CORTE DEI CONTI

SEZIONE CENTRALE DI CONTROLLO
SULLA GESTIONE DELLE AMMINISTRAZIONI DELLO STATO

AGENZIA DELLA CYBERSECURITY NAZIONALE

Deliberazione 05 febbraio 2025, n. 8/2025/G

CORTE DEI CONTI

SEZIONE CENTRALE DI CONTROLLO
SULLA GESTIONE DELLE AMMINISTRAZIONI DELLO STATO

AGENZIA DELLA CYBERSECURITY NAZIONALE

Relatore
Pres. Mauro Orefice

Hanno collaborato
per l'istruttoria e l'elaborazione dei dati: dr.ssa Miriam Pane

SOMMARIO

DELIBERAZIONE

CORTE DEI CONTI

SEZIONE CENTRALE DI CONTROLLO SULLA GESTIONE DELLE AMMINISTRAZIONI DELLO STATO

II Collegio

Camera di consiglio del 3 febbraio 2025

Presieduta dal Presidente Mauro Orefice

Composta dai magistrati:

Presidente della Sezione: Mauro OREFICE
Consiglieri: Paola COSA, Carlo PICUNO, Natale Maria Alfonso D'AMICO, Michele SCARPA, Gerardo de MARCO, Paolo ROMANO, Maria Rita MICCI, Giuseppina VECCIA, Daniela ALBERGHINI
Primi Referendari: Paola LO GIUDICE, Salvatore GRASSO, Simonetta INGROSSO
Referendari: David DI MEO

* * *

Visto l'art. 100, comma 2, Cost.;

vista la legge 14 gennaio 1994, n. 20 e, in particolare, l'art. 3, comma 4, ai sensi del quale la Corte dei conti svolge il controllo sulla gestione delle amministrazioni pubbliche verificando la corrispondenza dei risultati dell'attività amministrativa agli obiettivi stabiliti dalla legge e valutando comparativamente costi, modi e tempi dello svolgimento dell'azione amministrativa;

visto l'art. 7, c. 7, d.l. 31 maggio 2021, n. 77, convertito dalla l. 29 luglio 2021, n. 108, in base al quale "*la Corte dei conti esercita il controllo sulla gestione di cui all'art. 3, c. 4, l. 14 gennaio 1994, n. 20, svolgendo in particolare valutazioni di economicità, efficienza ed efficacia circa l'acquisizione e l'impiego delle risorse finanziarie provenienti dai fondi di cui al PNRR*";

vista la deliberazione della Sezione 1° marzo 2022, n. 3/2022/G, con la quale è stato approvato il documento concernente il "Quadro programmatico dei controlli sulla gestione delle Amministrazioni dello Stato per l'anno 2022 e nel contesto triennale 2022-2024";

visto il rapporto, presentato dal Presidente Mauro Orefice, che illustra gli esiti dell'intervento PNRR al 31 dicembre 2024 avente a oggetto "*Agenzia della Cybersecurity nazionale*";

visto il decreto n. 2/2020 e successive integrazioni e modificazioni del Presidente della Sezione con cui i Magistrati assegnati alla Sezione medesima sono stati ripartiti tra i diversi collegi;

visto il decreto n. 1/2025 con cui i Magistrati sono assegnati a tutti i collegi;

vista l'ordinanza n. 2/2025 prot. n. 223 del 20 gennaio 2025, con la quale il Presidente della Sezione ha convocato il II Collegio per la Camera di consiglio del 3 febbraio 2025, al fine della pronuncia sulla gestione in argomento;

udito il relatore, Presidente Mauro Orefice;

DELIBERA

di approvare, con le indicazioni formulate in sede di Camera di consiglio, il rapporto avente a oggetto "*Agenzia della Cybersecurity nazionale*".

La presente deliberazione e l'unito rapporto saranno inviati, a cura della Segreteria della Sezione, alla Presidenza del Senato della Repubblica e alla Presidenza della Camera dei deputati, alla Presidenza del Consiglio dei ministri, alla Presidenza della Commissione Bilancio del Senato della Repubblica, alla Presidenza della Commissione Bilancio della Camera dei deputati, al Ministro dell'economia e delle finanze, nonché alle seguenti amministrazioni:

- Presidenza del Consiglio dei Ministri:

Segretariato Generale;
Segreteria tecnica del PNRR;
Dipartimento per la trasformazione digitale;

- Ministero dell'economia e delle finanze:

Ufficio di Gabinetto del Ministro;
Servizio centrale per il PNRR;
Dipartimento della Ragioneria Generale dello Stato;

- AGID:

Direzione generale.

Le amministrazioni interessate comunicheranno alla Corte e al Parlamento, entro quattro mesi dalla data di ricevimento del presente rapporto, le misure consequenziali adottate ai sensi dell'art. 3, c. 6, l. 14 gennaio 1994, n. 20, come modificato dall'art. 1, c. 172, l. 23 dicembre 2005, n. 266 (legge finanziaria 2006).

Le medesime, ove ritengano di non ottemperare ai rilievi formulati, adotteranno, entro trenta giorni dalla ricezione del presente rapporto, l'eventuale provvedimento motivato previsto dall'art. 3, c. 64, l. 24 dicembre 2007, n. 244.

La presente deliberazione è soggetta a obbligo di pubblicazione, ai sensi dell'art. 31 d.lgs. 14 marzo 2013, n. 33 (concernente il "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni").

