bassano Bresciano, Locatello, Seregno, Desenzano Del Garda, San Rocco Al Porto, Bubbiano, Castello Di Brianza, San Genesio Ed Uniti, Motteggiana, Tremosine Sul Garda, Angera, Bione, Pontirolo Nuovo, Villa Carcina, Casatisma, Briosco, Barbianello, Pomponesco, Corteolona E Genzone, Marnate, Sumirago, Alzano Lombardo, Solbiate Olona, Vaiano Cremasco, Pisogne, Albosaggia, Agrate Brianza, Albiolo, Mozzanica, Cesano Maderno, Grantola, Ossona, Arcore, Caronno Pertusella, Lumezzane, Novate Mezzola, Carobbio Degli Angeli, Cazzano Sant'Andrea, Vigevano, Mariano Comense, Sordio, Vedano Al Lambro, Verrua Po, Zeccone

Si ringraziano: Giuseppe Emiliano Vaciago, Matteo Buffa, Raffaella Brighi, Danilo Bruschi, Davide Oliva, Antonella Russo, Stefano Aurelio , Francesco Della Corte, Carlo Camagni, Filippo Perego, Simone Chierichetti, Gabriele Milito, Marco Caudullo, Giovanni Corna , Rossella De vita, Fabio De Campo, Michele Colajanni, Maurizio Piazza, Andrea Lanzi, Andrea Piscopo, Antonella Russo, Sara D'Amico, Marco Caudullo, Giuseppe Coviello, Gerardo Biella, Roberto Pecorini, Aurelio Stefano, Francesco Bassi, Carolina Pettina-

to, Andrea PISCOPO, Mario Testino, Nicla Diomede, Luca Bramati, Enzo M. Tieghi, Claudio Russo, Antonio Giovenzana, Monica Trivella, Antonella Russo, Eleonora Ferrari

INDICE

1 INTRODUZIONE

1.1 PREMESSA

Tra gli scopi del progetto MUSA spoke 4 vi è quello di valutare lo stato della transizione al digitale della nostra pubblica amministrazione a tal proposito abbiamo deciso di intraprendere la nostra indagine valutando il livello di maturità delle amministrazioni locali rispetto a tre tematiche emergenti nel mondo digitale: la cybersecurity, l'adozione di tecniche di Intelligenza Artificiale e il ricorso ai Big data e tecniche di Data Analysis. Il primo anno di indagine è stato focalizzato sulla Cybersecurity, e questo documento espone i risultati ottenuti in questo senso.

1.2 INTRODUZIONE

In seguito saranno presentati i risultati di un'indagine svolta su un campione di comuni lombardi al fine di verificare la "prontezza" degli enti locali ad affrontare le sfide poste dalla transizione al digitale che l'intero pianeta sta attraversando. In particolare, in questo primo rapporto ci siamo soffermati a valutare le competenze di cui questi enti dispongono per far fronte ad una delle principali sfide poste dall'adozione delle tecnologie digitali: la cybersecurity. È stata scelta la cybersecurity perché la stessa costituisce fattore abilitante per lo sviluppo di una qualunque strategia di digitalizzazione che un ente volesse mettere in atto. Investire oggi in progetti di digitalizzazione che non tengano conto o sottovalutino il problema della sicurezza dei sistemi significa ignorare una parte consistente della conoscenza e cultura informatica che si è sviluppata in questi ultimi 40 anni e conseguentemente essere poco adatti a gestire la rivoluzione digitale che sta investendo il nostro pianeta. Tutto ciò è ulteriormente avvalorato dal fatto che negli ultimi anni il tema della Cybersecurity è stato oggetto di molte iniziative rivolte alla pubblica amministrazione con l'obiettivo di sensibilizzare e stimolare le stesse ad intraprendere azioni significative in questo contesto. Quindi i risultati della nostra indagine possono anche essere letti come un'indicazione sull'efficacia di queste iniziative ben descritte nel contributo di ANCILAB a questo volume. Il nostro focus non è quindi determinato dalle percentuali di enti che hanno o meno adottato particolare tecnologie o adottato particolare metodologie ma bensì il fattore umano. Quel fattore che tutti gli esperti a livello internazionale indicano come l'elemento determinante per poter sviluppare una strategia di cybersecurity davvero efficace. Contrariamente ai molti rapporti presenti sul "mercato" finalizzati principalmente a fornire stime quantitative sul fenomeno in termini di percentuali di enti che hanno adottato una certa contromisura piuttosto che hanno stilato una security policy, abbiamo deciso di concentrare, probabilmente tra i primi in questo contesto, la nostra attenzione sulla qualità. Più precisamente, abbiamo cercato di capire qual è il livello culturale sul tema cybersecurity presente nei nostri enti locali ed il loro livello di preparazione per affrontare sfide imminenti come quella del passaggio al cloud. Altro elemento

caratterizzante di questo lavoro è che una volta ottenuti i risultati ed aver proceduto alla loro analisi, non ci siamo fermati come avviene per tutte le indagini statistiche presenti sul mercato, ma, come spiegheremo in seguito, abbiamo voluto appurare sperimentalmente la loro validità. Non ci siamo quindi limitati ad elaborare con avanzate tecniche di machine learning non supervisionato i dati in nostro possesso per estrapolarne il maggior numero possibile di informazioni ma abbiamo voluto validare sul campo i risultati ottenuti. Abbiamo, cioè, cercato di verificare se le competenze riscontrate nella prima fase dell'indagine trovassero un riscontro pratico nella realizzazione dei sistemi di sicurezza approntati dai comuni a difesa dei propri siti web, memori del fatto che nel 2021 l'allora Ministro dell'innovazione Tecnologica e della Transizione Digitale Vittorio Colao aveva dichiarato che il 95% dei siti della pubblica amministrazione non era sicuro. Per effettuare questa verifica abbiamo sottoposto i siti web dei comuni, con l'assenso dei diretti interessati, ad un vulnerability assessment di tipo black box nonché alla simulazione di un attacco di phishing. Accanto ai risultati sulle competenze abbiamo colto l'occasione anche per valutare altri aspetti correlati con la cybersecurity quali la sensibilità degli enti locali al trattamento dei dati.

1.3 GLI OBIETTIVI

Gli aspetti della cybersecurity che abbiamo approfondito possono essere ricondotti alla seguente serie di domande ?

1. Esistono nei comuni competenze sulla cybersecurity? In caso affermativo di quali tipo di competenze parliamo? In una scala da 1 a 10 come possiamo valutare queste competenze ?

2. Quanto sono robusti i siti web dei nostri comuni? Qual è il loro livello di robustezza rispetto ad un attaccante esterno? Quali le forme di attacco più insidiose? Innanzitutto ci interessava capire se è poi così vero che il 95 % dei siti delle pubbliche amministrazioni non è sicuro, anche se l'affermazione si presta a diverse interpretazioni. Se si intende che un sito non è sicuro quando esiste un qualche modo per comprometterne il corretto funzionamento allora possiamo dire che la nostra pubblica amministrazione è in buona compagnia, difficilmente un qualunque sito può reggere un attacco cyber mirato. Il problema che ci siamo posti è quindi quello di capire quanto robusti fossero i sistemi degli enti locali di fronte ad un attaccante dal profilo medio, cioè una persona che usa strumenti di attacco "standard" e non ha possibilità di accessi all'infrastruttura di calcolo dell'ente dall'interno della stessa

3. Una volta stabilità la presenza di competenze ci siamo posti il problema di verificare la bontà di queste competenze nei due ambiti:
   - Tecnologico
   - Metodologico

4. Tutti gli enti pubblici sono alle prese con la migrazione dei propri dati e servizi in cloud, anche in questo caso eravamo interessati a le competenze presenti nei comuni per poter affrontare questa nuova sfida.

5. Abbiamo colto durante i focus group la mancanza di un interlocutore istituzionale a cui rivolgersi per poter chiedere una qualche forma di supporto, abbiamo quindi chiesto ai comuni di indicarci le loro preferenze

6. Abbiamo anche voluto riservare una domanda per valutare la sensibilità degli enti locali al tema della protezione dei dati.

Per approfondire queste problematiche, si è proceduto con alcune sessioni di Focus group a cui hanno partecipato circa 20 comuni che ci hanno consentito di focalizzare la nostra attenzione sui temi che sono maggiormente sentiti nell'ambito degli enti locali. A seguito dei focus group abbiamo predisposto un questionario che è stato mandato ai comuni.

2 LE COMPETENZE IN CYBERSECURITY NEI COMUNI LOMBARDI

Elemento fondamentale di ogni indagine statistica è il questionario. L'analisi della componente soggettiva della sicurezza informatica di un comune è stata svolta utilizzando un questionario. Si tratta, in effetti, di una metodologia che risulta di facile utilizzo, implementazione e scalabilità e può essere allargata a un campione molto ampio tramite la diffusione web. La maggiore difficoltà, in questo caso, risiede nel trovare le domande adeguate e qualora, come nel nostro caso, la risposta voglia essere multipla, di individuare le possibili risposte da sottoporre ai partecipanti. Per individuare queste due componenti, abbiamo deciso, prima di effettuare un sondaggio on-line massivo, di organizzare dei focus group. Durante questi eventi, gli invitati sono stati chiamati a rispondere a delle domande con tre key-word da scrivere e apporre su una lavagna. In questo modo, non solo si sono avute delle possibili key word da utilizzare per il sondaggio on-line, ma si è potuta organizzare una discussione in merito alle tematiche scelte. Quest'ultimo aspetto ha anche permesso di avere dei dati di prima mano sull'orientamento del personale dei comuni in merito. Infine, sulla base delle risposte fornite, si è implementato e diffuso un sondaggio on line.

2.0.1 I focus group

Al fine di definire il perimetro della nostra indagine abbiamo organizzato una serie di focus group il cui obiettivo era quello di fare una prima stima sul livello di consapevolezza e competenze presente in un comune sulla cybersecurity e dall'altra cercare di capire queli erano i maggiori ostacoli che i comuni incontrano nei confronti di questa disciplina. Vista la frammentarietà delle competenze che si può trovare in un ente locale abbiamo deciso di suddividere i partecipanti ai focus group in tre gruppi, e di dedicare un focus group a ciascuno di essi. In particolare, un gruppo a cui abbiamo invitato il personale politico e manageriale di un comune: si tratta dei decision maker che determinano la strategia, le voci di spesa e il personale dedicato. Un secondo gruppo ha coinvolto il personale che, specialmente nei piccoli comuni, svolge incarichi di varia natura tra cui eventualmente quelli che riguardano la sicurezza informatica. Infine abbiamo considerato un gruppo costituito da tecnici informatici. Durante ogni focus group sono state poste delle domande che miravano a:

- Valutare il livello di consapevolezza/preparazione su un tema della cybersecurity;
- Cogliere le preoccupazioni dei comuni rispetto ai temi trattati
- Raccogliere suggerimenti e indicazioni

Ai partecipanti è stato chiesto di rispondere con tre parole chiave, scritte su tre post-it diversi, in merito ai concetti che ritenevano più importanti. Nel momento in cui i partecipanti mostravano le loro risposte, queste venivano

poi apposte su una lavagna in modo da essere raggruppate per temi. Nel momento dell'affissione dei post-it i partecipanti hanno anche motivato le loro scelte fornendo così ulteriori elementi di analisi. E' importante sottolineare che, nella procedura, la scrittura e l'esposizione sono avvenute in due momenti rigorosamente separati: in questo modo le risposte di ciascun partecipante sono state indipendenti.

GRUPPO GOVERNANCE Lo scopo di questo focus group era quello di verificare la presenza all'interno degli enti locali di consapevolezza sul tema e competenze legate principlamente agli aspetti manageriali della disciplina. Parliamo tipicamente di discipline quali: la gestione del rischio informatico, la definizione di strategie e le politiche di sicurezza cibernetica etc. Si tratta di competenze che in base alle norme vigenti dovrebbe essere accorpate nel Responsabile alla Transizione Digitale, ma che difatti sono poco incentivate dalla strategia, sposata da AGID, di imporre ai comuni l'adozione di misure minime. Con questo approccio la fase di analisi del rischio si assume svolta da un entità superiore che poi detta l'operatività.
I partecipanti a questa giornata sono stati nove provenienti non solo dal dall'area metropolitana di Milano ma anche da altri capoluoghi lombardi. All'evento hanno partecipato dirigenti comunali ma nessun politico. Le domande discusse in quest'evento sono state le seguenti:

1. Se dico cybersicurezza quali sono le prime tre parole che vi vengono in mente ?
2. In ambito di cybersicurezza, quali sono le tue principali preoccupazioni ?
3. Quali sono le criticità che riscontri nell'adozione di misure di cybersicurezza nel tuo ente ?

Le principali risposte dei partecipanti, suddivise in cluster sono riportate nelle figure 2.1, 2.2 e 2.2.
Non è difficile cogliere nelle risposte alle prime due domande la forte propensione dei partecipanti ad un approccio alla cybersecurity molto orientato alla componente operativa e molto meno a quella progettuale. Come anticipato la risposta è in linea con quanto ci si poteva attendere poichè di fatto questo è proprio il tipo di approccio che è stato difatto richiesto ai comuni. Non stupiscono nemmeno le risposte alla terza domanda in cui prevalgono da una parte la carenza di risorse economiche necessarie per realizzare piani di cybersecurity e dall'altra una scarsa sensibilità al tema da parte della componente politica. Durante l'evento si è anche discusso del fatto che tramite il PNRR i fondi per la cybersecurity sono potenzialmente disponibili, ma vanno saputi spendere ed è necessario saper gestire i contratti con le società private. I comuni accusano la mancanza di competenze per poter svolgere queste mansioni. Con l'abolizione delle province è mancato un mediatore abbastanza grande che possa aver maggiore potere contrattuale/conoscenza del settore. E' stata proposta l'idea di creare una community fra i comuni per discutere delle offerte dei diversi fornitori.

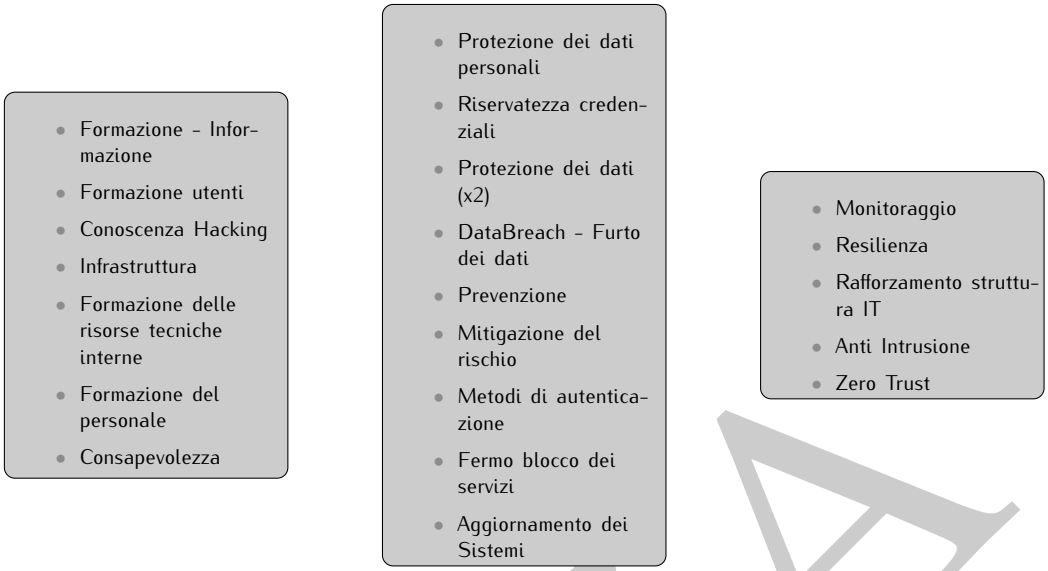

Figura 2.1: Alcune risposte alla prima domanda del gruppo governance *"Se dico cybersicurezza quali sono le prime tre parole che vi vengono in mente ?"*, raggruppate secondo le preferenze dei partecipanti

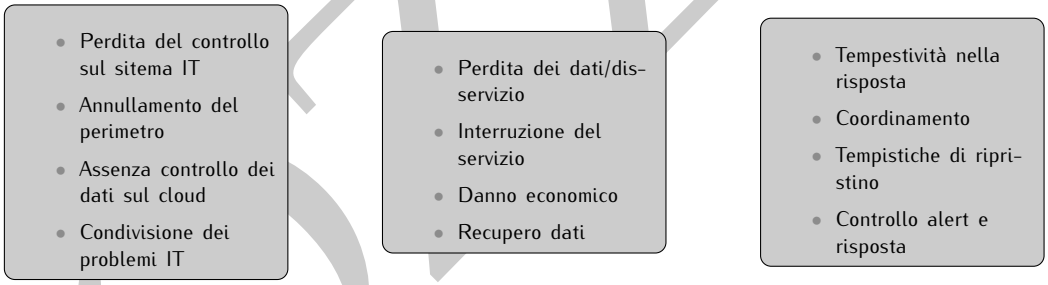

Figura 2.2: Alcune risposte alla seconda domanda del gruppo governance *"In ambito di cybersicurezza, quali sono le tue principali preoccupazioni ?"*, raggruppate secondo le preferenze dei partecipanti

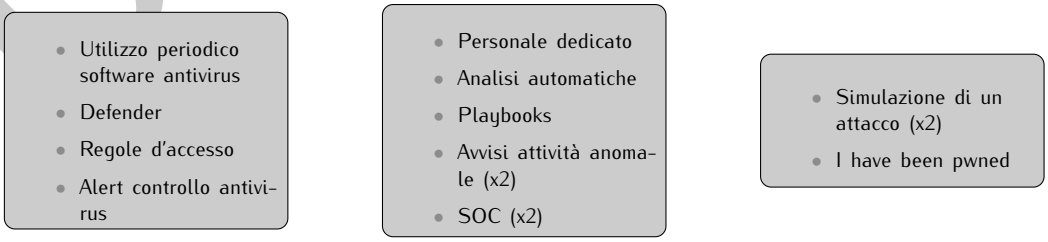

Figura 2.3: Alcune risposte alla terza domanda del gruppo governance *"Quali sono le criticità che riscontri nell'adozione di misure di cybersicurezza nel tuo ente ?"* , raggruppate secondo le preferenze dei partecipanti

GRUPPO TECNICO – BASE Questo focus group era dedicato a quella categoria di persone che pur non avendo nel loro ente mansioni specifiche garantiscono il funzionamento dei sistemi e l'adozione di misure di sicurezza. Anche in questo caso eravamo interessati a valutare il livello di preparazione di queste figure nonchè la loro capacità di tenersi aggiornati e in particolare di gestire i sistemi nella nuova configurazione a seguito della migrazione dei propri sistemi verso il cloud. Anche in questo caso hanno partecipato comuni fuori dalla città metropolitana di Milano. Le domande discusse nell'evento sono state:

1. Quali sono secondo te, le tre misure più efficaci da intraprendere in termini di prevenzione dagli attacchi informatici ?
2. Quali sono secondo te, le tre misure più efficaci da intraprendere in termini di controllo e monitoraggio degli attacchi informatici ?
3. Nel contesto della sicurezza informatica indica l' aspetto più positivo e quello più negativo del passaggio al cloud ?

