AGID | Agenzia per l'Italia Digitale

Vigilanza sui soggetti qualificati o accreditati

(QTS, PEC, Conservazione, SpID)

Rapporto di riepilogo

gennaio-dicembre 2019

AGID | via Liszt, 21 – 00144 Roma | protocollo@pec.agid.gov.it | www.agid.gov.it | tel. 06 85264.1

Presidenza del Consiglio dei Ministri

Indice

1 PREFAZIONE

La presente relazione illustra le attività svolte nel 2019 dall'Agenzia per l'Italia Digitale, nel suo ruolo di organismo preposto all'esercizio delle funzioni di vigilanza previste dal Codice dell'Amministrazione Digitale (CAD)[1].

Lo scopo è informare le parti interessate - gli utenti dei servizi vigilati[2], le istituzioni e gli stessi operatori ai quali si applicano le funzioni di vigilanza – delle attività svolte e dell'impegno dell'Agenzia nell'interpretare il ruolo di autorità di vigilanza come strumento per stimolare il miglioramento continuo dei processi di erogazione dei servizi, secondo livelli di qualità e sicurezza coerenti tra i diversi operatori e conformi alle indicazioni del quadro normativo europeo, prevenendo irregolarità o situazioni di degrado che, oltre ad essere sanzionabili, minano la fiducia degli utenti nell'utilizzo dei servizi *on line* e costituiscono un ostacolo allo sviluppo dei processi di digitalizzazione.

La relazione riepiloga le attività svolte nei confronti dei diversi *stakeholder*, illustrando in particolare le verifiche svolte sui soggetti vigilati e le relative modalità di esecuzione, e dando conto dei risultati ottenuti.

La pubblicazione della relazione è giunta al suo terzo anno. Il riepilogo annuale e i casi concreti affrontati, forniscono all'Agenzia lo spunto per rivedere i processi interni e le modalità di esecuzione dell'attività. **Nel 2019, rispetto all'anno precedente, molto è cambiato nella conduzione delle verifiche,** che si sono specializzate su particolari componenti dei servizi, selezionate anche in relazione ad eventi negativi che si sono verificati nel corso dell'anno[3]. Nelle verifiche sono state inoltre coinvolte **altre strutture specialistiche, con l'apporto delle loro competenze**: il *Computer Emergency Response Team della Pubblica Amministrazione* (CERT-PA)[4], che ha operato all'interno di AgID per la prevenzione e la risposta agli incidenti informatici nel dominio delle pubbliche am-

[1] L'art. 14-bis, comma 2, lettera i) del Codice dell'Amministrazione Digitale (CAD) stabilisce che «[…] *AgID svolge funzioni di vigilanza sui servizi fiduciari ai sensi dell'articolo 17 del Regolamento UE 910/2014 in qualità di organismo a tal fine designato, sui gestori di posta elettronica certificata, sui conservatori di documenti informatici accreditati, nonché sui soggetti, pubblici e privati, che partecipano a SPID di cui all'articolo 64; nell'esercizio di tale funzione l'Agenzia può irrogare per le violazioni accertate a carico dei soggetti vigilati le sanzioni amministrative di cui all'articolo 32-bis in relazione alla gravità della violazione accertata e all'entità del danno provocato all'utenza*».

[2] Gli utenti dei servizi vigilati (PEC. SpID, conservazione e servizi fiduciari qualificati, tra i quali ad esempio iservizi di firma digitale) sono cittadini, imprese e pubbliche amministrazioni.

[3] Attacchi informatici e campagne di diffusione di malware attraverso la posta elettronica certificata, che hanno avuto ampia eco sui mezzi di comunicazione di massa.

[4] Il CERT-PA, attivo dal mese di marzo 2014 fino al 6 maggio 2020, ha operato all'interno di AgID con il compito di supportare le pubbliche amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica. Dal7 maggio 2020, a seguito dell'entrata in vigore delle "Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team – CSIRT italiano" (DPCM 8 agosto 2019), le attività di supporto sono svolte dal CERT-AgID (https://cert-agid.gov.it) che ha sostituito il CERT-PA.

ministrazioni e il *Nucleo di Prevenzione delle Frodi Tecnologiche* della Guardia di Finanza, nell'ambito di un accordo stipulato a novembre 2018 ed attivato sin dall'inizio del 2019[5].

Ulteriori novità riguardano l'**introduzione, in via sperimentale, di strumenti e sistemi per migliorare la capacità di prevenzione** e di individuazione di potenziali irregolarità: l'ascolto della rete per rilevare eventuali elementi di attenzione[6] e l'analisi delle percezioni degli utenti possono fornire utili indicazioni per verifiche più mirate, volte a sollecitare gli operatori ad interventi correttivi in via preventiva. Un primo passo è stato realizzato nel 2019 e molto è ancora da fare negli anni che seguiranno.

Sempre restando nel quadro delle novità delle azioni 2019, un importante impegno è stato dedicato alla raccolta sistematica ed all'analisi delle segnalazioni di interruzioni di servizio, malfunzionamenti o incidenti pervenute dagli utenti e dagli stessi operatori. Indicatori basati su tali eventi, insieme ad altri che tengono conto delle caratteristiche di ciascun operatore, quali ad esempio dati dimensionali sull'utenza e sui volumi gestiti, soluzioni tecnologiche adottate e rete dei partner o subcontraenti, **concorrono alla profilazione degli operatori[7] secondo indici di rischio** che sono presi a riferimento per la programmazione delle verifiche e che in futuro consentiranno azioni sempre più mirate, nella consapevolezza, ad esempio, che l'assenza di segnalazioni per uno o più operatori, più che far configurare casi di eccellenza, possa essere riconducibile alla mancata applicazione o non adeguatezza di procedure e strumenti, a scarsa sensibilizzazione del personale o a non adeguata conoscenza degli obblighi posti in capo ad un soggetto qualificato o accreditato per un determinato servizio.

Parlando di **risultati,** viste le importanti novità che hanno caratterizzato le attività nel 2019 e l'impegno che hanno comportato a risorse invariate per AgID, è poco immediato un confronto con il 2018 che sia basato solo su aspetti dimensionali: si è passati da 61 procedimenti del 2018, per uno dei quali - avviato a fine 2018 - è stata attivata nel corso del 2019 la fase sanzionatoria, a 16 procedimenti più complessi avviati nel 2019, per 5 dei quali è stata attivata la fase sanzionatoria. Nel merito, le irregolarità riscontrate sono riconducibili talvolta alle stesse componenti di servizio risultate critiche in entrambi gli anni (controllo dei partner; misure di sicurezza; …), mentre per alcune componenti (organizzazione e documenti di riscontro; controllo dei partner) si è rilevata una reiterazione di irregolarità o un mancato adeguamento, nonostante il piano di azioni correttive trasmesso ad AgID per risovere le irregolarità riscontrate.

Alle attività sopra accennate sono dedicate specifiche sezioni della relazione; una sezione introduttiva riepiloga in appositi paragrafi cosa è la vigilanza, chi sono gli stakeholder, come è condotta e chi sono i soggetti vigilati, con un primo profilo per i soggetti vigilati e per quelli che nel 2019 so-

5 https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2019/03/06/agid-guardia-finanza-danno-il-ad-azioni-congiunte-rafforzare-fiducia-nelleconomia

6 Ad esempio argomenti o quesiti relativi ai servizi vigilati (QTS, PEC, Conservazione o SpID) più ricorrenti o più discussi tra gli utenti in un arco temporale. Per approfondimenti, si rimanda al § 7.

7 Le informazioni trasmesse dai gestori sono raccolte ed elaborate per individuare priorità nella programamzione delle verifiche secondo indici di rischio. Per approfondimenti si rimanda al § 2.2.

no stati coinvolti da almeno un procedimento di verifica. I risultati sono esposti in forma anonima ed in modalità aggregata. I dati si riferiscono al 31/12/2019.

2 LE FUNZIONI DI VIGILANZA SVOLTE DA AGID

2.1 Le regole e le modalità di esecuzione

Il Codice dell'Amministrazione Digitale (CAD)[8] conferisce all'Agenzia per l'Italia Digitale funzioni di vigilanza sui *prestatori di servizi fiduciari*, sui *gestori di Posta Elettronica Certificata*, sui *conservatori di documenti informatici* e sui *gestori di identità digitale SpID*, iscritti negli appositi elenchi. Con riferimento ai primi (Qualified Trust Services Provider, o QTSP), che erogano i servizi fiduciari individuati e disciplinati dal Regolamento UE 910/2014 (Regolamento eIDAS), AgID è l'organismo di vigilanza designato in Italia, con gli specifici compiti previsti dal Regolamento, che includono rendicontazioni verso istituzioni europee, collaborazione ed assistenza verso organismi di vigilanza di altri Stati Membri. Nell'esercizio delle proprie funzioni all'Agenzia è demandato il compito di accertare eventuali violazioni delle norme del CAD e del Regolamento eIDAS da parte dei soggetti vigilati e irrogare le conseguenti sanzioni amministrative[9]. Per approfondimenti si rimanda al § 11.

Al fine di disciplinare le modalità di esecuzione della vigilanza e di esercizio dei potere sanzionatorio previsto dalle norme, garantendo omogeneità di trattamento ai soggetti vigilati e assicurando certezza nei tempi di conclusione di eventuali procedimenti sanzionatori, AgID ha adottato un apposito Regolamento pubblicato sul sito istituzionale[10]. È parte integrante del Regolamento, il documento che descrive come sono svolte le verifiche sui soggetti vigilati e quali sono le norme ed i documenti di riscontro rispetto ai quali sono condotte le valutazioni.

Il Regolamento definisce i principi generali che guidano AgID nelle verifiche sui gestori: da un lato la vigilanza è volta a verificare che i soggetti qualificati o accreditati ed i servizi da essi prestati rispondano nel tempo ai requisiti previsti dalle norme, accertando violazioni o irregolarità o situazioni che siano indice di degrado dei processi in uso o delle capacità tecniche dimostrate in fase di qualificazione; dall'altro, le verifiche sono volte a favorire il miglioramento continuo dei processi di erogazione dei servizi stessi e all'adeguamento tecnologico, per far fronte all'evoluzione *in itinere* che rende *asset* e processi rapidamente obsoleti.

Per dare attuazione ai principi sopra richiamati, le verifiche, siano esse condotte su base documentale o anche attraverso verifiche ispettive portano alla formulazione di rilievi, distinti rispettivamente in 'Non Conformità[11]' e 'Osservazioni[12]'. Tutti i rilievi e le azioni conseguenti definite dai

[8] art. 14-bis, comma2 ,lettera i)

[9] art. 32-bis CAD

[10] https://www.agid.gov.it/it/agenzia/vigilanza - "Regolamento recante le modalità per la vigilanza e per l'esercizio del potere sanzionatorio ai sensi dell'art.32-bis del d.lgs. 7 marzo 2005, n.82 e successive modificazioni", adottato con Determinazione n. 191/2019 del 5 giugno 2019.

[11] Non Conformità: è una irregolarità o violazione accertata rispetto alle norme di riferimento (CAD, Regolamento eIDAS e norme attuative o correlate), classificata secondo tre livelli di gravità crescente: 'Lieve', 'Media', 'Grave'. Ciascuna Non Conformità richiede azioni correttive da adottare entro tempi massimi stabiliti.

gestori sono oggetto di monitoraggio nell'ambito delle verifiche svolte d'ufficio e sono tenute sotto controllo fino alla completa attuazione, anche a procedimento concluso.

2.2 La programmazione secondo priorità: i profili di rischio

I procedimenti di verifica (verifiche) sui soggetti vigilati si concludono in un tempo massimo di centottanta giorni, fatti salvi eventuali termini di sospensione.

Oltre ai procedimenti avviati in via estemporanea, a seguito di eventi specifici rilevati autonomamente o su segnalazione esterna, le verifiche sono programmate periodicamente, secondo priorità che tengono conto di un insieme di elementi che concorrono a determinare il "profilo di rischio" di un soggetto vigilato e permettono di individuare le componenti di servizio da verificare in via prioritaria:

a) dimensioni e tipologia di servizi e utenti, rilevati dai report periodici*;*
b) segnalazioni pervenute su incidenti, malfunzionamenti e interruzioni di servizio;
c) soluzioni tecnologiche adottate;
d) partner che gestiscono specifiche componenti del servizio;
e) analisi di tipo predittivo (sperimentazione avviata nel 2019);
f) verifiche precedenti e relativi esiti, con corrispondenti piani di rientro.

I punti b),c), d) ed f) consentono in particolare, come accaduto nella pratica, di individuare le vulnerabilità comuni a più gestori; il punto a) consente di capire quale diverso impatto potrebbe determinare una stessa vulnerabilità per più gestori; il punto b) consente inoltre di individuare potenziali inadeguatezze nelle procedure operative e gestionali adottate.

Tali elementi concorrono ad inquadrare tutti i soggetti vigilati per ciascun ambito in una matrice - da mantenere aggiornata nel tempo - che attribuisce ad ogni gestore/ambito un indice di rischio, in una scala da 0 a 1, dove 0 è il rischio nullo e 1 è il rischio massimo.

[12] Osservazione: è una raccomandazione o spunto per il miglioramento; ha l'obiettivo di invogliare i gestori a riesaminare i processi e ad adottare in via continuativa azioni volte ad adeguare l'offerta di servizi alle potenzialità offerte dalle evoluzoni tecnologiche in itinere, a migliorare la qualità erogata, nonché a prevenire situazioni di degrado.

2.3 Le parti interessate (*stakeholder*)

Le funzioni di vigilanza svolte da AgID vedono coinvolti a diverso titolo più organizzazioni esterne. Lo schema che segue ne fornisce una rappresentazione di sintesi.