Il presente rapporto è inviato, altresì, alle Sezioni Riunite in sede di controllo.

Il Presidente relatore
Mauro Orefice
f.to digitalmente

Depositata in segreteria il 05 febbraio 2025

Il Dirigente
Dott.ssa Anna Maria Guidi
f.to digitalmente

RAPPORTO

AGENZIA DELLA CYBERSECURITY NAZIONALE

Sommario: 1. Premesse. – 2. Deliberazione della sezione centrale di controllo sulla gestione n. 17, del 6 febbraio 2024. – 3. Novità nell'ambito del quadro normativo di riferimento. – 4. Cronoprogramma. - 5. Budget economico per l'anno 2025. - 6. Quadro contabile. – 7. Stato di avanzamento dei milestone e target relativi all'Investimento in esame in relazione alla sua pianificazione per l'anno 2024. - 8. Relazione annuale al Parlamento 2023. – 9. Stato di avanzamento dei progetti. – 10. Monitoraggio effettuato dall'Agenzia per la Cybersicurezza sulle attività di attuazione degli interventi da parte delle pubbliche amministrazioni, quali soggetti sub-attuatori, nonché le eventuali criticità riscontrate da parte delle stesse Amministrazioni. - 11. Conclusioni.

1. Premesse

La Sezione centrale di controllo sulla gestione delle Amministrazioni dello Stato con deliberazioni n. 31 del 14 luglio 2022, n. 5 del 9 febbraio 2023 e n. 17 del 6 febbraio 2024, ha esercitato la sua funzione di controllo sull'investimento in esame, ai sensi dell'art. 7, comma 7 del decreto-legge n. 77, del 31 maggio 2021, convertito dalla legge 29 luglio 2021, n. 108.

Il Report di che trattasi mira a fornire un aggiornamento delle attività svolte dall'Agenzia nel corso dell'anno 2024, in continuità con il processo di maturazione intrapreso dalla stessa Agenzia ai fini del raggiungimento degli obiettivi sottesi a tale investimento volti alla tutela degli interessi nazionali nel campo della cybersicurezza.

Come già profusamente rappresentato nelle delibere di cui sopra, l'Agenzia per la cybersicurezza nazionale (ACN) è l'Autorità nazionale per la cybersicurezza, istituita ai sensi del decreto-legge n. 82 del 14 giugno 2021, che ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

L'Agenzia, tra le sue varie attribuzioni, svolge il compito di garantire la sicurezza e la resilienza nello spazio cibernetico, nonché di prevenire e mitigare il maggior numero di attacchi cibernetici e di favorire il raggiungimento dell'autonomia tecnologica.

Tra i fondamentali compiti espletati dall'Agenzia si deve ricordare quello afferente all'attuazione della Strategia Nazionale di Cybersicurezza, adottata dal Presidente del

Consiglio, che contiene gli obiettivi da perseguire entro il 2026.

L'investimento, inoltre, ha l'obiettivo di rafforzare l'ecosistema digitale nazionale potenziando in maniera molto significativa le capacità di monitoraggio, prevenzione e risposta a rischi ed eventi cyber grazie a una rete di servizi cyber nazionali, opportunamente integrata con i principali partner pubblici e privati.

La misura, appare utile ricordare, prevede lo sviluppo di un sistema all'avanguardia che interconnetta strettamente, a livello nazionale e internazionale, il mondo delle Pubbliche Amministrazioni, dell'impresa e dei fornitori di tecnologia. L'investimento, dunque, è articolato in tre pilastri:

- fortificare le capacità di cyber resilience in modo diffuso nel Paese, favorendo sinergie e interconnessione delle capacità di monitoraggio, condivisione di informazioni e risposta agli eventi di natura cyber;
- potenziare le capacità nazionali di scrutinio e certificazione tecnologica al fine di valutare e certificare beni, sistemi e servizi ICT, nell'ambito dell'attivazione del Centro di Valutazione e Certificazione Nazionale (CVCN) presso l'ACN;
- potenziare le capacità cyber delle Pubbliche Amministrazioni per la messa in sicurezza dei dati e dei servizi dei cittadini.

Al vertice dell'Agenzia è posto come Direttore generale il Prefetto Bruno Frattasi, nominato con decreto del Presidente del Consiglio dei ministri del 10 marzo 2023, mentre il Vice-Direttore Generale dell'Agenzia, Nunzia Ciardi, svolge le sue funzioni di ausilio dal 16 settembre 2021.

2. Deliberazione della sezione centrale di controllo sulla gestione n. 17, del 6 febbraio 2024.

Con l'ultima deliberazione n. 17, del 6 febbraio 2024, questa Corte si era espressa in merito alle attività espletate dall'Agenzia per l'anno 2023, mettendo in evidenza i significativi risultati conseguiti volti a contribuire in modo rilevante nell'opera di potenziamento cyber del sistema Paese, per far fronte alle sfide del mondo digitale rispetto ai tre obiettivi fondamentali di protezione, risposta e sviluppo digitale del Paese, sottesi alla Strategia nazionale di cybersicurezza 2022-2026.

In tale sede, altresì, è stato posto l'accento sul dialogo costante intrapreso dall'Agenzia con le Amministrazioni che compongono l'architettura nazionale, incoraggiando la creazione di una rete di collaborazione interistituzionale e promuovendo un confronto continuo con il settore privato, la nuova imprenditorialità e il mondo accademico e della ricerca.

