AGID | Agenzia per l'Italia Digitale

Vigilanza sui soggetti qualificati o accreditati (QTS, PEC, Conservazione, SpID)

Rapporto di riepilogo

gennaio-dicembre 2020

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 3
2 LE FUNZIONI DI VIGILANZA SVOLTE DA AGID 6
2.1 Richiami relativi al quadro normativo 6
2.2 Le regole e le modalità di esecuzione 7
2.3 Le parti interessate (*stakeholder*) 8
3 TASSONOMIA DEI SOGGETTI VIGILATI 10
3.1 Prestatori di servizi fiduciari qualificati (QTSP) 10
3.3 Gestori PEC 11
3.4 Conservatori 14
3.5 Identity Provider SpID (IdP) 15
4 PROCEDIMENTI DI VERIFICA NEL 2020 19
4.1 Riepilogo delle verifiche 19
4.2 Verifiche di *seconda parte* e componenti di servizio 21
4.3 Riepilogo dei rilievi 22
4.4 Analisi dei rilievi più ricorrenti 27
5 SEGNALAZIONI DI INCIDENTI E MALFUNZIONAMENTI 29
6 SEGNALAZIONI DAGLI UTENTI 33
7 LE ATTIVITÀ IN AMBITO EUROPEO 34
8 LE SANZIONI 35
9 AZIONI SCATURITE DALLE VERIFICHE E PROSSIME ATTIVITÀ 36
10 APPENDICE 38
12.1 Glossario 38
12.1 Riferimenti normativi 38

1 PREFAZIONE

La presente relazione illustra le attività svolte nel 2020 dall'Agenzia per l'Italia Digitale ("AgID") ai fini dell'esercizio delle funzioni di vigilanza previste dal Codice dell'Amministrazione Digitale (CAD)[1].

La vigilanza riguarda servizi quali la firma digitale, l'identità digitale o la posta elettronica certificata, che abilitano le transazioni *on line* verso pubbliche amministrazioni o tra soggetti privati e che pertanto hanno un ruolo sempre più importante per lo sviluppo dell'economia digitale. Malfunzionamenti e disservizi frequenti o irregolarità nei processi di erogazione da cui possono derivare utilizzi impropri o a scopo fraudolento di tali servizi, minano la fiducia degli utenti e costituiscono un ostacolo allo sviluppo dei processi di digitalizzazione. In tale consapevolezza l'Agenzia, nel suo ruolo di autorità di vigilanza, promuove controlli non solo volti ad accertare presunte irregolarità, anche sulla base delle segnalazioni degli utenti, ma soprattuto in via preventiva e in un'ottica di miglioramento continuo dei processi di erogazione.

I poteri di vigilanza trovano fondamento in un quadro regolatorio costituito da norme comunitarie e nazionali e vedono coinvolti una rete di *stakeholder*- gli utenti[2], le istituzioni e gli stessi operatori ai quali si applicano le funzioni di vigilanza –ciascuno con diversi profili di interesse e di aspettative per le specifiche componenti dei servizi, che ne influenzano lo sviluppo e l'evoluzione.

La vigilanza consente di acquisire elementi per individuare e pianificare gli interventi correttivi ed evolutivi, sia dal punto di vista delle specifiche modalità realizzative di interesse dei gestori, sia per quanto riguarda gli aggiornamenti del quadro normativo a cura degli enti regolatori, sia con rifermento alle responsabilità degli utenti nell'utilizzo consapevole e secondo specifica dei servizi fruiti. L'Agenzia, con la presente relazione, rende conto annualmente delle attività svolte, informando gli *stakeholder* e il pubblico dei temi più rilevanti trattati nell'anno trascorso, dei problemi riscontrati e dei principali risultati relativi alle componenti dei servizi oggetto di esame.

Nel 2020 anche la vigilanza ha dovuto fare i conti con l'emergenza sanitaria e con le restrizioni legate alla pandemia da Covid-2019, che hanno **ridefinito esigenze e priorità e comportato modifiche nelle modalità di conduzione delle attività**. Le verifiche inizialmente programmate tenendo conto di indici di rischio dei soggetti vigilati e, come per gli anni precedenti, estese alle quattro tipologie di servizi indicate all'art. 14-bis, comma 2, lettera i) del CAD[3], dopo un regolare

[1] L'art. 14-bis, comma 2, lettera i) del Codice dell'Amministrazione Digitale (CAD), con le modifiche introdotte dal decreto-legge 16 luglio 2020, n. 76 s.m.i., prevede che AgID svolga «[…] *vigilanza sui servizi fiduciari ai sensi dell'articolo 17del regolamento UE 910/2014 ("Regolamento eIDAS") in qualità di organismo a tal fine designato, sui gestori di posta elettronica certificata, sui soggetti di cui all'articolo 34, comma 1-bis, lettera b), 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 (servizi fiduciari qualificati (tra i quali ad esempio i servizi di firma digitale), PEC, conservazione e SpID) sono persone fisiche e persone giuridiche (cittadini, imprese, pubbliche amministrazioni).

[3] Rispettivamente servizi fiduciari qualificati, PEC, SpID, conservazione a norma.

avvio nel primo bimestre 2020, hanno subito un fermo nel periodo marzo-aprile, a causa della sopravvenuta situazione di crisi pandemica; successivamente sono state rimodulate per tenere conto delle nuove priorità determinate dal particolare periodo. In considerazione, infatti, di un atteso aumento di transazioni on line a causa delle restrizioni sopravvenute, le verifiche hanno riguardato prevalentemente i gestori SpID e i QTSP, i cui servizi hanno un ruolo essenziale nell'erogazione/fruizione di servizi on-line, come peraltro dimostrato dall'**aumento di segnalazioni-utente** che hanno interessato tali tipologie di gestori nel secondo semestre 2020.

Le restrizioni sugli spostamenti in ambito nazionale hanno portato all'esecuzione di **verifiche ispettive da remoto,** con definizione delle relative procedure e revisione delle modalità di conduzione.

Come nell'anno precedente, anche nel 2020 le verifiche hanno visto l'apporto di **competenze specialistiche** dal Nucleo di Prevenzione delle Frodi Tecnologiche della Guardia di Finanza[4], dal Cert-AgID[5] e da auditor specializzati di organismi di certificazione per gli aspetti prevalentemente metodologici. La partecipazione alle verifiche di analisti del CERT-AgID ha consentito di approfondire i temi principalmente legati alle misure di sicurezza e ha fornito ai soggetti vigilati indicazioni rilevanti per migliorare le loro capacità di individuare vulnerabilità, prevenire attacchi e proteggere i sistemi.

Riguardo agli strumenti per l'esecuzione delle verifiche, pur nelle difficoltà determinate dalla situazione emergenziale, sono proseguite le attività per completare il **sistema per l'acquisizione dei dati strutturati**[6] dai gestori- in vista dell'emissione, nel 2021, di nuove regole per la trasmissione di dati statistici per i servizi vigilati[7] - e consolidare le funzioni realizzate nel 2019, che riguardano ad esempio l'analisi predittiva e la gestione delle segnalazioni dagli utenti.

Nel corso del 2020 il **quadro normativo** è stato oggetto di modifiche con impatto sui temi di specifico interesse della vigilanza: le disposizioni del *DL Semplificazioni*[8], entrate in vigore a luglio 2020, hanno comportato l'eliminazione del processo di accreditamento per i conservatori, in precedenza previsto dall'art. 29 del CAD; ulteriori modifiche per tali soggetti vigilati riguardano l'entità delle sanzioni comminabili ai sensi dell'art- 32-bis del CAD, che sono state fissate entro nuovi

---

[4] La collaborazione ricade nell'ambito dell'accordo stipulato a novembre 2018 (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).

[5] (https://cert-agid.gov.it). Il Cert-AgID è la struttura di AgID che da 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), ha sostituito il CERT-PA.

[6] Dati relativi alle notifiche di incidenti/malfunzionamenti; dati statistici periodici sui servizi.

[7] *Linee Guida per la normalizzazione dei dati statistici relativi ai servizi erogati dai gestori PEC, dai conservatori e dai prestatori di servizi fiduciari qualificati (QTSP) ai sensi dell'art. 20 del CAD*; Linee Guida relative all'*infrastruttura per l'acquisizione dei dati statistici*; *Linee guida per l'acquisizione di dati statistici SpID.*

[8] Decreto-Legge 16 luglio 2020, n. 76 s.m.i.

valori di minimo e massimo. Di tali nuoveprevisioni introdotte dal DL semplificazione, oltre che delle esperienze maturate in oltre due anni di attività dalla prima adozione, si è tenuto conto per una revisione del Regolamento di vigilanza, completata a fine 2020[9].

Parlando di **risultati,** pur in una fase emergenziale che si è dovuta affrontare a partire da fine febbraio 2020, che ha richiesto un primo periodo di riorganizzazione ed adeguamento dei processi, è stato successvamente possibile svolgere le attività con regolarità, in particolar modo con l'attivazione di verifiche ispettive basate su metodologie di audit da remoto che, pur precludendo specifici controlli che richiedono attività in presenza, hanno comunque consentito di approfondire delle tematiche di processo e di gestione della sicurezza. Tali verifiche si sono rese ancor più necessarie proprio in considerazione del particolare periodo emergenziale, che ha favorito l'aumento delle transazioni on line attraverso SpID o servizi di firma digitale, comportando un considerevole **incremento di volumi**: nel caso SpID, le identità digitali gestite a fine 2020 risultano triplicate rispetto al 2019; conseguentemente sono aumentate le occasioni di utilizzo di tali servizi a scopo fraudolento, con incremento, come già detto, anche delle segnalazioni utente.

Sono stati complessivamente avviati **12 nuovi procedimenti di verifica**, che in gran parte hanno riguardato QTSP e gestori SpID con un'utenza molto ampia e che in 4 casi hanno avuto origine da segnalazione o accertamenti per indagini di polizia giudiziaria. I **60 rilievi** formulatiferme restando le limitazioni sulle componenti di servizio esaminate- riguardano in maggior misura le componenti di processo svolte attraverso terze parti e gli aspetti di sicurezza per la prevenzione di accessi abusivi ai sistemi o utilizzi impropri dei servizi.

Alle attività sopra accennate sono dedicate specifiche sezioni della relazione; nella sezione introduttiva si richiamano le informazioni di contesto sulla vigilanza, evidenziando le modifiche intervenute rispetto al 2019.

I risultati delle verifiche sono esposti in forma anonima ed in modalità aggregata.

I dati si riferiscono al 31/12/2020.

[9] Il nuovo Regolamento è stato adottato con Determinazione N. 74/2021 del 19/01/2021 ed è entrato in vigore il 5 febbraio 2021. L'argomento sarà trattato nel Rapporto annuale relativo al 2021.

2 LE FUNZIONI DI VIGILANZA SVOLTE DA AGID

2.1 Richiami relativi al quadro normativo

Le funzioni di vigilanza svolte da AgID trovano fondamento in un contesto di regole nazionali e comunitarie. In base al Codice dell'Amministrazione Digitale (CAD)[10], AgID svolge funzioni di vigilanza sui *prestatori di servizi fiduciari qualificati*, sui *gestori di Posta Elettronica Certificata*, i *conservatori di documenti informatici* e i *gestori di identità digitale SpID*. Nell'esercizio di tale funzione l'Agenzia può irrogare per le violazioni accertate a carico dei soggetti vigilati le sanzioni amministrative di cui all'art. 32-bis in relazione alla gravità della violazione accertata e all'entità del danno provocato all'utenza.

Nel corso del 2020 sono entrate in vigore le disposizioni del *DL Semplificazioni*[11], che hanno introdotto alcune modifiche alle norme del CAD di riferimento per la vigilanza. Le principali novità riguardano i conservatori, per i quali è stato eliminato il processo di accreditamento con conseguente iscrizione nell'elenco pubblico nazionale tenuto da AgID[12]; per tali soggetti è stata inoltre ridotta l'entità delle sanzioni comminabili ai sensi dell'art- 32-bis del CAD in caso di violazioni accertate degli obblighi del CAD o del Regolamento eIDAS.