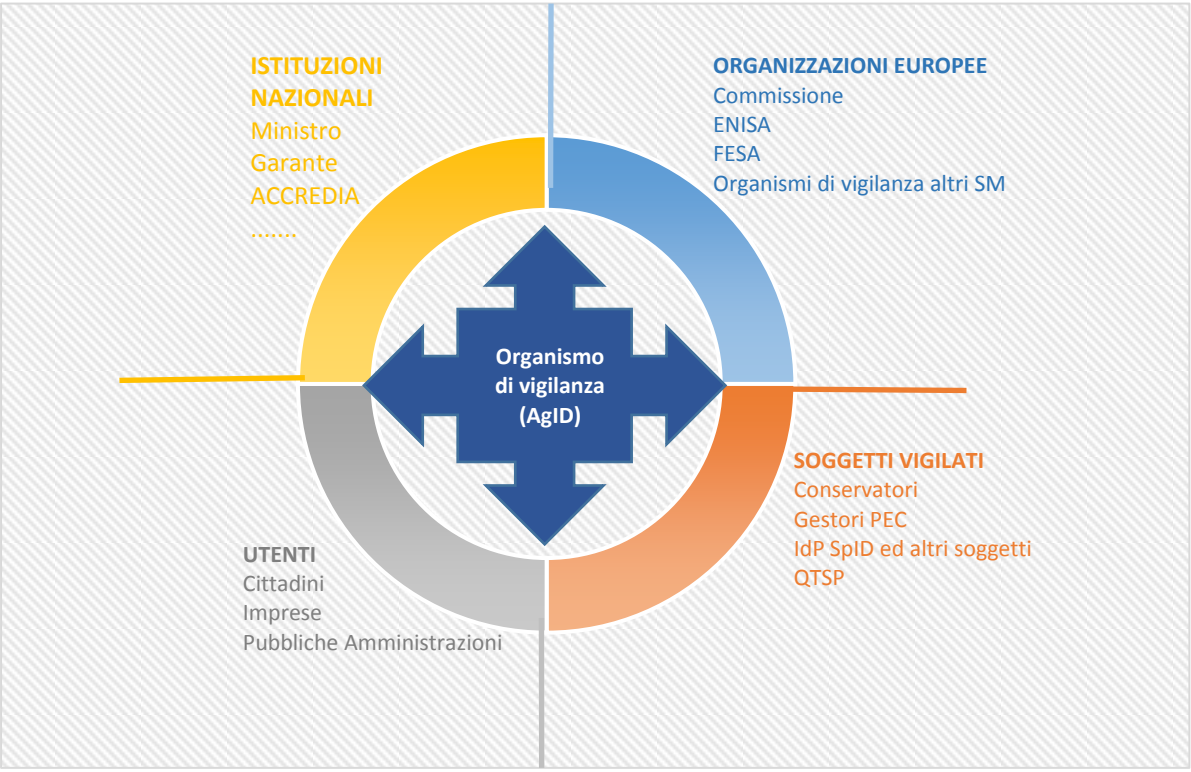

Fig. 2.1– La rete degli stakeholder

1. **Istituzioni nazionali**. Sono qui incluse:
   - le istituzioni alle quali compete la definizione degli obiettivi e degli indirizzi strategici che l'Agenzia deve mettere in atto e le organizzazioni alle quali compete dotare AgID, in quanto Organismo di vigilanza designato in Italia ai sensi dell'art. 17, comma 2 del Regolamento eIDAS, dei poteri e delle risorse adeguate per l'esercizio dei compiti previsti;
   - la altre organizzazioni nazionali direttamente coinvolte nei processi primari della vigilanza. Si citano, a titolo di esempio, il Garante, che, con proprio personale, può prendere parte alle attività ispettive presso i gestori SpID, o ACCREDIA, l'ente nazionale per l'accreditamento degli organismi di certificazione, con il quale AgID collabora ai fini della definizione degli schemi di accreditamento per le valutazioni di conformità di parte terza nell'ambito dei servizi vigilati.
2. **Soggetti vigilati**. Sono i soggetti ai quali si applicano le funzioni di vigilanza. Si veda il § 3.
3. **Utenti**. Sono le persone fisiche (cittadini) o giuridiche (imprese e pubbliche amministrazioni) che usufruiscono dei servizi erogati dai soggetti vigilati. Le segnalazioni verso AgID o le rilevazioni periodiche sulal qualità percepita forniscono indicazioni per pianificare le evoluzioni dei servizi e delle attività correlate, svolte da AgID.

4. **Organizzazioni europee**. Sono qui incluse le principali organizzazioni che operano ai fini dell'attuazione del Regolamento eIDAS. Includono:
   - Commissione Europea. È l'istituzione alla quale compete l'emanazione degli atti di esecuzione, o alla quale fanno riferimento i procedimenti di notifica. È anche l'istituzione alla quale AgiD, in quanto organismo di vigilanza designato, deve annualmente riferire, in attuazione delle previsioni di cui al punto (40) ed all'art. 17, comma 6, del Regolamento eIDAS.
   - ENISA (Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione). È il soggetto destinatario delle notifiche di violazioni alla sicurezza da parte di AgID, in attuazione delle previsioni di cui al punto (39) ed all'art. 19 del Regolamento eIDAS.
   - FESA (*Forum of European Supervisory Authorities for trust service providers*). E' un'associazione degli Organismi di vigilanza europei previsti all'art. 17 del Regolamento eIDAS, avente lo scopo di supportare e migliorare la cooperazione e l'assistenza reciproca, secondo quanto previsto dallo stesso Regolamento eIDAS. Sono svolti periodici incontri – di regola semestrali – per consentire la condivisione e lo scambio di informazioni e di buone pratiche.
   - Organismi di vigilanza degli altri Stati Membri. Con tali organismi sono previsti dal Regolamento eIDAS rapporti di collaborazione ed assistenza reciproca, nonché l'invio delle notifiche di incidenti di sicurezza e perdita di integrità dei dati ricevute dai QTSP nazionali che abbiano impatto su altri Stati Membri.

3 TASSONOMIA DEI SOGGETTI VIGILATI

Le funzioni di vigilanza riguardano circa 130 soggetti, qualificati o accreditati da AgID ed iscritti in elenchi pubblici di fiducia gestiti da AgID e consultabili sul sito istituzionale[13].

Si tratta in particolare di quattro categorie di seguito elencate, per ciascuna delle quali si presentano in forma anonima ed in modalità aggregate indicazioni che sono prese a riferimento per delineare i profili di rischio e per programmare le verifiche d'ufficio.

3.1 Prestatori di servizi fiduciari qualificati (QTSP)

Al 31/12/2019 risultano iscritti nell'elenco dei prestatori di servizi fiduciari qualificati attivi in Italia 20 soggetti, qualificati per uno o più servizi fiduciari (servizi di firma, sigillo, marche temporali e certificati qualificati per siti web).

Con riferimento agli elementi indicati al § 2.2, che concorrono a delineare i profili di rischio, si rilevano per i soggetti iscritti nell'elenco dei QTSP i seguenti criteri di classificazione:

- **servizi erogati e volumi gestiti**: tutti i QTSP sono qualificati per i servizi di firma, solo 2 per le quattro tipologie di servizi. 3 QTSP coprono il 75% dei certificati qualificati per firma con SC/Token, 3 QTSP diversi dai precedenti, coprono circa l'80% delle marche temporali qualificate;
- **caratteristiche dell'utenza**: 7 gestori rilasciano firme solo ad una clientela predefinita e limitata (interna al gestore stesso o limitata ad una rete specifica di utenze, come ad esempio la rete dei dottori commercialisti, la rete dei notai o la rete dei tabaccai); 13 gestori rilasciano firme sigilli certificati o marche sia a clientela business che a persone fisiche (cittadini);
- **soluzioni tecnologiche e partner**: per l'erogazione del servizio, alcuni QTSP si appoggiano all'infrastruttura software di un altro QTSP. Per alcuni gestori sono esternalizzate le attività di identificazione e gestione dei richiedenti.

Nel grafico che segue si riporta un estratto dell'andamento dei volumi dei servizi di firma e marca temporale al 31/12/2019, che costituiscono l'offerta più consistente per questa tipologia di soggetti vigilati.

[13] Elenco dei prestatori di servizi fiduciari attivi in Italia (https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia);

Elenco dei gestori PEC accreditati (https://www.agid.gov.it/it/piattaforme/posta-elettronica-certificata/elenco-gestori-pec);

Elenco dei conservatori accreditati (https://www.agid.gov.it/it/piattaforme/conservazione/conservatori-accreditati)

Elenco degli Identy Provider accreditati (https://www.agid.gov.it/it/piattaforme/spid/identity-provider-accreditati)

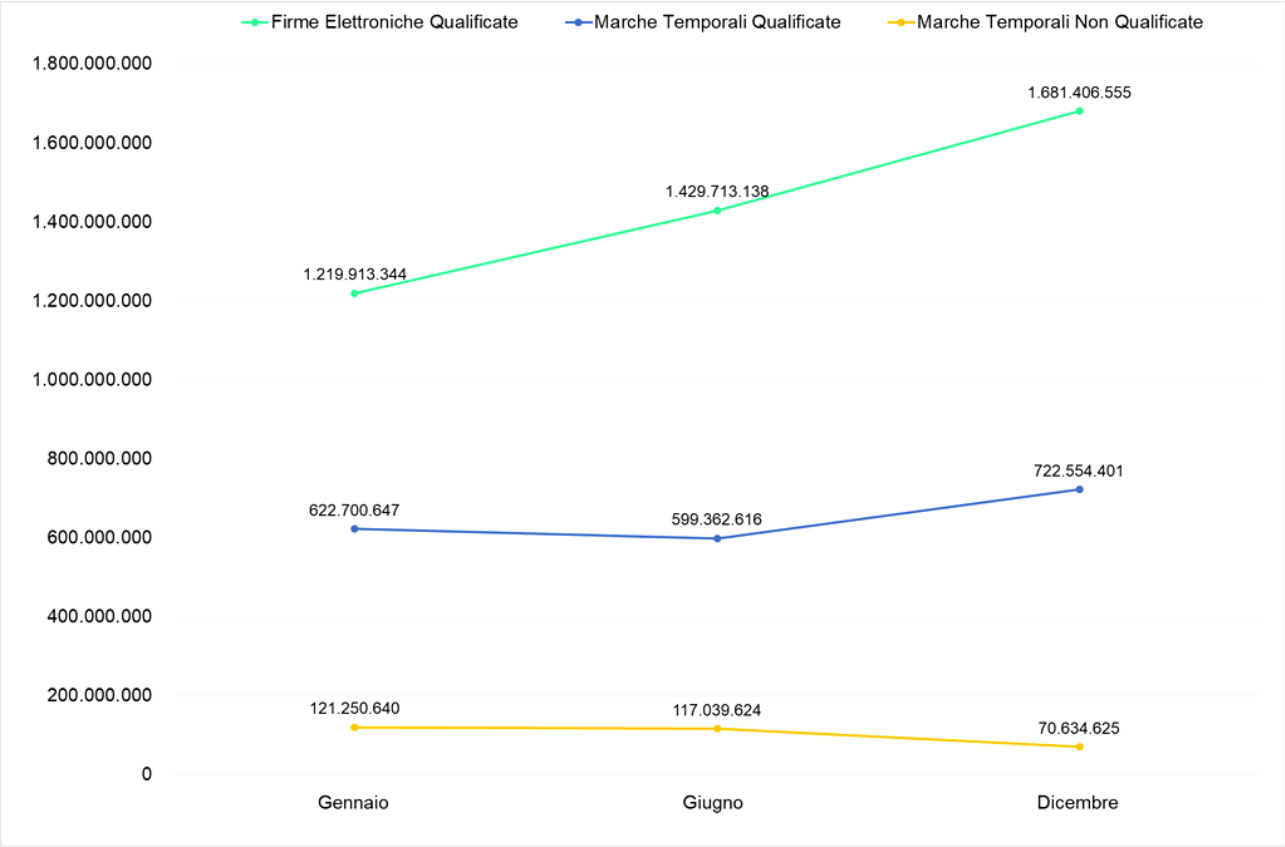

Fig. 3.1 —Andamento servizi di firma e marca temporale [gennaio-dicembre 2019]

È evidente l'incremento crescente per tutto il 2019 delle firme elettroniche qualificate e delle marche temporali qualificate; decrescono le marche non qualificate.

3.3 Gestori PEC

I gestori PEC al 31/12/2019 sono 19.

Con riferimento agli elementi indicati al § 2.2, che concorrono a delineare i profili di rischio, si rilevano per i 19 soggetti iscritti nell'elenco dei gestori PEC i seguenti criteri di classificazione:

- **volumi gestiti**: 1 solo gestore copre il 77% circa dei domini e il 60% delle caselle; 2 gestori insieme coprono l'80% circa delle caselle totali;
- **caratteristiche dell'utenza**: a parte alcuni gestori, per lo più i soggetti pubblici, che gestiscono ciascuno domini e caselle di una clientela predefinita e limitata ad una rete specifica di utenze per una percentuale inferiore all'1%, gli altri soggetti e soprattutto quelli a cui fanno riferimento i volumi più rilevanti, gestiscono domini e caselle sia per clientela business che per persone fisiche (cittadini);
- **soluzioni tecnologiche e partner**: per l'erogazione del servizio, alcuni gestori PEC si appoggiano all'infrastruttura software di altro gestore. Più gestori distribuiscono il servizio attraverso una rete di partner commerciali.