Tale approccio ha permesso di lavorare in sinergia con le omologhe organizzazioni internazionali europee, partner internazionali e Paesi like-minded, al fine di promuovere lo scambio informativo e la cooperazione, sia a livello strategico che in ambito tecnico, per far fronte al complesso fenomeno della minaccia cibernetica, in particolare con riferimento all'attuale quadro geopolitico.

La Sezione ha messo in rilievo che nell'ambito degli interventi sottesi all'investimento in esame, nell'arco di tempo preso in considerazione, non tutte le risorse disponibili risultavano impiegate nell'ambito delle finalità proprie dell'Agenzia, in considerazione anche del fatto che i progetti in esame spaziano sull'intero arco di vigenza del Piano, con scadenze ricadenti anche negli anni 2024/2026.

In ultimo, dall'approfondita disamina da parte di questa Corte sull'intera attività svolta dall'Agenzia per la cybersicurezza non sono emerse difficoltà sostanziali e criticità nel raggiungimento dei relativi obiettivi. È stato evidenziato, tuttavia, che una valutazione di merito sulla efficacia complessiva dell'attività in corso potrà essere effettuata solamente una volta ricomposto il quadro dei numerosi progetti previsti ed in fase di realizzazione, motivo per cui è proseguita l'attività di monitoraggio dell'intero complesso degli interventi e delle interazioni da essi determinate.

3. Novità nell'ambito del quadro normativo di riferimento.

Tra le novità più rilevanti nel panorama normativo in materia di cybersicurezza, nell'arco di tempo preso in considerazione, si devono necessariamente citare sia la legge n. 90 del 2024 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", che il decreto legislativo del 4 settembre 2024, n. 138 recante il «Recepimento della direttiva (UE) 2022/2555". Il primo provvedimento contiene importanti adempimenti per le pubbliche amministrazioni rientranti nel suo

perimetro di applicazione e risponde alla ratio di rafforzare la sensibilità e la protezione dei predetti soggetti sui rischi informatici aventi impatto su reti, sistemi informativi e servizi informatici, mentre il decreto legislativo n. 138 attiene alle misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 ed abroga la direttiva (UE) 2016/1148.

Nello specifico, la legge, n. 90 del 2024, entrata in vigore il 17 luglio, risulta composta da due Capi distinti, di estremo rilievo sia per quanto concerne la sicurezza dei sistemi informativi, sia perché sono volti al miglioramento degli standard di protezione dei sistemi informatici e informativi e per chi si occupa di individuare le relative misure tecniche ed organizzative che devono essere osservate dai diversi attori coinvolti nei processi di trattamento dei dati di carattere personale.

Il Capo I, in particolare, concerne le disposizioni in materia di rafforzamento della cybersicurezza nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario, di personale e funzionamento dell'Agenzia per la cybersicurezza nazionale e degli organismi di informazione per la sicurezza, nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici.

Il Capo II della legge in esame, invece, apporta delle modifiche al Codice Penale e, in particolare, alle previgenti norme in materia di prevenzione e contrasto dei reati informatici, oltre ad individuare disposizioni in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici; tematica successivamente fatta oggetto del Documento "Guida alla Notifica degli incidenti al CSIRT Italia", elaborato dall'Agenzia per La Cybersicurezza e diffuso il 26 luglio scorso.

A tal proposito, sul sito istituzionale dell'Agenzia per la cybersicurezza nazionale è possibile consultare le succitate Linea Guida, che illustrano ad ogni soggetto le informazioni necessarie per effettuare la notifica di incidente al CSIRT (Computer Security Incident Response Team) Italia. In tale ambito vi rientrano sia i soggetti con obbligo normativo di notifica, come i soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC), gli Operatori di Servizi Essenziali (OSE), i Fornitori di Servizi Digitali (FSD), i Telco, nonchè i soggetti sottoposti alle disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (di cui alla legge n.

90/2024), sia coloro che non operano in settori critici e che non abbiano vincoli in tal senso, come Piccole e Medie Imprese e cittadini.

In tale contesto, appare utile ricordare che il CSIRT Italia è il centro operative che opera all'interno dell'Agenzia per la Cybersicurezza Nazionale (ACN), al quale sono state conferite le azioni di preparazione, prevenzione, gestione e risposta ad eventi ed incidenti cibernetici. Il CSIRT è stato istituito ad opera del d.Lgs. 18 maggio 2018, n. 65 - attuativo della "Direttiva 2016/1148 del Parlamento europeo e del Consiglio recante misure per un livello comune ed elevato di sicurezza delle reti e dei sistemi informativi nell'Unione Europea" (cosiddetta Direttiva NIS) - che ha provveduto a dettagliarne compiti e funzioni, nonché ad individuare gli OSE e i FSD quali soggetti con obblighi di notifica degli incidenti al CSIRT Italia.

In seguito, il Decreto del Presidente del Consiglio dei ministri 8 agosto 2019, "Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT italiano" ha definito la costituzione, l'organizzazione ed il funzionamento del CSIRT italiano presso il Dipartimento delle informazioni per la sicurezza (DIS). In virtù delle modifiche apportate successivamente alla normativa in materia dal decreto-legge del 14 giugno 2021, n. 82, il CSIRT è ora attivo presso l'Agenzia per la Cybersicurezza con la nuova denominazione di CSIRT Italia. Di talchè, i soggetti pubblici e privati, in caso di incidente cibernetico e/o di notifica di evento, hanno quale nuovo ed unico interlocutore il CSIRT Italia, che già riceve le notifiche obbligatorie e volontarie degli OSE e dei FSD, ai sensi del d.Lgs. n. 65/2018.