Il DL Semplificazioni ha introdotto rilevanti modifiche anche per il sistema SpID, con alcune importanti novità circa gli effetti prodotti dall'autenticazione tramite identità digitale[13], che conferiscono all'identità SPID lo stesso valore di un qualsiasi documento d'identità nello svolgimento di pratiche amministrative online. Le nuove previsioni, inoltre, incentivano al massimo l'utilizzo di SPID, prevendendo che dal 28 febbraio 2021 l'accesso ai servizi digitali erogati da amministrazioni e enti pubblici avvenga esclusivamente attraverso l'identità digitale SPID e la Carta di identità elettronica.

---

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

[11] Decreto-Legge 16 luglio 2020, n. 76 s.m.i.

[12] L'art. 34, comma 1-bis, lettera b) del CAD introdotto dal *DL Semplificazioni* prevede in sostituzione l'obbligo, per le pubbliche amministrazioni che intendano affidare la conservazione di documenti informatici al di fuori della propria struttura organizzativa, di rivolgersi a soggetti *in possesso di requisiti di qualità, sicurezza e organizzazione individuati – nel rispetto della disciplina europea – nelle Linee guida di cui all'art . 71 del CAD relative alla formazione, gestione e conservazione dei documenti informatici, nonché in un apposito regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID, avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali, oltre alla qualità e la sicurezza del sistema di conservazione*.

[13] Nell'art. 64, comma 2-duodecies si stabilisce che se la verifica dell'identità digitale avviene con livello di garanzia *almeno significativo* – ai sensi dell'articolo 8, paragrafo 2, del Regolamento eIDAS – questa produce gli effetti del documento di riconoscimento equipollente. Inoltre, l'identità digitale, verificata con livello di sicurezza almeno significativo, attesta gli attributi qualificati dell'utente, ivi compresi i dati relativi al possesso di abilitazioni o autorizzazioni richieste dalla legge ovvero stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche (…).

Al regime di identificazione elettronica SpID e ai servizi fiduciari qualifificati si applica la disciplina del Regolamento UE 910/2014 (Regolamento eIDAS). Con riferimento, in particolare, ai servizi fiduciari qualificati, AgID è l'organismo di vigilanza designato in Italia, con gli specifici compiti previsti dal Regolamento[14].

In virtù delle previsioni dell'art. 29 del CAD, con le modifiche intervenute nel 2020, l'obbligo di soddisfare i requisiti indicati nell'art. 24 del Regolamento eIDAS per i prestatori di servizi fiduciari qualificati resta esteso ai soggetti che intendono operare come gestori PEC.

2.2 Le regole e le modalità di esecuzione

Le modalità di esecuzione della vigilanza e di esercizio dei poteri sanzionatori previsti dalle norme sono oggetto di un Regolamento[15], adottato nella prima versione a giugno 2018. A fine 2020 è stata completata una seconda stesura, per tenere conto delle modifiche normative intervenute e delle esperienze maturate a distanza di oltre due anni dalla prima emissione . La nuova versione è entrata in vigore a febbraio 2021.

I procedimenti di verifica gestiti nel 2020 fanno riferimento alla versione del Regolamento adottata nel 2018.

Il Regolamento richiama i principi generali della vigilanza: da un lato è volta ad accertare violazioni o irregolarità; dall'altro, è volta a favorire l'adozione di azioni preventive e di miglioramento continuo dei processi di erogazione dei servizi.

Le verifiche possono essere condotte su base documentale o prevedere anche l'esecuzione di verifiche ispettive, on site o da remoto; tale ultima modalità è stata quella più frequentemente seguita nel 2020 a causa delle restrizioni legate all'emergenza sanitaria.

Un procedimento di verifica può essere avviato a seguito di una segnalazione o nell'ambito di un programma di audit predisposto periodicamente, tipicamente con frequenza quadrimestrale, sulla base di indici di rischio[16]; nel 2020 la programmazione periodica ha dato priorità alle verifiche sui servizi erogati dai QTSP e dai gestori SpID con un'utenza più ampia, vista l'accresciuta rilevanza di tali servizi nel particolare periodo, dimostrata anche dall'aumento dei volumi, come si rileva al § 3.

---

[14] Il ruolo ed i compiti di un Organismo di vigilanza sonoindicati nell'art. 17 del Regolamento (UE) N.910/2014. Sono previste inoltre attività di collaborazione ed assistenza reciproca tra gli Organismi di vigilanza dei diversi Stati Membri

[15] 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.

[16] L'indice di rischio relativo ad un gestore è previsto che sia valorizzato sulla base di alcune caratteristiche (dimensioni e tipologia di servizi e utenti; soluzioni tecnologiche adottate; segnalazioni pervenute; partner che gestiscono specifiche componenti del servizio; verifiche precedenti; analisi di tipo predittivo).

I procedimenti di verifica si concludono in un tempo massimo di centottanta giorni, fatti salvi eventuali termini di sospensione possono portare alla formulazione di rilievi, distinti rispettivamente in 'Non Conformità[17]' e 'Osservazioni[18]'. Tutti i rilievi e le azioni conseguenti definite dai 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.

2.3 Le parti interessate (*stakeholder*)

Le funzioni di vigilanza vedono coinvolti a diverso titolo più organizzazioni esterne.

- **Istituzioni nazionali**: organizzazioni preposte alla definizione degli obiettivi e degli indirizzi strategici che l'Agenzia deve mettere in atto; 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; altre organizzazioni nazionali direttamente coinvolte nei processi primari della vigilanza[19].
- **Soggetti vigilati:** soggetti ai quali si applicano le funzioni di vigilanza. Si veda il § 3.
- **Utenti**: persone fisiche (cittadini) o giuridiche (imprese e pubbliche amministrazioni) che usufruiscono dei servizi erogati dai soggetti vigilati.
- **Istituzioni internazionali**: enti regolatori o di standardizzazione; principali organizzazioni europee che operano ai fini dell'attuazione del Regolamento eIDAS, tra i quali:
    - la Commissione Europea, competente per 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), 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;

[17] 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.

[18] 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.

[19] Ad 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.

- FESA (*Forum of European Supervisory Authorities for trust service providers*), 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 alle quali si fa riferimento nel presente rapporto riguardano tre tipologie di soggetti, rispettivamente i QTSP, i gestori PEC e i gestori SpID, qualificati da AgID ed iscritti in elenchi pubblici[20]; riguardano inoltre i conservatori di documenti informatici per i quali, in via transitoria, in attesa che sia completato il quadro delle regole previste dall'art. 34, comma 1-bis del CAD, è attivo un elenco pubblico[21].

Si tratta in particolare di quattro categorie di seguito elencate, per ciascuna delle quali si presentano in forma anonima ed in modalità aggregate le principali caratteristiche[22], evidenziando le modifiche rispetto alla situazione relativa al 2019.

3.1 Prestatori di servizi fiduciari qualificati (QTSP)

Nel 2020 sono stati qualificati **tre nuovi prestatori di servizi fiduciari qualificati.**

Al 31/12/2020 risultano iscritti nell'elenco dei prestatori di servizi fiduciari qualificati attivi in Italia 22 soggetti, qualificati per uno o più servizi fiduciari (servizi di firma, sigillo, marche temporali e certificati qualificati per siti web).

Si rilevano per i soggetti iscritti nell'elenco dei QTSP le seguenti caratteristiche:

- **servizi erogati e volumi gestiti**: tutti i QTSP sono qualificati per i servizi di firma, ad eccezione di due, che sono qualificati solo per servizi di validazione temporale; 3 QTSP sono qualificati per le quattro tipologie di servizi. 4 QTSP coprono il 90% dei certificati qualificati per firma remota, 3 QTSP, coprono oltre il 70% delle marche temporali qualificate; 4 QTSP coprono oltre l'80% dei certificati qualificati per firma remota;
- **caratteristiche dell'utenza**: 10 QTSP operano solo per 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, la rete dei tabaccai); 13 gestori rilasciano firme sigilli certificati o marche sia a clientela business che a persone fisiche (cittadini);

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

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

[22] Le caratteristiche che riguardano la numerosità e la tipologia di utenti; la rete dei partner tecnologici; i volumi gestiti concorrono a valorizzare indici di rischiio, che sono esaminati ai fini della programmazione delle verifiche periodiche.

– **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 del processo di servizio nei confronti dei richiedenti.

Nel grafico che segue si riporta un estratto dell'andamento dei volumi dei servizi di firma e marca temporale al 31/12/2020, che costituiscono l'offerta più consistente per questa tipologia di soggetti vigilati.

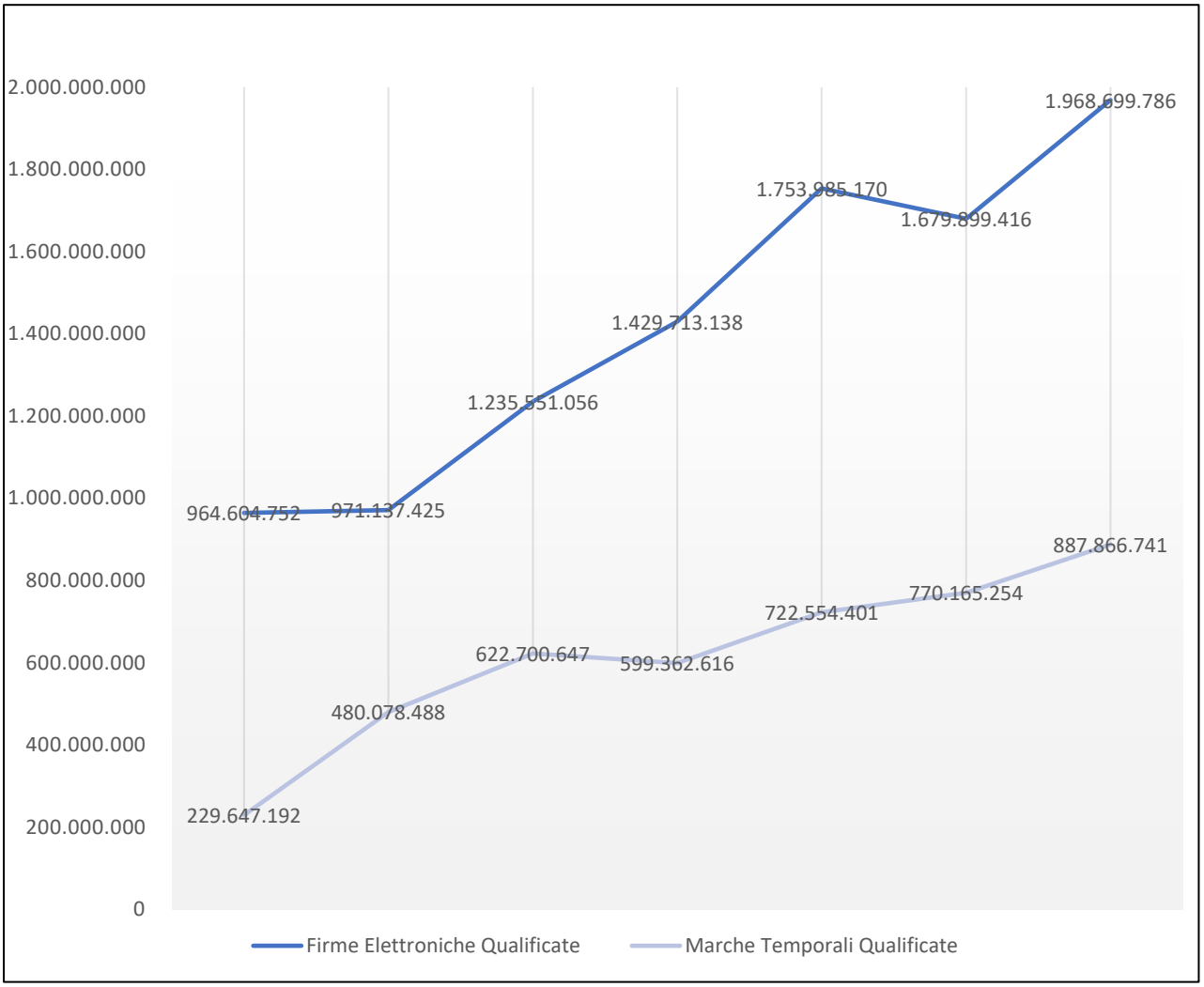

Fig. 3.1 —Andamento servizi di firma e marca temporale [gennaio-dicembre 2020, dati aggregati per bimestre]

Da dicembre 2019 si nota un andamento in crescita fino a dicembre 2020 del 10% per le firme elettroniche qualificate e del 20% circa per le marche temporali qualificate.