Nei grafici che seguono si riporta un estratto dell'andamento al 31/12/2019 dei volumi di domini, caselle PEC e messaggi scambiati, indicatori che mettono in evidenza l'importanza dei numeri

di questo servizio (totale annuo di 2.378.460.670 messaggi scambiati) e la rilevanza che sempre più assume per lo sviluppo della società digitale:

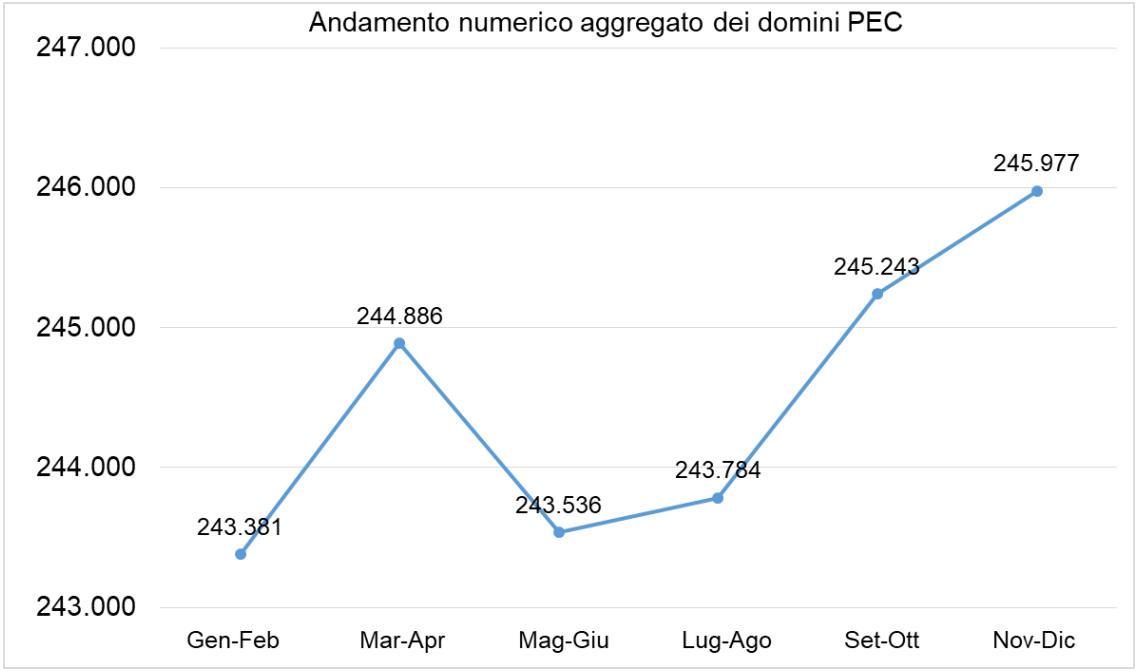

Fig. 3.2 - Andamento domini PEC nel 2019 (dati aggregati per bimestre)

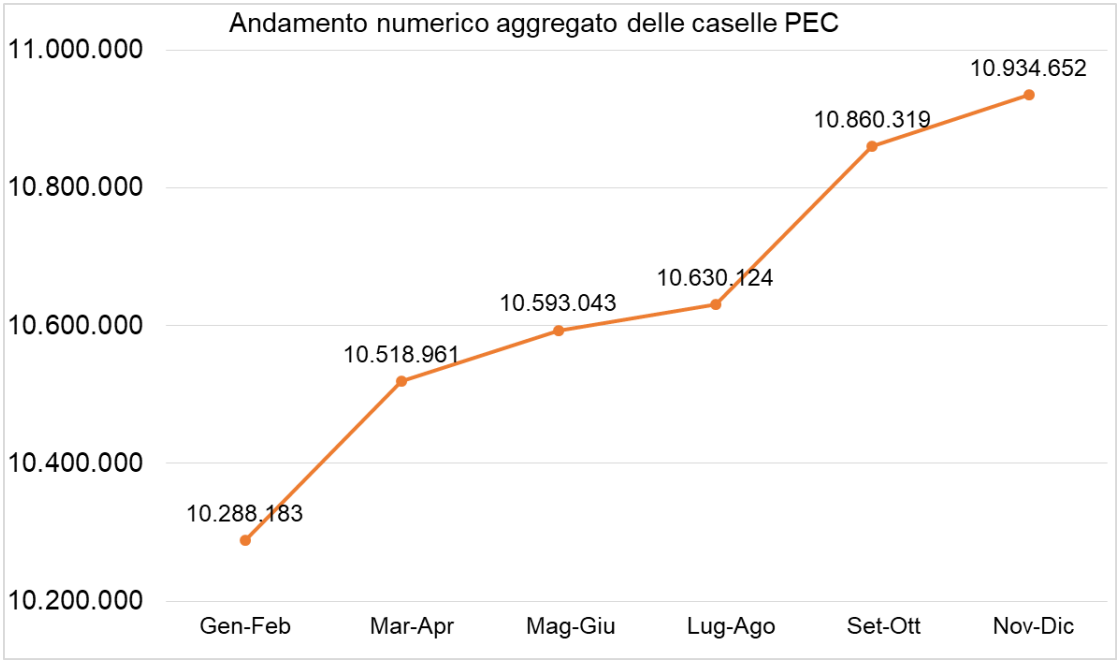

Fig. 3.3 - Andamento caselle PEC nel 2019 (dati aggregati per bimestre)

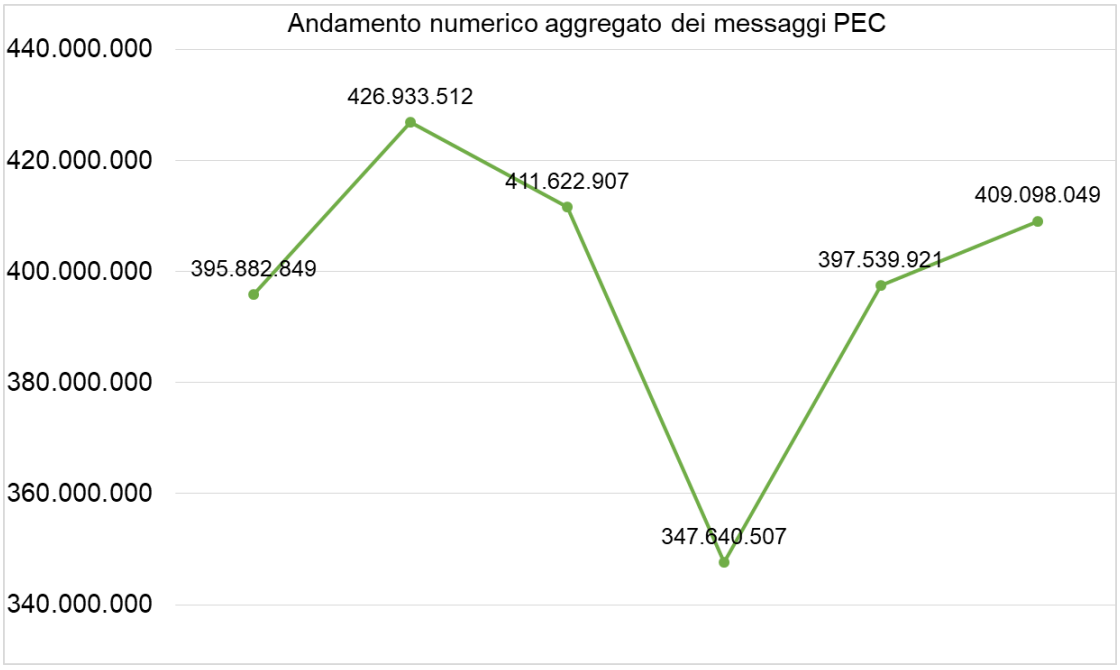

Fig. 3.4 - Andamento messaggi PEC nel 2019 (dati aggregati per bimestre)

3.4 Conservatori

I soggetti iscritti al 31/12/2019 nell'elenco dei conservatori accreditati sono 80.

Il servizio di conservazione può essere erogato dal conservatore accreditato a soggetti privati e a pubbliche amministrazioni, nell'ambito di appositi contratti, che definiscono, tra l'altro, la tipologia di oggetti sottoposti a conservazione. Mentre le pubbliche amministrazioni, qualora non realizzino il servizio di conservazione all'interno della propria organizzazione, sono tenute ad avvalersi di conservatori accreditati, tale obbligo non sussiste per i soggetti privati.

Con riferimento agli elementi indicati al § 2.2, che concorrono a delineare i profili di rischio, si rilevano per i soggetti iscritti nell'elenco dei conservatori accreditati i seguenti criteri di classificazione:

- **volumi gestiti e caratteristiche dell'utenza**: gli indicatori utilizzati per comparare i conservatori accreditati in base ai volumi gestiti ed alle caratteristiche dell'utenza servita sono la numerosità di contratti attivi con pubbliche amministrazioni e/o con soggetti privati e la quantità dei dati conservati, espressa in GB (gigabyte). Con riferimento ai dati 2019, 4 gestori detengono il 77% circa dei contratti attivi con le PA; 4 gestori coprono l'80% dei GB totali conservati;
- **soluzioni tecnologiche e partner**: per l'erogazione del servizio, molti gestori utilizzano l'infrastruttura hardware e/o software fornita da un altro gestore.

Nei grafici che seguono si riporta un estratto dell'andamento dei volumi al 31/12/2019.

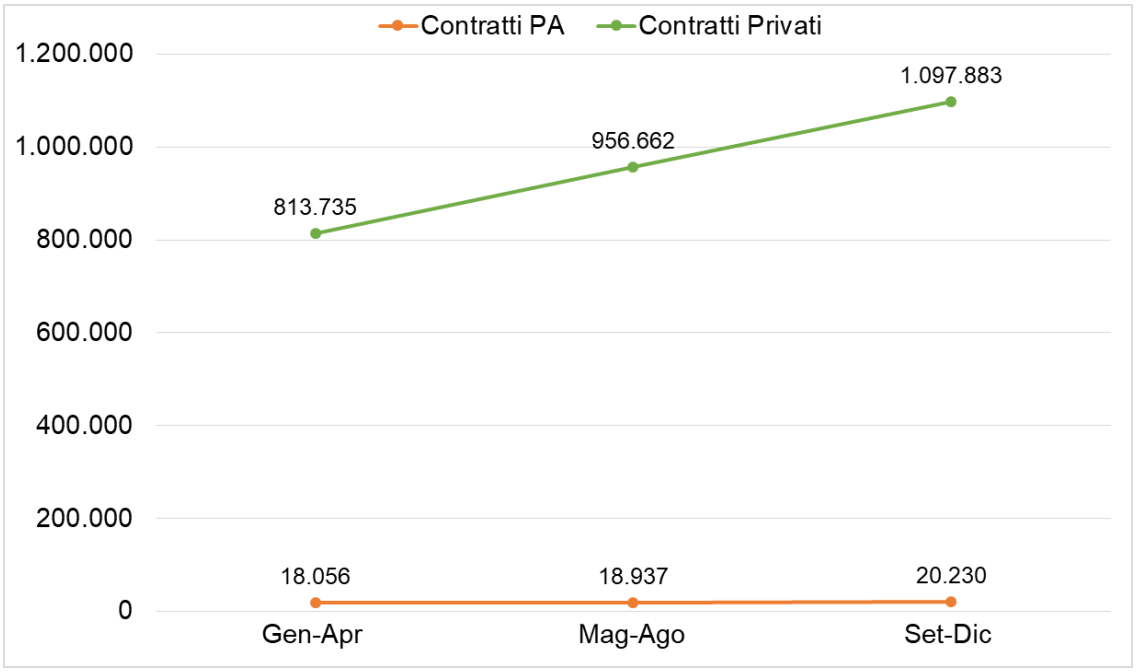

Fig. 3.5 - Andamento contratti 2019 (dati aggregati per quadrimestre)

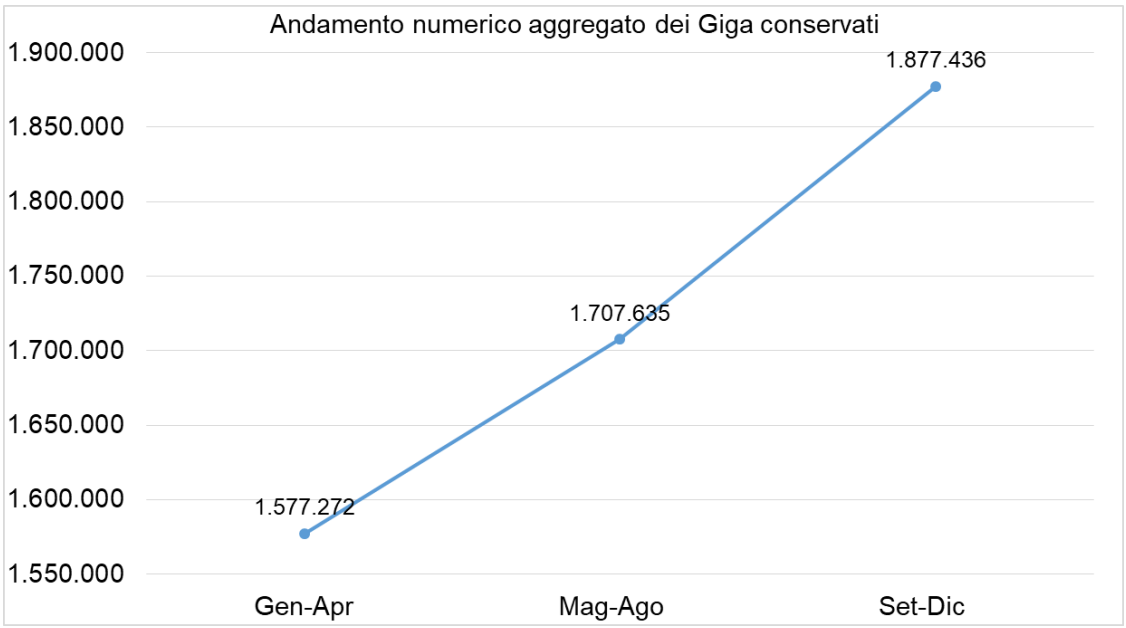

Fig. 3.6 - Volumi (GB) gestiti (dati aggregati per quadrimestre)

3.5 Identity Provider SpID (IdP)

I gestori SpID al 31/12/2019 sono 9, caratterizzati principalmente in base ai volumi gestiti. Su circa 5.500.000 di identità rilasciate al 31/12/2020, 1 IdP ne gestisce circa l'83%.

Ciascun gestore produce periodicamente un insieme di dati di riepilogo sui servizi, che consentono di valorizzare indicatori di tipo quantitativo e qualitativo, con riferimento ad esempio alla gestione delle identità attraverso il *Custome Care*, alle indagini annuali di *Customer Satisfaction*, a ri-

levazioni relative ai servizi a cui le identità hanno fatto accesso con più frequenza, agli incidenti e malfunzionamenti e relative segnalazioni.

Tali dati di riepilogo sono in fase di rivisitazione in vista dell'emanazione di prossime Linee Guida per sistematizzare le modalità di produzione ed invio.

Nel grafico che segue si riporta l'andamento nel 2019 delle identità complessivamente rilasciate dai soggetti vigilati.