I cluster delle risposte sono riportate nelle figure 2.4,2.5 and 2.6. Analizzando le risposte si nota una significativa prevalenza di misure di tipo organizzativo quali la formazione, a ricalcare la necessità che queste figure hanno di migliorare la propria formazione che è tipicamente fai da te. Questo dato è ulteriormente suffragato dal fatto che mentre sulla prima domanda le risposte sono tutte corrette, sulla seconda domanda ci sono diverse imprecisioni. La differenza tra prevenzione e monitoraggio non è così immediata da cogliere. Rispetto alla domanda 3 si può dire che i partecipanti al focus group hanno mostrato di conoscere le problematiche legate al cloud, con un po' di confusione in merito ai vantaggi in termini di sicurezza.
Durante l'incontro si è discussa la transizione al cloud: diversi partecipanti ritengono che il suo utilizzo sia meno sicuro rispetto all'utilizzo locale. In secondo luogo è emerso il tema dei corsi di formazione fornite da aziende private: viene fatto presente che i costi di questi sono molto alti. Infine si è discusso della gestione dei SOC: i partecipanti hanno segnalato che i costi di questi sono particolarmente gravosi (specialmente per la gestione degli alert), e hanno suggerito che ACN dovrebbe farsi carico del problema.

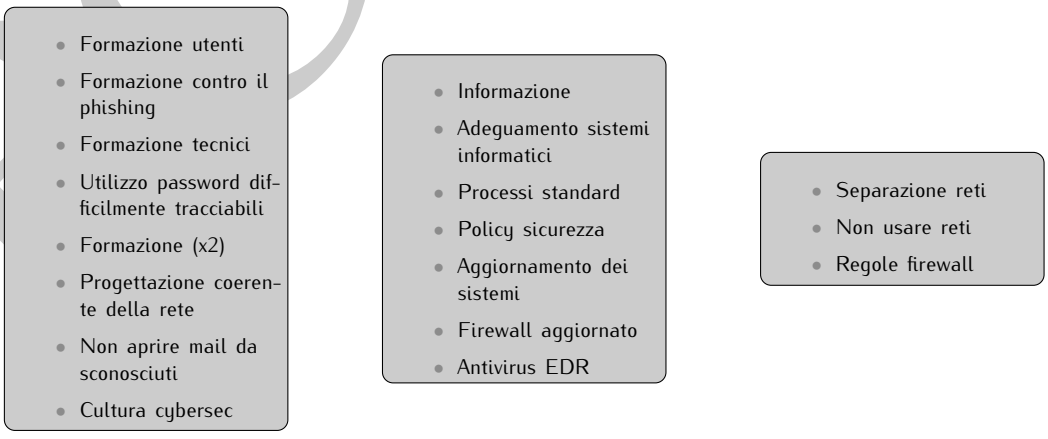

Figura 2.4: Alcune risposte alla prima domanda del gruppo tecnico *"Quali sono secondo te, le tre misure più efficaci in termini di prevenzione dagli attacchi informatici ?"*, raggruppate secondo le preferenze dei partecipanti

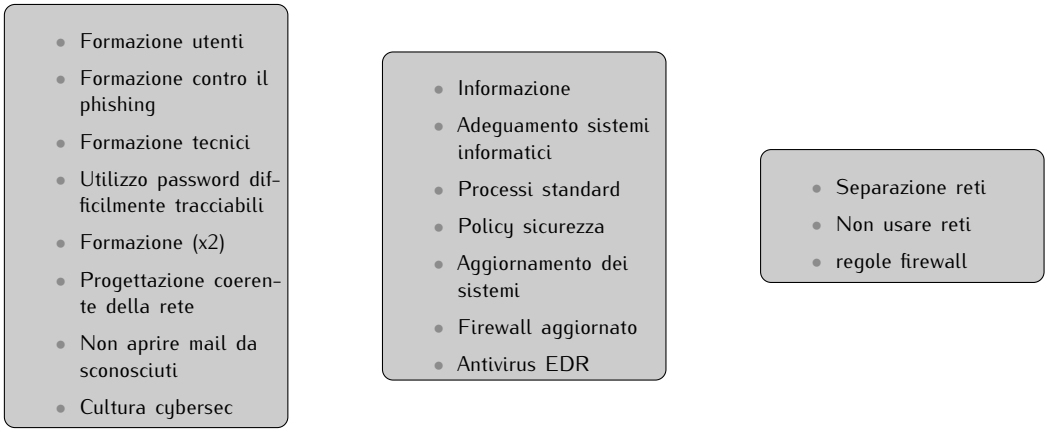

Figura 2.5: Alcune risposte alla seconda domanda del gruppo tecnico *"Quali sono secondo te, le tre misure più efficaci da intraprendere in termini di controllo e monitoraggio degli attacchi informatici ?"*, raggruppate secondo le preferenze dei partecipanti

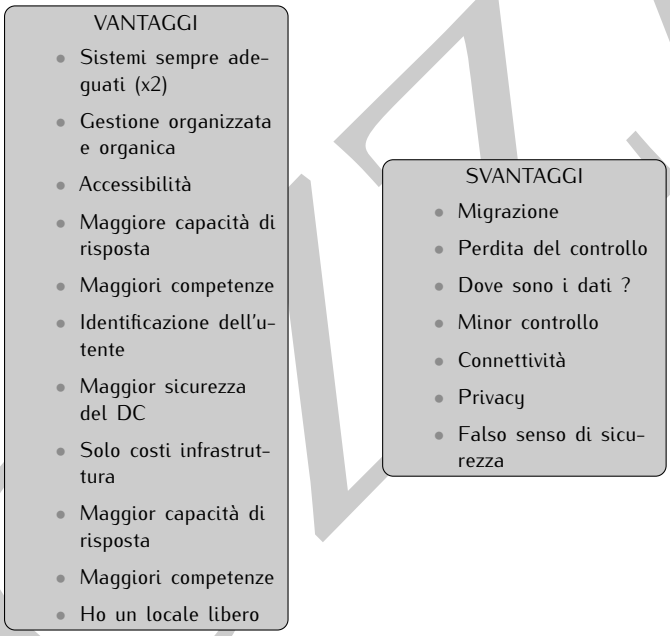

Figura 2.6: Alcune risposte alla terza domanda del gruppo tecnico *"Nel contesto della sicurezza informatica indica l' aspetto più positivo e quello più negativo del passaggio al cloud ?"*, raggruppate secondo le preferenze dei partecipanti

GRUPPO TECNICO – AVANZATO Questo focus group era dedicato alle figure professionali che operano nei comuni in qualità di tecnici informatici, si tratta tipicamente di persone con un background formativo tecnologico, difficilmente specialistico soprattutto in termini di cybersecurity, ma che governano i diversi processi che coinvolgono le tecnologie digitali. Nel loro caso eravamo interessati a valutare non solo il livello delle competenze ma anche se e come hanno intrapreso il processo di migrazione al cloud, la loro visione su quali dovrebbero essere gli attori di riferimento per i comuni nella gestione della cybersecurity, e la loro sensibilità alle problematiche di protezione dei dati. Le domande discusse nell'evento sono state:

1. Se dovesse predisporre una strategia di sicurezza cibernetica per il suo

ente, quali sarebbero le prime tre azioni che metterebbe in atto ?

2. Quali sono i tre soggetti più importanti (anche a livello nazionale) che dovrebbero supportare i comuni nell'implementazione della loro strategia di sicurezza ?

3. Quali sono le tre azioni principali che intendi mettere in campo/-hai già messo in campo, per la dismissione del data center, in una prospettiva di miglioramento del sistema di protezione cibernetico ?

4. Secondo te il tuo ente dispone di dati/servizi la cui compromissione può comportare un rischio critico ?

I cluster delle risposte sono riportati nelle figure Fig. 2.7.2.8,2.9 and 2.10. Dalla prima risposta emerge l'orientamento operativo alla cybersecurity che caratterizza questo gruppo di persone, la maggior parte delle risposte fanno riferimento a misure di tipo tecnologico, non sempre appropriate con la definizione di una strategia di sicurezza. Riprendendo però il discorso fatto ad inizio paragrafo si tratta del tipo di approccio alla cybersecurity sinora "insegnato" agli enti locali. Dalla seconda risposta emerge la necessità di avere un interlocutore a livello nazionale rispetto ad interlocutori locali, la motivazione in questo caso è probabilmente dovuta al fatto che nel contesto della sicurezza informatica i comuni hanno sinora avuto solo interlocutori a livello nazionale. Le risposte alla domanda 3, pur con declinazioni diverse, evidenziano una buona consapevolezza delle sfide che attendono i comuni con il trasferimento dei propri data center nel cloud. Altrettanto le risposte alla domanda 4 stanno ad indicare che c'è una buona sensibilità rispetto alle problematiche di privacy che possono essere presenti in un ente locale. Durante l'incontro si è affrontato sopratutto il tema del cloud: si è discusso del fatto che i dati affidati al cloud non dovrebbero uscire dal perimetro europeo (come peraltro già sancito dalle diverse circolari emanate da ACN in merito alla strategia Cloud First). Il dibattito si è anche incentrato sul valore che possono avere i dati posseduti dai comuni e se gli stessi potrebbero divenire una fonte di valore per l'ente stesso.

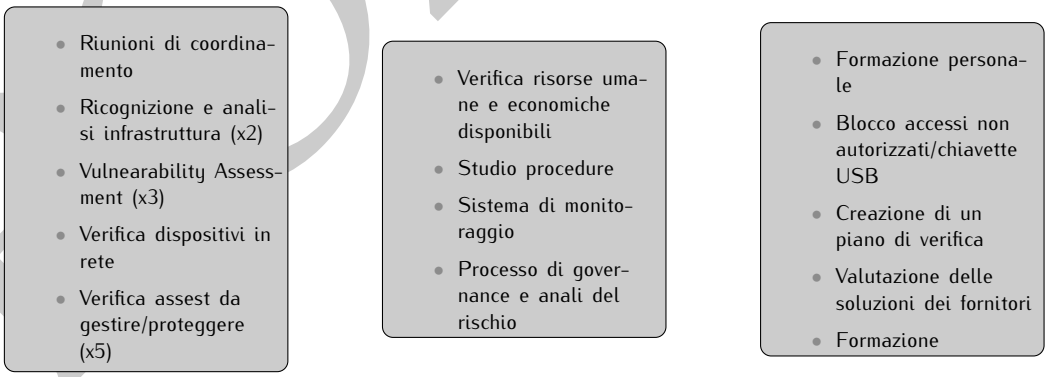

Figura 2.7: Alcune risposte alla prima domanda del gruppo tecnico avanzato *"Se dovesse predisporre una strategia di sicurezza cibernetica per il suo ente, quali sarebbero le prime tre azioni che metterebbe in atto ?"*, raggruppate secondo le preferenze dei partecipanti

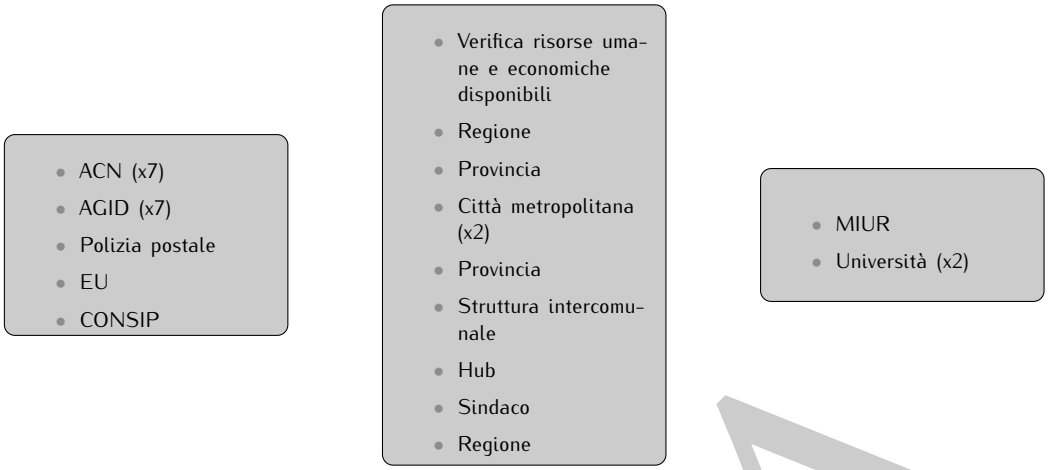

Figura 2.8: Alcune risposte alla terza domanda del gruppo tecnico avanzato *"Quali sono i tre soggetti più importanti (anche a livello nazionale) che dovrebbero supportare i comuni nell'implementazione della loro strategia di sicurezza ?"*, raggruppate secondo le preferenze dei partecipanti

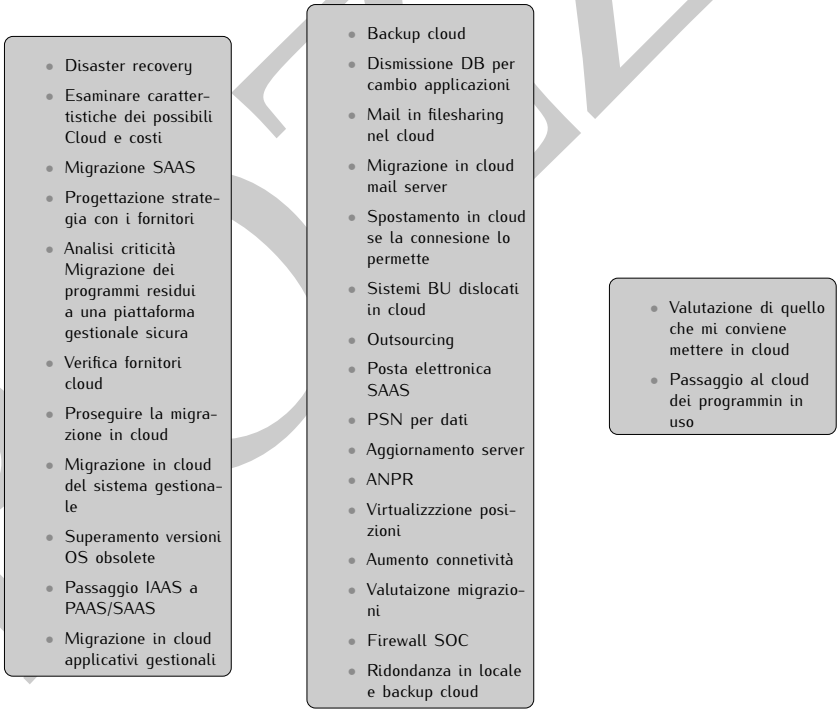

Figura 2.9: Alcune risposte alla quarta domanda del gruppo tecnico avanzato *"Quali sono le tre azioni principali che intendi mettere in campo/hai già messo in campo, per la dismissione del data center, in una prospettiva di miglioramento del sistema di protezione cibernetico ?"*, raggruppate secondo le preferenze dei partecipanti