3.3 Gestori PEC

I gestori PEC al 31/12/2020 sono 18. Un gestore PEC è cessato nel corso del 2020.

Si rilevano per i 18 soggetti iscritti nell'elenco dei gestori PEC le seguenti caratteristiche:

- **volumi gestiti:** 1 solo gestore copre circa l'80% dei domini e il 60% delle caselle; 2 gestori insieme coprono l'85% 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 ramificata sul territorio.

Nei grafici che seguono si riporta un estratto dell'andamento al 31/12/2020 dei volumi di domini, caselle PEC e messaggi scambiati, indicatori che mettono in evidenza l'importanza dei numeri di questo servizio (totale annuo di 2.258.047.494 messaggi scambiati) e la rilevanza che sempre più assume per lo sviluppo della società digitale:

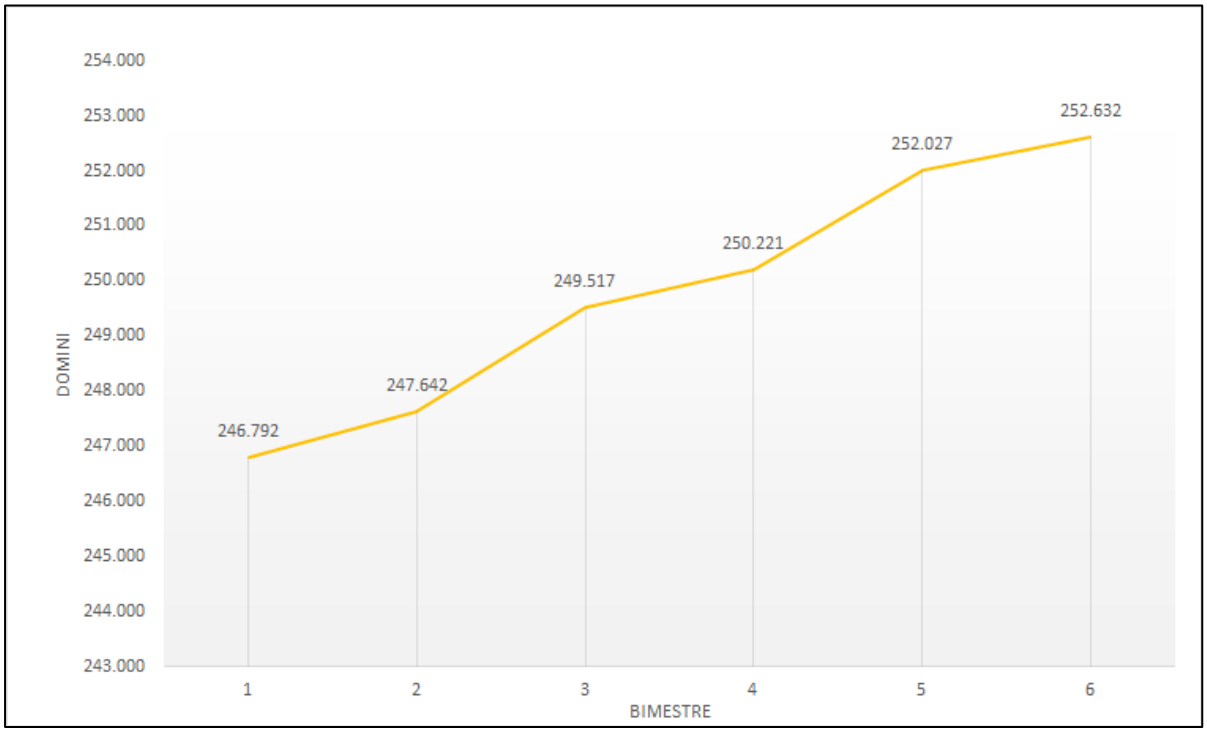

Fig. 3.2 - Andamento domini PEC nel 2020 (dati aggregati per bimestre)

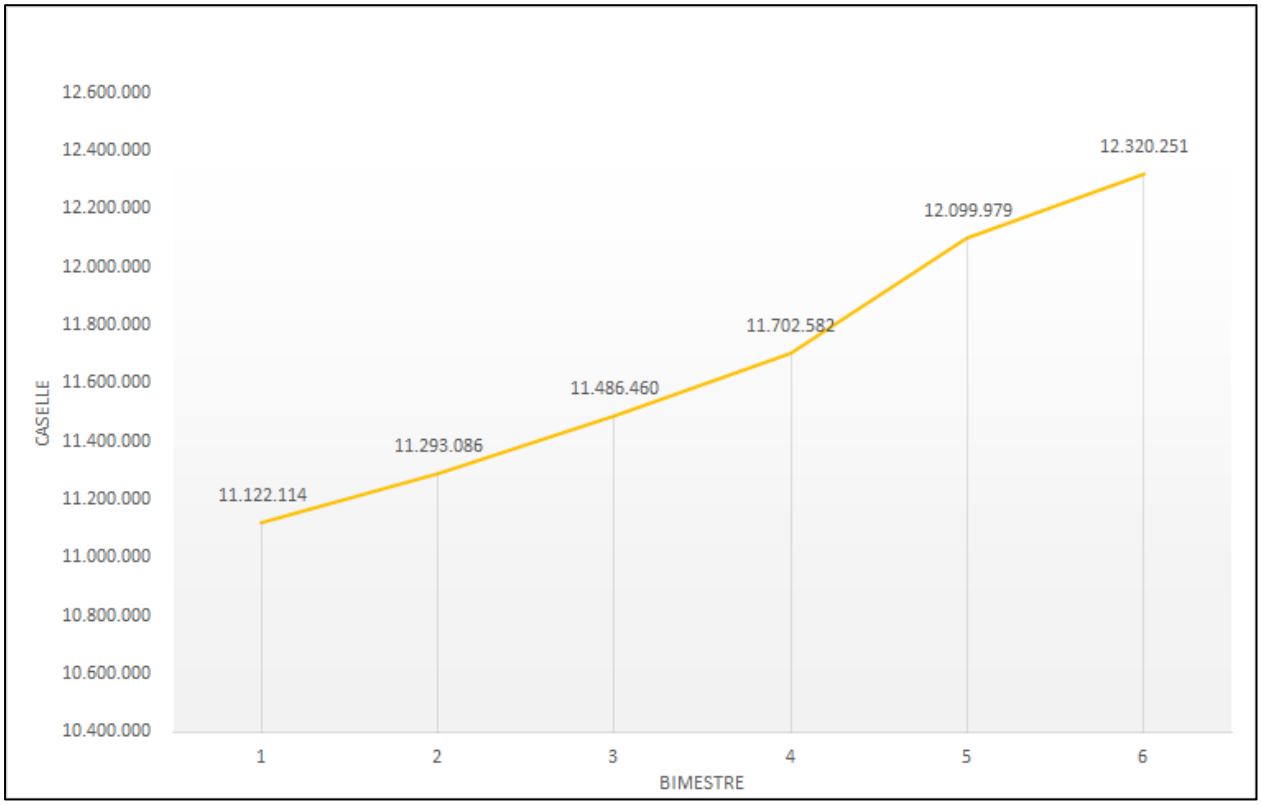

Fig. 3.3 - Andamento caselle PEC nel 2020 (dati aggregati per bimestre)

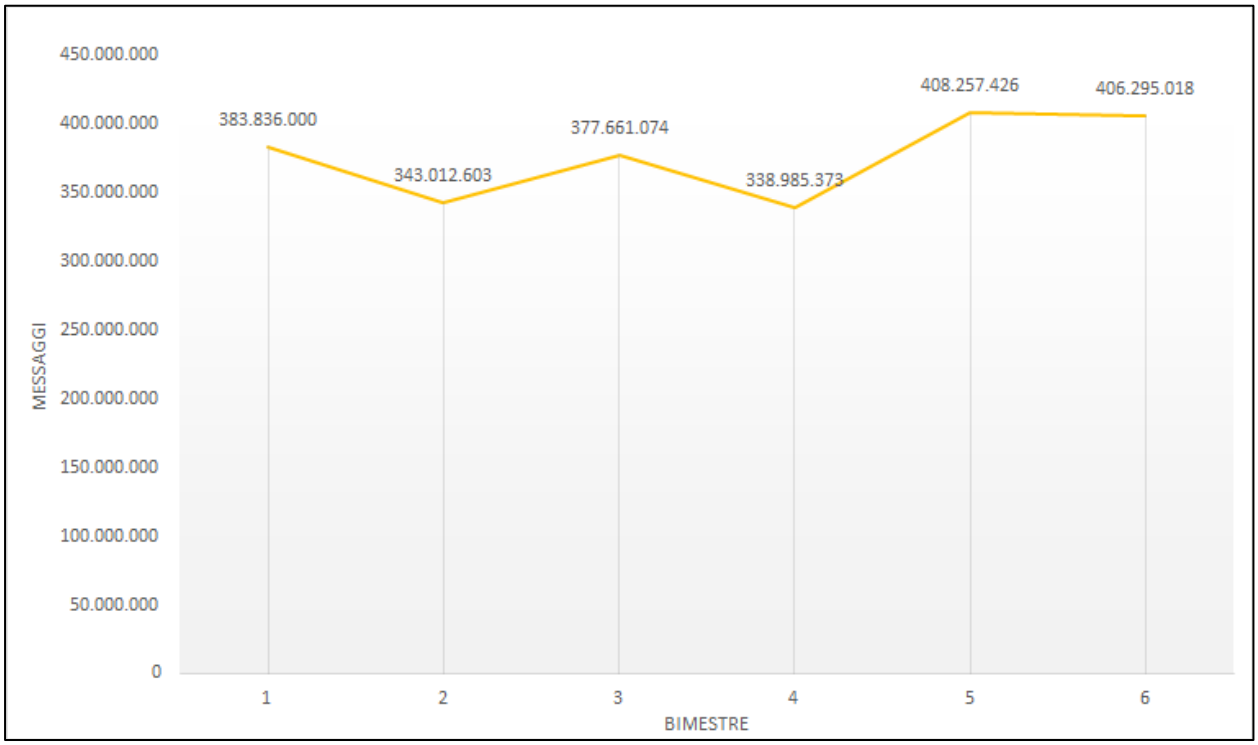

Fig. 3.4 - Andamento messaggi PEC nel 2020 (dati aggregati per bimestre)

3.4 Conservatori

Nel 2020 sono stati accreditati **7 nuovi soggetti** per la conservazione a norma, per un totale di 84 soggetti iscritti al 31/12/2020 nell'elenco dei conservatori accreditati.

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.

Si rilevano per i soggetti iscritti nell'elenco dei conservatori accreditati le seguenti caratteristiche:

- **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 2020, 5 gestori detengono il 90% circa dei contratti attivi con le PA, un solo gestore ne detiene il 40%; 7 gestori coprono circa l'85% 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 o servizi comuni afferenti allo stesso partner tecnologico.

Nei grafici che seguono si riporta un estratto dell'andamento dei volumi al 31/12/2020.