Pertanto, a fronte di quanto esposto, il CSIRT Italia assume il ruolo di:

• struttura tecnica di prevenzione, coordinamento e risposta agli eventi e incidenti informatici con impatto, effettivo o potenziale, sul territorio nazionale;

• punto di riferimento per le notifiche degli incidenti occorsi in danno di tutte le infrastrutture digitali della pubblica amministrazione e private, con particolare riferimento alle notifiche previste ai sensi di legge, ad opera dei soggetti inclusi nel PSNC, degli OSE e dei FSD individuati dalla Direttiva NIS e per i soggetti sottoposti ad obbligo di notifica ai sensi del Codice delle comunicazioni elettroniche e della legge n. 90 del 2024.

Nell'ambito della legge n. 90 del 2024, di strategica importanza appare sicuramente la norma afferente alla "Disciplina dei contratti pubblici di beni e servizi informatici

impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e disposizioni di raccordo con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133", di cui all'art. 14 della predetta legge.

La disposizione, che si connota per una formulazione particolarmente articolata, prevede che il Presidente del Consiglio dei ministri deve adottare, entro centoventi giorni dalla data di entrata in vigore della citata legge, su proposta dell'Agenzia per la cybersicurezza nazionale e previo parere del Comitato interministeriale per la sicurezza della Repubblica, un Decreto con cui sono individuati, per specifiche categorie tecnologiche di beni e servizi informatici, gli elementi essenziali di cybersicurezza che i soggetti di cui all'articolo 2, comma 2, del CAD, o codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, quindi le pubbliche amministrazioni, i gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse e le società a controllo pubblico, sono tenuti ad assicurare.

In ordine al fattore relativo agli "elementi essenziali di cybersicurezza", è utile ricordare che il codice dei contratti pubblici impone alle stazioni appaltanti un obbligo generale di considerare gli elementi di cybersicurezza. Tale obbligo assume carattere più stringente in tutti quei casi in cui l'appalto riguardi attività incidenti sugli interessi strategici nazionali. L'art. 14 fornisce, così, una definizione normativa di "elementi essenziali di cybersicurezza", da intendersi come «l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela di cui al primo periodo». Si deve evidenziare che la definizione introdotta dall'art. 14 sembra rivolta a colmare una lacuna normativa derivante dalla formulazione, per certi aspetti carente, dell'art. 108, comma 4, del d.lgs. n. 36/2023 (Codice dei contratti pubblici), contribuendo a determinare, con maggiore chiarezza, il perimetro concettuale e operativo degli elementi di cybersicurezza richiamati nella disposizione.

Nel corso delle attività di approvvigionamento di beni e servizi informatici impiegati nello specifico contesto, individuato come strettamente connesso alla tutela degli interessi nazionali strategici, devono essere previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi

appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi che sono parte di accordi di collaborazione con l'Unione europea o con la NATO.

Tali beni e servizi informatici dovranno essere acquisiti da parte delle stazioni appaltanti o dalle possibili relative centrali di committenza con apposite e specifiche attività di approvvigionamento, vista la rilevanza dei settori in cui gli stessi dovranno essere impiegati, e quindi la necessaria elevata qualità che i relativi fornitori devono assicurare. In tale contesto, la stazione appaltante o la centrale di committenza può decidere di non aggiudicare l'appalto all'offerente che ha presentato l'offerta economicamente più vantaggiosa qualora abbia accertato che l'offerta stessa non assicura che il bene o servizio offerto possegga gli elementi essenziali di cybersicurezza.

Si aggiunga, altresì, che la stazione appaltante deve inoltre tenere conto degli elementi essenziali di cybersicurezza nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione. Nell'ipotesi, poi, in cui la stazione appaltante utilizzi quale criterio di affidamento quello del minor prezzo, la stessa deve inserire tra i requisiti minimi dell'offerta gli elementi di cybersicurezza, diversamente nel caso in cui voglia utilizzare il criterio dell'offerta economicamente più vantaggiosa, poichè nella valutazione dell'elemento qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, si stabilisce un tetto massimo per il punteggio economico entro il limite del 10 per cento.

Passando ora alla disamina del decreto legislativo del 4 settembre 2024, n. 138, di recepimento della direttiva (UE) 2022/2555, è necessario premettere che tale direttiva (NIS2), muove dal presupposto che «la rapida trasformazione digitale e l'interconnessione della società […] ha portato a un'espansione del panorama delle minacce informatiche, con nuove sfide che richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri», imponendo pertanto agli stessi Stati membri di adottare strategie nazionali efficaci in materia di cybersicurezza.

Il recepimento della direttiva, per mezzo del decreto legislativo del 4 settembre 2024, n. 138, mira a garantire l'aumento del livello di sicurezza informatica del tessuto produttivo e delle Pubbliche Amministrazioni del Paese, in armonia con gli altri Stati

membri dell'Unione Europea.

La Direttiva NIS 2, dunque, costituisce un importante avanzamento nella strategia di cybersecurity dell'Unione Europea, superando le disposizioni della precedente Direttiva Network and Information Systems (NIS).