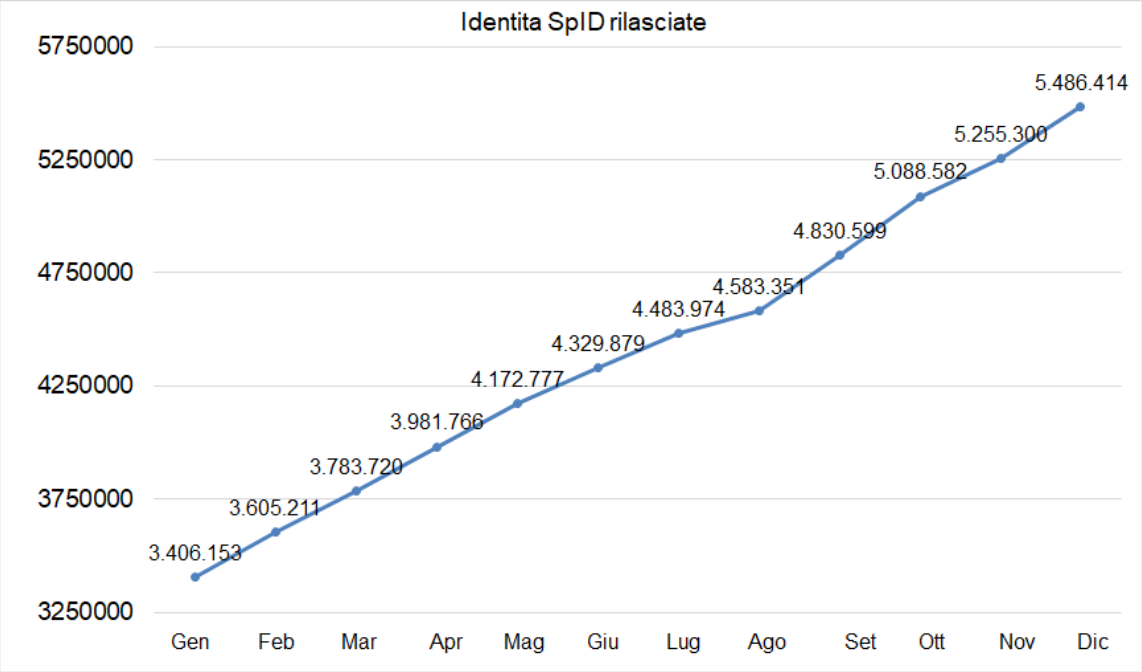

Fig. 3.7- Identità rilasciate nel 2019

Per ulteriori indicatori riferiti al servizio SpID, si può far riferimento all'apposita sezione del portale di avanzamento digitale (https://avanzamentodigitale.italia.it/it/progetto/spid).

4 PROCEDIMENTI DI VERIFICA NEL 2019

Nel 2019 sono state introdotte importanti modifiche nella conduzione delle verifiche. Le attività svolte in sede e presso i gestori hanno visto l'apporto di competenze specialistiche dalle seguenti strutture:

- il *Nucleo di Prevenzione delle Frodi Tecnologiche* della Guardia di Finanza. Ad inizio 2019 è diventato operativo l'accordo stipulato a novembre 2018[14] e le verifiche svolte hanno potuto beneficiare di importanti spunti nelle metodologie di analisi documentale e conduzione delle ispezioni;
- il *Computer Emergency Response Team della Pubblica Amministrazione* (CERT-PA)[15], che ha operato all'interno di AgID per la prevenzione e la risposta agli incidenti informatici nel dominio delle pubbliche amministrazioni. La partecipazione alle verifiche di analisti del CERT-PA ha consentito di approfondire ulteriormente gli aspetti principalmente legati alle misure di sicurezza ed ha fornito ai soggetti vigilati importanti spunti per migliorare le loro capacità di individuare vulnerabilità, prevenire attacchi e proteggere i sistemi.

La pianificazione delle verifiche ha tenuto conto di alcuni eventi che si sono verificati nel corso dell'anno[16] e delle priorità individuate mediante prime valutazioni sui profili di rischio dei soggetti vigilati.

4.1 Riepilogo delle verifiche

Nel corso del 2019, oltre alle verifiche svolte d'ufficio per tutti i soggetti sottoposti a funzioni di vigilanza, sono stati attivati **16 procedimenti di verifica,** dei quali 4 a seguito di segnalazione esterna e 12 nell'ambito di verifiche programmate.

La diminuzione considerevole, di circa il 73%, dei procedimenti attivati rispetto all'anno precedente è da attribuire, oltre alle modifiche nella conduzione delle verifiche che hanno comportato un maggior impegno per la condivisione delle attività preparatorie con strutture specialistiche esterne :

- al superamento dell'esigenza iniziale – determinata nel 2017 e nel 2018 dal nuovo quadro normativo che ha introdotto e successivamente inasprito le sanzioni[17] - di raggiungere con le

[14] https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2019/03/06/agid-guardia-finanza-danno-il-ad-azioni-congiunte-rafforzare-fiducia-nelleconomia

[15] Il CERT-PA, attivo dal mese di marzo 2014 fino al 6 maggio 2020, ha operato all'interno di AgID con il compito di supportare le pubbliche amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica. Dal 7 maggio 2020, a seguito dell'entrata in vigore delle "Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team – CSIRT italiano" (DPCM 8 agosto 2019), le attività di supporto sono svolte dal CERT-AgID (https://cert-agid.gov.it) che ha sostituito il CERT-PA.

[16] Attacchi informatici e campagne di diffusione di malware attraverso la posta elettronica certificata, che hanno avuto ampia eco sui mezzi di comunicazione di massa

[17] Le modifiche al CAD entrate in vigore il 14/9/2016 hanno introdotto sanzioni per violazioni degli obblighi del CAD e del Regolamento eIDAS per importi da un minimo di 4.000,00 a un massimo di euro 40.000,00; dal 26/1/2018 sono

verifiche sul campo il maggior numero di soggetti vigilati, sia a scopo conoscitivo, sia per stimolare azioni correttive nelle componenti che nel corso degli anni si sono rivelate tra le più critiche, sia per sollecitare le rendicontazioni e le notifiche dovute ex lege[18], sulla base delle quali avviare la costruzione dei profili di rischio;

- alla concomitante predisposizione di strumenti ad uso di AgiD, per migliorare l'azione di intervento preventivo (cfr. § 7), e ad uso sia di AgID che dei soggetti vigilati, per sistematizzare ed automatizzare la raccolta dei dati strutturati;
- alla specializzazione ed al protrarsi delle verifiche su specifiche componenti dei servizi, a seguito del verificarsi di particolari eventi (attacchi informatici e campagne di diffusione di malware attraverso la PEC).

Come si rileva dal grafico che segue, i 16 procedimenti hanno riguardato le quattro tipologie di soggetti vigilati: i QTSP (2), i gestori PEC (5), i Conservatori (6), i gestori SpID (3); da notare che in alcuni casi i gestori sottoposti a verifica erogano servizi ad una utenza estremamente ampia.

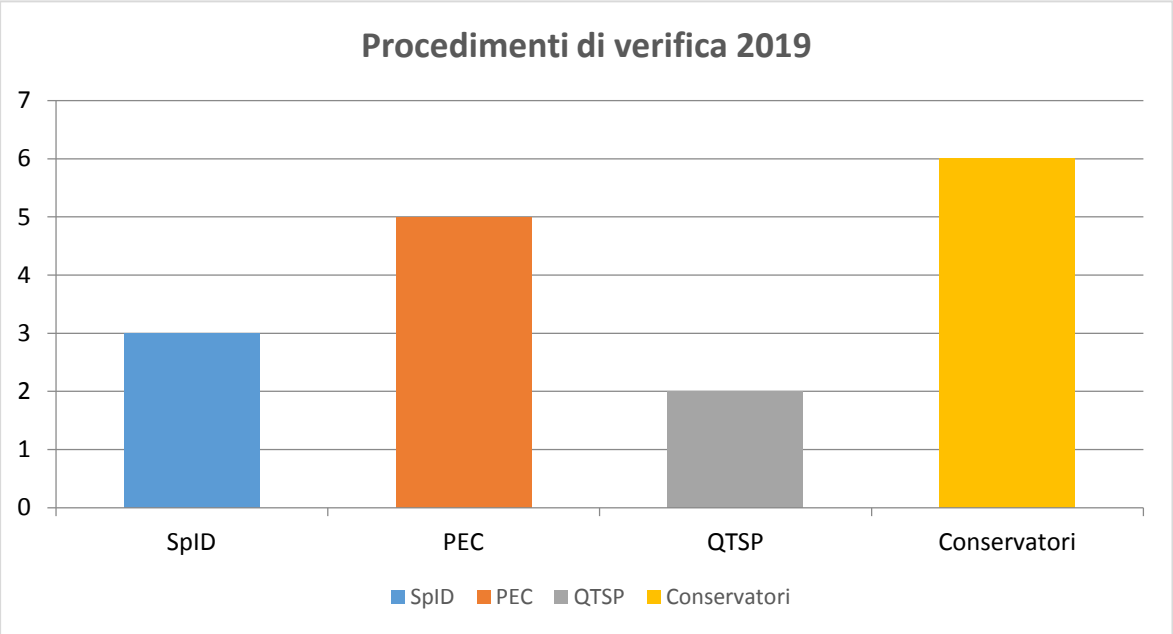

Fig. 4.1 – Procedimenti di verifica nel 2019 per elenco

Per i 2 procedimenti in ambito QTSP:

- 1 procedimento attivato su segnalazione; 1 procedimento attivato da programmazione
- i 2 QTSP, con riferimento ai volumi, coprono il 50% circa dei certificati qualificati per firma con SC/Token, il 50% circa delle firme elettroniche qualificate ed il 28% circa delle marche temporali qualificate;

entrate in vigore ulteriori modifiche al CAD che hanno incrementato tali importi, prevedendo valori da un minimo di 40.000,00 ad un massimodi 400.000,00 Euro. Per approfondimenti si rimanda al § 11.

[18] Dati periodici di riepilogo sui servizi erogati; segnalazioni di incidenti di sicurezza, malfunzionamenti o interruzioni di servizio.

- con riferimento alle caratteristiche dell'utenza, 1 QTSP rilascia firme solo ad una clientela predefinita e limitata ad una rete specifica di utenza; l'altro rilascia firme, sigilli, certificati e marche temporali sia a clientela *business* che a persone fisiche.

Per i 5 procedimenti in ambito PEC:

- 3 procedimenti attivati su segnalazione; 2 procedimenti attivati da programmazione; 2 procedimenti hanno riguardato uno stesso gestore;
- i 5 gestori PEC, con riferimento ai volumi, coprono l'82% dei domini e l'89% delle caselle PEC complessivamente gestiti al 31/12/2019.

Per i 6 procedimenti in ambito Conservazione:

- 6 procedimenti attivati da programmazione (soggetti con profilo di rischio alto).

Per i 3 procedimenti in ambito SpID:

- 3 procedimenti attivati da programmazione
- I 3 IdP, con riferimento ai volumi, si collocano nella fascia più bassa e coprono poco più del 3% delle identità complessivamente gestite al 31/12/2019. In questo caso nella programmazione delle verifiche, ai fini della determinazione del profilo di rischio, si è dato un maggior peso agli indicatori relativi alle ultime verifiche svolte ed alle segnalazioni di incidenti, malfunzionamenti e interruzioni di servizio, selezionando di conseguenza gli operatori non ancora visitati o non visitati nell'anno precedente, o per i quali non risultavano pervenute segnalazioni nemmeno per attività di manutenzione programmata.

Le verifiche complessivamente svolte per le quattro tipologie di soggetti vigilati hanno portato:

- in 2 casi alla cessazione dell'attività per scelta del gestore, comunicata in sede di ispezione;
- in 5 casi all'attivazione della fase sanzionatoria.

4.2 Verifiche di *seconda parte* e componenti di servizio

Diversamente dalle verifiche di "terza parte" svolte dagli organismi di certificazione accreditati dall'ente nazionale di accreditamento[19], finalizzate a certificare la conformità di un sistema di gestione ad una norma o ad uno standard internazionale[20], le verifiche svolte da AgID ai fini della vigilanza si configurano come verifiche di "seconda parte"[21], sono in genere diverse l'una dall'altra e limitate ad aspetti specifici ("componenti del servizio"), in relazione agli obiettivi di ciascuna verifi-

[19] In Italia, Accredia.

[20] Es. ISO 27001 o ISO 9001.

[21] Le verifiche di "seconda parte" sono condotte da chi ha un intersse primario nella coretta erogazione dei servizi, in tal caso AgID, che opera comunque nell'interesse di tutti gli stakeholder.

ca (verifica conseguente ad una segnalazione, o disposta a fronte di un evento negativo come per esempio un attacco informatico, o da programmazione).

Al fine di rendere comparabili i risultati ed in considerazione del fatto le quattro tipologie di servizi, pur nelle diverse modalità realizzative, includono componenti analoghe, si è adottata una classificazione che prevede una nomenclatura standard per quelle comuni alle quattro tipologie di servizi vigilati. A titolo di esempio, sono comuni a tutti i servizi le seguenti componenti:

a) Organizzazione
b) Documentazione di riscontro
c) Politiche, procedure e misure di sicurezza
d) Infrastruttura per l'erogazione del servizio
e) Gestione del processo
f) Analisi dei rischi e VA/PT(Vulnerability Assessment e Penetration Test)
g) Gestione delle terze parti
h) Gestione e segnalazione di incidenti, malfunzionamenti e interruzioni di servizio
i) Piano di cessazione
j) Report periodici

A titolo di esempio:

- la componente "Organizzazione", fa riferimento all'insieme dei requisiti di ciascun servizio (QTS, PEC, Conservazione ,SpID), inerenti l'organizzazione, le procedure e il personale);
- la componente "Documentazione di riscontro", riguarda la documentazione (Manuale operativo, Piano di sicurezza, o equivalenti) prevista ai fini della qualificazione o dell'accreditamento;
- la componente "Gestione del processo" rigurda l'insieme delle attività che attengono al processo specifico (QTS, PEC, Conservazione, SpID) in tutto il ciclo di vita del servizio (dall'avvio, alla cessazione).

Le verifiche condotte nell'ambito dei 16 procedimenti hanno preso in esame alcune componenti, non necessariamente le stesse per i quattro elenchi, essendo selezionate in fase di pianificazione in relazione agli obiettivi di ciascuna verifica, come sopra indicato. Alle componenti esaminate si riferiscono i rilievi indicati nel paragrafo che segue.

4.3 Riepilogo dei rilievi

Complessivamente sono stati formulati **109 rilievi**, distinti in 80 "Non Conformità" e 29 "Osservazioni", che per il 12% circa hanno riguardato i QTSP, il 31% i gestori PEC, il 34% i Conservatori, e il 23% i gestori SpID.

Tali dati si riferiscono alla quasi totalità dei procedimenti sopra indicati, con esclusione di due procedimenti peri quali il gestore ha comunicato la cessazione, nell'ambito dei quali non sono stati quindi formulati rilievi.

Servizi / Rilievi	QTS	PEC	Conservazione	SPID
Gravi	2	8	1	0
Medie	5	12	11	8
Lievi	3	5	15	10
Osservazioni	3	9	10	7

Tab.4.1 - Distribuzione dei rilievi per servizio

Dai dati sopra indicati e in relazione ai procedimenti di verifica eseguiti nel 2019 si ottiene una indicazione di risultato medio per gestore/servizio[22], come mostra il seguente grafico. Complessivamente, un procedimento di verifica ha portato in media alla formulazione di 7-8 rilievi.