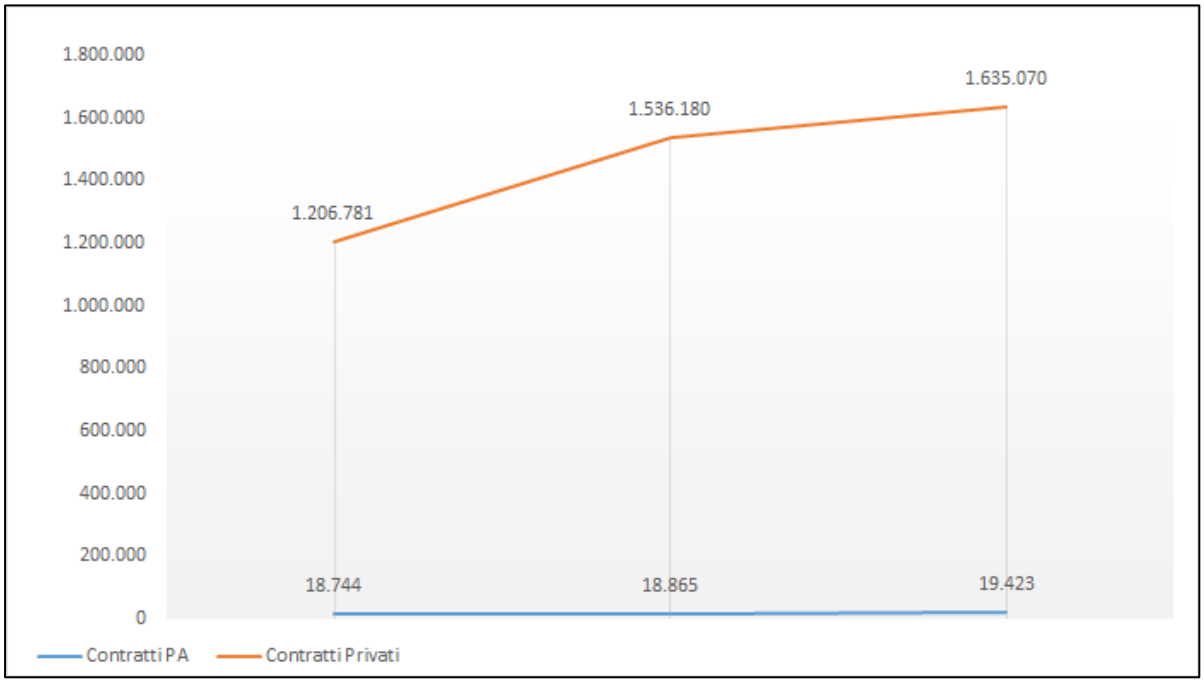

Fig. 3.5 - Andamento contratti PA e privati (dati aggregati per quadrimestre)

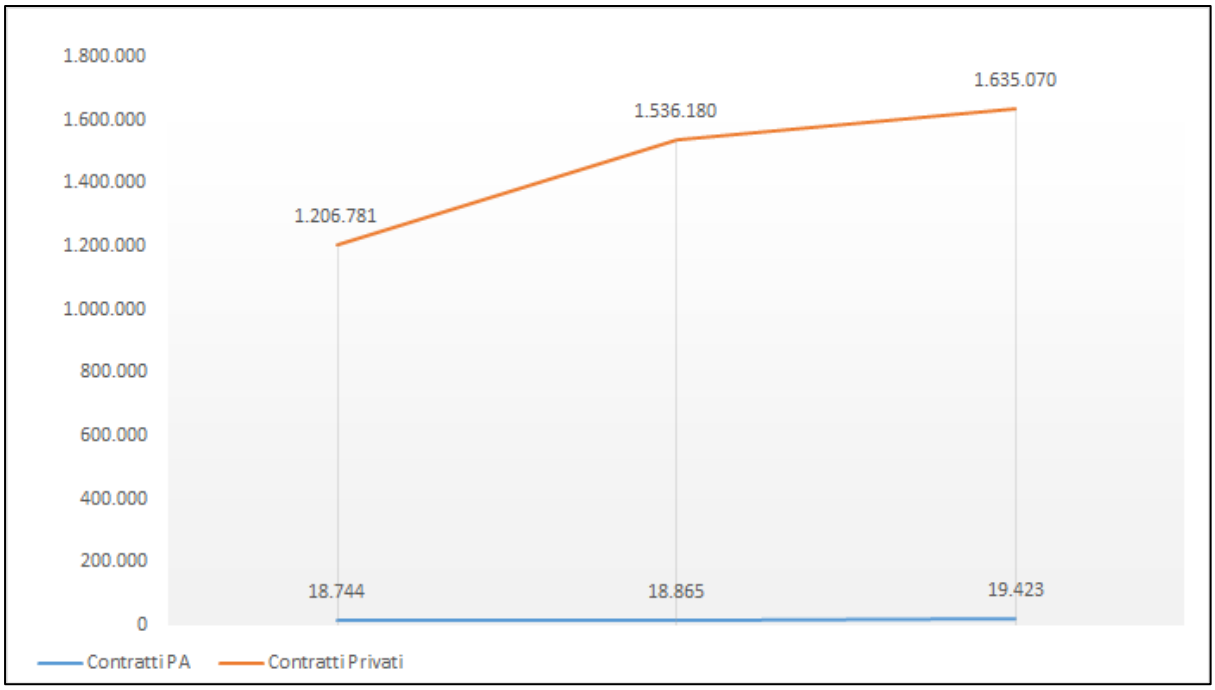

Fig. 3.6 - Volumi (GB) gestiti (dati aggregati per quadrimestre)

3.5 Identity Provider SpID (IdP)

Nel 2020 sono state **rilasciate oltre 10.000.000 di identità**, per un totale di identità gestite al 31/12/2020 dai 9 IdP di oltre 15.000.000; un IdP ne gestisce circa l'84%, come si rileva dal grafico seguente.

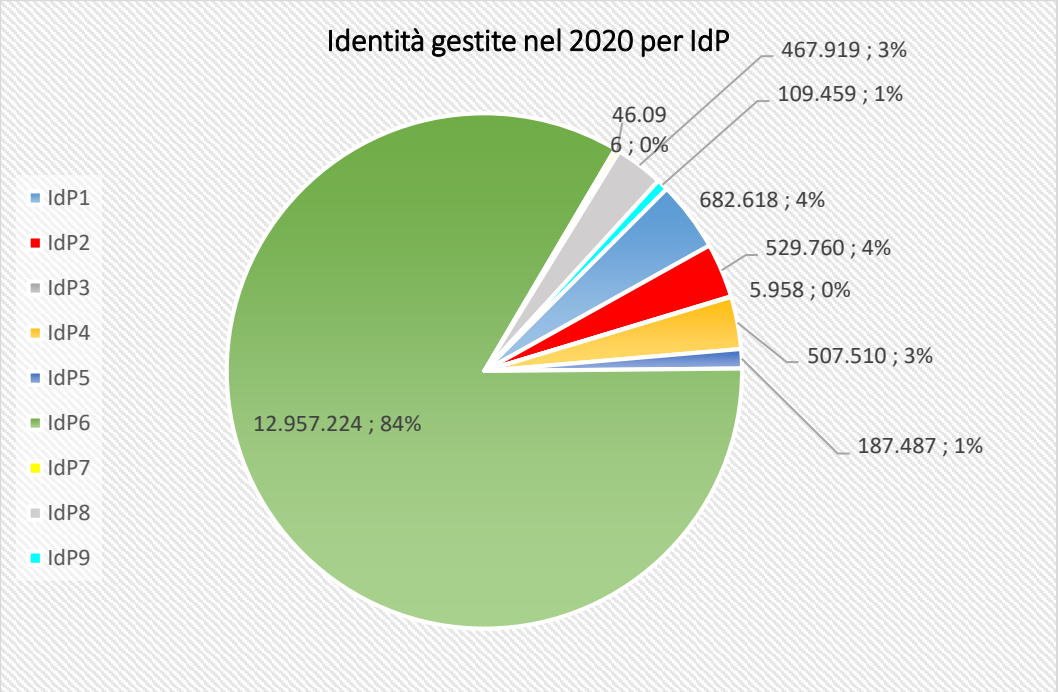

Fig. 3.7- Identità gestite a fine dicembre 2020

Il totale delle identità a fine 2020 è circa il triplo del valore registrato a fine 2019. Nella figura che segue si riporta l'andamento delle identità gestite[23] nel triennio 2018-2020.

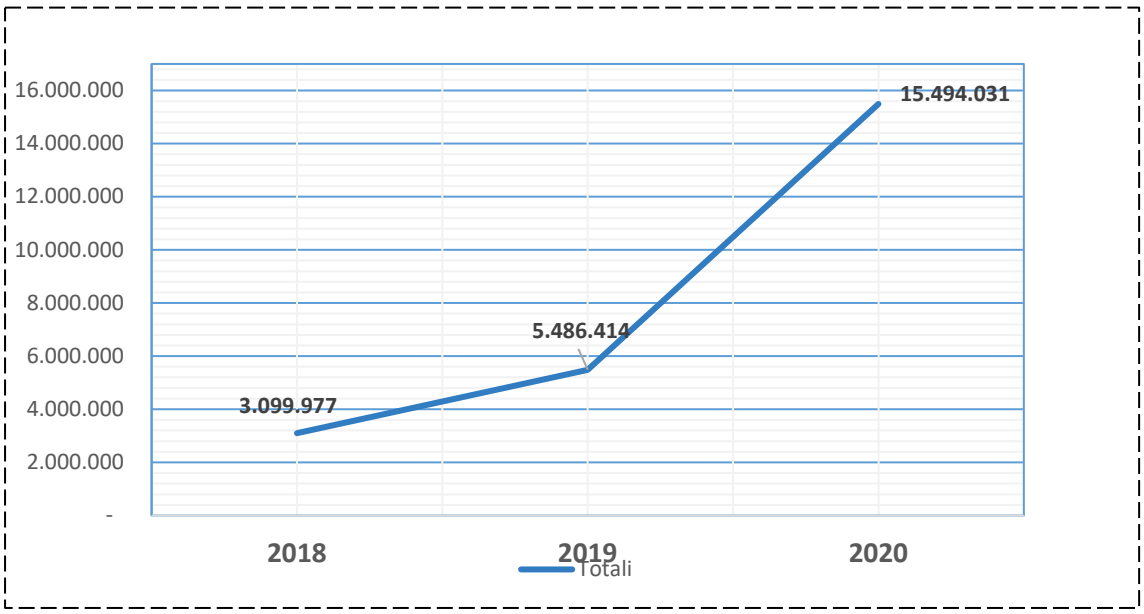

Fig. 3.7- Identità gestite nel triennio 2018-2020

[23] Valori da statistiche fornite dai gestori relativi all'ultima settimana di dicembre dell'anno di riferimento.

Nel 2020 tutti gli IdP hanno raddoppiato e in più casi triplicato le identità gestite rispetto al 2019. L'incremento considerevole rispetto al 2019 è stato certamente determinato anche dalle numerose iniziative legate al periodo Covid, che hanno richiesto l'accesso con SPID su diversi portali di pubbliche amministrazioni (bonus; dismissione PIN Inps, transazioni con le pubbliche amministrazioni in modalità on line; ecc.). Dalle relazioni annuali di riepilogo[24] fornite dai gestori, si rileva infatti che i servizi più acceduti attraverso SpID riguardano servizi INPS (previdenza nazionale)(http:// www.inps.it), Agenzia delle Entrate (https://spid.agenziaentrate.gov.it); bonus e cashback di Stato (https://access.mef.gov.it/oam/fed; https://app-backend.io.italia.it; https://spid.18app.italia.it; https://spid.cartadeldocente.istruzione.it); Camere di commercio (https://spid.infocamere.it)); Istituzioni scolatiche/MIUR (https://spid.pubblica.istruzione.it); pagamenti (https://pagopa.gov.it), nonché servizi INAIL (prevenzione); servizi regionali (es. prestazioni sanitarie; pagamenti bollo auto) e servizi comunali (es. pagamenti tasse/tributi).