Occorre ricordare che la NIS 2 è entrata in vigore il 17 gennaio 2023 e gli Stati membri dell'UE hanno dovuto introdurre la direttiva nella legislazione nazionale entro il 17 ottobre 2024. Le organizzazioni coperte dalla direttiva, pertanto, hanno dovuto conformarsi alla legislazione nazionale che implementa la NIS 2 entro questa scadenza.

Il decreto di che trattasi, che recepisce la Direttiva, conferma il ruolo dell'Agenzia per la Cybersicurezza nazionale come Autorità nazionale competente NIS, oltre a rappresentare un Punto di contatto unico.

Il nuovo impianto normativo contiene diverse novità. La prima riguarda l'ampliamento del campo di applicazione a 18 settori di cui 11 altamente critici e 7 critici, imponendo obblighi all'intera infrastruttura ICT, coinvolgendo, altresì, oltre 80 tipologie di soggetti, distinguendoli tra essenziali e importanti – definiti agli articoli 6 e 7 della legge n. 138 - in relazione al livello di criticità delle attività svolte e del settore in cui operano. Si deve porre in evidenza che entro il 31 marzo di ogni anno successivo alla data di entrata in vigore del presente decreto, l'Autorità nazionale competente NIS, redige, secondo le modalità di cui all'articolo 40, comma 5 della legge in esame, l'elenco dei soggetti essenziali e dei soggetti importanti.

Ne consegue, che sono previsti maggiori obblighi per le misure di sicurezza e per la notifica degli incidenti e più potere di supervisione all'Agenzia e agli organi preposti alla risposta agli incidenti e alla gestione della crisi.

In tale ambito, vengono, altresì, identificati 9 Ministeri quali Autorità di settore, che supportano l'attuazione della normativa con la propria competenza settoriale, collaborando nel contesto del Tavolo per l'attuazione della disciplina NIS presieduto dalla stessa Agenzia, a cui prendono parte anche rappresentanti della Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. I Ministeri coinvolti sono: la Presidenza del Consiglio dei ministri, il Ministero dell'economia e delle finanze, il Ministero delle imprese e del made in Italy, il Ministero dell'agricoltura, della sovranità alimentare e delle foreste, il Ministero dell'ambiente e

della sicurezza energetica, il Ministero delle infrastrutture e dei trasporti, il Ministero dell'università e della ricerca e il Ministero della cultura.

Ora, l'adeguamento alla nuova normativa NIS prevede un percorso sostenibile con una graduale implementazione degli obblighi da parte dei soggetti interessati, i quali sono tenuti a registrarsi al portale ACN.

A tal proposito, lo scorso 26 novembre il Direttore dell'Agenzia per la Cybersecurity Nazionale (ACN) ha firmato la prima determina attuativa relativa agli obblighi della direttiva NIS2, la quale è stata pubblicata il giorno successivo sul sito ufficiale dell'ACN. Tale determina stabilisce la creazione di una piattaforma digitale – disponibile dal 1° dicembre 2024 – destinata alla registrazione dei "soggetti NIS", ossia tutti gli enti pubblici e privati che sono tenuti a registrarsi entro il 28 febbraio 2025. La registrazione dovrà essere effettuata attraverso un "punto di contatto", una persona fisica designata responsabile delle comunicazioni e degli adempimenti per ciascun ente. Le informazioni fornite saranno sottoposte a verifica per assicurare la loro correttezza e coerenza da parte delle strutture dell'ACN incaricate.

Dal sito istituzionale dell'Agenzia si evince che per agevolare il recepimento degli obblighi di notifica di incidente e delle misure di sicurezza, gli stessi verranno definiti in maniera progressiva e a valle delle consultazioni nell'ambito dei tavoli settoriali in seguito alle determine del Direttore Generale di ACN che saranno adottate entro il primo quadrimestre del 2025.

È stata, inoltre, prevista una finestra temporale di implementazione differenziata: 9 mesi per le notifiche e 18 mesi per le misure di sicurezza, decorrenti dalla data di consolidamento dell'elenco dei soggetti NIS (fine marzo 2025).

L'Agenzia per la cybersicurezza ha provveduto a pubblicare sul proprio sito istituzionale un video esplicativo volto a recepire più agevolmente le novità intervenute in materia.

Diversamente la precedente normativa, la quale focalizzava l'attenzione sulla disponibilità delle reti e dei sistemi relativi ai servizi essenziali di pochi soggetti altamente critici. Con la nuova normativa NIS, gli obblighi riguardano le tre dimensioni classiche della sicurezza informatica (riservatezza, integrità e disponibilità) secondo un approccio multi-rischio e riguardano, oltre alla registrazione, diversi ambiti, come la

gestione del rischio, la responsabilità aziendale, gli obblighi di comunicazione, la continuità del business e la sicurezza della catena di approvvigionamento.

La revisione del meccanismo di identificazione dei soggetti importanti o essenziali prevede un criterio omogeneo basato sulla dimensione (cosiddetto "size-cap rule") che estende l'applicazione della normativa a tutte le medie e grandi imprese operanti nei settori identificati (in taluni casi, anche a piccole e microimprese), nonché a numerose pubbliche amministrazioni.

Resta ferma la possibilità per l'Autorità nazionale competente NIS, su proposta delle Autorità di settore, di individuare ulteriori soggetti ritenuti critici.