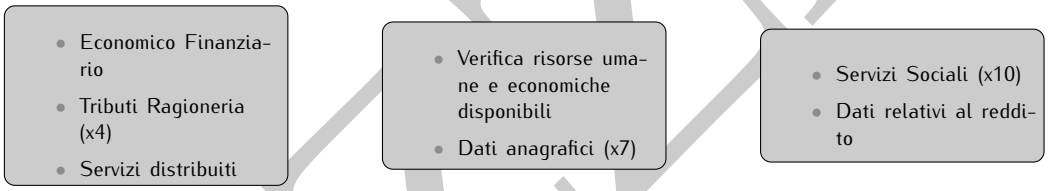

Figura 2.10: Alcune risposte alla quarta domanda del gruppo tecnico avanzato *"Secondo te il tuo ente dispone di dati/servizi la cui compromissione può comportare un rischio critico ?"*, raggruppate secondo le preferenze dei partecipanti

CONSIDERAZIONI COMPLESSIVE SUI FOCUS GROUP Da quanto emerso nei focus group, e in particolare dalle discussioni, si possono enucleare le seguenti considerazioni. Il problema sicurezza informatica è sentito dai comuni che nel corso di questi ultimi anni hanno cercato di "attrezzarsi" per affrontare le sfide poste da questa problematica. Il reperimento di risorse in questo ambito ha rappresentato sicuramente un freno all'attuazione di progetti per il miglioramento della postura di sicurezza cibernetica dell'ente così come la carenza di competenze specifiche e di supporto da parte della componente politica. Risalta in modo abbastanza evidente la natura "fai-da-te" della formazione in cybersecurity degli addetti comunali che non a caso sottolineano l'urgenza di azioni di formazione per se stessi e di sensibilizzazione per i loro colleghi. La carenza di competenze ha creato non poche difficoltà anche nella gestione dei progetti PNRR per quanto riguarda gli aspetti contrattuali. La stessa problematica è emersa per la transizione al cloud: se è vero che in questo caso le aziende private si fanno virtualmente carico di gran parte della gestione dei servizi, è anche vero che mancano le competenza per gestire i contratti con il settore privato.
La natura delle competenze presenti nei comuni vede come componente privilegiata quella tecnologica, questo fa sì che in termini di strumentazione siano adeguatamente forniti, manca però la necessaria enfasi su alcuni aspetti organizzativi. Questa caratteristica trova immediato riscontro nella pratica. Difatti, come avremo modo di illustrare in seguito, dai test compiuti dal Laboratorio di Sicurezza e reti del Dipartimento di Informatica, i siti di front end dei comuni risultano resistenti a diverse forme di attacco, mentre gli enti presentano diverse criticità sul fronte degli attacchi di ingegneria sociale a cui si può far fronte solo con soluzioni organizzative appropriate.
Un ultimo aspetto che ci sembra significativo menzionare: sembra esserci una tendenza significativa degli enti locali nell'individuare un entità a livello nazionale come referente per la cybersecurity.

2.1 SONDAGGIO ON-LINE

Le domande e le key words precedenti sono state utilizzate per sviluppare un sondaggio on-line, inviato a tutti i comuni (e relativi dipendenti/collaboratori) della Lombardia. Questo ci ha permesso di utilizzare un format già consolidato nell'esperienza descritta in precedenza per un campione più ampio. Prima di presentare i risultati ottenuti, vorremmo illustrare la metodologia con cui sono stati raccolti ed elaborati i dati.

METODOLOGIA E FORMAT Il sondaggio è stato somministrato dal 15 agosto fino al 10 settembre 2023. L'invito è stato spedito via posta elettronica da Ancilab a tutti i comuni della Lombardia oltre che segnalato sulla pagina web dello stesso ente. I rispondenti sono stati 206.Al sondaggio ha partecipato sia sia il personale che nei comuni svolge un ruolo tencico sia il personale che svolge un servizio amministrativo. La distribuzione geografica è riportata nella Fig. 2.11, mentre la distribuzione secondo il ruolo e la classe demografica del comune sono riportate rispettivamente nella Fig. 2.12.

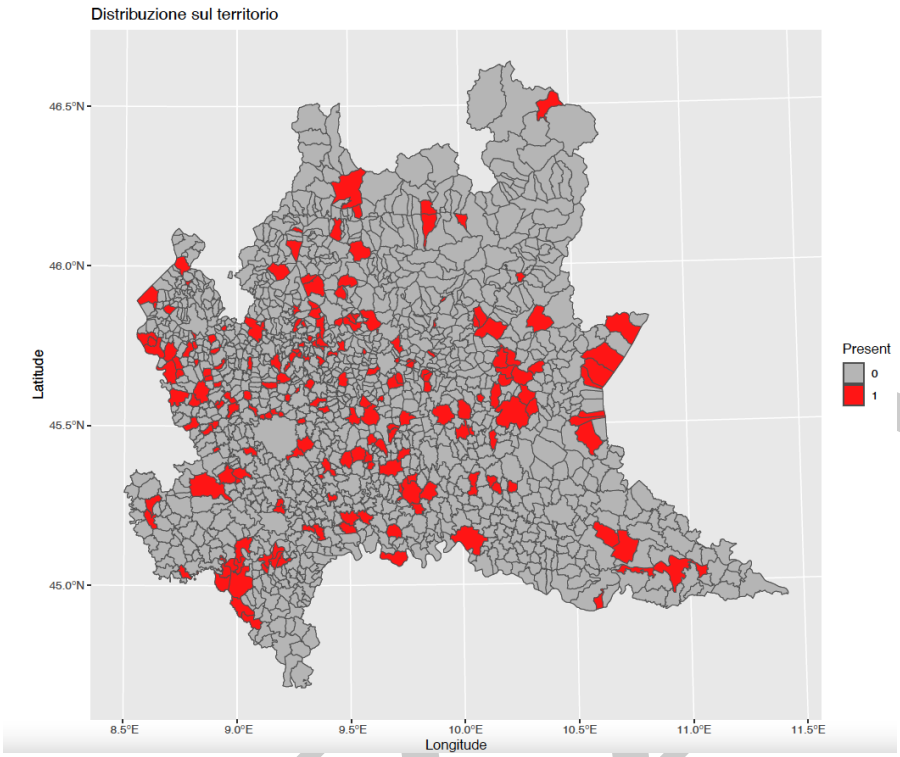

Figura 2.11: Distribuzione geografica dei comuni rispondenti al sondaggio on line

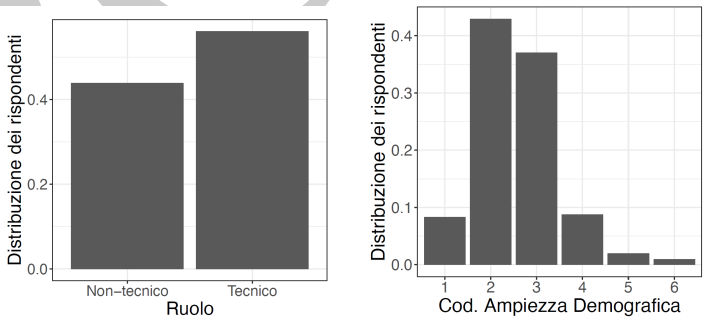

Figura 2.12: Distribuzione del ruolo e della classe demografica dei rispondenti al sondaggio on line

Le domande e le key words tra cui i rispondenti potevano scegliere, sulla base di quanto emerso dai focus group, sono state le seguenti:

Dati rispondente

Qual è il suo comune ?

Dati rispondente - Lei è il resposabile della transizione digitale ?

- Si
- No

Dati rispondente

Qual è il suo ruolo all'interno del comune ?

1) Cosa le fa venire in mente il termine cybersicurezza ?

- Formazione del personale non IT
- Consapevolezza/partecipazione attiva
- Protezione dati
- Riservatezza delle credenziali
- Definizione del perimetro
- Metodi di autenticazione
- Aggiornamento dei sistemi
- Monitoraggio
- Mitigazione del rischio/rimedio e cura

2) In ambito di cybersicurezza quali sono le sue principali preoccupazioni ?

- Responsabilità
- Reputazione ente
- Perdita del controllo sulla struttura IT
- Perdita del controllo sul perimetro dell'infrastruttura IT
- Comprensione da parte del resto del personale delle problematiche IT
- Perdita dei dati/loro recupero
- Danno economico
- Disparità offesa/difesa
- Essere aggiornati
- Tempestività nella risposta all'attacco
- Obsolescenza software usati
- Procedure interne poco sicure in termini di cybersecurity

3) Quali sono le tre misure più efficaci da intraprendere in termini di prevenzione dagli attacchi informatici ?

- Formazione/informazione personale IT
- Progettazione corerente della rete
- Adeguamento sistemi informatici
- Adeguamento processi
- Policy sicurezza
- Firewall/Antivirus aggiornati
- Separazione delle reti
- Regole firewall
- Monitoraggio traffico

4) Quali sono le tre misure più efficaci da intraprendere in termini di controllo e monitoraggio degli attacchi informatici ?

- Vulnerability Assesment
- Siti con password compromesse
- Recupero rapido
- Formazione specifica personale IT Antivirus
- Monitoraggio velocità della rete/esecuzione dei programmi
- Regole d'accesso
- SOC/Analisi statistiche
- Personale dedicato
- Cyber response playbook

5) Nel contesto della sicurezza informatica indichi l'aspetto più positivo del passaggio al cloud ?

- Sistemi sempre aggiornati
- Accessibilità
- Maggior sicurezza datacenter
- Riduzione dei costi
- Maggiori competenze dei gestori

6) Nel contesto della sicurezza informatica indichi l'aspetto più negativo del passaggio al cloud ?

- Migrazione
- Perdita del controllo dei dati
- Privacy
- Connettività
- Falso senso di sicurezza

7) Se dovesse predisporre una strategia di sicurezza cibernetica per il suo ente

- Ricognizione e analisi infrastruttura
- Vulnerability assesment
- Verifica dei dispositivi in rete
- Verifica degli assets da gestire e proteggere
- Sistema di autenticazione forte
- Security Policies Recovery response plan
- Sistema di monitoraggio
- Analisi del rischio
- Formazione personale IT
- Formazione personale non IT
- Survey fornitori

8) Quali sono i tre soggetti più importanti (anche a livello nazionale) che dovrebbero supportare i comuni nell'implementazione della loro strategia di sicurezza ?

- ACN
- AGID
- Regione
- Città metropolitana
- Sindaco/Assessori
- Struttura intercomunale
- Polizia Postale
- CONSIP
- Università/MIUR
- UE

9) Quali sarebbero le tre azioni principali da mettere in campo per la dismissione del data center in una prospettiva di miglioramento del sistema di protezione cibernetico ?

- Migrazione in cloud SAAS applicativi e produttivita
- Disaster recovery
- Superamento versioni OS obsolete
- Passaggio da IAAS a PAAS/SAAS
- Backup cloud
- Migrazione in cloud del mail server
- Virtualizzazione postazioni
- SOC
- Migrazione dei dati in cloud
- Aggiornamento server

10) Elenchi i principali insieme di dati o servizi la cui compromissione può comportare un rischio critico per l'ente

- Tributi/Ragioneria
- Atti amministrativi (appalti)/Registro protocollo
- Servizi timbratura
- Dati del personale
- Dati anagrafici
- Dati relativi al settore sociale/sanitario
- Dati relativi al reddito
- Dati della polizia locale
- Telecamere sicurezza
- Dati delle mail dei dipendenti

2.2 I RISULTATI DELL'INDAGINE STATISTICA

Riportiamo in questa sezione i risultati ottenuti nel corso della nostra indagine che ricordiamo essere principalmente focalizzata a definire il profilo di competenze in cybersecurity che caratterizza i comuni lobardi. In questo contesto è necessario fare alcuni chiarimenti. La cybersecurity è risaputo essere una materia multidisciplinare, sono tre le sue principali componenti: tecnologica, giuridica e manageriale. Non esistono esperti in cybersecurity che conoscano allo stesso livello di profondità tutti questi settori, solitamente un esperto predilige una di queste componenti. Quindi quando parliamo di valutare le competenze in cybersecurity dobbiamo tenere conto di due fattori uno qualitativo legato alla tipologia di competenza posseduta ed una quantitativo che rappresenta la profondità delle conoscenza acquisite. Per effettuare quest'ultimo tipo di valutazioni ci siamo avvalsi del supporto di esperti di cybersecurity suddivisi nelle tre componenti sopra indicate, a cui abbiamo sottoposto il questionario sopra descritto. Le risposte degli esperti sono poi state utilizzate come punto di riferimento per valutare sia qualitativamente che quantitativamente le risposte dei comuni. In breve, più le risposte date da un comune si avvicinavano a quelle degli esperti e più alta era la valutazione delle competenze assegnate a quel comune. Ad esempio, se le risposte di un comune coincidevano con quelle degli esperti giuristi ma solo parzialmente con quelle degli esperti tecnologi, il comune sarà valutato con il massimo della valutazione in termini di competenze giuridiche e con un voto intermedio per le competenze tecniche. In una valutazione quantitativa oltre al livello massimo è necessario anche definire il livello minimo, cioè lo zero di riferimento. Nel nostro caso avevamo due scelte assumere come zero nessuna conoscenza pregressa dell'argomento, oppure prevedere un livello minimo di conoscenze. Abbiamo optato per entrambe le soluzioni e siamo in grado di mostrare il livello di competenze assoluto e uno relativo. Il livello di competenze assoluto è definito su una scala da 0 a 10, più la risposte di un comune si avvicina a quella degli esperti e più il suo voto si avvicina a 10. Il livello di competenze relativo viene calcolato assumendo un base minima di conoscenza che abbiamo stimato essere quella dell'uomo della strada che è stata determinata nel seguente modo. Il questionario è sotto sottoposto ad un gruppo di persone scelte a caso il cui unico requisito era quello di non essere esperti di cybersecurity. Le risposte così ottenute sono state considerate come "livello minimo" per la valutazione delle risposte date dai comuni.
Un ulteriore variabile da considerare nella nostra valutazione è la dimensione dei comuni. E' ragionevole anche se non scontato che tale parametro sia una discriminante significativa , per cui è più che opportuno valutare le risposte al questionario suddivise per classe di comuni omogenee in termini di dimensione del comune. Quindi, il dataset delle risposte è stato strutturato suddividendo i comuni secondo la classe demografica riportata in Tab. 2.1. Per il lettore più rigoroso abbiamo riportato nell'Appendice ?? la metodologia adottata per la valutazione delle domande, mentre il metodo con cui è stata svolta l'analisi descrittiva è riportato nell'Appendice ??. Nel seguito riportiamo i risultati ottenuti dall'elaborazione delle risposte al questionario raggruppate per tematiche, riportando le conclusioni che sul tema si possono ottenere sia dal punto di vista qualitativo che quantitativo.

Tabella 2.1: Corrispondenza fra il codice della classe demografica e la popolazione considerata

Classe demografica	Popolazione (2020)
1	Fino a 999 abitanti
2	1.000 - 4.999 abitanti
3	5.000 - 19.999 abitanti
4	20.000 - 59.999 abitanti
5	60.000 - 99.999 abitanti
6	100.000+

2.2.1 Quali sono le competenze di cybersecurity nei comuni lombardi?

Per fornire una risposta a questa domanda ci siamo basati essenzialmente sulle riposte fornite alle domande 1 e 2 del questionario, che ricordiamo essere:

- Se dico cybersicurezza quali sono le prime tre parole che vi vengono in mente ?
- In ambito di cybersicurezza, quali sono le vostre principali preoccupazioni ?

CONSIDERAZIONI QUANTITATIVE Come emerge dalle figure 2.13-2.14 esiste nei comuni un discreto livello di competenze sulla tematica, dai grafici presentati si può anche notare come i risultati migliori siano ottenuti nell'ambito tecnico a conferma del dato già emerso in fase di focus group in cui era emersa una preponderanza di competenze di questo tipo. La cosa importante da sottolineare è che questo tipo di competenze sembra essere abbastanza diffuso nel senso che anche anche personale non tecnico e che quindi dovrebbe privilegiare un altro tipo di competenze di fatto risponde al questionario nello stesso modo dei tecnici.