Con riferimento alle campagne periodiche di *Customer Satisfaction* e, in particolare, alle valutazioni sul livello di soddisfazione complessiva, passaparola e utilità del servizio, i gestori hanno evidenziato nelle relazioni annuali valori in crescita rispetto agli anni precedenti per le quote di clienti molto soddisfatti o soddisfatti, con riduzione della quota di clienti che esprime valutazioni insufficienti. Il servizio è ritenuto molto utile dalla maggior parte degli utenti ed aumenta la quota di clienti propensi a raccomandarlo. Nelle relazioni si evidenzia come, in pressoché tutte le domande, le *performance* risultino migliorate, con i valori ottenuti nell'analisi 2020 superiori agli analoghi riferiti al triennio precedente. Questo risultato è verosimilmente dovuto sia alla maturità del servizio che, con ogni probabilità, alla migliore percezione degli utenti sull'utilità del servizio SPID, grazie anche all'ampliamento dei servizi resi dai *Service Provider* e dalle numerose iniziative legate al periodo Covid rese fruibili attraverso SpID.

I principali motivi di insoddisfazione indicati da un gestore riguardano principalmente il processo ("complessità e scarsa flessibilità"; "mancanza di una chat on line"; "tempi di registrazione/attivazione troppo lunghi") e l'assistenza ("mancata risoluzione dei problemi"; "difficoltà di accesso al servizio di assistenza"); un altro gestore riporta problemi legati alla lunghezza ed alla complessità delle procedure ("troppe informazioni richieste", "troppi diversi tipi di account e password"), di comprensione (talvolta anche dovuti alla scarsa conoscenza del servizio) e problemi tecnici (dal punto di vista della connessione, della compatibilità del sistema operativo o dello smartphone o di funzionalità del sito/app), anche se in alcuni casi sono percepiti come malfunzionamenti dell'identità SpID problemi tecnici dei dispositivi utilizzati dagli utenti o dovuti al fornitore di servizi (Service Provider SPID).

[24] La Convenzione che ciascun IdP stipula con AgID ai sensi dell'art. 10, comma 2 del DPCM 24 ottobre 2014 prevede che entro il 31 marzo di ciascun anno, il gestore predispone una relazione sui risultati conseguiti nel precedente esercizio; la relazione fornisce dati di riepilogo sui servizi, con indicatori di tipo quantitativo e qualitativo, con riferimento ad esempio ai volumi gestiti (identità rilasciate/revocate; richieste di assistenza attraverso il *Custome Care*), alle modalità di utilizzo del servizio (servizi più frequentemente acceduti), ai livelli di servizio eogati e ai risultati di periodiche valutazione degli utenti sulla qualità del servizio (indagini di *Customer Satisfaction*).

I dati di riepilogo periodici sono in fase di rivisitazione ed è prossima l'entrata in vigore di Linee Guida per sistematizzare le modalità di produzione ed invio.

Ulteriori indicatori riferiti al servizio SpID sono disponibili nell'apposita sezione del portale di avanzamento digitale (https://avanzamentodigitale.italia.it/it/progetto/spid).

4 PROCEDIMENTI DI VERIFICA NEL 2020

Le attività svolte nel 2020 hanno dovuto tenere conto delle esigenze e delle priorità connesse alla subentrata situazione di emergenza sanitaria, aspetti che hanno condizionato la pianificazione e la modalità di conduzione delle verifiche sui soggetti vigilati.

Con riferimento alla pianificazione, le verifiche inizialmente programmate tenendo conto degli indici di rischio dei soggetti vigilati ed estese alle quattro tipologie di servizi, dopo un regolare avvio nel primo bimestre 2020, hanno subito un fermo nel periodo marzo-aprile, a causa della sopravvenuta situazione di crisi pandemica; successivamente sono state rimodulate per tenere conto delle nuove priorità determinate dal particolare periodo. In considerazione, infatti, di un atteso aumento di transazioni on line a causa delle restrizioni sopravvenute, le verifiche hanno riguardato prevalentemente i gestori SpID e i QTSP, i cui servizi hanno un ruolo essenziale nell'erogazione/fruizione di servizi on-line, come peraltro dimostrato dall'aumento dei volumi e delle segnalazioni-utente che hanno interessato tali tipologie di gestori soprattutto nel secondo semestre 2020.

Le restrizioni sugli spostamenti in ambito nazionale hanno portato all'esecuzione di verifiche ispettive da remoto, con definizione delle relative procedure e revisione delle modalità di conduzione.

Come nell'anno precedente, anche nel 2020 le verifiche hanno visto l'apporto di competenze specialistiche dal Nucleo di Prevenzione delle Frodi Tecnologiche della Guardia di Finanza (nell'ambito dell'accordo stipulato a novembre 2018), dal Cert-AgID (https://cert-agid.gov.it), la struttura di AgID che da 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), ha sostituito il CERT-PA e da auditor specializzati di organismi di certificazione[25] per gli aspetti prevalentemente metodologici.

La partecipazione alle verifiche di analisti del CERT-AgID ha consentito di approfondire gli aspetti principalmente legati alle misure di sicurezza e ha fornito ai soggetti vigilati indicazioni rilevanti per migliorare le loro capacità di individuare vulnerabilità, prevenire attacchi e proteggere i sistemi.

4.1 Riepilogo delle verifiche

Nel corso del 2020, oltre alle verifiche svolte d'ufficio per tutti i soggetti sottoposti a funzioni di vigilanza, sono stati attivati **12 procedimenti di verifica,** dei quali 4 a seguito di segnalazione esterna e 8 nell'ambito di verifiche programmate. Inoltre 4 verifiche sono state svolte in presenza le altre 8 da remoto.

[25] Rina Services SpA e Bureau Veritas Italia SpA, aggiudicatari di una procedura di gara che ha portato nel 2019 alla stipula di due contratti per il supporto nella conduzione di verifiche ispettive svolte da AgID.

La diminuzione del numero di procedimenti rispetto all'anno precedente è da attribuire al blocco completo dell'attività di ispezione nel periodo marzo-aprile 2020, per la necessità di una riorganizzazione a seguito delle sopravvenute restrizioni.

Le verifiche che hanno comportato un maggior impegno sono certamente quelle in remoto. La conduzione degli audit a distanza ha comportato delle limitazioni per l'esecuzione di alcuni controlli, che sono significativi solo se eseguiti in presenza, come per esempio i controlli relativi alle misure di sicurezza fisica implementate nei CED. È stato invece possibile analizzare senza limitazioni rilevanti le componenti di servizio che riguardano ad esempio gli aspetti di processo e di gestione dei sistemi.

Come si rileva dal grafico, i 12 procedimenti hanno riguardato i QTSP (6), i gestori SpID (2), i gestori PEC (2), i Conservatori (2); i procedimenti relativi ai due Conservatori ed un procedimento relativo ad un gestore PEC, quest'ultimo conseguente ad una segnalazione, sono stati avviati con la programmazione ordinaria, nel primo periodo dell'anno; i procedimenti in ambito SpID e QTSP sono stati avviati a seguito della ripianificazione successiva al fermo delle attività ed hanno riguardato soggetti con un' utenza estremamente ampia,.

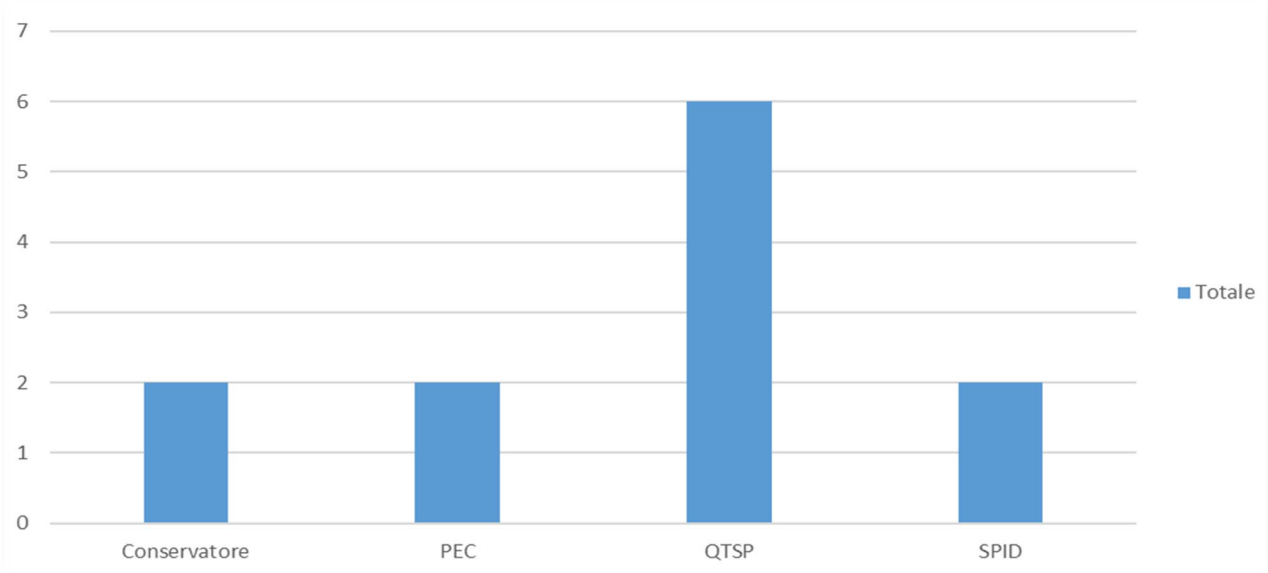

Fig. 4.1 – Procedimenti di verifica nel 2020 per elenco

Per i 6 procedimenti in ambito QTSP, 2 procedimenti sono stati avviati su segnalazione, 4 da programmazione. I 6 QTSP, in riferimento ai volumi, coprono il 40% dei certificati qualificati per firma con SC/Token, il 15% dei certificati di firma remota, quasi il 40% delle firme elettroniche qualificate ed il 30% circa delle marche temporali qualificate; con riferimento, invece, alle caratteristiche dell'utenza, 4 QTSP rilasciano firme solo ad una clientela predefinita e limitata ad una rete specifica di utenza; gli altri 2 QTSP rilasciano firme, sigilli, certificati e marche temporali sia a clientela business che a persone fisiche, coprendo insieme il 97% di certificati di firma remota e il 90% dei certificati di firma SmartCard/Token.

Per i 2 procedimenti in ambito PEC, 1 procedimento è stato avviato su segnalazione; 1 procedimento da programmazione..

Con riferimento all'ambito Conservazione, i 2 procedimenti avviati nel 2020 sono scaturiti dalle attività programmate (soggetti con profilo di rischio alto).

I 2 procedimenti in ambito SpID hanno riguardato lo stesso gestore e sono stati avviati rispettivamente da programmazione e a seguito di segnalazione. Con riferimento ai volumi, il gestore interessato copre più dell'80% delle identità complessivamente gestite al 31/12/2020.

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

- in 1 caso alla cessazione dell'attività per scelta del gestore, comunicata in fase di istruttoria;
- in 2 casi all'attivazione della fase sanzionatoria in entrambi i casi il procedimento era stato avviato su segnalazione.

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, finalizzate a certificare la conformità di un sistema di gestione ad una norma o ad uno standard internazionale, le verifiche svolte da AgID ai fini della vigilanza si configurano come verifiche di "seconda parte", sono in genere diverse l'una dall'altra e limitate ad aspetti specifici ("componenti del servizio"), in relazione agli obiettivi di ciascuna verifica (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, ecc.) 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 per singolo utente o azienda).

Le verifiche condotte nell’ambito dei 12 procedimenti hanno preso in esame alcune componenti, non necessariamente le stesse per le quattro tipologie di servizio. Alle componenti esaminate si riferiscono i rilievi indicati nel paragrafo che segue.

4.3 Riepilogo dei rilievi

Complessivamente sono stati formulati **60 rilievi**, distinti in 44 "Non Conformità" e 16 "Osservazioni”; quasi il 60% dei rilievi ha riguardato i QTSP, il 25% i Conservatori, il restante 15% è per 80% relativo ai gestori SpID e il resto ai gestori PEC.