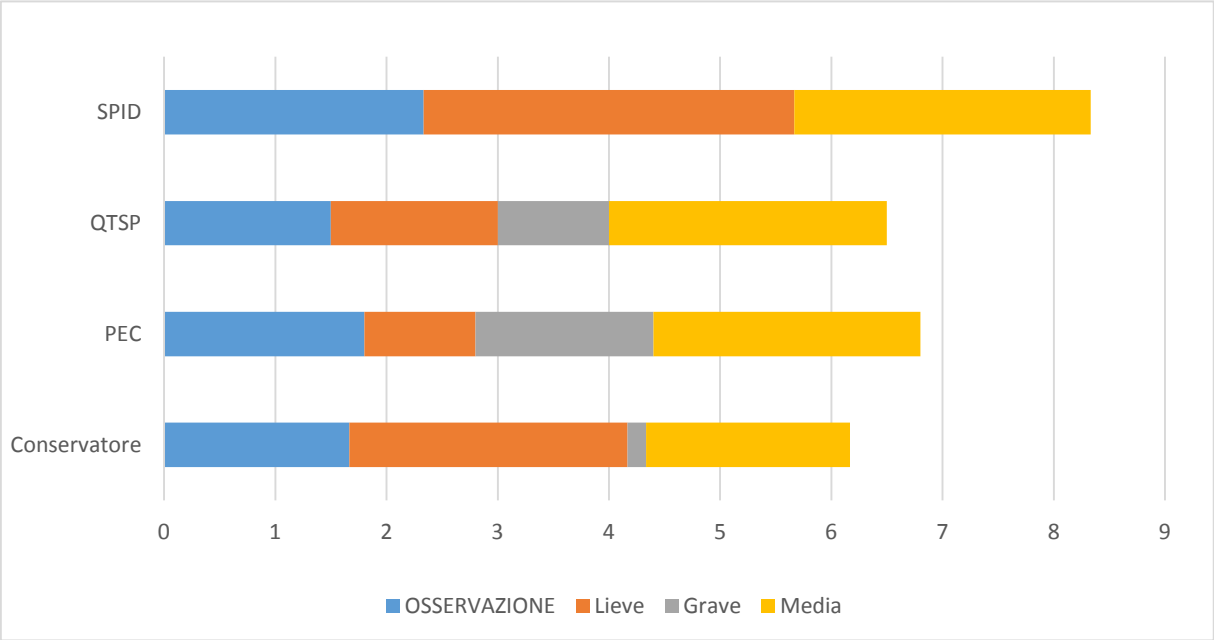

Fig. 4.2- Media rilievi gestori per servizio

Dal grafico che segue si rileva la distribuzione in percentuale dei rilievi per servizio. Il 30% dei rilievi è costituito da Osservazioni, che consistono in raccomandazioni o spunti di miglioramento.

[22] Un gestore qualificato per più servizi (ad es, PEC e QTSP) è contato come se si trattasse di due gestori distinti

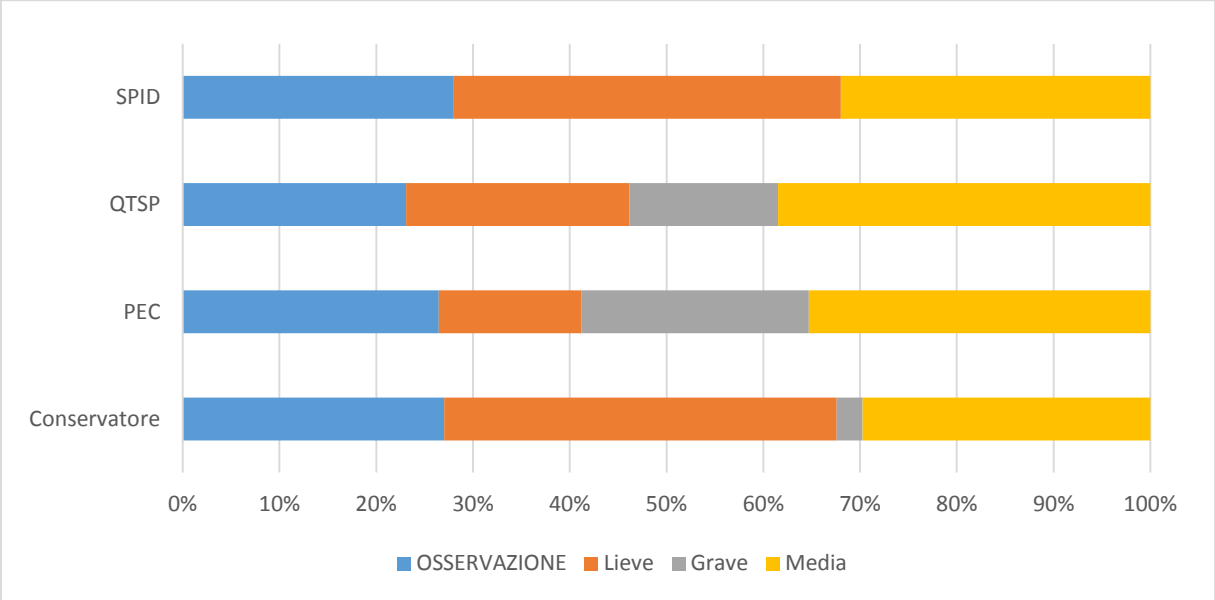

Fig. 4.3 - Distribuzione percentuale dei rilievi per servizio

I rilievi sono stati formulati rispetto alle componenti di servizio esaminate nell'ambito dei procedimenti.

La tabella ed il grafico che seguono mostrano la distribuzione dei rilievi per servizio e per le specifiche componenti del servizio a cui sono riferiti.

Servizio / Componenti	QTS	PEC	Conservazione	SPID	Totale
Politiche e procedure di sicurezza	1	11	12	1	25
Gestione Caselle PEC	n.a	4	n.a[23]	n.a	4
Gestione terze parti	2	5	5	3	15
Gestione del processo	4	2	-	6	12
Organizzazione	-	4	5	3	12
Gestione degli incidenti	1	2	3	3	9
VA/PT	1	-	2	3	6
Analisi dei rischi	2	1	2	-	5
Documentazione di riscontro	-	2	1	2	5
Piano di cessazione	1	-	2	1	4
Gestione delle comunicazioni	-	1	2	-	3
Report periodici	-	-	2	1	3
Formazione	-	1	-	2	3
Infrastruttura per l'erogazione del servizio	1	-	1	-	2
Trattamento dei dati personali	-	1	-	-	1
Totale complessivo	**13**	**34**	**37**	**25**	**109**
Media per procedimento/servizio	6,5	6,8	6,17	8,3	

Tab.4.2 - Distribuzione dei rilievi per servizio

[23] Componente non applicabile alla tipologia di servizio.

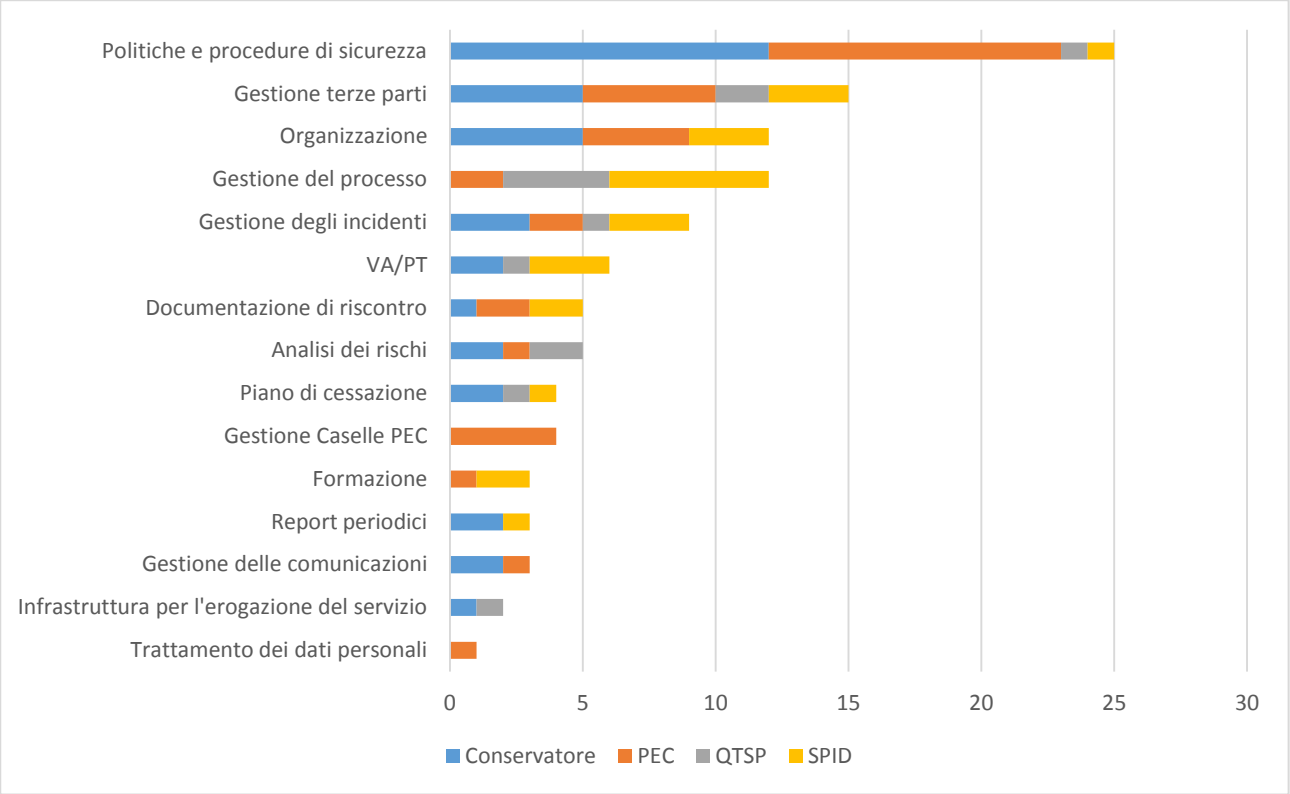

Fig.4.4 – Distribuzione dei rilievi per servizio e componenti di servizio

Si può osservare che ad esempio, nel caso del servizio PEC, il 30% circa dei rilievi ha riguardato la componente "Politiche e procedure di sicurezza", che, con riferimento alle sole componenti di servizio esaminate, è risultata quella maggiormente affetta da rilievi anche nel caso del servizio di Conservazione.

In Fig.4.5 sono evidenziate le sette componenti per le quali, in relazione alle componenti esaminate, è risultato più frequente rilevare una Non Conformità o una Osservazione.

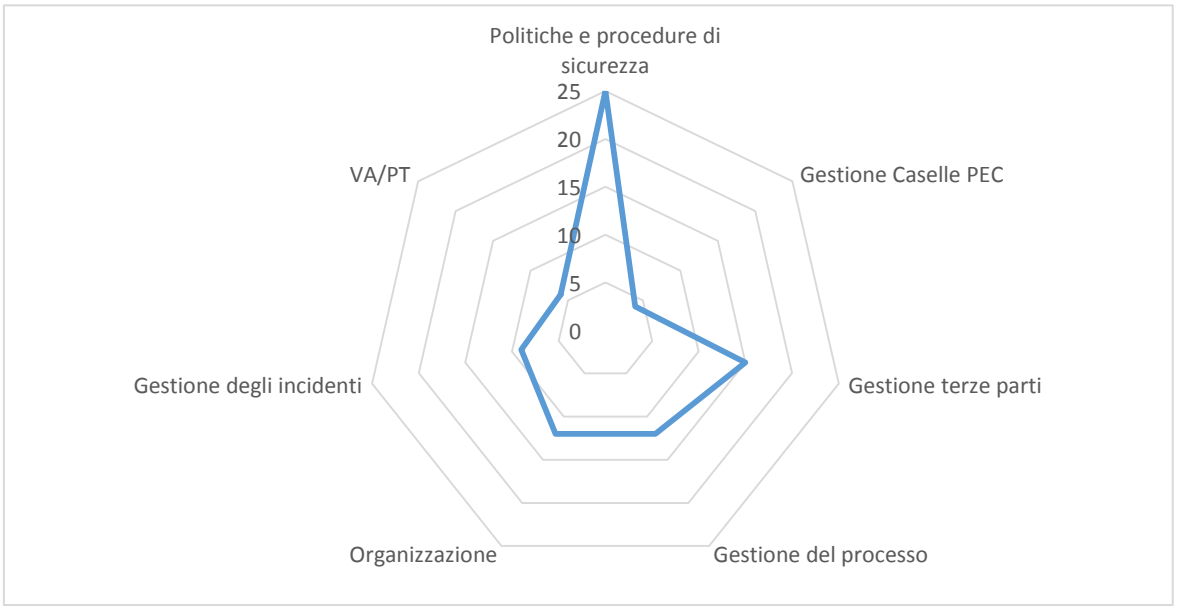

Fig. 4.5 – Top 7 componenti di servizio affette da rilievi

Tutti i rilievi devono essere indirizzati dal gestore in un Piano di azioni, da attuare entro tempi massimi stabiliti nel caso di Non Conformità, o entro tempi massimi indicati dallo stesso gestore, nel caso di Osservazioni. Il piano definito dal gestore è oggetto di successivo monitoraggio, sia ai fini della conclusione del procedimento, sia nell'ambito di nuove verifiche d'ufficio nel caso in cui gli interventi da attuare, per particolare complessità, non possono essere completati in tempi contenuti.

La figura che segue mette in confronto i tempi minimi, medi e massimi di risoluzione in giorni (gg) rilevati per le tre tipologie di Non Conformità.