Il nuovo impianto normativo del d.lgs. n. 138/2024 contiene diverse novità, le quali, in estrema sintesi, stabiliscono una serie di misure afferenti:

a) una Strategia nazionale di cybersicurezza;

b) l'integrazione del quadro di gestione delle crisi informatiche;

c) la conferma dell'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente NIS, punto di contatto unico NIS e Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente in ambito nazionale;

d) la designazione dell'Agenzia per la cybersicurezza nazionale e del Ministero della difesa quali Autorità nazionali di gestione delle crisi informatiche su vasta scala;

e) l'individuazione di Autorità di settore NIS che collaborano con l'Agenzia per la cybersicurezza nazionale;

f) l'indicazione dei criteri per l'individuazione dei soggetti a cui si applica il presente decreto e la definizione dei relativi obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e di notifica di incidente;

g) l'adozione di misure in materia di cooperazione e di condivisione delle informazioni ai fini dell'applicazione del presente decreto.

In merito al provvedimento innovativo di che trattasi, si riportano gli schemi estrapolati dal sito ufficiale dell'Agenzia per la cybersicurezza concernenti i principali provvedimenti attuativi del decreto legislativo n. 138, unitamente alle operazioni sia di recepimento della nuova normativa che di attuazione negli anni 2025 e 2026.

Secondo quanto rappresentato dall'Agenzia per la cybersicurezza, congiuntamente dal Dipartimento per la trasformazione digitale - Unità di missione PNRR, nella nota pervenuta il 24 dicembre 2024, le novità normative intervenute appena esposte risultano pienamente in linea con gli obiettivi dell'Investimento e rappresentano anche un rafforzamento e sostegno della sostenibilità delle iniziative e investimenti messi in campo.

Per completezza espositiva, si riportano qui di seguito gli schemi concernenti i principali provvedimenti attuativi del più volte summenzionato d.lgs. n. 138 del 2024, tratti dal sito istituzionale dell'Agenzia per la cybersicurezza:

Principali provvedimenti attuativi D.Lgs. 138/2024

Termine	Atto	Contenuto
Entro 30 giorni dalla data di entrata in vigore del D.Lgs NIS2	DPCM su proposta ACN, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere Comitato per la Cybersicurezza	Criteri per l'applicazione della clausola di salvaguardia
	DPCM su proposta ACN, d'intesa con le Autorità di settore, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere Comitato per la Cybersicurezza	Eventuali ulteriori specifiche dei settori
	DPCM su proposta ACN, d'intesa con Le Amministrazioni interessate, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere Comitato per la Cybersicurezza	Cooperazione con le autorità nazionali
	Determinazione ACN, sentito il Tavolo per l'attuazione della disciplina NIS	Composizione del Tavolo per l'attuazione della disciplina NIS - Copia del documento con gli estremi del protocollo: apre un link esterno Organizzazione e funzionamento del Tavolo per l'attuazione della disciplina NIS - Copia del documento

Termine	Atto	Contenuto
		con gli estremi del protocollo: apre un link esterno Organizzazione e funzionamento del Tavolo per l'attuazione della disciplina NIS - Originale firmato digitalmente: apre un link esterno
	Determinazione ACN, sentito il Tavolo per l'attuazione della disciplina NIS	Modalità di accesso alla piattaforma e informazioni aggiuntive che i soggetti devono condividere - Copia del documento con gli estremi del protocollo: apre un link esterno Modalità di accesso alla piattaforma e informazioni aggiuntive che i soggetti devono condividere - Originale firmato digitalmente: apre un link esterno
	Determinazione ACN, su proposta delle Autorità di settore interessate, sentito il Tavolo per l'attuazione della disciplina NIS	Individuazione dell'Autorità di soggetti in ambito di applicazione NIS anche in assenza dei requisiti dimensionali prescritti
Entro il 31 marzo 2025	Determinazione ACN, su proposta delle Autorità di settore interessate, sentito il Tavolo per l'attuazione della disciplina NIS	Se necessaria, dispone l'applicazione della clausola di salvaguardia
	Determinazione ACN, sentito il Tavolo per l'attuazione della disciplina NIS	Elenco dei soggetti NIS
Entro 6 mesi dalla data di entrata in vigore del D.Lgs. NIS2	DPCM su proposta ACN, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere Comitato per la Cybersicurezza	Criteri, procedure e modalità per le attività di monitoraggio, vigilanza ed esecuzione
	DPCM su proposta ACN, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere Comitato per la Cybersicurezza	Modalità di applicazione degli strumenti deflattivi del contenzioso
	DPCM su proposta ACN, d'intesa con Autorità di settore, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere Comitato per la Cybersicurezza	Modalità di collaborazione con le Autorità di settore
	Determinazione ACN, d'intesa con il Ministero della Giustizia, sentito il Tavolo per l'attuazione della disciplina NIS	Politica nazionale di divulgazione coordinata delle vulnerabilità
	Determinazione ACN, sentito il Tavolo per l'attuazione della disciplina NIS	Modalità di notifica all'Autorità nazionale compente NIS degli accordi di condivisione tra soggetti

Termine	Atto	Contenuto
	Determinazione ACN, sentito il Tavolo per l'attuazione della disciplina NIS	Obblighi di base

Recepimento e attuazione

FEBBRAIO 23 - METÀ OTTOBRE 2024

Recepimento

- Avvio di alcuni tavoli settoriali
- **7 agosto 2024**: adozione definitiva in CDM
- **1° ottobre 2024**: pubblicazione in Gazzetta Ufficiale
- **16 ottobre 2024**: entrata in vigore