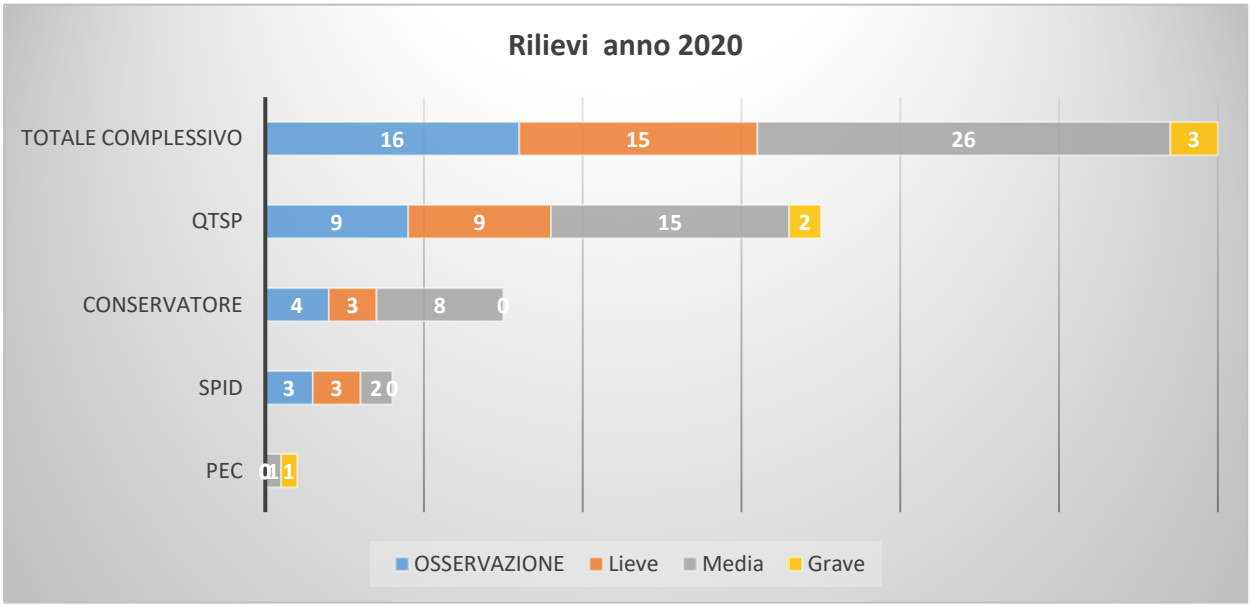

Fig. 4.2- Totale rilievi gestori per servizio

Tali dati si riferiscono alla totalità dei procedimenti sopra indicati, con esclusione di un procedimento per il quale il gestore ha comunicato la cessazione e nell'ambito dei quali non sono stati quindi formulati rilievi.

Servizi / Classificazione	Conservazione	PEC	QTS	SPID
Grave	0	1	2	0
Lieve	3	0	9	3
Media	8	1	15	2
Osservazione	4	0	9	3

Tab.4.1 - Distribuzione dei rilievi per servizio

I rilievi sono stati formulati rispetto alle componenti di servizio esaminate nell'ambito dei procedimenti. Le tabelle ed il grafico che seguono mostrano la distribuzione dei rilievi per servizio e per le specifiche componenti del servizio a cui sono riferiti.

Componenti di servizio	Grave	Lieve	Media	OSS.	Totale
Analisi dei rischi e VA/PT		2	5	4	11
Gestione terze parti	2	3	4	1	10
Gestione del processo	1		4	3	8
Politiche e procedure di sicurezza		2	2	3	7
Documentazione di riscontro		2	4	1	7
Piano di cessazione		3	1	1	5
Organizzazione		1	2		3
Gestione degli incidenti		1	1	1	3
Formazione			3		3
Commercializzazione dei servizi		1			1
Gestione delle segnalazioni				1	1
Log				1	1
Totale complessivo	**3**	**15**	**26**	**16**	**60**

Tab.4.2 - Distribuzione dei rilievi per classificazione e componenti di servizio

Componenti di Servizio	Conserv.	PEC	QTSP	SPID	Totale
Analisi dei rischi e VA/PT	3		5	3	11
Gestione terze parti	2		8		10
Gestione del processo		1	6	1	8
Politiche e procedure di sicurezza	3		4		7
Documentazione di riscontro	2		3	2	7
Piano di cessazione	2		2	1	5
Organizzazione	2		1		3
Gestione degli incidenti	1		1	1	3
Formazione		1	2		3
Commercializzazione dei servizi			1		1
Gestione delle segnalazioni			1		1
Log			1		1
Totale complessivo	**15**	**2**	**35**	**8**	**60**

Tab.4.3 - Distribuzione dei rilievi per servizio e componenti

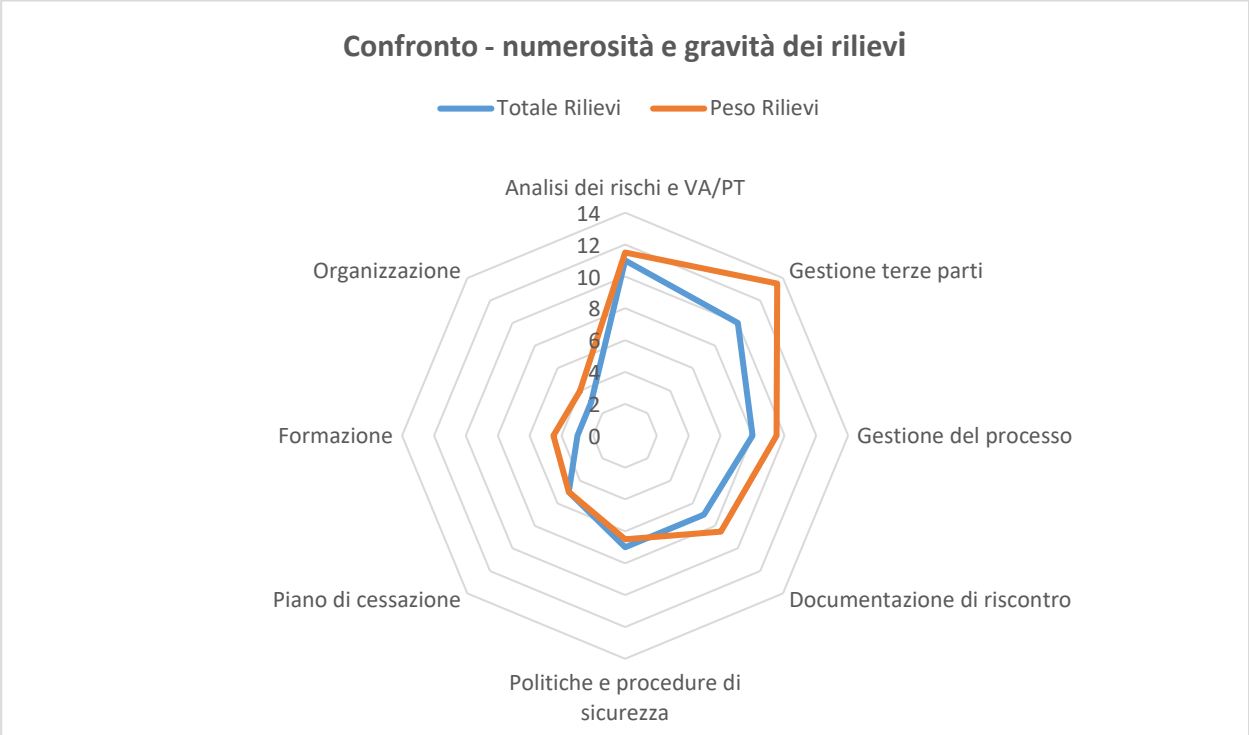

Fig. 4.3 – Top 8 componenti di servizio affette da rilievi in confronto con la gravità dei rilievi

In particolare nella Fig.4.4 sono evidenziate le componenti per le quali, limitatamente agli aspetti esaminati, è risultato più frequente rilevare una Non Conformità o una Osservazione. È fatto un raffronto anche con la gravità dei rilievi.

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.

Il grafo mostra che per le componenti di servizio come ad esempio “Politiche e procedure di sicurezza” o “Analisi dei rischi e VA/PT”, sono stati formulati rilievi prevalentemente con classificazione lieve, mentre ad esempio la componente di “Gestione delle terze parti” è stata affetta da rilievi con classificazionedi gravità più elevata. In sintesi, l’area all’interno della spezzata in rosso (indicativa del livello di gravità dei rilievi) maggiore rispetto all’area sottesa dalla spezzata in blu (indicativa semplicementei del numero dei rilievi), e più in generale le differenze tra le due aree, mettono in evidenza quali componenti di servizio, limitatamente alle verifiche condotte ed agli aspetti esaminate,sono risultate più critiche. Le stesse note di lettura si applicano per le figure che seguono.

Nel seguito vengono messi a confronto i risultati dei sei procedimenti avviati per i QTSP; anche se ogni procedimento è sempre differente da un altro in quanto non sempre sono verificate le stesse componenti di servizio o eseguite identiche verifiche per una stessa componente, la raffigurazione che segue è comunque utile per avere un confronto tra i gestori.

Come si vede in nessun caso le aree blu sono più grandi delle aree rosse. In un paio di casi risultano paragonabili. Essenzialmente ciò che va ancora una volta evidenziato è l’esigenza di entrare nel merito dei processi di gestione del servizio, esaminando nel dettaglio ogni singolo aspetto.

Fig.4.7 – Confronto tra 6 QTSP per profilo di qualità (in base ai rilievi)

4.4 Analisi dei rilievi più ricorrenti

Merita un breve approfondimento il tema delle tipologie dei rilievi riferiti alle componenti di servizio esaminate nell'ambito dei 12 procedimenti sintetizzati nelle Tab.4.2 e Tab.4.3.

Come si vede, alle prime tre componenti di servizio con il più alto numero di rilievi fa riferimento quasi la metà dei rilievi complessivamente riscontrati; mentre alle prime sei (pari alla metà delle componenti esaminate) è riferibile circa l'80% dei rilievi. Informazioni interessanti si rilevano dall'analisi delle singole non conformità o osservazioni.

Per la componente di servizio **Analisi dei rischi e VA/PT,** i rilievi riguardano le attività di Vulnerability Assessment e Penetration Test. I gestori eseguono con periodicità più o meno definite questi controlli di sicurezza; tuttavia dalle evidenze acquisite durante le verifiche si rileva che frequentemente gli esiti di un VA/PT sono sottovalutati, determinando una reazione non sempre adeguata , spesso accompagnata da ulteriori aspetti che compromettono un efficace trattamento delle vulnerabilità riscontrate: problemi di natura organizzativa; mancato o incompleto tracciamento delle azioni di risoluzione; non corretta valutazione dei livelli di gravità in funzione del rischio e, in alcuni casi, assenza totale di azioni di trattamento. Talvolta, soprattutto nei casi in cui il gestore è una realtà di piccole dimensioni, l'azione di VA/PT viene limitata al solo ambito di servizio pur se l'infrastruttura tecnologica è utilizzata anche per altri servizi, riducendone così l'efficacia.

Anche esaminando la componente di **Gestione delle Terze Parti** emergono situazioni confrontabili. Irilievi formulati su tale componente riguardano in gran parte l'assenza di piani di audit o la loro mancata/inadeguata esecuzione. Generalmente i gestori assumono che i vincoli contrattuali siano sufficienti affinchè una terza parte operi nel rispetto delle procedure definite per l'erogazione del servizio. Tuttavia, come emerso in sede ispettiva, questo non avviene se l'accordo non definisce compiutamente gli obblighi e le responsabilità tra le parti. In ogni caso, quando specifiche componenti del servizio sono delegate a terzi, è evidente la necessità che il gestore svolga audit periodici per verificare che siano rispettate le condizioni di erogazione del servizio. Ulteriori casi, sebbene non strettamente legati agli audit, riguardano il mancato controllo del gestore sui prodotti forniti dalla terza parte in esecuzione dell'accordo contrattuale o delle procedure condivise. Dalle verifiche sono emerse spesso incongruenze rispetto alla documentazione di riscontro o alle procedure previste, non rilevate dal gestore.