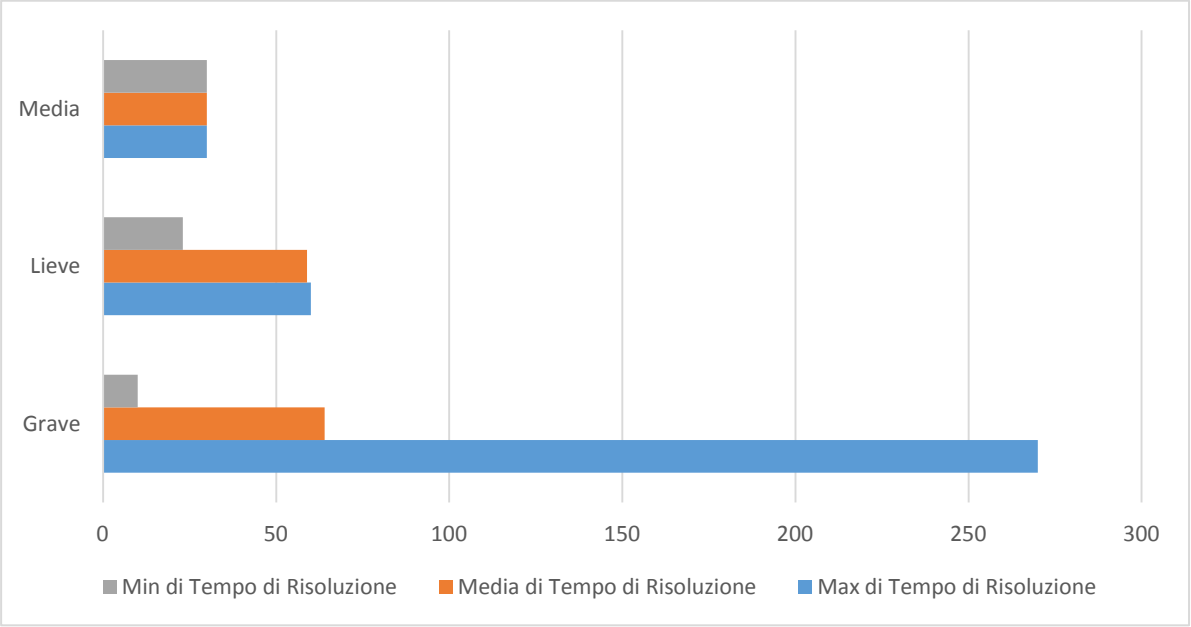

Fig. 4.6 – Tempi di risoluzione (gg) per le Non Conformità

Al fine di comparare i diversi gestori secondo un profilo di qualità, nella figura che segue viene riportato a titolo di esempio, il grafo di confronto di tre Conservatori, eseguito rispetto ai rilievi formulati sulle diverse componenti di servizio nell'ambito dei rispettivi procedimenti.

Nel caso specifico, per rendere confrontabile la classificazione, ad ogni Osservazione e ad ogni Non Conformità è stato attribuito un peso crescente (Osservazione 0,5; NC Lieve 1; NC Media 1,5; NC Grave 2) ed è stato sommato il peso dei rilievi della stessa componente.

L'area racchiusa dalla spezzata determina una visione dello scostamento dal punto ottimo (assenza di rilievi).

É bene sottolineare che l'assenza di punteggio per una componente non equivale ad assenza di rilievi: la componente potrebbe non essere stata oggetto di verifica.

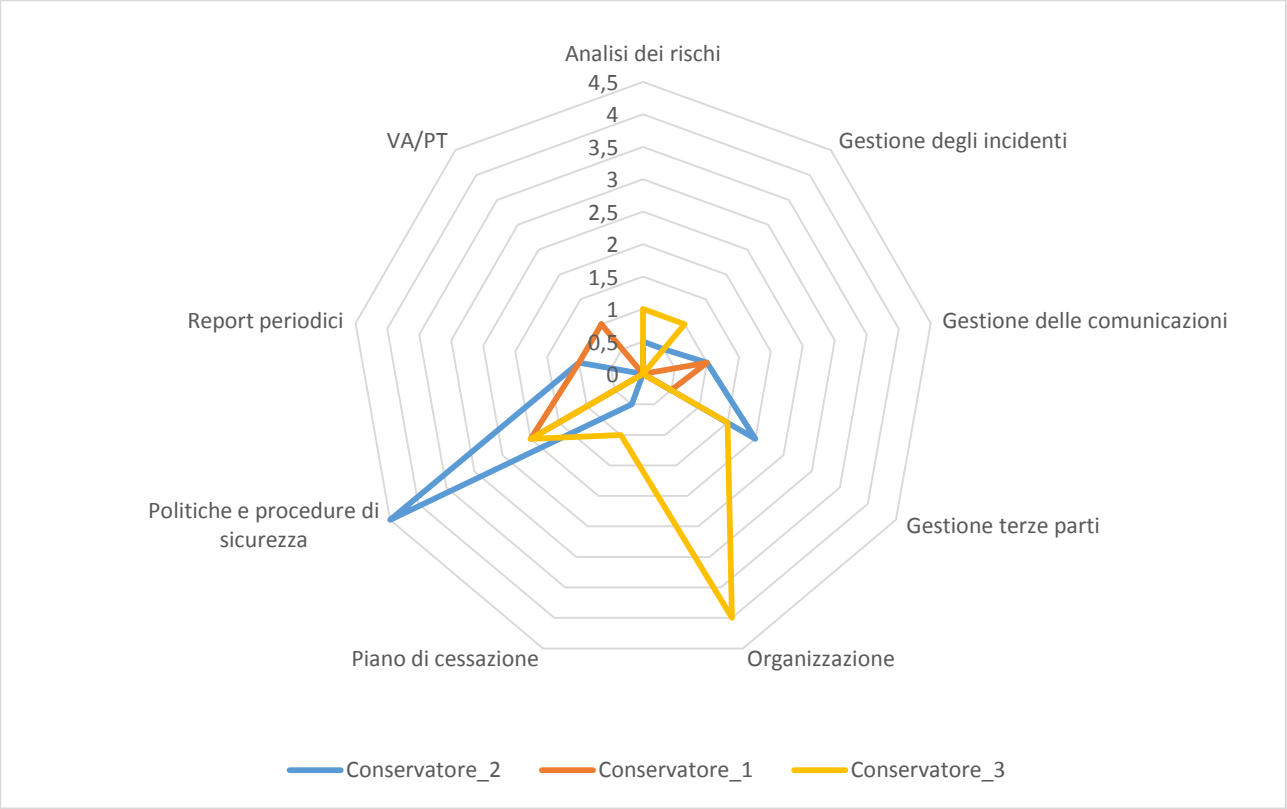

Fig.4.7 – Confronto tra 3 Conservatori per profilo di qualità(in base ai rilievi)

Le stesse note di lettura si applicano per le due figure che seguono.

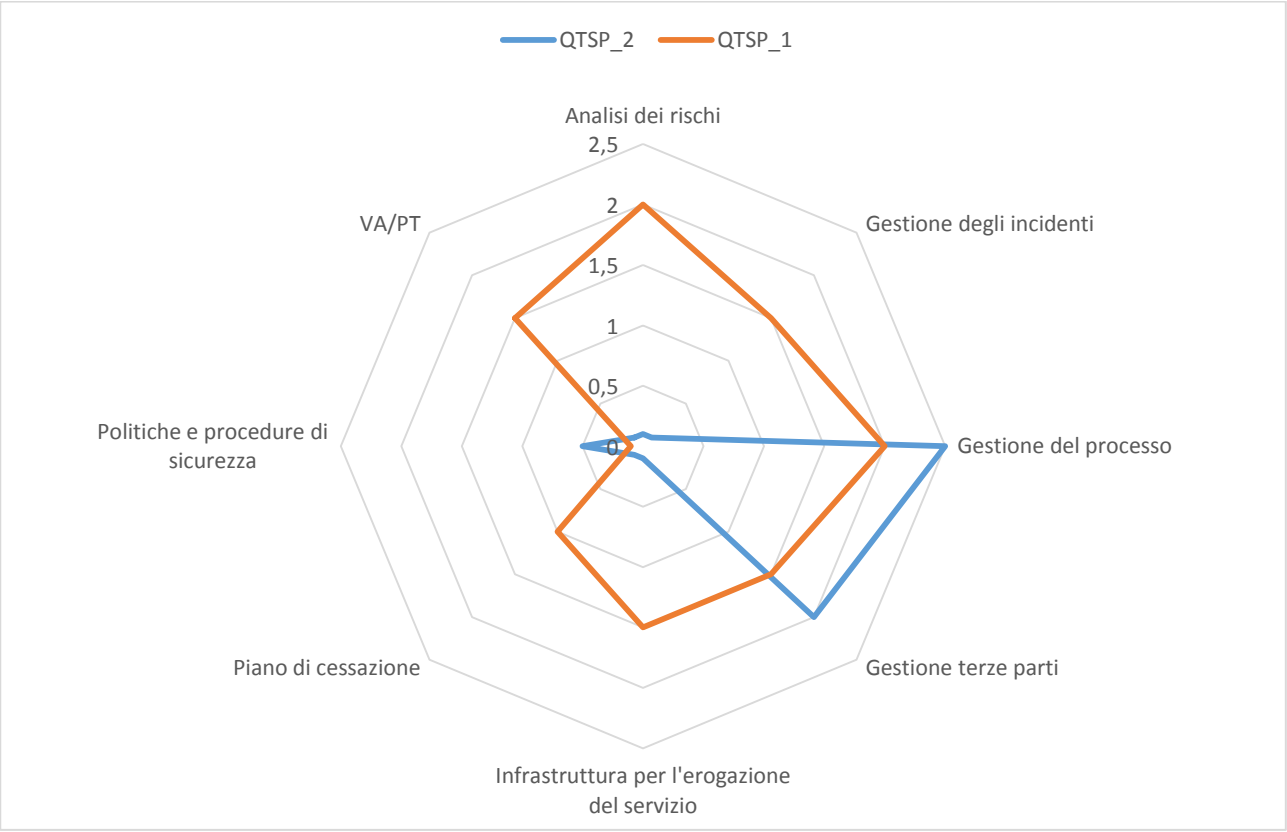

Fig. 4.8 – Confronto tra 2 QTSP per profilo di qualità(in base ai rilievi)

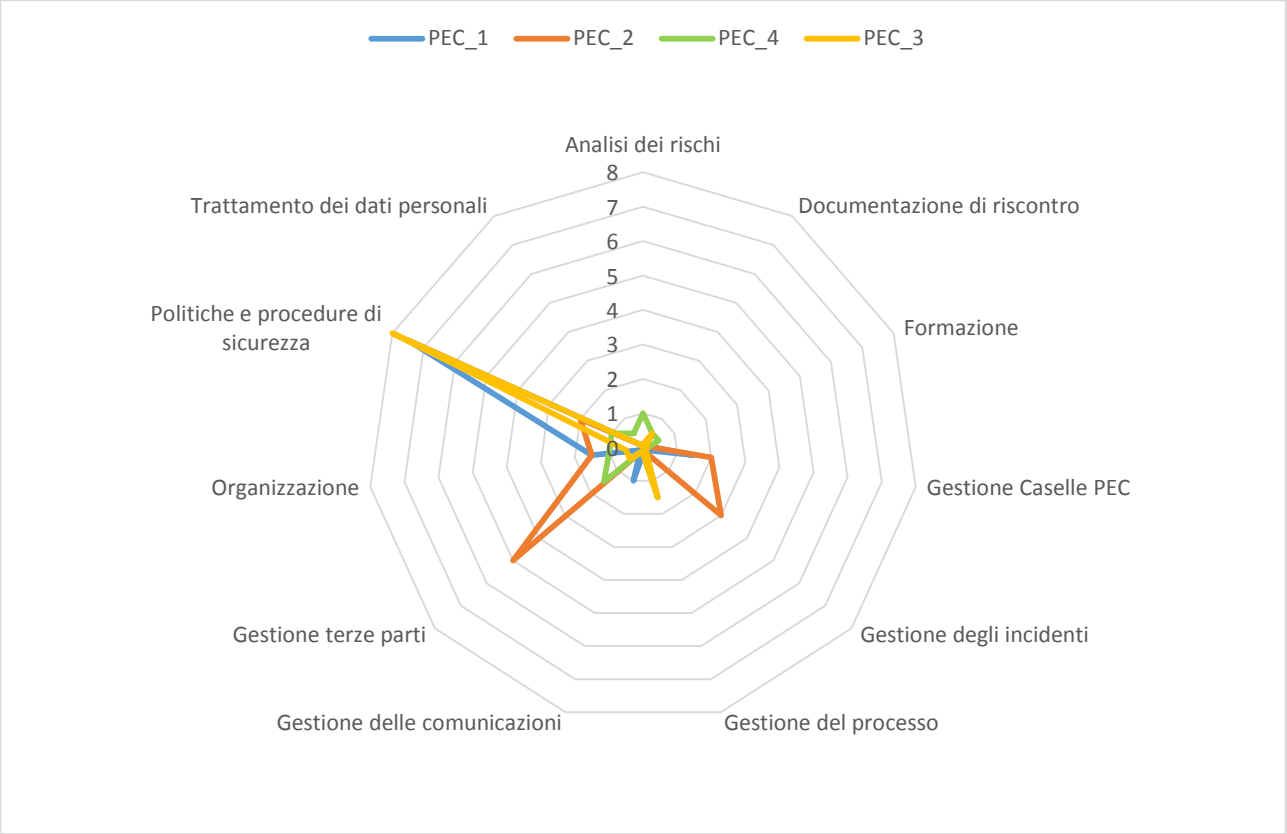

Fig. 4.9 – Confronto tra 4 Gestori PEC per profilo di qualità (sulla base dei rilievi)

5 SEGNALAZIONI DI INCIDENTI E MALFUNZIONAMENTI DA PARTE DEI SOGGETTI VIGILATI

I soggetti vigilati sono tenuti a segnalare ad AgID e, quando ne ricorrano le circostanze[24] alle altre autorità preposte, gli incidenti di sicurezza o gli eventi che si configurino come malfunzionamenti o interruzioni di servizio.

Nel corso del 2019 sono stati notificati complessivamente 49 incidenti e/o malfunzionamenti, che hanno interessato le quattro tipologie di servizi.

La figura che segue mostra il totale degli eventi di cui è stata data notifica nel corso delle settimane dell'anno.

Sono evidenti quattro picchi: uno con sei eventi nella settimana 23° (3-10/06/2019) e tre picchi con quattro eventi nella 5° (28/01-3/02/2019), 7° (18-25/02/2019) e 29° (22-29/07/2019) settimana.

Fig. 5.1 –Incidenti e malfunzionamenti segnalati nel corso del 2019

Un evento in particolare (settimana 23) ha interessato l'infrastruttura di un gestore che opera nell'ambito dei quattro elenchi e che è utilizzata anche da un altro gestore per due servizi; pertanto, a fronte di un doppia segnalazione prodotta dai due gestori e sebbene la causa sia la stessa, l'evento è stato considerato sei volte, poiché ha avuto impatto su diverse tipologie di servizi/utenti, comportando pertanto anche un maggior livello di rischio.

[24] Per esempio nel caso di violazioni di dati personali, i gestori sono tenuti ad effettuare le notifiche al Garante per la protezione dei dati personali.

Nella figura che segue, con riferimento agli eventi del 2019, è stata eseguita una valutazione del tasso di rientro in termini statistici. Viene mostrata la percentuale di eventi rientrati rispetto al tempo trascorso dall'inizio del disservizio. In particolare sono evidenziati 5 punti di riferimento indicati con le etichette da 1 a 5. Ad esempio il punto con etichetta 2 mostra che quasi l'80% degli eventi è stato risolto in meno di 5 ore e mezzo. L'etichetta 4 mostra che nel 95% dei casi l'evento è stato risolto entro le 24 ore.