CONSIDERAZIONI QUALITATIVE Dall'analisi delle risposte emerge una netta prevalenza a considerare la cybersecurity alla pari della protezione dati. Difatti alle domande 1 e 2 le risposte più frequenti sono state rispettivamente *Protezione dati* e *Perdita dei dati*. Se è indubbio che l'intersezione tra le due discipline sia significativa, è altrettanto vero che il dominio d'applicazione della cybersecurity è decisamente più vasto. Per contro va detto che indubbiamente l'aspetto di cybersecurity più enfatizzato da leggi e regolamenti di interesse per gli enti comunali è proprio quello legato alla protezione dati. Accanto a questo va detto che, in base ad un'analisi più approfondita dei dati, gli aspetti della disciplina che più emergono sono contenuti nel cluster *riservatezza credenziali*, *aggiornamento dei sistemi* e *metodi di autenticazione* sulla prima domanda e sulle parole chiave *tempestività della risposta* e *disparità offesa/difesa* che denotano una forte propensione del campione a considerare aspetti più implementativi della disciplina. Non mancano parola chiave come *mitigazione del rischio*, *formazione* reputazione ente e *responsabilità* che denotano una visione più ampia della disciplina e delle sue implicazioni a livello sistemico, ma risultano quantitativamente minoritarie. Un ultima osservazione, la parola chiave *reputazione dell'ente* che appare tra i principali rischi organizzativi della cybersecurity è tra le meno "votate", un'indicazione di come sia poco percepita la dimensione sistemica del problema.

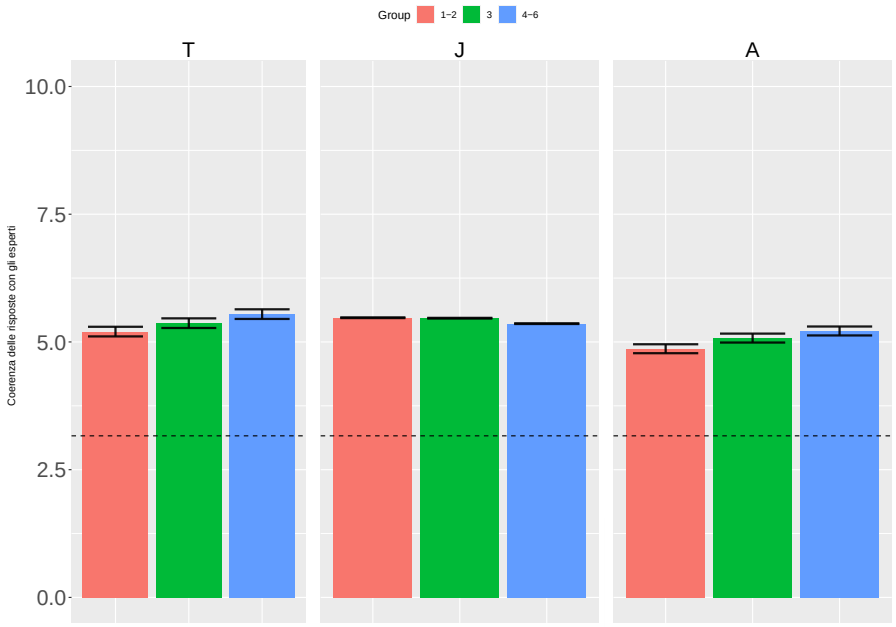

Figura 2.13: Valutazione supervisionata: coerenza delle risposte fornite dai partecipanti al sondaggio (raggruppati per classe demografica) rispetto alla domanda 1 per le diverse aree di competenza Tecnica (T), Giuridica (J) e Amministrativo-Manageriale (A). La linea trattegiata riporta il punteggio ottenuto da un gruppo di persone non competenti in materia

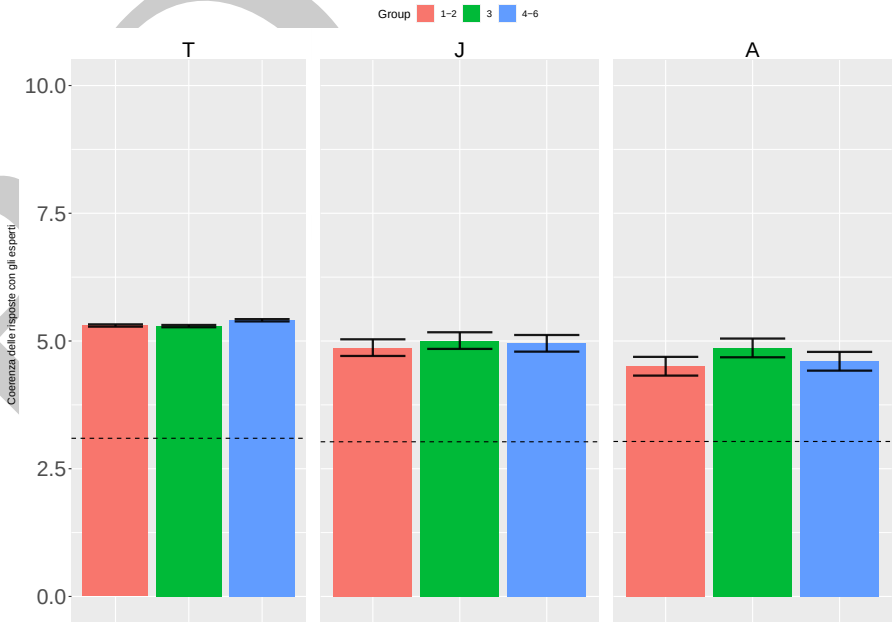

Figura 2.14: Come in Fig. 2.13, ma per la domanda 2

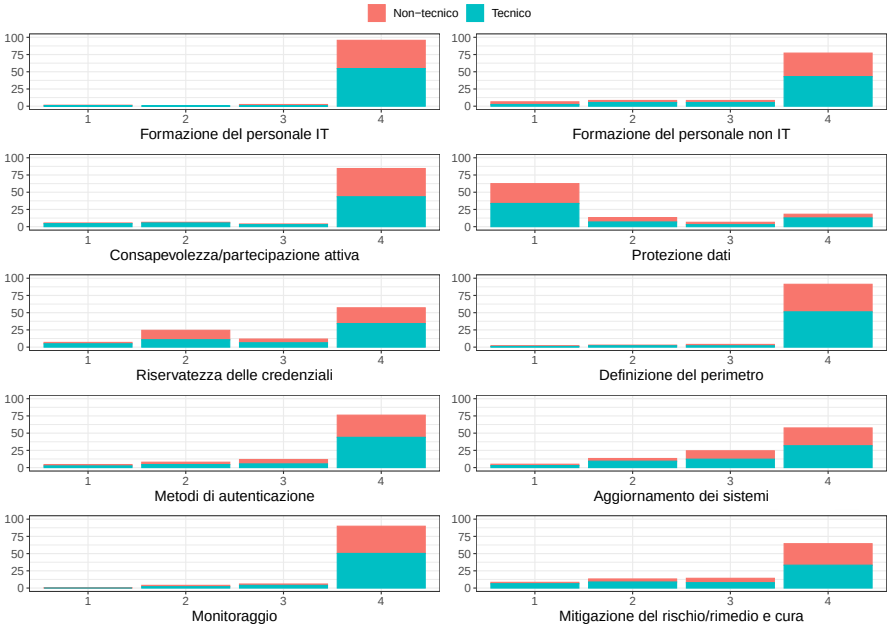

Figura 2.15: Istogramma di distribuzione delle risposte per la domanda 1. I valori in ordinata sono in percentuale, mentre in ascissa 1) indica che la percentuale con cui quella risposta è stata scelta come prima, 2) come seconda, 3) come terza e 4) non fra le prime tre

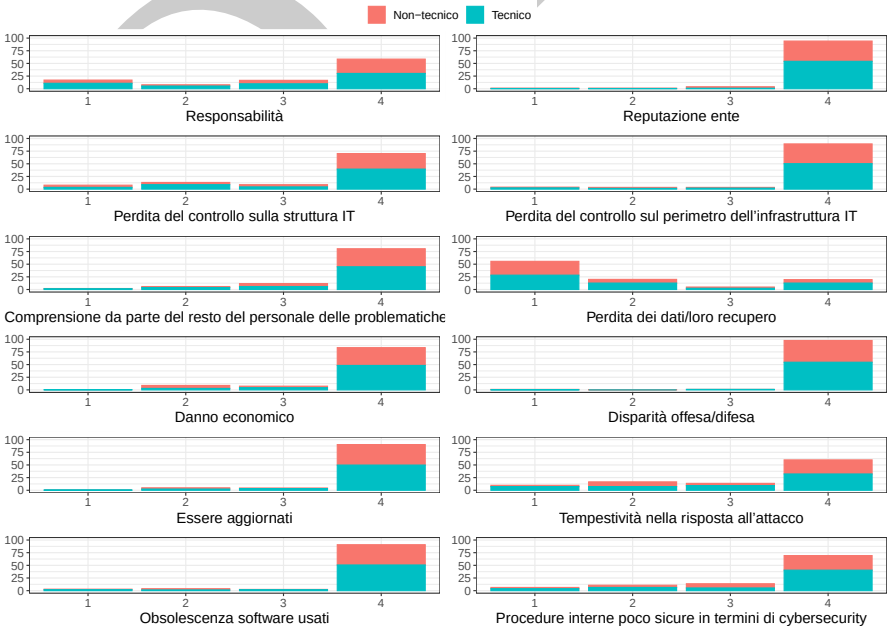

Figura 2.16: Come in Fig. 2.15, ma per la domanda 2

2.2.2 Quali competenze tecniche

Oltre a verificare la presenza di conoscenze di tipo generale sulla cybersecurity all'interno degli enti locali ci siamo anche posti il problema di verificare più in dettaglio il livello di competenze tecniche e gestionali. A questo proposito è probabilmente utile ricorda che si tratta di competenze molto difficili da reperire sul mercato anche per il settore privato che ha sicuramente maggiori strumenti attrattivi del settore pubblico. In questa sezione riportiamo i dati ottenuti rispetto alla prima tematica. Questi dati sono stati ottenuti elaborando le risposte alle seguenti domande:

- Quali sono, secondo lei, le tre misure più efficaci da intraprendere in termini di prevenzione dagli attacchi informatici ?
- Quali sono, secondo lei, le tre misure più efficaci da intraprendere in termini di controllo e monitoraggio degli attacchi informatici?

CONSIDERAZIONI QUANTITATIVE Come emerge dalle figure 2.19,2.20 esiste nei comuni un discreto livello di competenze sulla tematica, dai grafici presentati si può notare come non ci sia una prevalenza di qualche tipologia di competenza sulle altre anche perchè il contesto era ben delimitato dalle potenziali risposte. Contrariamente a quanto emerso nel caso precedente possiamo notare una differenziazione di opinioni tra il personale tecnico e non tecnico nella seconda domanda.

CONSIDERAZIONI QUALITATIVE Al fine di poter verificare il livello di competenze in gioco abbiamo inserito tra le opzioni alle domande che i comuni potevano selezionare alcune risposte evidentemente sbagliate. Anche se quindi complessivamente le risposte sono state congruenti come peraltro dimostra il guadagno di competenze riportato nei grafici 2.17 e 2.18, non sono mancate risposte che indicavano il monitoraggio come meccanismo di prevenzione, ovvero l'antivirus e il vulnerability assessment come sistema di monitoraggio. Questo a dimostrare che siamo di fronte ad un tipo di conoscenze acquisite principalmente da autodidatti. A questa considerazione si collega il fatto che ad entrambe le domande un numero significativo di enti ha correttamente indicato come misura da adottare la formazione di personale IT, quasi a esplicitare la consapevolezza del proprio livello di preparazione. Per contro richiamando quando sopra detto rispetto alle difficoltà di reperire questo tipo di professionalità sul mercato, se non esistessero nei comuni questi tipi di competenze "fai-da-te" i nostri enti sarebbero completamente scoperti rispetto a queste professionalità.