Sulla **Gestione del Processo,** si sono rilevate situazioni diverse, spesso dipendenti dalla differente natura del servizio (conservazione a norma, Posta elettronica certificata, Firma qualificata e Identità digitale spid). Particolarmente rilevanti i sono stati i controlli volti a verificare il processo di rilascio di certificati qualificati di firme digitali e di identità digitali svolto attraverso terze parti operanti nel ruolo di Registration Authority ("RA"). Per l'ambito dei servizi fiduciari in particolare, diversi rilievi hanno riguardato la mancata o non adeguata attuazione di azioni volte a verificare la disponibilità di contatti (e-mail/numero di telefono) univocamente riconducibile ai titolari di certificati qualificati. È bene notare come questi aspetti di processo siano molto correlati con la gestione delle terze parti

dal momento che la registrazione dei dati dei soggetti che richiedono un certificato qualificato di firma digitale, tra i quali ad esempio le informazioni di contatto dei clienti, vengono raccolte in sede di sottoscrizione dei contratti di servizio, tipicamente presso le RA. Si è frequentemente rilevato, ad esempio, che un operatore incaricato dell'identificazione e registrazione del richiedente ("RAO" o "IR",), , assecondando la richiesta del cliente, faccia uso del proprio numero di telefono e/o indirizzo email oppure inserisca i dati di contatto di un professionista (ad esempio commercialista) indicato dal cliente. Si tratta di comportamenti che, seppur comprensibili nella logica di orientamento alla clientela, sono assolutamente da evitare perché possono far configurare situazioni anomale .

Per quanto riguarda le **Politiche e procedure di sicurezza**, i principali temi che si evidenziano riguardano le procedure di gestione delle password e le policy sugli accessi ai locali aziendali o alle sale CED.

Sulla **Documentazione di Riscontro** (Manuali operativi, Certification Practice Statement, Piani di Sicurezza, etc) si è rilevato frequentemente che tali documenti non sono allineati alla situazione in esercizio, verificata in sede di ispezione.

5 SEGNALAZIONI DI INCIDENTI E MALFUNZIONAMENTI

I soggetti vigilati sono tenuti a segnalare ad AgID e, quando ne ricorrano le circostanze[26] alle altre autorità preposte, gli incidenti di sicurezza o gli eventi che si configurino come malfunzionamenti o interruzioni di servizio.

Nel corso del 2020 sono stati notificati complessivamente 45 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.

Salta all'occhio il picco della settimana 43 (2/11-8-/11) legato all'evento ClickDay Mobilità.

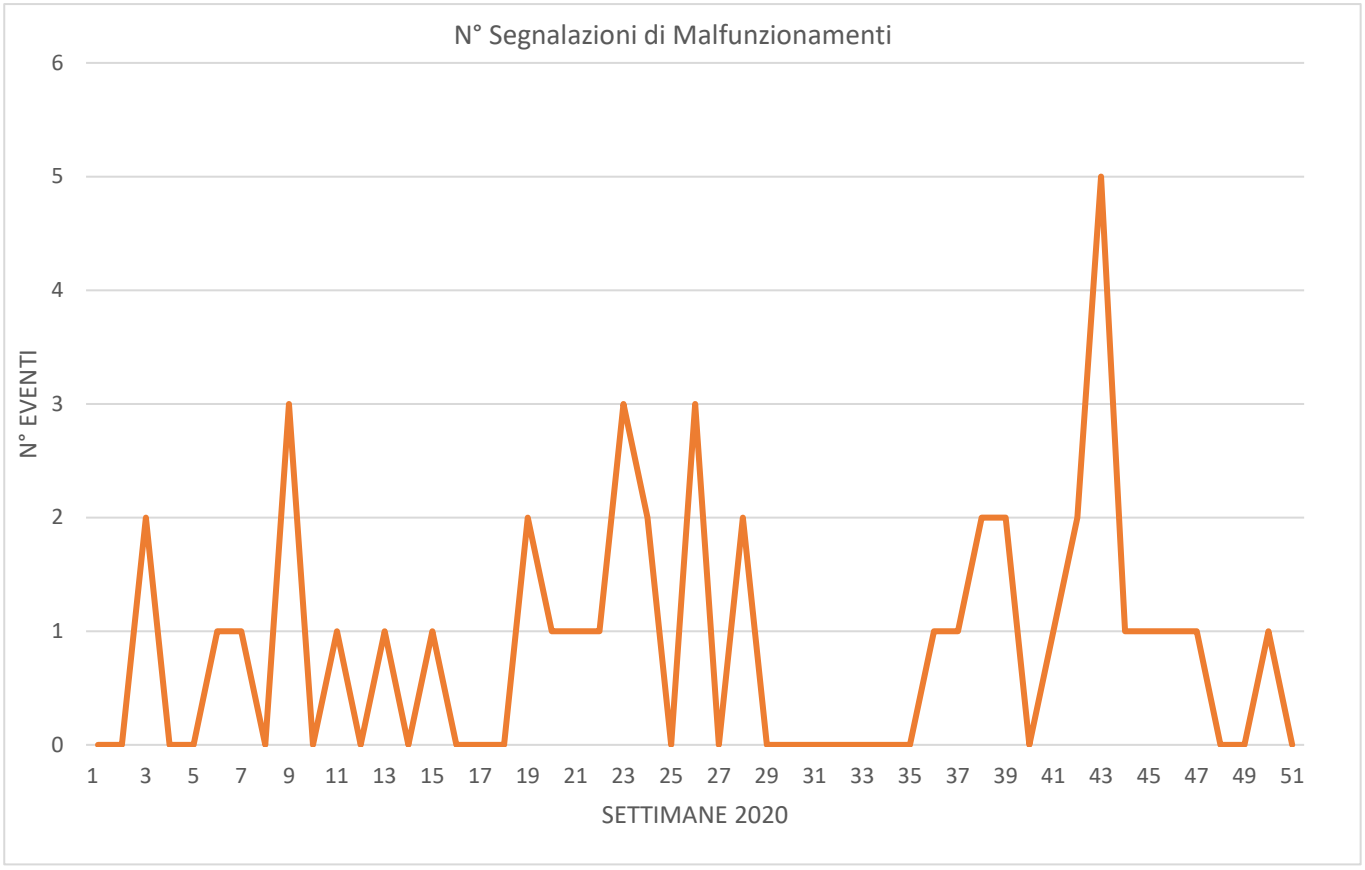

Fig. 4.1 – Incidenti e malfunzionamenti segnalati nel corso del 2020

Nella seguente tabella sono mostrati i totali, ovvero i gestori che hanno effettuato segnalazioni di incidenti o malfunzionamento.

[26] 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.

Come si può notare prendendo come riferimento l'ultima colonna, 117 gestori su 134 non ha mai effettuato una segnalazione. Il dato più rilevante è quanto accade per i Cnservatori: 81su 85 non hanno effettuato alcuna segnalazione.

Segnalazioni	Conservazione	PEC	QTSP	SpID	Totale Gestori
0	**81**	14	**19**	**3**	**117**
1	3	2	0	2	7
2	1	1	3	2	7
3	0	0	0	1	1
4	0	1	0	0	1
17	0	0	0	1	1
Totale Gestori	**85**	**18**	**22**	**9**	**134**

Tab.5.1 – Segnalazioni rispetto al totale dei gestori

Nella successiva figura è stata eseguita una valutazione della distribuzione dei tempi di rientro ovvero la distribuzione della durata del disservizio. Viene mostrata la numerosità degli eventi rientrati rispetto al tempo trascorso dall'inizio del disservizio. Le etichette mostrano l'ora e la numerosità di eventi risolti in quell'ora. Pertanto per comprendere quanti eventi sono stati risolti nelle prime 4 ore occorre sommare il dato con etichetta da 1 a 4 (intervallo orario), in questo caso 10, 6, 3 e 6, per un totale di 25. Quindi oltre la metà degli eventi ha avuto positiva risoluzione entro le 4 ore.

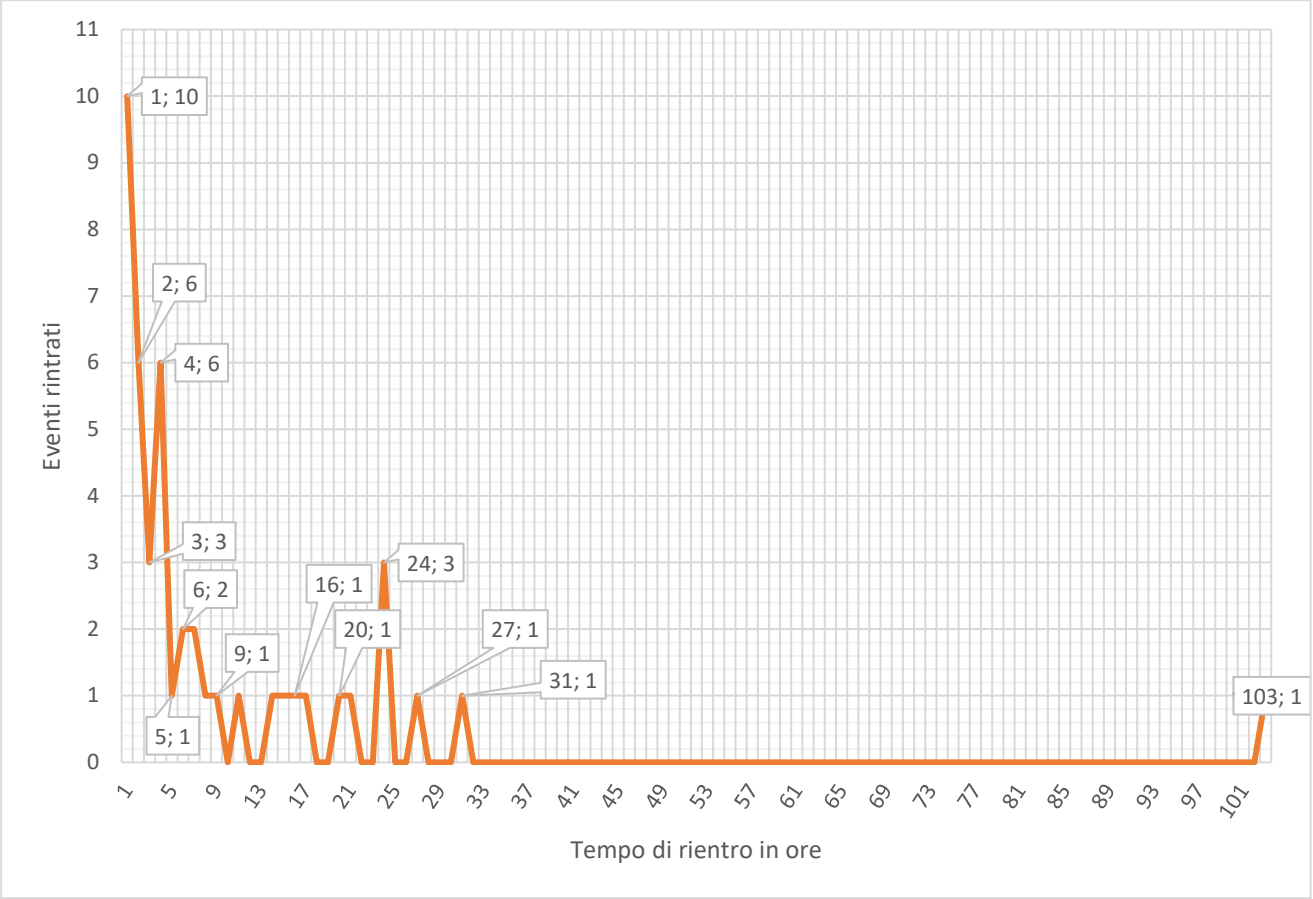

Fig. 5.25 – Distribuzione degli eventi rispetto alla durata del disservizio nel corso del 2020

Da questa ultima considerazione segue il grafico successivo dove è stata eseguita una valutazione del tasso di rientro dei malfunzionamenti. Nella seguente figura 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. Facendo riferimento a quanto detto prima, ovvero che nelle prime 4 ore più del 50% dei problemi riscontrati dai gestori è stato risolto, la figura mostra che dopo 3,67h ovvero 3h 40' si sono chiusi 23 dei 46 malfunzionamenti segnalati. Inoltre il punto con etichetta 2 mostra che quasi l'80% degli incidenti è stato risolto in circa 14 ore. L'etichetta 4 mostra che nel 95% dei casi l'incidente è stato risolto entro le 24 ore. In linea con quanto verificato lo scorso anno.