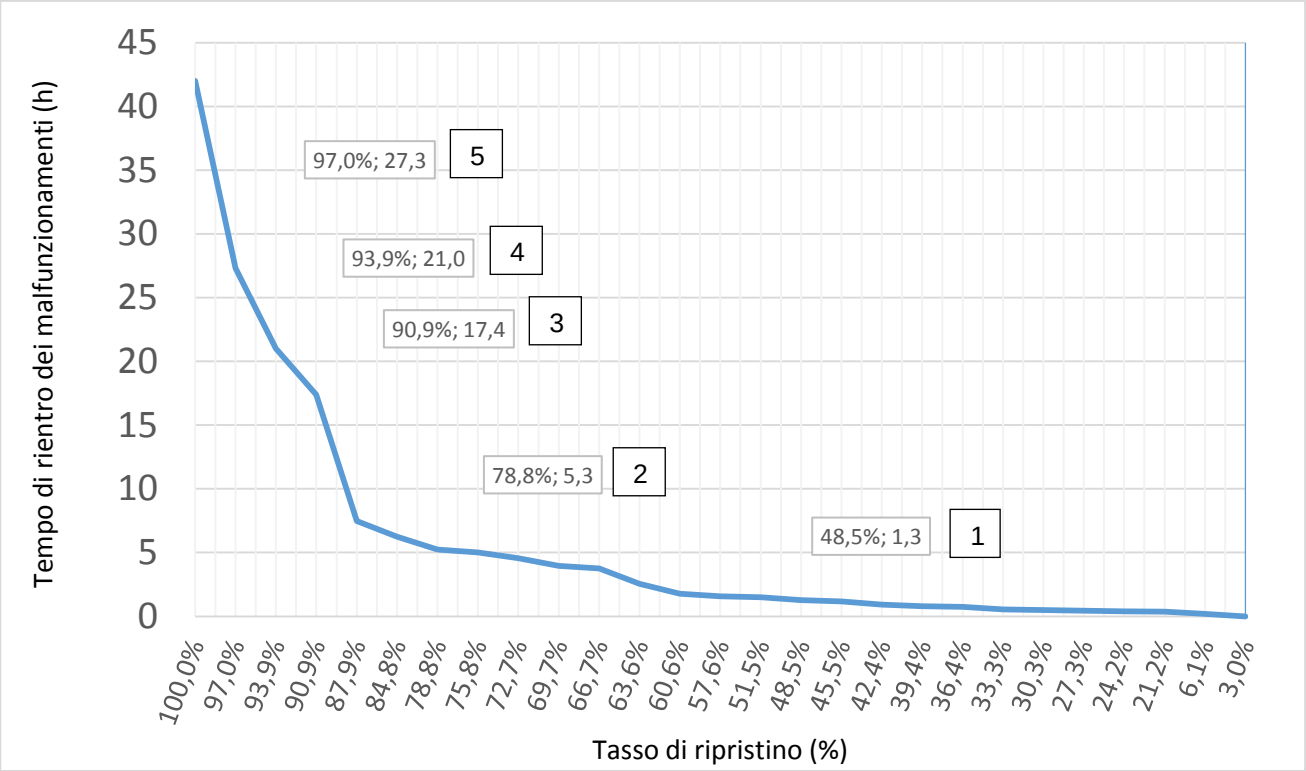

Fig. 5.3 – Distribuzione degli eventi 2019 rispetto alla durata (ore)

Nella tabella che segue sono mostrate le percentuali - per servizio e totali - di quanti gestori hanno effettuato segnalazioni di incidenti, malfunzionamenti o interruzioni di servizio. Nel computo non sono considerati i gestori accreditati o qualificati nel 2019, né quelli che hanno cessato l'attività nel 2019.

Segnalazioni (#)	QTS		PEC		Conservazione		SpID		Totale complessivo	
0	10	55,56%	13	68,42%	64	88,89%	5	50,00%	92	77,31%
1	6	33,33%	3	15,79%	7	9,72%	-	0,00%	16	13,45%
2	-	0,00%	2	10,53%	1	1,39%	3	30,00%	6	5,04%
3	-	0,00%	1	5,26%	-	0,00%	-	0,00%	1	0,84%
4	-	0,00%	-	0,00%	-	0,00%	2	20,00%	2	1,68%
5	2	11,11%	-	0,00%	-	0,00%	-	0,00%	2	1,68%
Totale	**18**	100,00%	**19**	100,00%	**72**	100,00%	**10**	100,00%	**119**	**100,00%**

Tab. 5.1 – Segnalazioni per servizio

Come si può notare prendendo come riferimento l'ultima colonna, il 77% dei gestori non ha mai effettuato una segnalazione. Il 13% ha segnalato un solo evento, il 5% ne ha segnalati due, e via di seguito.

Le segnalazioni pervenute o l'assenza di segnalazioni concorrono alla definizione del profilo di rischio, sulla base del quale sono programmate le verifiche periodiche.

6 SEGNALAZIONI DAGLI UTENTI

Il Regolamento di vigilanza prevede che gli utenti o i soggetti interessati possono segnalare ad AgID presunte violazioni normative o irregolarità da parte dei gestori. Le segnalazioni, a pena di irricevibilità, devono essere trasmesse esclusivamente con le modalità indicate nel Regolamento[25].

La nota di segnalazione, a pena di inammissibilità, deve indicare almeno:

a. i recapiti completi del soggetto che effettua la segnalazione;

b. la descrizione della presunta violazione o irregolarità, il gestore coinvolto, i fatti e le circostanze all'origine della segnalazione, il periodo al quale la presunta violazione o irregolarità sarebbe riferita;

c. la documentazione, se disponibile, a sostegno della presunzione di violazione normativa o irregolarità.

Le segnalazioni che non siano archiviate per irricevibilità o per inammissibilità possono comportare l'avvio di un procedimento di verifica.

Nel 2019 le segnalazioni gestite dal Servizio Vigilanza sono state 20, delle quali 4 hanno dato luogo all'avvio di procedimenti di verifica (più segnalazioni facevano riferimento ad uno stesso evento); le altre sono state risolte attraverso interlocuzioni con l'utente o con il gestore.

La tabella che segue mostra la distribuzione delle segnalazioni per servizio.

QTS	PEC	Conservazione	SpID	Totale
3	12	3	2	20

Tab. 6.1 - Segnalazioni utente per servizio

Le segnalazioni pervenute per ciascun servizio (QTS, PEC, Conservazione, SpID) fanno riferimento a diverse componenti, come si rileva dalla tabella che segue.

[25] Il Regolamento prevede che le segnalazioni vanno presentate ai sensi dell'art. 65 del CAD - "Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica".

Servizio Componenti:	QTS	PEC	Conservazione	SPID	Totale
Politiche e procedure di sicurezza	1	6[26]	2		9
Gestione terze parti	1	4			5
Gestione del processo		2	1[27]	2[28]	5
Commercializzazione	1				1
Totale per servizio	**3**	**12**	**3**	**2**	**20**

Tab.6.2 – Segnalazioni per componenti di servizio

[26] 4 delle 6 segnalazioni sono relative a campagne di diffusione malware.

[27] Processo di conservazione.

[28] Processo per il rilascio e la gestione dell'identità digitale.

7 L'ANALISI PREDITTIVA

Come indicato al capitolo 2, la programmazione delle verifiche si basa su profili di rischio, aggiornati periodicamente,che tengono conto della combinazione di un iniseme di indicatori, quali ad esempio le verifiche precedenti ed i relativi esiti, le dimensioni del gestore (ad esempio il capitale sociale e il numero dei dipendenti), le caratteristiche dell'utenza (customer base), i dati periodici trasmessi, le segnalazioni degli incidenti o delle interruzioni di servizio, le soluzioni tecnologiche adottate, la numerosità dei subcontraenti o dei partner commerciali e tecnologici.

Queste ed altre infomazioni vengono fornite dai gestori stessi, raccolte e strutturate in un sistema che, attraverso correlazioni, consente di delineare un profilo di rischio per il singolo gestore e tra gestori dello stesso servizio. Questa analisi nel corso del 2019 è stata progressivamente implementata in un sistema semi automatico in fase di caratterizzazione e consolidamento nei primi mesi del 2020.

A questo sistema, che si poggia su un'infrastruttura di raccolta dati statistici strutturati ed analisi di andamenti periodici, è stato affiancato in via sperimentale un sistema, sviluppato parallelamente nel corso dell'anno, per l'analisi del sentiment[29] in rete. Con questa piattaforma è possibile monitorare, tramite connettori in vari punti della rete Internet, quanto accade e viene scritto in siti web, canali social, blog, ecc. L'enorme quantità di *feed*[30] che si possono ottenere sulle quattro tipologie di servizi vigilati, viene filtrata tramite l'uso di *keyword* ed associazioni tra le stesse, in modo da rilevare gli elementi realmente di interesse, istruendo il sistema e filtrando per quanto possibile i falsi positivi o i falsi negativi. L'obiettivo a cui tendere è disporre di elementi che consentano di migliorare la capacità di individuazione di potenziali problemi in via preventiva, attivando verifiche prima che tali problemi diano luogo adeventi negativi; l'obiettivo è anche rilevare i punti di forza attraverso le percezioni degli utenti.

Al momento, pur in una fase iniziale di avvio sperimentale, l'utilizzo di questa tecnologia ha consentito spesso di verificare, in corrispondenza di problemi noti occorsi a uno o più gestori, andamenti anomali di uno o più indicatori, quali ad esempio variazioni degli *indici di sentiment*[31] rispetto alla media o a periodi precedenti, o picchi di conversazioni su specifiche tematiche di interesse. La definizione ed il monitoraggio nel tempo di uno o più indicatori, può fornire elementi utili a fissare delle soglie specifiche, in maniera da generare segnali di allarme per la Vigilanza in caso di superamento di tali soglie, consentendo, per quanto possibile, di prevenire o anticipare la risoluzione di eventuali anomalie.

[29] Analisi che non prevede alcun trattamento di dati personali (profilazione di persone), essendo finalizzata esclusivamente a rilevare eventi o percezioni degli utenti relativi ai servizi vigilati.

[30] I *feed* sono dei file di testo che, con linguaggio informatico, avvisano l'utente della pubblicazione di un nuovo contenuto online.

[31] Il sistema è addestrato per la ricerca dei valori del sentiment "positivo", "negativo", "neutro" attribuiti sui contenuti social selezionati in base a specifici parametri di ricerca, impostati per le diverse tassonomie d'interesse dei servizi vigilati.

A titolo di esempio, nel grafico che segue si riporta l'analisi di un caso specifico in un arco temporale di un mese del 2019, per un incidente in ambito PEC che ha avuto ampia risonanza sui mezzi di comunicazione. Il grafico è stato ottenuto filtrando per semplicità solo 2 fonti in particolare (Twitter e Facebook) e correlando il servizio scelto (PEC), il periodo temporale di interesse e la combinazione di *keyword* per estrarre eventi di interesse (disservizi, *data breach*, incidenti, …).

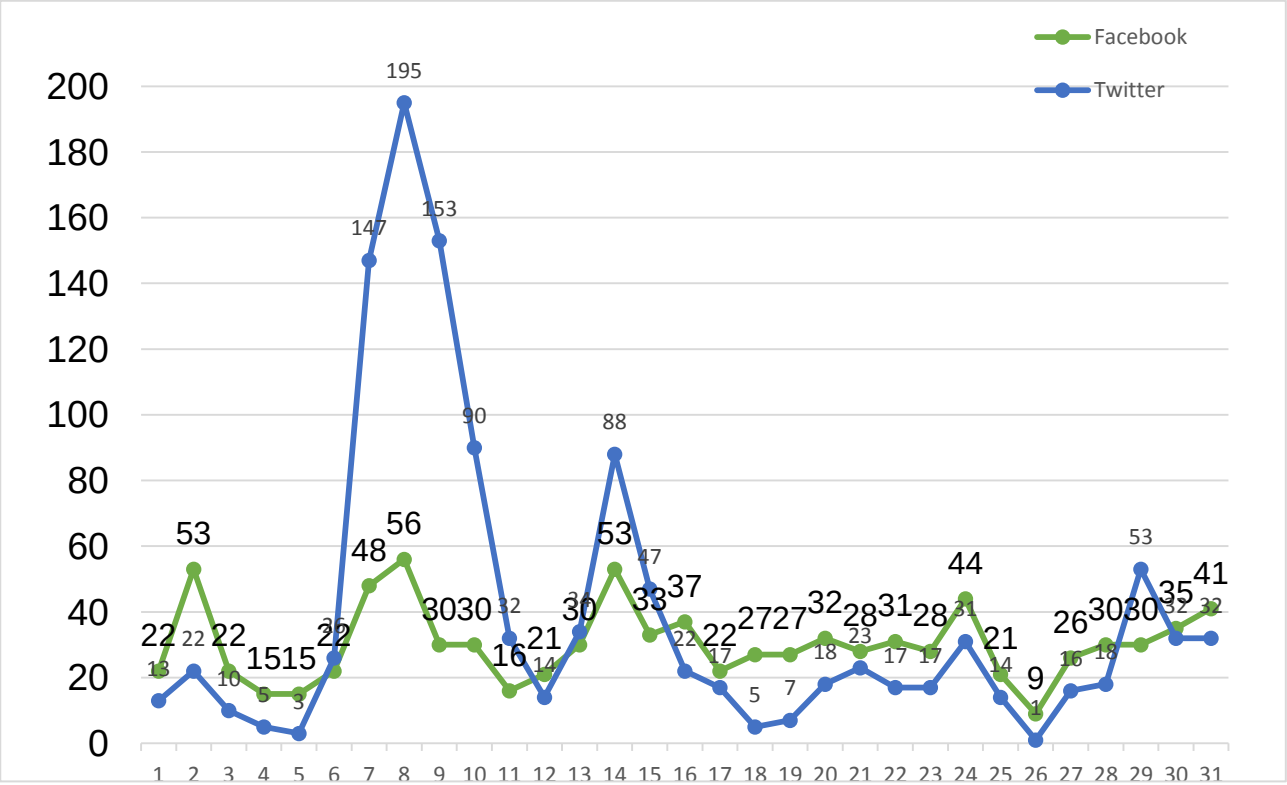

Fig. 7.1- Andamento feed da fonti social per un evento relativo al servizio PEC (maggio 2019)

Il grafico mostra in corrispondenza di alcuni giorni specifici dei picchi indicativi, più evidenti su Twitter ma che hanno comunque un andamento simile su entrambi i social.