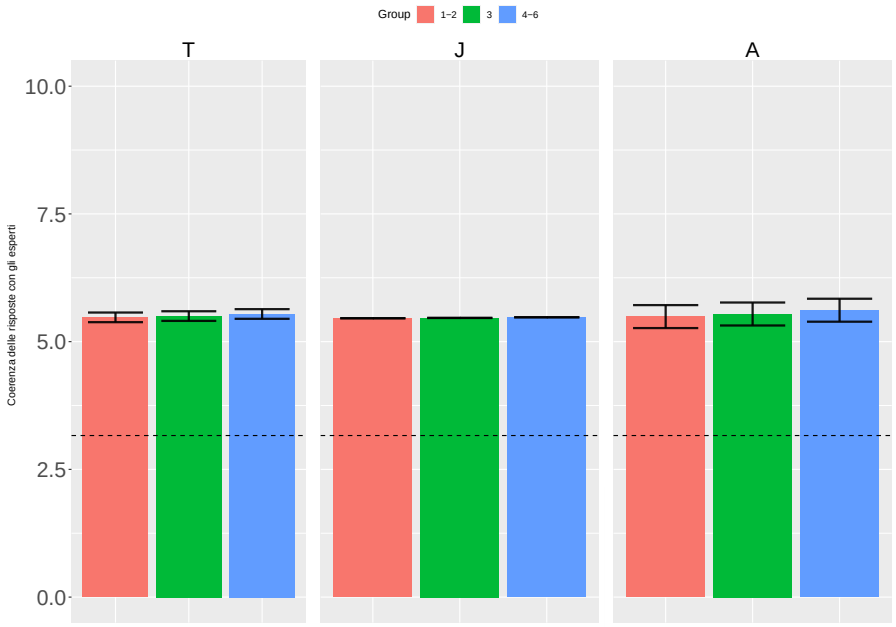

Figura 2.17: Come in Fig. 2.13, ma per la domanda 3

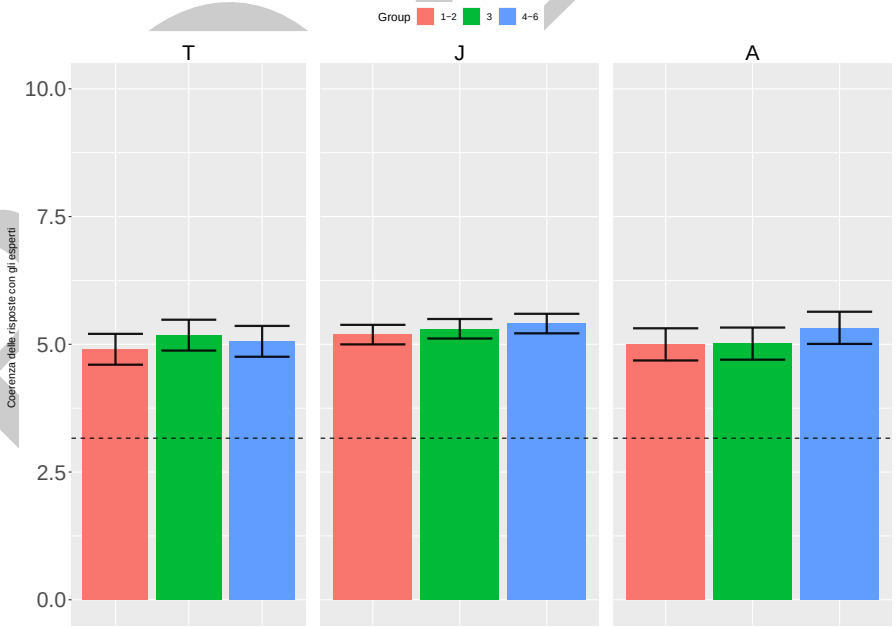

Figura 2.18: Come in Fig. 2.13, ma per la domanda 4

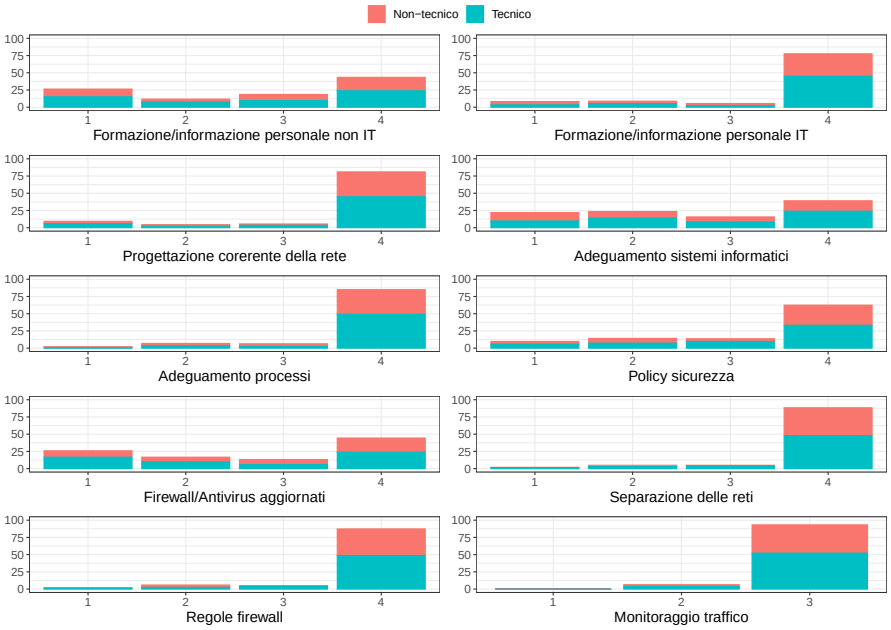

Figura 2.19: Come in Fig. 2.15, ma per la domanda 3

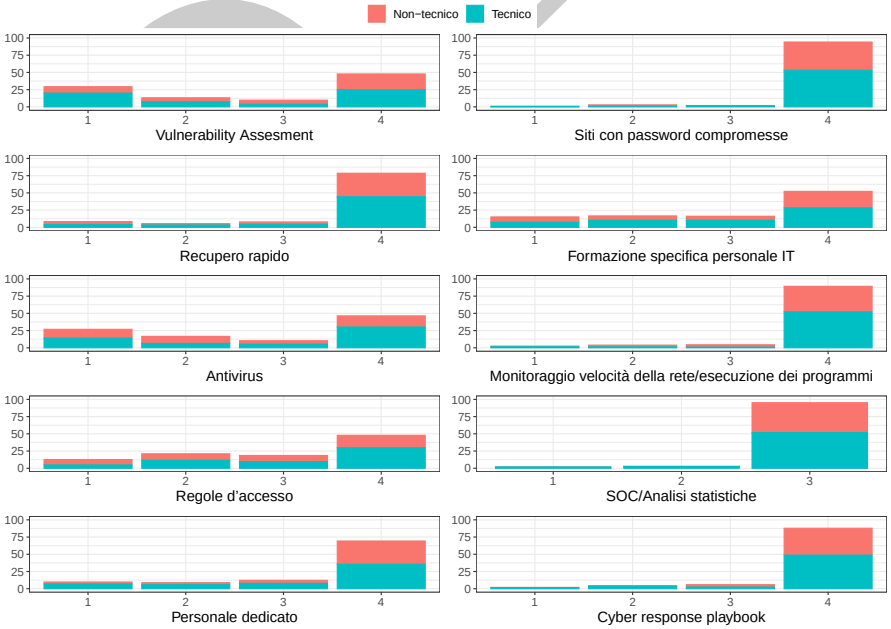

Figura 2.20: Come in Fig. 2.15, ma per la domanda 4

2.2.3 Quali competenze metodologiche

L'altra componente di conoscenze considerata è quella legata alla definizione di strategie e/o politiche di sicurezza. Come abbiamo già avuto modo di dire si tratta di un tipo di competenze in un certo senso "scoraggiato" negli enti locali che sino ad ora si sono di fatto visti dettare, almeno in parte, l'agenda delle azioni da compiere per la messa in sicurezza dei propri sistemi da enti nazionali, in parte anche perchè negli enti locali, come per il profilo tecnico sopra descritto non è facile trovare questi tipi di professionalità. Resta comunque l'importanza di poter avere negli enti locali una figura di riferimento che possa avere una visione non diciamo strategica ma almeno d'insieme della disciplina.

CONSIDERAZIONI QUANTITATIVE Come emerge dalla figure 2.22 anche in questo caso esiste nei comuni un discreto livello di competenze sulla tematica, in questo caso si può notare come ci sia una maggiore aderenza con le opinioni espresse dagli esperti di area manageriale. Anche in questo caso vi è una certa divergenza di vedute tra il personale tecnico e non tecnico

CONSIDERAZIONI QUALITATIVE Le risposte a questa domanda si accorpano intorno a due risposte *Formazione del personale non IT* e *Vulnerability Assessment* come si può vedere dalla Fig. 2.22. La prima non è certo una misura propedeutica alla definizione di una strategia di sicurezza, ma probabilmente i comuni hanno voluto con questo indicare l'urgenza di un problema particolarmente sentito. L'altra riposta menzionata è sicuramente una pratica che può essere svolta in preparazione di una strategia ed è accompagnata da risposte come Security Policies, Recovery response plan tutte congrue con la domanda posta.

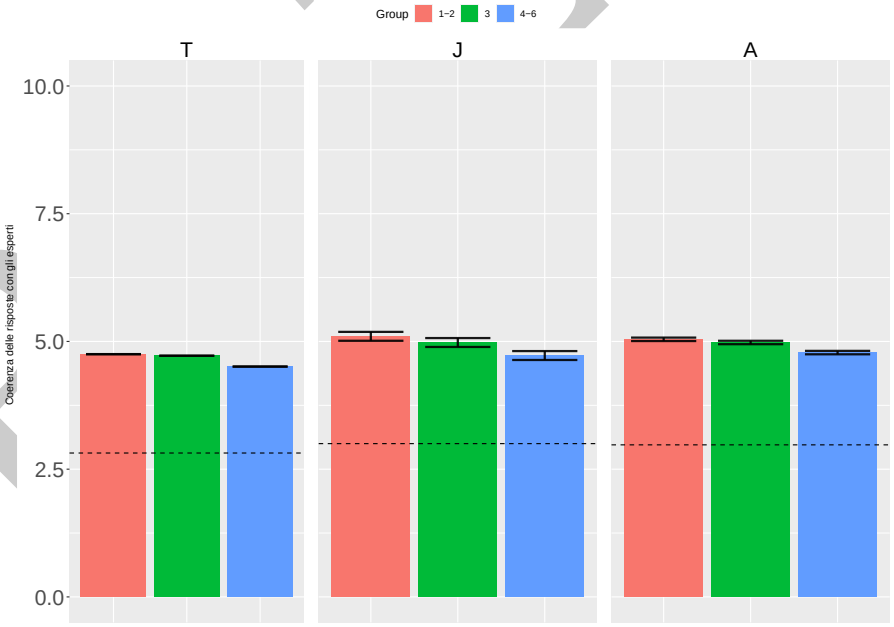

Figura 2.21: Come in Fig. 2.13, ma per la domanda 7

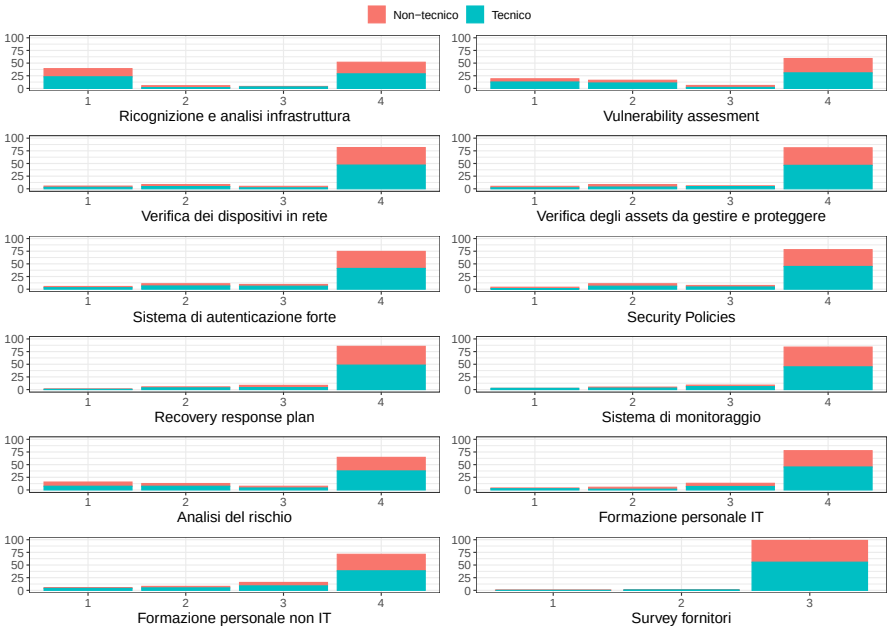

Figura 2.22: Come in Fig. 2.15, ma per la domanda 7

2.2.4 Le competenze sul cloud

La migrazione al cloud è una delle fasi che tutti gli enti locali stanno effettuando in ottemperanza alla strategia "cloud first" imposta ai comuni da ACN. In questo contesto abbiamo voluto valutare il bagaglio di competenze presente nei comuni anche nella prospettiva che questa sarà la modalità di gestione del patrimonio informatico dei comuni a partire dal prossimo anno. La verifica è stata fatta valutando le risposte ai seguenti quesiti:

- Nel contesto della sicurezza informatica indichi l'aspetto più positivo del passaggio al cloud ?
- Nel contesto della sicurezza informatica indichi l'aspetto più negativo del passaggio al cloud ?
- Quali sono le tre azioni principali da mettere in campo per la dismissione del data center in una prospettiva di miglioramento del sistema di protezione cibernetico ?

CONSIDERAZIONI QUANTITATIVE A differenza di quanto accaduto per il caso precedente, per questa domanda la situazione è più complessa: infatti per la prima e la seconda domanda, sulla base delle valutazione degli esperti riportata in Fig. 2.23 la situazione è positiva solo per i comuni medio grandi (vedi Fig. 2.24), mentre non vi è una competenza aggiunta per i comuni più piccoli. Questa debolezza dei comuni di piccole dimensioni si nota anche dal valutazione delle risposte alla terza domanda riportata in Fig. 2.25: sebbene per tutti i casi è presente un guadagno positivo, esso è decisamente inferiore per i comuni più piccoli. In sostanza, i dati raccolti evidenziano una carenza di competenze sul tema del cloud nei piccoli comuni, ma anche nei comuni di dimensioni medio grandi si può notare come il guadagno di competenze sia mediamente inferiore a quello precedentmente considerato.

CONSIDERAZIONI QUALITATIVE Le prime due domande poste richiedono di possedere la capacità di individuare aspetti positivi/negativi del cloud e di conseguenza richiedono una buona conoscenza della materia. La terza domanda è molto più legata all'operatività nella quale in realtà i comuni sono immersi proprio in questa fase. Dalle risposte ottenute possiamo quindi concludere che manca in generale nei comuni, ma soprattutto in quelli di piccole dimensioni, una buona conoscenza delle problematiche legate al cloud, basti segnalare che sono pochissimi i comuni che hanno indicato la perdita di privacy come uno dei principali rischi della migrazione al cloud. Contrariamente ai dati riportati nella sezione precedente e a difesa dei comuni va detto che il cloud è un argomento relativamente nuovo ed la comprensione del suo funzionamento, anche basilare, non è così immediata. Per contro nella terza domanda i comuni hanno dimostrato di conoscere adeguatamente i passi da compiere per migrare i propri sistemi, anche perchè si tratta di processi in cui sono direttamente coinvolti proprio in questa fase. Infine, è interessante notare come su questo tema vi sia, al contrario del caso precedente, una polarizzazione fra il cluster dei tecnici e non.

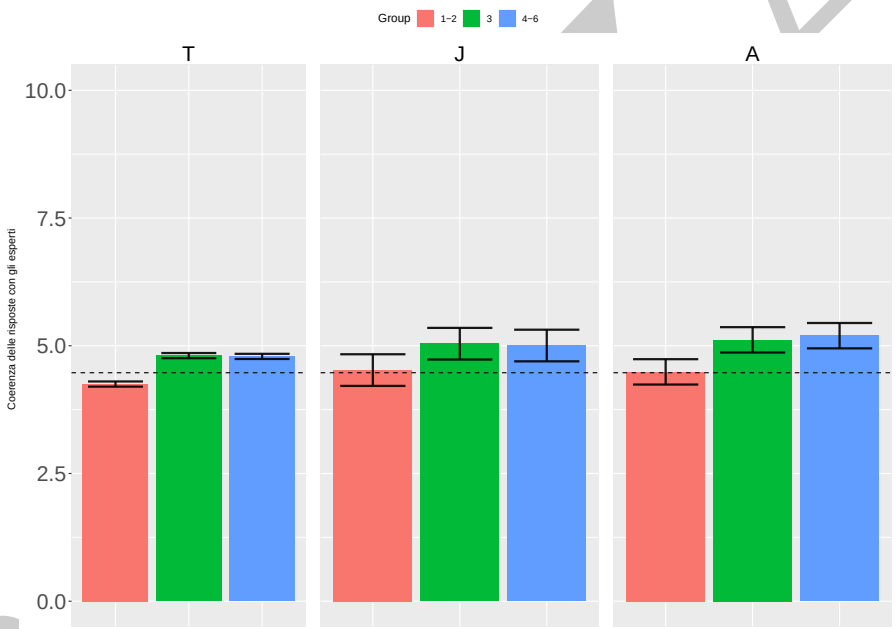

Figura 2.23: Come in Fig. 2.13, ma per la domanda 5

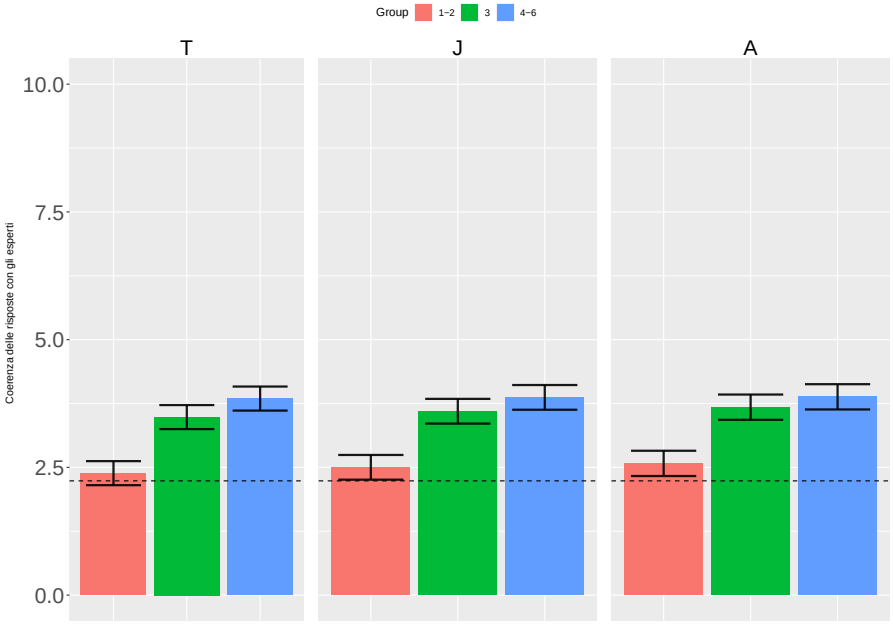

Figura 2.24: Come in Fig. 2.13, ma per la domanda 6

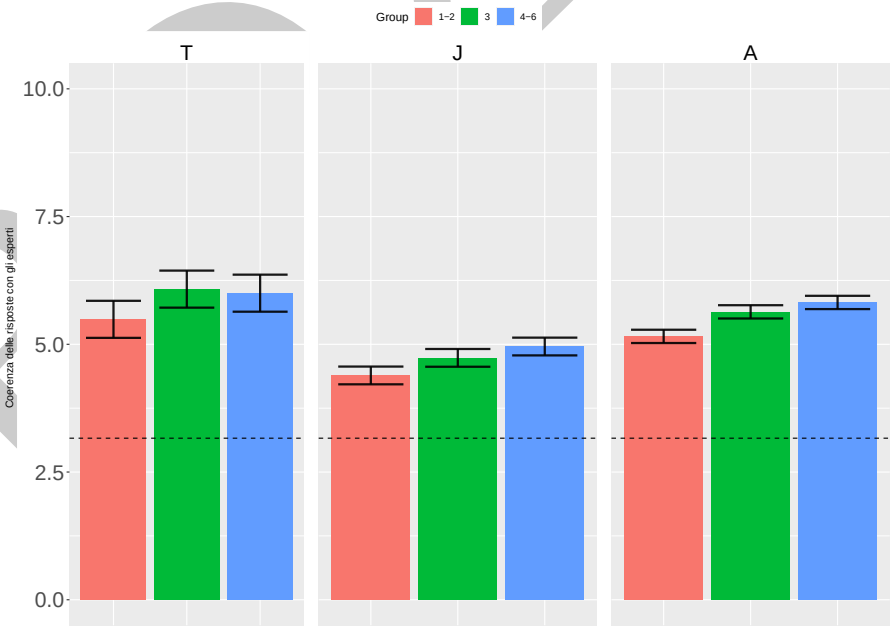

Figura 2.25: Come in Fig. 2.13, ma per la domanda 9

2.2.5 Interlocutori istituzionali

Questa domanda è orientata a valutare il tipo di interlocutore che i comuni gradirebbero avere nella gestione delle problematiche di sicurezza informatica. Ricordiamo che l'Agenzia Nazionale per la Cybersicurezza è per legge il referente di tutte le PA sul tema, la nostra domanda voleva verificare se al di là della scelta del legislatore i comuni prediligessero ad esempio un referee più "vicino" sia in termini istituzionali che geografici. La domanda quindi posta agli enti locali è stata

- Quali sono i tre soggetti più importanti (anche a livello nazionale) che dovrebbero supportare i comuni nell'implementazione della loro strategia di sicurezza ?