METÀ OTTOBRE 24 – METÀ APRILE 2025

Prima fase attuativa

- Avvio formale di tutti i tavoli settoriali
- **Entro febbraio 2025**: censimento e registrazione dei soggetti
- **Entro marzo 2025**: adozione dell'elenco dei soggetti NIS
- **Entro aprile 2025**: notifica ai soggetti NIS
- **Entro aprile 2025**: elaborazione e adozione obblighi di base

METÀ APRILE 25 – METÀ APRILE 2026

Seconda fase attuativa

- Monitoraggio e supporto
- **A partire da gennaio 2026**: obbligo di notifica di base
- **Entro aprile 2026**: elaborazione e adozione del modello di categorizzazione delle attività e dei servizi

- **Entro aprile 2026**: elaborazione e adozione degli obblighi a lungo termine
- **Entro settembre 2026**: completa implementazione delle misure di sicurezza di base

DA METÀ APRILE 2026

Terza fase attuativa

- Categorizzazione delle attività e dei servizi
- Implementazione degli obblighi a lungo termine

4. Cronoprogramma.

Per quanto concerne la descrizione dei milestone/target con le relative scadenze, appare utile riportare la tabella esplicativa estrapolata direttamente dal sistema Regis, riportante i singoli goal e relative scadenze per gli anni 2022-2024.

M1C1I1.5 Cybersecurity | **Amministrazione titolare:** **PCM - DIPARTIM. TRASFORMAZIONE**

Importo previsto **0,62 mld**

Descrizione Milestone/Target

Codice	Descrizione	Scadenza	Goal
M1C1-19	Almeno 50 interventi di potenziamento effettuati nei settori del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e delle reti e sistemi informativi (NIS). I tipi di intervento riguardano, ad esempio, i centri operativi per la sicurezza (SOC), il miglioramento della difesa dei confini informatici e le capacità interne di monitoraggio e controllo nel rispetto dei requisiti NIS e PSNC. Gli interventi nei settori NIS devono riguardare in particolare i settori dell'assistenza sanitaria, dell'energia e dell'ambiente(approvvigionamento di acqua potabile e gestione dei rifiuti).	31/12/2024	50
M1C1-20	Il traguardo è completato con l'attivazione delle squadre di pronto intervento informatico (CERT), la loro interconnessione con il team italiano di risposta agli incidenti di sicurezza informatica (CSIRT) e con il centro nazionale di condivisione e di analisi delle informazioni (ISAC) e l'integrazione di almeno 5 centri operativi di sicurezza (SOC) con l'HyperSOC nazionale, la piena operatività dei servizi di gestione dei rischi di cybersecurity, compresi quelli per l'analisi della catena di approvvigionamento e i servizi di assicurazione contro i rischi informatici.	31/12/2024	N.A.
M1C1-21	Attivazione di almeno 10 laboratori di screening e certificazione e di 2 centri di valutazione (CV).	31/12/2024	N.A.
M1C1-22	Piena operatività dell'unità centrale di audit con almeno 30 ispezioni completate.	31/12/2024	N.A.
M1C1-5	Il traguardo deve essere conseguito mediante 1) la conversione in legge del decreto-legge che istituisce l'Agenzia per la cybersicurezza nazionale, attualmente in fase avanzata di elaborazione; 2) la pubblicazione nella Gazzetta Ufficiale della Repubblica italiana del Decreto del Presidente del Consiglio dei Ministri (DPCM) contenente il regolamento interno dell'Agenzia per la cybersicurezza nazionale.	31/12/2022	N.A.
M1C1-6	Il traguardo deve essere conseguito con la definizione dell'architettura dettagliata dell'intero ecosistema della cybersicurezza nazionale (ossia un centro nazionale di condivisione e di analisi delle informazioni (ISAC), una rete di squadre di pronto intervento informatico (CERT), un HyperSOC nazionale, il calcolo ad alte prestazioni integrato dagli strumenti di intelligenza artificiale/apprendimento automatico (AI/ML) per analizzare gli incidenti di cybersicurezza di portata nazionale).	31/12/2022	N.A.
M1C1-7	Il traguardo deve essere conseguito mediante: i) l'individuazione, da parte dell'Agenzia per la cybersicurezza nazionale, dei luoghi in cui sorgeranno i laboratori e i centri di screening e certificazione, i profili degli esperti da assumere, la piena definizione dei processi e delle procedure da condividere tra laboratori; ii) l'attivazione di un laboratorio. Le attività create per l'istituzione e l'attivazione dei laboratori di esame devono essere oggetto di supervisione da parte del Ministero dello Sviluppo Economico (MISE) in collaborazione con il Centro di Valutazione e Certificazione Nazionale (CVCN) della cybersicurezza, integrati con il centro di valutazione (CV) dai Ministeri dell'Interno e della Difesa.	31/12/2022	N.A.
M1C1-8	In seno all'Agenzia per la cybersicurezza nazionale deve essere istituita un'unità interna con il mandato di svolgere le attività di unità centrale di audit per quanto riguarda le misure di sicurezza PSNC e NIS. I processi, la logistica e le modalità operative devono essere formalizzati in una documentazione adeguata, con particolare attenzione ai processi operativi, ossia le regole di ingaggio e le procedure di audit e di rendicontazione. I dati di audit, raccolti, gestiti e analizzati mediante strumenti informatici, devono essere elaborati e utilizzati dall'unità di audit. Deve essere fornita la documentazione attestante che lo sviluppo degli strumenti è stato completato.	31/12/2022	N.A.
M1C1-9	Almeno cinque interventi per migliorare le strutture di sicurezza completati nei settori del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e delle reti e sistemi informativi (NIS). Tra i tipi di intervento figurano l'aggiornamento dei centri operativi per la sicurezza (SOC), il miglioramento della difesa dei confini informatici e le capacità interne di monitoraggio e controllo. Gli interventi devono riguardare in particolare i settori del l'assistenza sanitaria, dell'energia e dell'ambiente (approvvigionamento di acqua potabile).	31/12/2022	5