L'evento ha avuto ampia risonanza nel periodo tra il 7 ed il 10 del mese, pur potendo non necessariamente essere avvenuto in tali giorni, con successivi strascichi nelle settimane seguenti.

Selezionando i valori di interesse, è poi possibile effettuare un *drill down* e risalire agli utenti[32] che hanno postato l'informazione, alla loro efficacia sul social (numero di like, di re-tweet) ed al contenuto stesso dell'informazione rilevata, fino alla granularità dell'informazione a livello di utente. Non è esclusa la possibilità di falsi negativi o falsi positivi; tuttavia l'analisi che può facilmente essere eseguita sulle informazioni raccolte consente di capire la rilevanze di un determinato evento, il gestore coinvolto, l'eventuale impatto sulla *customer base*, il sentiment (percepito come evento positivo/negativo/neutro).

[32] Non è prevista la raccolta o il trattamento di dati personali.

Sulla base di tali informazioni possono essere intraprese verifiche mirate a prevenire eventuali problemi o ad accertare, in caso ad esempio di percezioni in senso negativo, se si tratti effettivamente di un evento che abbia comportato disservizi per gli utenti.

8 LE ATTIVITÀ IN AMBITO EUROPEO

Per quanto riguarda la vigilanza sui prestatori di servizi fiduciari qualificati, AgID, in quanto organismo designato in Italia ai sensi del Regolamento eIDAS, è coinvolta in un insieme di attività che da un lato riguardano la cura di adempimenti previsti dal Regolamento stesso, dall'altro rientrano nelle attività di collaborazione ed assistenza reciproca o sono volte a favorire lo scambio di *best practice* tra gli organismi di vigilanza dei diversi Stati Membri.

Annualmente, entro il 31 marzo di ogni anno, AgID trasmette alla Commissione una relazione sulle principalti attività di vigilanza svolte sia ai fini della qualificazione di nuovi TSP (prestatori di servizi fiduciari) che sui prestatori già qualificati. È parte integrante della relazione annuale, una sintesi delle notifiche di violazioni su incidenti di sicurezza o perdite di integrità ricevute dai QTSP ai sensi dell'art. 19 del Regolamento eIDAS.

Per dare attuazione a tali obblighi di notifica relativi all'art. 19 del Regolamento eIDAS, è stato costituito un tavolo di lavoro, *art. 19 Expert Group*, coordinato da ENISA[33], Agenzia dell'Unione Europea per la Cybersecurity che si occupa di coordinale le modalità per le rendicontazioni di tali eventi tra i diversi organismi di vigilanza degli Stati Membri, per adottare pratiche comuni di classificazione e gestione. ENISA annualmente pubblica un report che riepiloga, in forma anonima e con dati aggregati, gli incidenti notificati dai diversi Stati membri, al fine di creare una conoscenza comune dei punti deboli riscontrati e delle vulnerabilità più ricorrenti.

L'art. 19 Expert Group si riunisce periodicamente, in genere con frequenza semestrale, agendo tramite scambi di email e documentazione, anche al fine di trovare soluzioni tecniche o metodologiche per affrontare temi di comune interesse quali integrazione con nuove tecnologie, response a nuovi business case o esigenze di mercato anche locali, strumenti di validazione di soluzioni e verifica della conformità delle stesse. L'esito di questi incontri è, ove non secretato per ragioni di sicurezza e riservatezza, disponibile sul portale europeo in numerose sezioni interne.

Sempre in ambito QTSP, il team AgID è parte attiva del FESA, *Forum of European Supervisory Authorities for trust service providers*, con lo scopo già accennato al § 2.3 di coordinarsi nelle attività di vigilanza, nelle metodologie e nell'assistenza reciproca con gli organismi di vigilanza degli altri Stati Membri.

[33] L'ENISA, Agenzia dell'Unione europea per la cibersicurezza, è un centro di competenze in materia di sicurezza informatica in Europa. Aiuta l'UE e i paesi membri dell'UE a essere meglio attrezzati e preparati a prevenire, rilevare e reagire ai problemi di sicurezza dell'informazione. Rif. https://www.enisa.europa.eu/about-enisa.

9 LE SANZIONI

Il CAD[34] definisce i casi per i quali possono essere irrogate sanzioni amministrative.

Nel 2019 AgID ha istruito 6 procedimenti sanzionatori, 1 dei quali attivato a fine 2018. Tali procedimenti sono stati attivati:

- 1 in ambito QTSP;
- 4 in ambito PEC;
- 1 in ambito Conservazione.

Quattro dei sei procedimenti sopra indicati a fine 2019 risultavano ancora in corso; due procedimenti si sono invece conclusi a seguito della positiva verifica che le irregolarità accertate fossero state correttamente indirizzate e dell'avvenuto pagamento in oblazione delle sanzioni pecuniarie irrogate per le violazioni contestate, per un ammontare complessivo di circa 660.000 Euro.

Tali risorse saranno destinate a rafforzare le iniziative già intraprese, rivolte ai soggetti vigilati, volte a migliorare la capacità di prevenzione degli stessi gestori.

Le irregolarità riscontrate nell'ambito dei due procedimenti conclusi hanno riguardato in linea di massima:

- l'adozione di pratiche operative e gestionali inadeguate, non conformi con le procedure autorizzate o corrispondenti a norme internazionali;
- l'utilizzo di sistemi in alcuni casi non in grado di garantire l'affidabilità e la sicurezza tecnica;
- l'utilizzo di subcontraenti non dotati della necessaria affidabilità e sui quali il gestore non esercitava un adeguato controllo.

[34] Art. 32-bis

10 AZIONI SCATURITE DALLE VERIFICHE E PROSSIME ATTIVITÀ

I procedimenti di verifica ed i rilievi formulati hanno comportato l'adozione di azioni correttive e di miglioramento, in più casi definite dai gestori anche di propria iniziativa.

L'analisi svolta sui risultati delle verifiche ha consentito di individuare criticità comuni a più gestori o irregolarità potenzialmente presenti presso più soggetti vigilati:

- nel caso del servizio PEC, sulla base dei risultati emersi dai procedimenti di vigilanza e correlati agli eventi negativi che si sono verificati nel corso dell'anno, AgID, nell'ambito delle funzioni di indirizzo previste dal CAD[35], ha emesso indicazioni per il rafforzamento delle misure minime di sicurezza e per la prevenzione dell'uso improprio del servizio PEC. Tali istruzioni sono state elaborate dal CERT-PA (attuale CERT-AgID[36]), integrando e rafforzando le proposte formulate dagli stessi gestori per il tramite delle associazioni di categoria;
- nel caso dei servizi fiduciari qualificati, sulla base delle criticità rilevate attraverso i procedimenti di verifica che hanno coinvolto due soli soggetti, sono state emesse indicazioni per migliorare i controlli al momento dell'identificazione dei richiedenti i certificati di firma digitale, fornendo indicazioni specifiche a tutti i QTSP, che hanno prontamente messo in campo specifici controlli.

Il ruolo propositivo e collaborativo dei gestori, rilevato in occasione dell'espletamento delle funzioni di vigilanza, è indicativo di un'accresciuta consapevolezza della rilevanza di servizi, quali la PEC e la firma digitale che, come risulta evidente dai valori esposti al § 3, coprono una porzione importante dell'offerta di servizi erogati da gran parte degli operatori e che hanno assunto nuova rilevanza nel contesto nazionale.

I risultati delle attività di vigilanza e le esperienze maturate sul campo sono messe a disposizione delle unità organizzative di AgID[37] preposte alla revisione delle regole ed all'emanazione delle Linee Guida previste dal CAD, attività per le quali sono attivi diversi tavoli tecnici che vedono la partecipazione di rappresentanti dei gestori.

Gli impegni futuri sono certamente orientati a consolidare e migliorare sempre più gli strumenti disponibili ad AgID per costruire conoscenza a partire dai dati. In particolare:

- parallelamente all'emissione delle nuove Linee Guida per la produzione di dati statistici per le quattro tipologie di servizi, è previsto che sia attivato in modo incrementale e previo test congiunto con un insieme di gestori, il sistema informatico per collezionare tali dati strutturati attraverso interfacce applicative;
- come già indicato al § 7, sono previste ulteriori attività per consolidare gli strumenti disponibili per l'analisi predittiva.

[35] Art. 14 bis, comma 2, lett. a)

[36] https://cert-agid.gov.it

[37] La struttura organizzativa d AgD prevede una separazione di ruoli tra le funzoni di qualificazione/accreditamento (attivtà cosiddette "ex-ante"), le funzioni di vigilanza (attività "ex-post") e le funzioni regolatorie.

I procedimenti attivati nel 2019 hanno messo in luce anche alcuni aspetti che forniscono lo spunto per riesaminare le regole e le modalità di esecuzione delle verifiche, anche a fronte delle esigenze determinate dall'emergenza sanitaria emersa già a fine 2019.

11 ANALISI GIURIDICA

Nell'esercizio delle proprie funzioni all'Agenzia è demandato il compito di accertare eventuali violazioni delle norme del CAD e del Regolamento eIDAS da parte dei soggetti vigilati e irrogare le conseguenti sanzioni amministrative,

L'art. 32 bis del CAD, nel testo vigente dal 26 gennaio 2018[38] prevede l'applicazione di sanzioni amministrative pecuniarie per importi da un minimo di €40.000,00 a un massimo di €400.000,00 Euro, ai prestatori di servizi fiduciari qualificati (QTSP), ai gestori di posta elettronica certificata, ai conservatori accreditati e ai gestori dell'identità digitale.

Tali sanzioni si applicano per la violazione degli obblighi del Regolamento eIDAS o del CAD, in relazione alla prestazione dei rispettivi servizi, e in caso di malfunzionamento che determini l'interruzione del servizio, anche per la mancata o intempestiva comunicazione ad AgID dell'avvenuta interruzione. La quantificazione delle sanzioni da applicare nel caso concreto dipende dalla gravità della violazione e dall'entità del danno provocato all'utenza. Nei casi più gravi oltre alla sanzione pecunaria si aggiunge la cancellazione dall'elenco pubblico e il divieto di accreditamento per un periodo fino a un massimo di due anni. AgID può inoltre applicare la sanzione accessoria della pubblicazione dei provvedimenti che diffidano il gestore al ripristino del servizio o di quelli che dispongno la cancellazione del gestore dall'elenco pubblico.

La cancellazione dall'elenco pubblico è una sanzione che ha impatto non solo sul gestore, ma anche sugli utenti dei servizi e sulla collettività, per questo la sua applicazione deve essere valutata tenendo conto dei molteplici interessi in gioco e disposta in casi di particolare gravità: per le violazioni idonee ad esporre a rischio i diritti e gli interessi di una pluralità di utenti, relative a significative carenze infrastrutturali, in caso ripetute interruzioni del servizio.

Il procedimento sanzionatorio è disciplinato dal Regolamento recante le modalità per la vigilanza e per l'esercizio del potere sanzionatorio già citato in precedenza[39], che integra l'art. 32 bis, che prevede che le sanzioni siano irrogate dal direttore generale di AgID, sentito il *Comitato di indirizzo*[40], e rinviando alla disciplina della legge 689/1981, in quanto compatibile. Esso prevede che il gestore possa svolgere le proprie difese in contraddittorio con l'Agenzia, attraverso audizioni e il deposito di memorie e documenti, nonché la possibilità di definizione senza applicazione di sanzioni, con provvedimenti di archiviazione da parte dell'Agenzia o con l'accesso all'oblazione da parte del gestore.

Per quanto riguarda la determinazione delle sanzioni, si tiene conto dei parametri contenuti nell'articolo 32 bis: la gravità della violazione accertata, l'entità del danno provocato all'utenza, l'idoneità a esporre a rischio diritti e interessi di una pluralità di utenti, l'esistenza significative carenze infrastrutturali e entità delle carenze di processo del gestore, l'avvenuta interruzione del

[38] Vedi D.Lgs. 13 dicembre 2017, n. 217

[39] https://www.agid.gov.it/it/agenzia/vigilanza - "Regolamento recante le modalità per la vigilanza e per l'esercizio del potere sanzionatorio ai sensi dell'art.32-bis del d.lgs. 7 marzo 2005, n.82 e successive modificazioni", adottato con Determinazione n. 191/2019 del 5 giugno 2019.

[40] Il Comitato è l'organo di indirizzo strategico dell'Agenzia.

servizio, la mancanza o intempestiva informazione ad AgID o agli utenti (se dovuta), il mancato adeguamento del gestore alle indicazioni fornite da AgID, la reiterazione. Soccorrono inoltre – per quanto compatibili – i principi della legge 689/1981 e in particolare si ha riguardo alla gravità della violazione, all'opera svolta dal gestore per l'eliminazione o attenuazione delle conseguenze della violazione, alla condotta generale del gestore e alle sue dimensioni.

In sintesi, nella valutazione delle violazioni e nella determinazione delle sanzioni, l'Agenzia deve tenere in considerazione il fatto che l'osservanza delle regole tecniche che disciplinano l'attività dei soggetti vigilati è volta a garantire la sicurezza e la tenuta dei sistemi, nell'interesse degli utenti e della collettività.

12 APPENDICE

12.1 Glossario

AgID - Agenzia per l'Italia Digitale

CAD - Codice dell'Amministrazione digitale (decreto legislativo 7 marzo 2005, n. 82 s.m.i.)

IdP –gestore dell'identità digitale SpID

NC - Non Conformità-irregolarità classificata secondo tre livelli di gravità crescente (Lieve, Media, Grave), che richiede azioni correttive entro tempi massimi stabiliti

QTS - Qualified Trust Service- Servizi fiduciari qualificati- servizi elettronici, normalmente forniti a pagamento, che soddisfano un insieme di requisiti validi su tutto il territorio dell'Unione europea (requisiti stabiliti dal Regolamento eIDAS) fornendo agli utenti mutue garanzie di sicurezza e qualità. I più diffusi servizi fiduciari qualificati in Italia sono i servizi di firma digitale.

QTSP - Qualified Trust Service Provider- Prestatori di servizi fiduciari qualificati- Soggetti qualificati perl'erogazione di uno o più servizi fiduciari qualificati (QTS) e sui quali AgID esercita le funzioni di vigilanza

SpID -Sistema pubblico di identità digitale

12.1 Riferimenti normativi

Decreto Legislativo 7 marzo 2005, n.82 s.m.i — Codice dell'Amministrazione Digitale ("CAD")

Regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 ("eIDAS"), in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno

Regolamento recante le modalità per la vigilanza e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del d. lgs. 7 marzo 2005, n. 82 e successive modificazioni