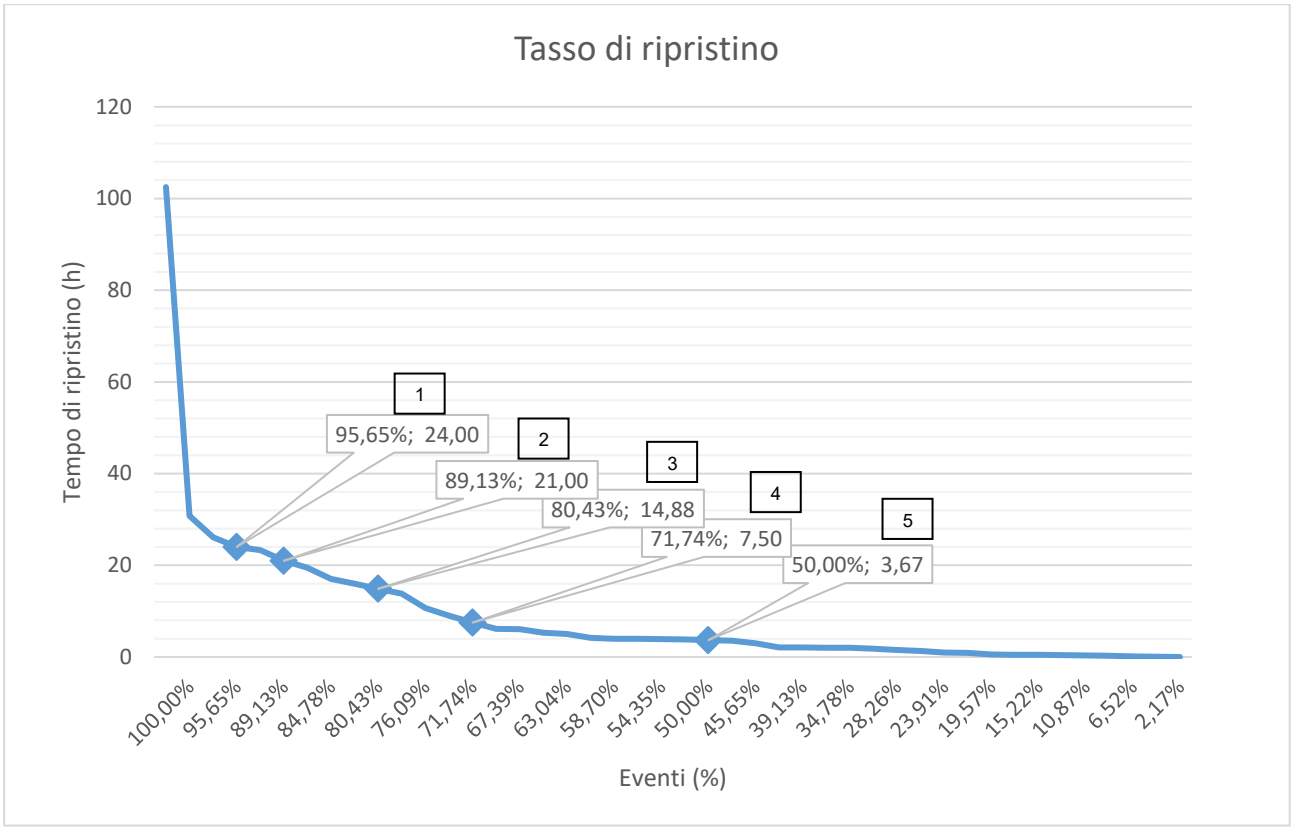

Fig. 5.3 – Tasso di ripristino degli eventi rispetto alla durata nel corso del 2020

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.

La nota di segnalazione 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 2020 le segnalazioni gestite dal servizio Vigilanza sono state 55, delle quali: 6 hanno dato luogo all'avvio di 4 procedimenti di verifica (2 segnalazioni sono confluite in uno stesso procedimento); 27 sono relative ai ritardi dell'autenticazione SPID per il ClickDay del Bonus Mobilità; le rimanenti sono state risolte attraverso interlocuzioni con l'utente o con il gestore.

La tabella che segue mostra la distribuzione delle segnalazioni per servizio

Conservazione	PEC	SpID	QTS	Totale
0	5	45	5	55

Tab. 6.1- Segnalazioni utente per servizio

Le segnalazioni pervenute per ciascun servizio fanno riferimento a diverse problematiche (sono escluse le segnalazioni del ClickDay Mobilità).

Tipo di Segnalazione	PEC	SpID	QTS	Totale
Problemi di accesso e/o di autenticazione		5		5
Problemi connessi al rilascio dell'identità SPID		10		10
Problemi su invio/ricezione messaggi/notifiche del servizio PEC	2			2
Problematiche inerenti la cancellazione di una o più caselle PEC	3			3
Impossibilità di firmare un documento con il dispositivo di firma			2	2
Furto di identità			2	2
Richieste per indagini di PG o da altre Autorità		5	1	6

Tab. 6.2- Segnalazioni per tipologia

7 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[27], 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.

Il quadro per la segnalazione degli incidenti ai sensi dell'articolo 19 è stato preparato da ENISA in consultazione con i membri del gruppo di esperti e rivisto anche dal settore privato e dal Forum delle autorità europee di vigilanza per le firme elettroniche (FESA) L'ENISA ha sviluppato uno strumento in linea (CIRAS-T), ad uso degli organismi di vigilanza degli Stati Membri, per facilitare la procedura di notifica degli incidenti con impatto transfrontaliero.

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. Nel corso del 2020, a causa delle restrizioni dovute all'emergenza Covid, i due incontri si sono svolti da remoto, in modalità videoconferenza.

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

[27] 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.

8 LE SANZIONI

Il CAD[28] definisce i casi per i quali possono essere irrogate sanzioni amministrative.

Nel 2020 **sono stati istruiti 2 procedimenti in fase sanzionatoria,** dei quali uno in ambito PEC e l'altro in ambito QTSP, entrambi avviati a seguito di segnalazioni pervenute da utenti. Uno dei due procedimenti si è concluso nel 2020.

Le irregolarità riscontrate 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;
- le modalità definite per l'identificazione dei richiedenti certificati di firma attraverso terze parti e l'utilizzo di subcontraenti che operavano disattendendo le specifiche procedure per l'identificazione e registrazione dei richiedenti, o che non erano adeguatamente formati su tali temi specifici.

Nel corso del 2020 **è stata inoltre completata l'istruttoria per 4 procedimenti 2019** (2 in ambito PEC, 1 in ambito QTSP e 1 in ambito conservazione) per i quali era stata avviata la fase sanzionatoria.

Dei 6 procedimenti in fase sanzionatoria nel 2020, 4 si sono conclusi a seguito della positiva verifica che le irregolarità accertate fossero state correttamente indirizzate e dell'avvenuto pagamento (in 3 casi in oblazione) delle sanzioni pecuniarie irrogate per le violazioni contestate, per un ammontare complessivo di circa 540.000,00 Euro, di cui circa 420.000,00 in oblazione.

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

[28] Art. 32-bis

9 AZIONI SCATURITE DALLE VERIFICHE E PROSSIME ATTIVITÀ

I procedimenti di verifica comportano l'adozione da parte dei gestori di azioni correttive o di miglioramento.

Quando nel corso di un procedimento sono rilevate criticità che possono riguardare più soggetti vigilati, sono richiesti specifici controlli o avviate iniziative che coinvolgono tutti i gestori.

Con riferimento all'ambito PEC, già nel 2019, sulla base dei risultati emersi dai procedimenti di vigilanza attivati nell'anno e correlati alle frequenti campagne di diffusione di malware attraverso messaggi PEC, il CERT-AgID ha emesso indicazioni ai gestori per il rafforzamento delle misure minime di sicurezza, integrando e ampliando le proposte formulate dagli stessi gestori, che prevedevano un insieme di interventi da attuare rispettivamente nel breve, medio e lungo termine.

Nel 2020 sono stati completati gli interventi pianificati nel breve termine[29]; sono proseguite le attività per gli interventi nel medio e lungo termine[30], che si prevede di concludere entro il 2021.

Per quanto riguarda i prestatori di servizi fiduciari qualificati, i procedimenti avviati nel 2020 hanno preso in esame gli esti dei controlli richiesti nel corso del 2019 e le misure conseguentemente adottate per verificare/sanare anomalie nei processi di identificazione dei richiedenti e registrazione dei dati dei titolari di certificati qualificati di firma digitale svolti attraverso terze parti (Registration Authority ("RA") [31]. Sono state sollecitate anche azioni da parte dei gestori volte a verificare l'avvenuta adeguata formazione del personale delle RA che opera in qualità di incaricato alla registrazione, in riferimento alle tematiche specifiche del riconoscimento ed alle relative responsabilità, nonchè alle specifiche procedure definite dal gestore per l'identificazione certa del richiedente un certificato di firma elettronica qualificata.

Nel corso delle attività svolte nel 2020 le suddette indicazioni e verifiche sono state estese ai gestori SpID che si avvalgono di terze parti nel ruolo di RA. Ulteriori iniziative vedono coinvolti il Cert-AgID e i gestori che erogano servizi SpID e di firma digitale e sono volte a **contrastare fenomeni sempre più frequenti di furti di identità** e di utilizzo di tali servizi a scopo fraudolento. In base alle segnalazioni degli utenti che nel 2020 hanno dato luogo all'avvio di procedimenti ed alle richieste pervenute ai fini di indagini di polizia giudiziaria, i furti di identità sono perpetrati per operazioni specifiche (es. accesso ai bonus di iniziativa governativa[32]; accensione di conti correnti on-line; richiesta di finanziamenti o di prestiti). Un'identità SpID e una firma digitale basata su un certificato

[29] Ad esempio: coondivisione di URL malevoli; utilizzo parallelo di diverse tecnologie antivirus; ecc.

[30] Ad esempio; implementazione di servizi per la condivisione di indicatori di compromissione ("IoC") per campagne malevole attraverso PEC; condivisione di una piattaforma di blocklist per i nomi di caselle e domini, con funzioni di alerting in caso di registrazioe di utenze riservate; attivazione di sistemai di autenticazione a due fattori; ecc.

[31] Registration Authority: soggetti cui un gestore, nel suo ruolo di Certification Authority, conferisce specifico mandato con rappresentanza con il quale affida lo svolgimento di una o più attività proprie del processo di registrazione, come ad esempio: l'identificazione del richiedente; la registrazione dei dati; l'inoltro dei dati ai sistemi del gestore; la raccolta della richiesta del certificato qualificato o dell'identità digitale.

[32]Es. bonus vacanze; bonus 18app.

qualificato sono entrambi strumenti di identificazione ed hanno uguale rilevanza negli scenari di utilizzo sopra richiamati: una firma digitale può essere ottenuta anche utilizzando lo SPID come sistema di riconoscimento e, viceversa, è possibile ottenere un'identità digitale disponendo di una firma digitale. La condivizione di piattaforme e di informazioni tra i gestori è importante per mettere a fattor comune indicatori/notizie su casi anomali di rilascio di identità SpID o di firme digitale. Parallellemente, è necessario che le terze parti e gli incaricati al riconoscimento che operano per conto dei gestori acquisiscano una maggiore consapevolezza sulle responsabilità civili e penali nelle quali incorrono in caso di violazione degli obblighi previsti per il rilascio dell'identità digitale e dei certificati qualificati di firma digitale, risultando in particolare necessaria l'adozione di ogni misura idonea per l'identificazione certa del richiedente.

10 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