Ovviamente in questo caso non ha alcun senso effettuare una valutazione quantitativa delle risposte ottenute o confrontare le stesse con quelle degli esperti. Ci interessava raccogliere l'opinione dei comuni. I risultati possono essere così riassunti. Come emerge dalle Fig. 2.28 e 2.28 l'ente più segnalato dagli enti comunali è l'AGID seguita da ACN e Regione. Da sottolineare che chi ha indicato AGID, nella stragrande maggioranza dei casi, non ha indicato ACN come seconda o terza scelta. Un numero consistente di comuni ha indicato anche la polizia postale. Emerge un quadro non completamente chiaro di quali potrebbero essere gli interlocutori privilegiati dei comuni su questa materia.
Protezione dei dati A quasi 6 anni dall'entrata in vigore del GDPR abbiamo voluto verificare la sensibilità sviluppata dai comuni in merito alla criticità dei dati da loro trattati, lo abbiamo fatto ponendo ai comuni la seguente domanda

- Elenchi i principali insieme di dati o servizi la cui compromissione può comportare un rischio critico per l'ente

CONSIDERAZIONI QUANTITATIVE Come evidenziato dalla Fig. 2.27, la valutazione fra le diverse aree di competenza (Tecnica, Giuridica e Manageriale) sono molto sbilanciate. Mentre i comuni grandi e medi hanno un valore aggiunto di competenza significativo per tutte le aree, quelli più piccoli non ne hanno in ambito giuridico e nelle altre due aree in misura molto ridotta rispetto ai comuni di dimensioni più ampie.

CONSIDERAZIONI QUALITATIVE La valutazioni quantitative indicano che la strada da percorrere sulla sensibilizzazione degli enti locali in merito alla criticità dei dati da loro trattati sembra essere ancora lunga, anche se comunque come abbiamo visto nella sezione sulle competenze in cybersecurity nei comuni lombardi, il problema della protezione dei dati è ben presente. Va comunque segnalato che dall'analisi delle sole risposte forniti dagli esperti di ambito giuridico vi è una forte divergenza di opinioni su quali sono gli archivi comunali più critici in termini di privacy. Questo segnala sicuramente una certa instabilità del tema.

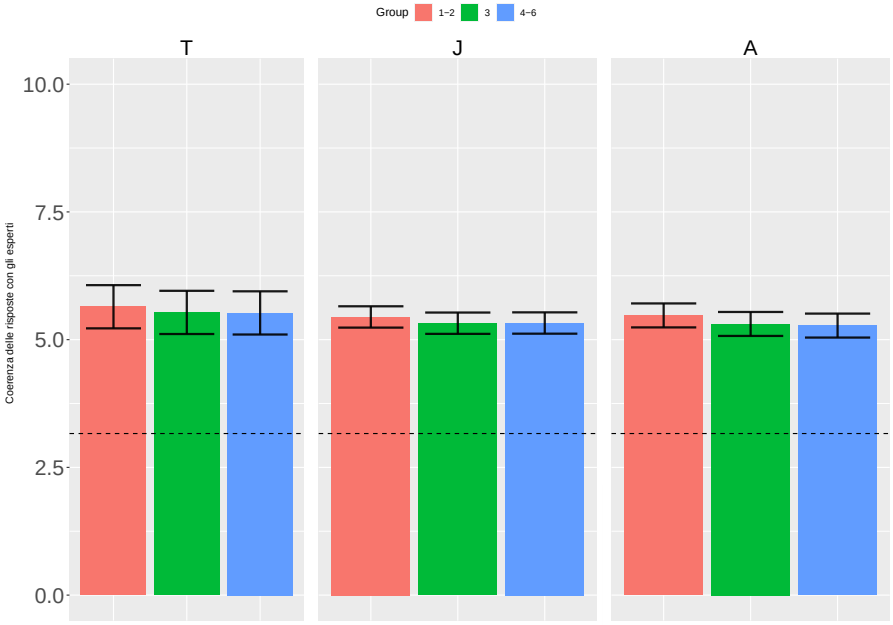

Figura 2.26: Come in Fig. 2.13, ma per la domanda 8

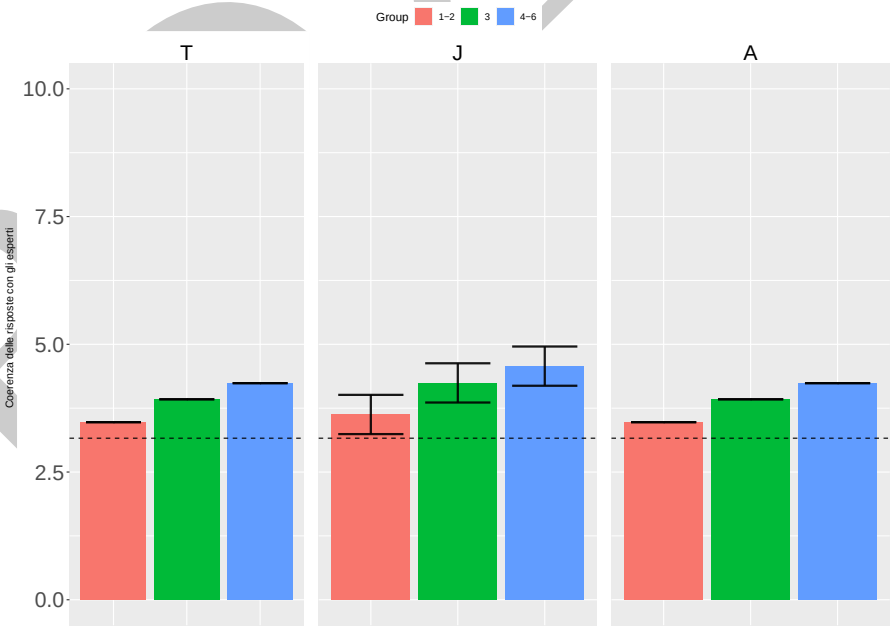

Figura 2.27: Come in Fig. 2.13, ma per la domanda 10

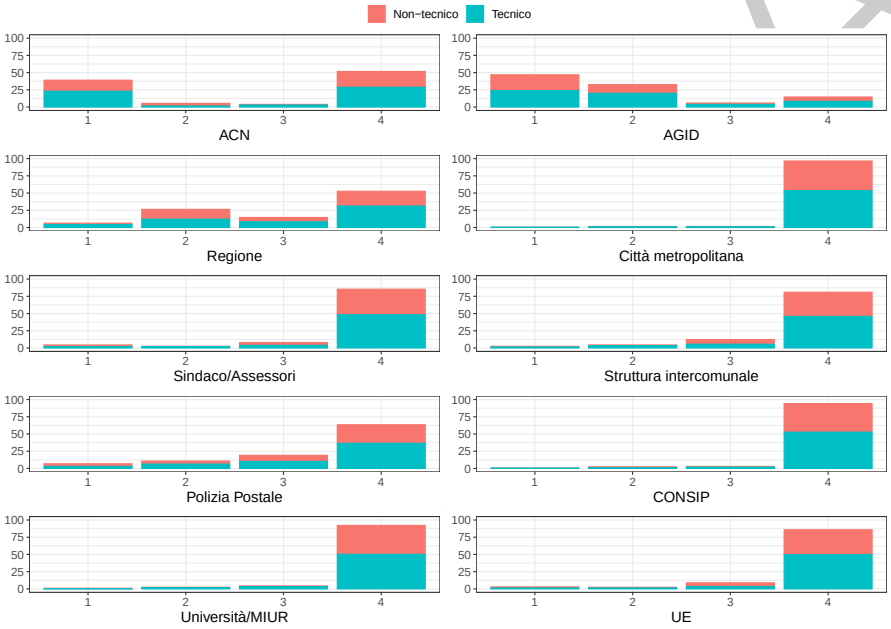

Figura 2.28: Come in Fig. 2.13, ma per la domanda 8

2.3 LA CYBERSECURITY IN PRATICA

Coma già anticipato dopo aver valutato analiticamente il livello di competenze in ambito cybersecurity all'interno degli enti locali ci siamo posti il problema di verificare se i risultati, incoraggianti, ottenuti avessero anche un riscontro pratico. Vale a dire se le competenze tecniche rilevate fossero state correttamente applicate sul campo consentendo la realizzazione di sistemi sufficientemente robusti, e per contro se la scarsa propensione agli aspetti più manageriali della disciplina accanto alla denunciata scarsa consapevolezza del problema nel resto del personale degli enti locali avessero qualche riflesso in termini di cybersecurity. Per la verifica di questi aspetti abbiamo effettuato con l'accordo di un gruppo di enti volontari un vulnerability assessment ed una campagna di phishing veicolata tramite e-mail.

2.3.1 Il Vulnerability Assessment

Il vulnerability assessment è una procedura attraverso la quale si simulano le modalità con le quali un attaccante cerca di individuare delle "falle" in un sistema al fine di comprometterne il funzionamento. Esistono diverse modalità con cui effettuare questo test in funzione dell'informazione sul sistema da attaccare che sono fornite all'attaccante. Nel nostro caso abbiamo adottato la modalità black-box, che simula il comportamento di un attaccante che non conosce nulla sul sito da attaccare, di fatto la situazione più comune. Per condurre questa attività, abbiamo sviluppato all'interno del laboratorio Laser un tool ad-hoc mirato ad assessment e penetration test delle infrastrutture comunali. Questo strumento utilizza una serie di tecniche come la DNS enumeration, la ricerca di vulnerabilità XSS e SQL injection oltre all'esecuzione di port scanning per individuare servizi vulnerabili o deprecati. Il tool sviluppato é basato su strumenti di punta nel campo del penetration testing, come *nmap*[3], *dnsscan*[1], *xssstrike*[5] e *sqlmap*[4], affiancati da metodi e modelli appositamente programmati per adattarsi al contesto applicativo specifico. Lo strumento, é anche in grado di confrontare le versioni dei servizi rilevati con un database di vulnerabilità noto, al fine di individuare eventuali CVE (Common Vulnerabilities and Exposures). La prima fase dell'assessment è stata dedicata ad un'analisi approfondita dei sistemi online attraverso una combinazione di scansioni automatizzate e revisioni manuali. L'obiettivo principale era individuare eventuali servizi vulnerabili esposti. L'analisi delle vulnerabilità ha rilevato un elevato numero di record DNS di cui i comuni non sono consapevoli, alcuni di questi puntano a risorse abbandonate altri invece reindirizzano a portali attivi dei comuni. Inoltre, è significativo il numero di servizi, con una media di 11 servizi esposti per comune. È evidente che quasi tutti i comuni 2.3 espongono siti web (HTTP, HTTPS), servizi di trasferimento file (FTP) e protocolli per la gestione delle email (IMAP). È stata riscontrata la presenza di diverse versioni non aggiornate ma nessuna di esse è risultata contenere vulnerabilità critiche.

2.3.2 La campagna di phishing

Parallelamente all'attività di vulnerability assessment è stata condotta una campagna di phishing mirata a testare la componente umana ma anche organizzativa del sistema informatico comunale. La campagna è stata avviata utilizzando indirizzi e-mail dei dipendenti comunali forniti in fase di raccol-

Tabella 2.2: La tabella riassume l' attività di vulnerability assessment indicando il numero di indirizzi IP che sono stati rilevato nell'attività di profiling del comune, i nomi DNS che di cui il comune non era a conoscenza, i servizi esposti sulla rete internet con eventuali versioni e vulnerabilità e le diverse versioni di sistemi operativi e server che espongono i servizi.

	Provider cloud	IP rilevati	DNS non dichiarati	Servizi rilevati	Server / OS e versioni
Comuni <10K	3,9	1	4	6,6	6
Comuni >10K	4,2	4,9	58,5	15,3	20,7
Tutti i comuni	4	2,9	34,3	11,4	14,1

Tabella 2.3: La tabella mostra i servizi più comuni che sono stati rilevati in base all'insieme di indirizzi IP forniti dai comuni.

	Porta	Servizio
1	443	https
2	80	http
3	21	ftp
4	8000	http-alt
5	995	pop3
6	143	imap
7	993	imap

ta dati dai" responsabili" dei comuni. Una campagna di phishing consiste nell'invio di email di phishing distribuite nel tempo, simulando a tutti gli effetti una campagna di phishing malevola. La mail di phishing si caratterizza da un contenuto che deve essere costruito per essere attrattivo per l'utente al fine di indurlo a cliccare sul link malevolo incorporato che caratterizza ogni messaggio di phishing. In particolare individuiamo due tipologie di email ricevute dai dipendenti comunali: email generiche (ad esempio una notifica di acquisto indesiderato su un noto sito di e-commerce) oppure email personalizzate (come la condivisione di un link *OneDrive* contenente presunte nuove norme approvate nell'ultima delibera di aprile 2023). A fronte di questi messaggi di email un utente può:

1. considerare il messaggio sospetto in base al mittente e/o all'oggetto ed ignorarlo completamente;
2. aprire il messaggio e dopo averne letto il contenuto, eliminarlo senza svolgere nessuna azioni;
3. aprire il messaggio ritenere valido il suo contenuto e cliccare sul link presente nel messaggio.

Il comportamento virtuoso è quello indicato al 1). Il comportamento 2) non è di per sè pericoloso ma è indice di una certa predisposizione a rimanere vittima in futuro, mentre nel caso 3) l'attacco raggiunge il suo obiettivo.
Il principale strumento utilizzato per la campagna è stato *Gophish*[2]; per le e-mail è stato registrato un dominio ad-hoc, `comunemi.it`. . Un esempio di messaggio usato per la campagna è riportato in Fig. 2.30. Ogni email inviata contiene un pixel bianco, noto come tracking pixel, questo elemento consente al tool Gophish di identificare l'apertura della mail e l'eventuale click sul link proposto. Una volta effettuato il click, si viene reindirizzati su una landing page che comunemente ospita un login o un form che richiede

all'utente di inserire dati personali, come ad esempio le credenziali di un account. La mail può essere anche personalizzata per chi la riceve in modo da rendere più efficace l'attacco. L'efficacia della campagna è stata attentamente monitorata attraverso l'analisi delle email ricevute, aperte e cliccate. Questi i principali risultati ottenuti. Nella tabella 2.4 riportiamo anche alcuni dati sulle tecnologie che sonos tate rilevate durante l'attacco. Il sistema operativo più utilizzato dai dipendenti comunali è Microsoft Windows da postazione desktop, seguito dispositivi mobili con Android ed iOS. Si nota la predominanza del browser Edge (presumibilmente legato al sistema operativo Windows), seguito da Chrome e Firefox (disponibili cross-platform). I provider di posta elettronica sono piuttosto diversificati; nella tabella 2.4 sono presenti i primi tre; da notare come ancora al primo posto troviamo Microsoft con Outlook.
L'attività di phishing ha previsto l'invio complessivo di 4230 email durante un periodo di tre mesi, come indicato nella tabella 2.29. Si può osservare che i comuni con il più alto numero di dipendenti sono anche quelli più suscettibili agli attacchi di phishing, con un numero di clic su link malevoli superiore di circa tre volte, ed un numero di credenziali inviate superiore di circa venti volte rispetto ad altri comuni. Tale fenomeno risulta coerente, poiché è probabile che nei comuni più piccoli il passaparola abbia contribuito a ridurre il numero di attacchi di phishing, mentre nei comuni di dimensioni maggiori, dove gli uffici sono più numerosi e strutturati, si riscontra una maggiore complessità nella gestione delle minacce informatiche di questo tipo.

Tabella 2.4: La seguente tabella indica: provider di servizi mail cloud, i browser ed i sistemi operativi più usati che sono stati rilevati durante l'attività di phishing.

	Mail provider	Browser	Sistema operativo
1	Outlook	Edge	Windows
2	Zimbra	Chrome	Android
3	Gmail	Firefox	iOS

Tabella 2.5: La tabella indica le 3 tipologie di campagne di phishing che hanno avuto il maggior grado di successo (maggior numero di aperture, click e inserimento credenziali)

	Campagna	Descrizione
1	Generica	Phishing classico es. rinnovo password SPID
2	Mirata	Mail contenente la condivisione di un documento Sharepoint inerente al comune (ultimo consiglio comunale)
3	Rapida	Mail del provider antivirus che richiede una azione tempestiva sul proprio account compromesso

2.4 CONCLUSIONI

Avviato con l'obiettivo principale di fare una stima delle competenze di cybersecurity presenti nei comuni, elemento chiave per poter effettuare efficacemente una transizione digitale lo studio qui descritto ci ha consentito, grazie alla metodologia utilizzata, di individuare anche gli elementi critici del sistema e poter proporre alcune misure correttive.

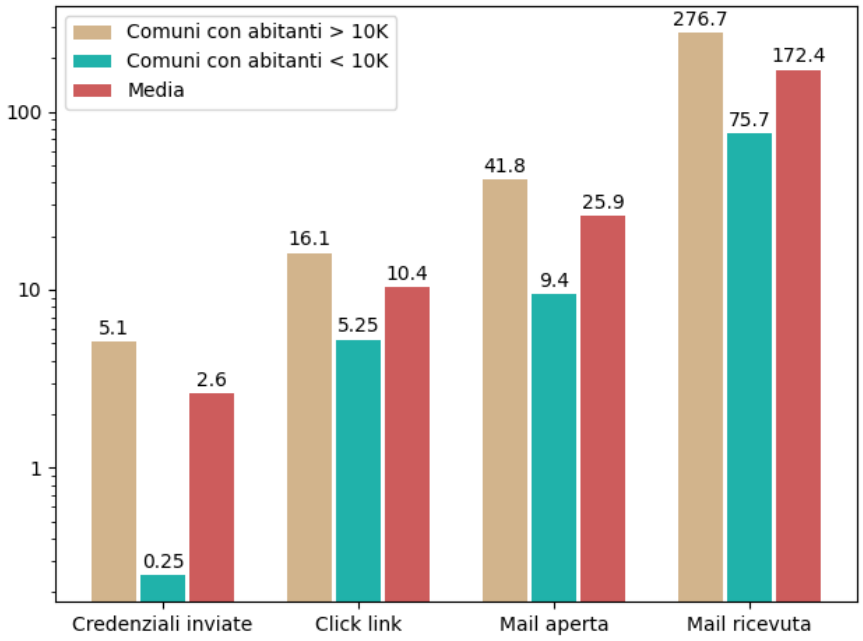

Figura 2.29: Il grafico indica il numero assoluto di mail ricevute senza azioni, mail aperte, link malevoli clickati e credenziali inviate all'attaccante. In rosso é presente la media tra comuni di piccole dimensioni e comuni di grandi dimensioni.

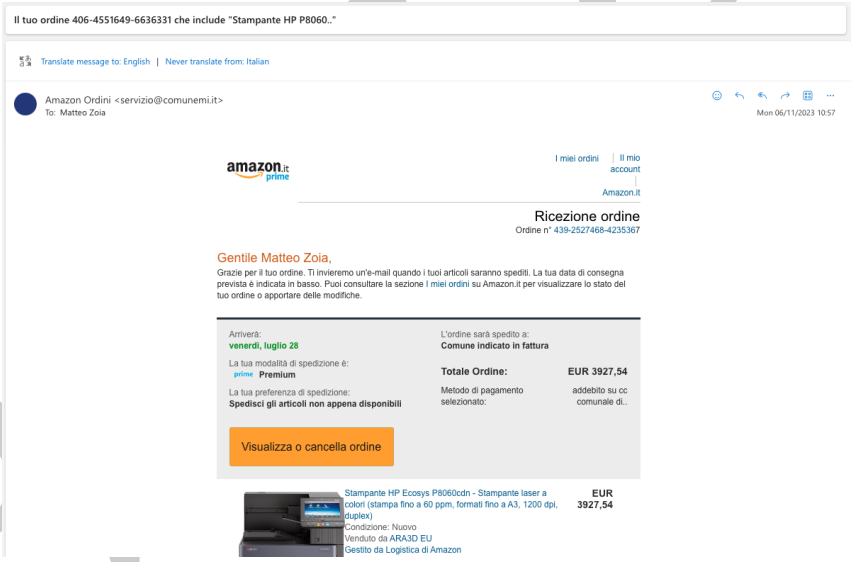

Figura 2.30: Esempio di e-mail di phishing non mirata. É possibile notare alcuni tratti distintivi di phishing, l'indirizzo del sender `@comunemi.it` non é istituzionale, metodo di pagamento con addebito sul cc senza specificare il comune, indirizzo di spedizione indicato in fattura

Il quadro generale che emerge è quello di un sistema (quello dei comuni) in cui esiste la consapevolezza del problema cybersecurity ma anche il rammarico di non avere gli strumenti necessari per poterlo affrontare come si deve. Con il PNRR i comuni hanno potuto disporre di risorse economiche da dedicare alla cybersecurity ma hanno anche denunciato la carenza di competenze per poterli gestire e monitorare correttamente. Si tenga presente che

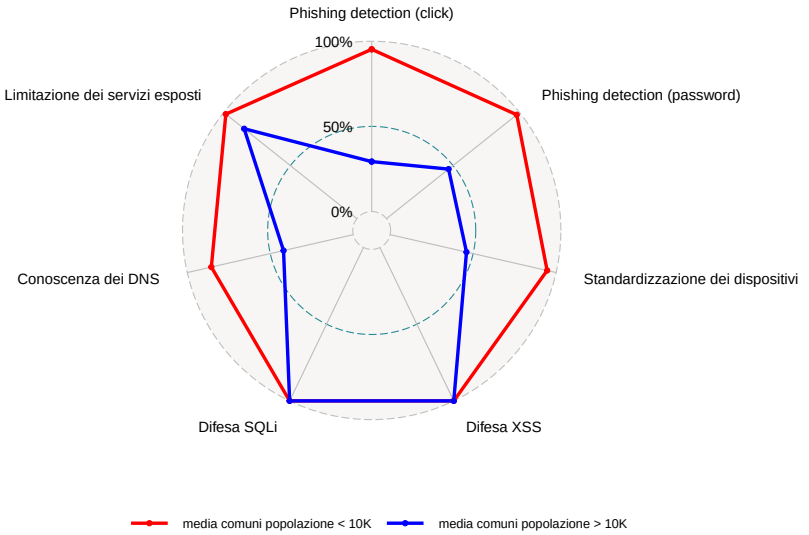

Figura 2.31: Esito aggregato del vulnerability assessment per i comuni coinvolti secondo le diverse caratteristiche analizzate

sugli enti locali pesa un blocco del turn over che nell'ultimo decennio non ha certo facilitato l'inserimento di giovani e conseguentemente nuove competenze e dall'altra il trattamento economico riservato ai dipendenti non è certo attrattivo su un mercato altamente competitivo come quello delle competenze in cybersecurity, quindi difficilmente nei comuni si trova personale con una formazione specifica non solo in cybersecurity ma anche in informatica o materie affini. Questo è ancora più vero per i comuni di piccole dimensioni spiega molti dei fenomeni che abbiamo annotati.
La formazione è de facto il problema più critico che emerge dalla nostra analisi, una formazione che i comuni si sono fatti da soli per affrontare i problemi del day by day ma che ora che le sfide ed i problemi diventano più grossi non basta più. Di questo i comuni ne sono consapevoli e sono disponibili a porvi rimedio, sembra però mancare l'interlocutore. Più in dettaglio questi sono i tratti caratteristici della situazione rilevata.

- nei comuni esiste un buon livello di consapevolezza del problema cybersecurity, è mancato un approccio di sistema alla disciplina ed ogni ente si è come si suol dire "arrangiato" con i propri mezzi. Esiste una certa confusione tra cybersecurity e protezione dati ma a questo livello di approssimazione può essere tollerata.

- Qualitativamente parlando prevalgono negli enti competenze di tipo tecnico, quelle tipicamente che trovano applicazione immediata e che possono essere testate sul campo. Sono molto rare le competenze di tipo manageriale di più difficile reperimento ma anche non così immediatamente applicabili nel contesto di un comune medio/piccolo (ricordiamo che nel nostro "campione" come nella realtà i piccoli comuni sono la stragrande maggioranza dei comuni italiani). Il risultato è la presenza di personale con competenze in grado di risolvere le urgenze, un po' meno elaborare un piano a medio - lungo termine.

- Quantitativamente parlando siamo di fronte ad un livello di competenze sufficiente, se pensiamo che sono competenze che ogni addetto comunale si è costruito in proprio, ma che non sono certo sufficienti a far fronte alle sfide della trasformazione digitale come ad esempio la transizione al cloud. Su questo specifico aspetto abbiamo approfondito la nostra analisi ed è emerso che su questa tematica i comuni sono decisamente in affanno, in particolare i piccoli comuni. Abbiamo rilevato difficoltà a cogliere gli aspetti salienti di questo nuovo modello di erogazione dei servi ICT.

- Abbiamo riscontrato ancora un po' di confusione sulle tematiche di protezione dei dati, anche questa una materia su cui probabilmente l'approccio impositivo ha prevalso su quello educativo.

- Dal punto di vista più pratico dobbiamo sottolineare che grazie alle loro competenze i comuni sono stati in grado di installare direttamente o indirettamente dei siti web robusti. Un hacker che (stante il livello di vulnerabilità ad oggi noto) volesse provare a insidiare uno di questi siti web con il suo armamentario di strumenti tecnologici troverebbe pane per i suoi denti. Troverebbe purtroppo la strada spianata se invece della tecnologia usasse l'ingegneria sociale, in particolare il phishing. Questo dato non deve però sorprendere, è la situazione in cui oggi si trova un qualunque ente pubblico o privato, e gli attacchi informatici più significativi degli ultimi anni lo stanno a dimostrare.

A fronte di questa situazione, quali sono le misure più urgenti che ci sentiamo di suggerire ai decision-maker? Verrebbe da dire sono tre: formazione, formazione e formazione. E' indubbio che la formazione è sicuramente la misura che nell'ambito della cybersecurity i nostri comuni necessitano maggiormente in questa fase, ma anche dando voce alle criticità emerse durante i focus group riteniamo che le misure più urgenti da intraprendere siano:

- **formazione** attualmente come abbiamo potuto rilevare la maggior parte del personale dei comuni che è coinvolto nella gestione di aspetti di cybersecurity si è è auto formato. E' necessario fornire a questo personale ulteriori conoscenze e competenze che travalichino anche l'orizzonte delle competenze tecniche. Per gestire i rapporti con Internet Service Provider, o Cloud Service Provider non bastano le conoscenze tecniche è necessario avere anche competenze di tipo manageriale anche solo per trattare i livelli di servizio. Si può obiettare che per un piccolo comune queste figure professionali "sono uno spreco", ci si attrezzi allora con forme di associazione per fornire a questi comuni queste competenze con un'altra modalità. Un ulteriore appunto, dalla nostra indagine emerge che la protezione dei dati potrebbe essere un ulteriore elemento su cui intraprendere approfondimenti.

- **risorse** la sicurezza è risaputo costa, la cybesecurity non è da meno. Chiedere ai comuni di effettuare interventi di cybersecurity usando risorse proprie non è realistico.

- **supporto** durante i focus group è emersa la necessità di avere direttive più precise sulle azioni da intraprendere e di poter avere un qualche soggetto con cui poter interagire per l'implementazione delle stesse, il nostro sondaggio mostra una forte preferenza per un ente a livello nazionale. Non ci pare che la strategia nazionale di cybersecurity

contempli un'entità con queste prerogative, riteniamo però che sia importante dar seguito a questa esigenza, anche perché in questo modo si potrebbe in parte ovviare alla carenza di competenze che abbiamo riscontrato. Se non corriamo presto ai ripari, rischiamo di "azzoppare" la transizione digitale

3 LA SICUREZZA INFORMATICA DEI COMUNI: OBBLIGO E CONSAPEVOLEZZA

L'architettura legislativa in materia di sicurezza informatica nella Pubblica Amministrazione italiana poggia le fondamenta su quelle che possiamo metaforicamente considerare le sue tre pietre angolari: il Codice dell'Amministrazione Digitale (CAD), le Linee Guida e le circolari emesse dall'AgID e il Regolamento Generale sulla Protezione dei Dati (GDPR). Per capire meglio la natura degli obblighi relativi alla sicurezza informatica, è opportuno analizzare le intenzioni alla base di questi strumenti normativi e il loro ruolo fondamentale nello sviluppo e nell'attuazione delle strategie più avanzate nazionali ed europee.

3.1 CODICE DELL'AMMINISTRAZIONE DIGITALE (CAD)

Il CAD (D.lgs. 82/2005) è un testo unico che disciplina le norme riguardanti l'informatizzazione nei rapporti con i cittadini e le imprese e regola la digitalizzazione della pubblica amministrazione italiana. Il Codice istituito con il decreto legislativo 7 marzo 2005, n. 82, è stato successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n. 217. Negli anni, e nelle rivisitazioni del codice è stato modificato e integrato il concetto di "Sicurezza dei dati", un tema che nasce come obbligo di custodia e controllo rispetto alla conservazione e che, nel tempo, evolve in sicurezza "dei sistemi e delle infrastrutture delle pubbliche amministrazioni". Oggi, per definire quali siano gli obblighi dei Comuni in tema di sicurezza è importante tenere in considerazione che la norma è costantemente aggiornata in relazione alle misure legate all'evoluzione della tecnologia, per questo motivo il CAD prevede al suo interno la possibilità di rinviare a fonti secondarie la predisposizione di misure di sicurezza.
Fatte queste premesse, risulta chiaro il motivo per il CAD rinvii continuamente alla regolamentazione predisposta dall'AgID, ai sensi dell'art. 71 del Codice stesso e al fine di individuare le soluzioni tecniche idonee proprio per l'attuazione del Codice. L'AgID è solo uno dei soggetti richiamati e coinvolti dal CAD nelle funzioni in materia di sicurezza informatica in quanto l'articolo 16 del decreto affida al Presidente del Consiglio dei Ministri o al Ministro delegato, oltre alle funzioni di indirizzo generale in materia, funzioni specifiche in fatto di sicurezza dei sistemi. L'articolo 17 stabilisce l'individuazione un Responsabile per la Transizione al Digitale, la funzione e gli obiettivi di questa figura trovano conferma nel Piano Triennale ICT di AgID. Il codice stabilisce che: "ciascuna pubblica amministrazione affida a un unico ufficio dirigenziale generale, [...] la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla

realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità. Al suddetto ufficio sono inoltre attribuiti i compiti relativi a:

1. coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
2. indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
3. indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;
4. accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
5. analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
6. cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);
7. indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
8. progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
9. promozione delle iniziative attinenti all'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
10. pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis.
11. pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b).

3.2 LA REGOLAMENTAZIONE ATTRAVERSO LINEE GUIDA E CIRCOLARI. AGID E LE MISURE MINIME DI SICUREZZA ICT.

L'Agenzia per l'Italia Digitale riveste un ruolo determinante per la formulazione e divulgazione di linee guida e circolari per la sicurezza informatica all'interno della pubblica amministrazione.

- Le "Linee per la sicurezza nel procurement ICT" forniscono istruzioni sulle misure di sicurezza che le PA devono adottare nel processo di acquisto di beni e servizi ICT;
- Le "Linee per lo sviluppo del software sicuro" forniscono indicazioni per garantire un ciclo di sviluppo di software sicuro all'interno delle amministrazioni e si inseriscono nel contesto delle linee guida per la sicurezza ICT;
- Le "Linee guida per la configurazione per adeguare la sicurezza del software di base" definiscono le regole per affrontare e risolvere correttamente le problematiche legate alla sicurezza del software di base e di individuare le misure da adottare per difendere ogni componente da possibili minacce accidentali e/o intenzionali;
- Le Raccomandazioni AgID - TLS e Cipher Suite redatte in accordo con il Dipartimento per la trasformazione digitale, forniscono un insieme di raccomandazioni in merito ai protocolli di sicurezza e alle Cipher Suite. Data la continua evoluzione tecnologica e la possibile scoperta di nuove criticità il documento è aggiornato ciclicamente;
- Le Misure minime di sicurezza ICT adottate da AgID nel 2017 contengono indicazioni utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica e per contrastare le minacce cibernetiche più frequenti della pubblica amministrazione italiana.

L'obiettivo delle Misure Minime è quello di orientare le Amministrazioni, specialmente quelle più piccole e che hanno meno possibilità di avvalersi di professionalità specifiche, attraverso riferimenti operativi direttamente utilizzabili (checklist), standard comuni di misure tecniche e strumenti per monitorare lo stato di fatto e poter tracciare percorsi di miglioramento. Le Misure minime di sicurezza ICT sono state determinate da circolari, di cui la circolare AgID del 18 aprile 2017 n. 2/2017 rappresenta un punto di riferimento per valutare e potenziare il livello di sicurezza delle informazioni gestite dalle amministrazioni, con l'obiettivo di contrastare le minacce informatiche più comuni. La pubblicazione di circolari semplifica il procedimento per la revisione della normativa in materia di sicurezza, consentendo un'attuazione più rapida delle misure del CAD da parte dell'AgID. Questo tipo di regolamentazione permette un miglioramento progressivo, tenendo conto della complessità del sistema informativo coinvolto e della struttura organizzativa di ciascuna amministrazione. A seconda di tali caratteristiche, le misure minime possono essere implementate in modo graduale seguendo tre livelli di esecuzione:

- Minimo: è il livello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente rendersi conforme.

- Standard: superiore al livello minimo, ogni amministrazione lo deve considerare come base di riferimento in termini di sicurezza.
- Avanzato: deve essere adottato dalle organizzazioni maggiormente esposte a rischi (per la criticità delle informazioni trattate o dei servizi erogati), e visto come obiettivo di perfezionamento da parte delle altre organizzazioni.

Le misure minime si basano sull'esperienza consolidata dell'insieme di controlli noto come SANS 20 / CSC (Critical Security Control). I primi cinque controlli sono quelli indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni e da questi si è partiti per definire le misure minime di sicurezza per la pubblica amministrazione italiana. I macro-gruppi di controlli previsti dalle misure minime sono i seguenti:

- ABSC 1 (CSC 1): inventario dei dispositivi autorizzati e non autorizzati Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia fornito solo ai dispositivi autorizzati, e impedito a quelli non autorizzati;
- ABSC 2 (CSC 2): inventario dei software autorizzati e non autorizzati Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo il software autorizzato, mentre il software non autorizzato sia individuato e ne venga impedita l'installazione e l'esecuzione;
- ABSC 3 (CSC 3): proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server; Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.
- ABSC 4 (CSC 4): valutazione e correzione continua della vulnerabilità; Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici;
- ABSC 5 (CSC 5): uso appropriato dei privilegi di amministratore Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi;
- ABSC 8 (CSC 8): difese contro i malware Controllare l'installazione, la diffusione e l'esecuzione del codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive;
- ABSC 10 (CSC 10): copie di sicurezza Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità;
- ABSC 13 (CSC 13): protezione dei dati Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti.

3.3 REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (GDPR)

Il regolamento UE 2016/679, detto anche GDPR (General Data Protection Regulation) è un regolamento europeo in materia di trattamento e protezione di dati personali, esteso anche alle pubbliche amministrazioni italiane, che ha come obiettivo semplificare e standardizzare il contesto normativo sulla privacy imponendo specifici obblighi riguardo alla sicurezza dei dati e delle persone fisiche. Il GDPR, nell'art. 4, par. 1, definisce il dato personale come "qualsiasi informazione riguardante una persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". Questo include tutte le informazioni che, anche indirettamente, permettono di identificare una persona, ad esempio il nome, il cognome, il numero di telefono, l'indirizzo e-mail, l'indirizzo IP e perfino l'identificativo pubblicitario del dispositivo mobile. Al contrario, i numeri di registrazione aziendale, gli indirizzi e-mail generici e i dati resi anonimi non sono considerati dati personali. Il GDPR fornisce una tutela rafforzata per le categorie particolari di dati, come quelli che rivelano l'etnia, le opinioni politiche, le idee religiose o filosofiche, i dati genetici, biometrici, relativi alla salute o all'orientamento sessuale, a condanne penali o reati, nonché dati concernenti i minori. Il concetto di trattamento di dati personali, definito nell'art. 4, par. 2, include qualsiasi operazione su dati personali: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione." Il Regolamento Europeo stabilisce che ogni trattamento di dati personali deve rispettare i principi fondamentali enunciati nell'articolo 5.

1. I dati personali sono:
   - trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»). Il principio di trasparenza impone al Titolare del trattamento di mettere al corrente i diretti interessati sul trattamento dei loro dati, attraverso un'informativa concisa, trasparente, intellegibile e facilmente accessibile. Deve inoltre fornire le informazioni richieste in caso di esercizio dei diritti e informare gli interessati in caso di violazione dei dati personali (Data Breach);
   - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»). Il Principio di responsabilizzazione ("accountability") impone al Titolare di dimostrare il rispetto dei principi di trattamento dei dati. Uno degli aspetti più innovativi del regolamento, risiede in questo principio, ovvero nell'indicare i caposaldi di gestione della sicurezza informatica basati sulla valutazione del rischio, che impongono l'accountability ai titolari e ai responsabili del trattamento. Tuttavia, gli scopi di sicurezza dei dati non possono eccedere i diritti di privacy e di conseguenza la tenuta sotto controllo delle informazioni private altrui. Questi due concetti sono illustrati nell'articolo 25 del Regolamento:
   - Protezione dei dati fin dalla progettazione "security by design": comporta una valutazione sin dalla fase di progettazione del trattamento dei dati personali e degli strumenti utilizzati, con una verifica costante durante l'intero processo.
   - Protezione per impostazione predefinita: richiede al Titolare di instaurare misure preventive per garantire il trattamento solo dei dati strettamente necessari per ciascuna finalità specifica. In base al principio di accountability, il Titolare è tenuto a individuare adeguate misure tecniche e organizzative per garantire un livello di sicurezza proporzionato al rischio associato alle operazioni di trattamento (art. 32 del GDPR). "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (...)".

Il GDPR identifica specifici ruoli, alcuni dei quali già noti e previsti dalla normativa precedentemente in vigore:

- Il Titolare del trattamento: vale a dire il soggetto che decide in merito a finalità e mezzi del trattamento. A tale figura, il GDPR attribuisce la maggior parte degli adempimenti di compliance, alcuni dei quali sono condivisi con un altro soggetto estremamente rilevante: il Responsabile del trattamento.

- Il Responsabile del trattamento è il soggetto che esegue un trattamento di dati personali per conto di un titolare. Il titolare dovrà individuare tali soggetti, provvedendo a stipulare un contratto di trattamento dati (i cui contenuti sono indicati all'art. 28 del GDPR).

- Il GDPR introduce all'articolo 37 il Data Protection Officer (DPO), una figura obbligatoriamente designata in caso di trattamento effettuato da un'Autorità o da un organismo pubblico e altamente qualificato a livello di data protection, cybersecurity, privacy e protezione dei dati e gestione dei sistemi informatici. Può essere un dipendente del Titolare o del Responsabile oppure un soggetto esterno. I DPO non rispondono personalmente in caso di inosservanza della normativa, in quanto la responsabilità ricade sempre sul Titolare. La figura del DPO, individuata mediante atto di designazione, le cui competenze, mansioni e responsabilità sono previste dagli artt. 37-39 del Regolamento Europeo 2016/679, svolge un ruolo di supporto al titolare oltre che da punto di contatto per l'Autorità Garante della Privacy. È prevista inoltre la possibilità di costituire un ufficio strutturato per lo svolgimento dei compiti stabiliti. Il soggetto individuato per il ruolo di DPO funge da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, come previsto dall'art. 39 del GDPR deve avere esperienza nel settore della Pubblica Amministrazione. L'articolo 39 del GDPR definisce i compiti del DPO:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti sia dal presente regolamento che da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

- sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

- fornire, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera opportunamente i rischi inerenti al trattamento, tenuto conto dell'ambito di applicazione, del contesto e delle finalità dell'anzidetto. Ogni

organizzazione mette in atto adeguamenti per operare in aderenza alle normative relative alla protezione dei dati personali, edificando un sistema di gestione strutturato in continua evoluzione e miglioramento. Le azioni da prevedere sono:

- Analisi dello stato di esecuzione ed implementazione del sistema di gestione privacy dell'organizzazione e di possibili scenari evolutivi;
- Revisione della documentazione di nomina dei responsabili e degli autorizzati;
- Revisione ed eventuale modifica dei processi per la redazione dell'analisi di impatto sulla privacy nell'eventualità di nuovi trattamenti e di Data Breach.
- Formazione da erogare al personale inerente a: Obblighi e responsabilità derivanti dal trattamento dei dati personali; Politiche e modalità di lavoro adottate dall'Ente in tema di protezione dati personali per tutto il personale; Rischi e Misure di sicurezza; Pubblicazione dati personali on-line e redazione degli atti amministrativi.
- Redazione dell'analisi di impatto, prevista dall'art. 35 GDPR (DPIA), relativa a trattamenti che potrebbero comportare elevati rischi per i dati personali, ad esempio la videosorveglianza fissa, le fototrappole, le dashcam, le bodycam e le procedure legate al Whistleblowing.

Ciascuna amministrazione ha il compito di definire internamente qual è l'ufficio che si occupa di coordinare il processo di adeguamento al GDPR unitamente agli altri adempimenti previsti dalla normativa vigente, in particolare quelli previsti dal Codice dell'Amministrazione Digitale.

3.4 LA STRATEGIA NAZIONALE DI CYBERSICUREZZA E LA STRATEGIA CLOUD

L'Agenzia per la cybersicurezza nazionale (ACN) è stata istituita dal Decreto-legge n.82 del 14 giugno 2021 quale "Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza" con "il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico". Tra i principali compiti dell'Agenzia c'è l'attuazione della Strategia Nazionale di Cybersicurezza, adottata dal Presidente del Consiglio nel 2022 in linea con quanto previsto dalla Strategia dell'Unione Europea per la cybersicurezza. Tale strategia, di cui proprio l'ACN è uno dei quattro pilastri tecnico-operativi, definisce gli obiettivi da perseguire entro il 2026. Per la sua attuazione è stato predisposto un "Piano di implementazione" articolato in 82 misure ed un "Manuale operativo" la cui funzione è quella di "declinare, per ogni misura, le metriche e gli indicatori di misurazione individuati, l'anno di prevalente implementazione delle stesse, oltre alle relative linee guida". Il Piano di implementazione copre l'intero ambito operativo della cybersicurezza, individuando i settori critici e le vulnerabilità dell'intero sistema Italia, fra cui quelli relativi alla sicurezza dei dati e dei sistemi, a tutela del funzionamento e dell'operatività della Pubblica Amministrazione e per la disponibilità e la fruibilità dei servizi ai cittadini e alle imprese. Infatti, fra le sfide da affrontare, la prima identifica proprio la necessità di

"Assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione (PA) e del tessuto produttivo" considerando la "cybersicurezza degli assetti e dei servizi digitali" quale "elemento imprescindibile della loro fruibilità da parte del cittadino" in condizioni di "totale fiducia e con la consapevolezza che i suoi dati sono adeguatamente protetti". E proprio una delle misure del Piano di implementazione sopra citato, la numero 58, ha come obiettivo di "Sviluppare servizi pubblici digitali per la Pubblica Amministrazione a livello centrale e locale". Fra i compiti affidati ad ACN rientra la presa in carico e la gestione del Cloud Marketplace, precedentemente gestito da AgID, la piattaforma che espone i servizi e le infrastrutture Cloud qualificate per la Pubblica Amministrazione. E proprio il processo di qualificazione è attualmente in via di revisione ed aggiornamento secondo quanto disposto nel Decreto direttoriale prot. N. 29 del 02/01/2023, come modificato dal Decreto prot. N. 20610 in data 28/07/2023 e dal Decreto prot. N. 2927 in data 30/01/2024. Tale strumento è fondamentale per l'acquisizione da soggetti privati dei servizi Cloud qualificati da parte delle Pubbliche Amministrazione, come previsto dalla normativa vigente in tema di procurement delle pubbliche amministrazioni (Codice degli appalti). La Strategia Cloud Italia contiene gli indirizzi per la migrazione verso il cloud qualificato della Pubblica Amministrazione. È stata pubblicata nel settembre del 2021 e realizzata dal Dipartimento per la trasformazione digitale e dall'Agenzia per la cybersicurezza nazionale. Come si legge sul sito dedicato: "La strategia applica il principio cloud first, favorendo l'adozione prioritaria da parte delle Pubblica Amministrazione di strumenti e tecnologie di tipo cloud nello sviluppo di nuovi servizi e nell'acquisizione di software. La strategia, inoltre, individua tre obiettivi strategici che caratterizzano il percorso di trasformazione:

- incentivare le PA all'adozione di soluzioni basate sul cloud computing, attraverso il modello cloud della PA, per proporre un'offerta di servizi digitali e infrastrutture tecnologiche sicure, efficienti, affidabili e autonome, in linea con i principi di tutela della privacy e le raccomandazioni destinate all'intero mercato europeo;
- garantire la sicurezza degli asset strategici per il Paese mediante lo sviluppo del Polo Strategico Nazionale, un'infrastruttura ad alta affidabilità promossa dalla Presidenza del Consiglio dei ministri, consentendo il consolidamento dei data center delle pubbliche amministrazioni centrali;
- valorizzare le pubbliche amministrazioni e la loro capacità di offrire servizi digitali". Per la sua attuazione sono state avviate iniziative che si articolano in:
- costituzione di un Polo Strategico Nazionale, un'infrastruttura cloud ad alta affidabilità per i dati e i servizi, critici e strategici, delle pubbliche amministrazioni italiane;
- adozione di un modello per la Classificazione di dati e servizi che individua come strategici, critici e ordinari, le tipologie di dati in possesso delle Pubbliche Amministrazioni in base al danno che una loro compromissione potrebbe provocare al Paese;
- messa a disposizione di finanziamenti attraverso le Misure del Piano Nazionale di Ripresa e Resilienza fra cui quelle specifiche per la migrazione al cloud dei dati e dei servizi: 1.1 "Infrastrutture digitali" e 1.2 "Abilitazione al Cloud per le PA Locali".

Per la Pubblica Amministrazione Locale, il tema della transizione digitale è al centro delle anche di importanti iniziative finanziate con i fondi PNRR che vedono i Comuni fra i principali Soggetti Attuatori e che richiamano espressamente la sicurezza informatica degli assetti e dei servizi fra gli obiettivi dichiarati. In particolare, la Misura 1.2 "Abilitazione al Cloud per le PA Locali" prevede, quali modalità di migrazione al Cloud proprio, il "Trasferimento in sicurezza" e l'"Aggiornamento in sicurezza" dei dati e dei servizi, in linea con il processo di razionalizzazione dei data center pubblici, avviato da AgID fin dal 2019, e che vede nel 2026 la dead-line per il raggiungimento degli obiettivi prefissati. Infatti, l'investimento è collegato all'obbligo per la PA di migrare i propri CED verso ambienti cloud, introdotto dall'art. 35 "Consolidamento e razionalizzazione delle infrastrutture digitali del Paese" del D.L. 76/2020. Altra misura cardine per i Comuni, anche per la rilevanza dei fondi messi a disposizione, è la 1.4.1 "Esperienza del Cittadino nei servizi pubblici" che ha come obiettivo dichiarato il "miglioramento della qualità e dell'utilizzabilità dei servizi pubblici digitali" in linea e "in conformità con le Linee guida emanate ai sensi del CAD e l'e-government benchmark relativamente agli indicatori della 'user-centricity' e della trasparenza". In un'ottica di sistema, sono da considerare anche la Misura 1.4.4 "Estensione dell'utilizzo delle piattaforme nazionali di Identità Digitale (SPID e CIE)" che ha fra gli obiettivi l'adozione dello standard Open ID Connect, in sostituzione dell'attuale SAML2, per garantire un più elevato livello di sicurezza nell'impiego dell'identità digitale per l'accesso e l'utilizzo dei servizi online della Pubblica Amministrazione, e la Misura 1.3.1 "Piattaforma Nazionale Digitale Dati", sviluppata in attuazione del modello di interoperabilità della Pubblica Amministrazione, che comporta, oltre che una semplificazione dei processi, anche un maggior livello di sicurezza nell'interscambio dei dati e la fruizione dei servizi da parte di tutti gli attori coinvolti.

3.5 SUPERARE LE CRITICITÀ, AUMENTARE LA CONSAPEVOLEZZA

In conclusione, dopo aver esplorato il tema della cybersecurity insieme ai rappresentanti comunali coinvolti nel progetto MUSA, emerge chiaramente che l'assenza di normative facilmente identificabili, la complessità nella loro interpretazione e l'ampia diversificazione delle norme e delle linee guida su vari livelli (tecnico, giuridico, strategico e gestionale) rendono particolarmente ardua la comprensione del tema e l'attuazione delle relative misure di sicurezza nei Comuni. La difficoltà nell'intelligibilità si aggrava ulteriormente quando si considerano le sfide legate alla necessità di investire risorse: l'adeguatezza degli investimenti in sicurezza è spesso incalcolabile, i danni subiti difficilmente quantificabili in termini economici e l'obiettivo di raggiungere una protezione al 100% appare irrealizzabile.
Per affrontare le numerose sfide nella gestione della sicurezza informatica, l'approccio più efficace per i Comuni risiede nella valutazione dei rischi, sia attuali che potenziali. Tale valutazione consente di stabilire le priorità nell'impegno a proteggere le risorse digitali. La consapevolezza del rischio è fondamentale per identificare e analizzare le minacce potenziali e comprendere la vulnerabilità dei sistemi informatici e dei dati sensibili. Un'analisi accurata permette di riconoscere le proprie debolezze e di elaborare una strategia di sicurezza mirata, in grado di contrastare le minacce specifiche

del settore pubblico, come furti di dati, virus, malware e ransomware. La valutazione dei rischi, la tutela dei dati sensibili, la prevenzione degli attacchi informatici e una risposta efficace agli incidenti costituiscono i pilastri fondamentali per assicurare un livello adeguato di cybersicurezza nei Comuni, elementi cruciali per proteggere i dati dei cittadini, garantire la continuità dei servizi e mantenere la fiducia nelle istituzioni. Dall'analisi della situazione nei Comuni emerge che la consapevolezza del rischio è il punto chiave per gestire le criticità. Oltre all'adozione di misure tecniche preventive, è essenziale formare i dipendenti sull'importanza della sicurezza. Incrementare la consapevolezza del personale sui rischi e sulle minacce contribuisce a modulare il loro comportamento, invertendo la tendenza generale a sottovalutare gli attacchi informatici.

4 BIBLIOGRAFIA

[1] dnsscan. https://github.com/rbsec/dnscan.

[2] Gophish. https://github.com/gophish/gophish.

[3] nmap. https://nmap.org/.

[4] SqlMap. https://sqlmap.org/.

[5] XSSStrike. https://github.com/s0md3v/XSStrike.