Appare interessante riportare qui di seguito anche una tabella contenenti gli ulteriori "Monitoring steps" collegati all'investimento in esame, comprensiva della descrizione degli step procedurali, con le relative scadenze.

I dati contenuti nella tabella sono il frutto della consultazione effettuata, al 31 dicembre 2024, sul sistema REGIS, componente "Cronoprogramma procedurale".

M1C1I1.5 Cybersecurity				Amministrazioni	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	
				Importo previsto	€ 0,62 mld	
	Ulteriori - Monitoring Steps					
Codice	**Tipologia**	**Descrizione**	**Categoria**		**Step Procedurale**	**Scadenza**
-	Ulteriore Step	Adozione atti di organizzazione dell'Agenzia	RIFORME		Approvazione Regolamento	09/12/2021
-	Ulteriore Step	Selezione profili professionali	FORNITURE BENI E SERVIZI		Pubblicazione Avvisi/Bandi	22/02/2022
-	Ulteriore Step	Attivazione del CVCN	RIFORME		Attivazione servizi	30/06/2022
-	Ulteriore Step	Procedure di selezione delle amministrazioni oggetto di intervento	FORNITURE BENI E SERVIZI		Pubblicazione Avvisi/Bandi	01/07/2022
-	Ulteriore Step	Nuove procedure di selezione delle amministrazioni oggetto di intervento	FORNITURE BENI E SERVIZI		Pubblicazione Avvisi/Bandi	31/12/2023
-	Ulteriore Step	Avanzamento nello stato di attivazione dei servizi nazionali di cybersecurity	FORNITURE BENI E SERVIZI		Monitoraggio stato avanzamento target	31/12/2023
-	Ulteriore Step	Avanzamento del sostegno al potenziamento delle strutture di sicurezza T2	FORNITURE BENI E SERVIZI		Monitoraggio stato avanzamento target	31/12/2023
-	Ulteriore Step	Avanzamento nello stato di attivazione della rete dei laboratori e dei centri di valutazione per la valutazione e certificazione della cybersecurity	FORNITURE BENI E SERVIZI		Monitoraggio stato avanzamento target	31/12/2023
-	Ulteriore Step	Avanzamento attivazione dei Centri di Valutazione di Difesa e Interno	FORNITURE BENI E SERVIZI		Monitoraggio stato avanzamento target	31/12/2023
-	Ulteriore Step	Avanzamento verso la piena operatività dell'unità di audit per le misure di sicurezza PSNC e NIS con il completamento di almeno 15 ispezioni	FORNITURE BENI E SERVIZI		Monitoraggio stato avanzamento target	30/06/2024

5. Budget economico per l'anno 2025.

Con nota del 12 dicembre 2024, prot. n. 4166, il Ministero dell'Economia e delle Finanze ha trasmesso, per conoscenza, a questa Sezione il documento riportante il budget economico annuale 2025, adottato dal Direttore Generale dell'Agenzia per la Cybersicurezza, sentito il Vicedirettore generale, con delibera 8 novembre 2024.

Il documento previsionale in esame risulta corredato dai seguenti allegati, in armonia con quanto previsto dall'articolo 9, comma 6, del DPCM 9 dicembre 2021, n. 222, concernente "Regolamento di contabilità dell'Agenzia per la cybersicurezza nazionale":

a) budget economico pluriennale 2025-2027;

b) relazione illustrativa;

c) relazione del Collegio dei revisori dei conti;

d) prospetto di previsione di spesa complessiva articolato per missioni e programmi;

e) budget di cassa;

f) piano degli indicatori e dei risultati attesi di bilancio.

Nel documento di che trattasi, inoltre, sono indicati anche i dati concernenti il budget degli investimenti per l'esercizio 2025.

Dalla disamina dei documenti contabili è stato rilevato che il budget economico annuale 2025 presenta una previsione di pareggio economico, che consegue dalla somma algebrica tra il risultato positivo di 5.243.000 euro – determinato dalla differenza tra il valore e i costi della produzione, rispettivamente, di 185.131.000 euro e di 179.887.000 euro – gli oneri finanziari di 2.429.000 euro e le imposte di esercizio di 2.815.000 euro.

A sostegno di quanto espresso, nella nota del Ministero dell'Economia e delle Finanze viene fornita una tabella in cui vengono menzionati i dati contabili in esame, posti a raffronto con i dati del budget economico annuale revisionato 2024.

Nel dettaglio, segue:

Descrizione	Budget economico 2024 (stime iniziali)	Budget economico revisionato 2024 (Del. ACN 29/7/2024)	Budget economico 2025	Variazioni tra dati del budget revisionato 2024 e budget economico 2025	
				assolute	%
VALORE DELLA PRODUZIONE	**A**	**B**	**C**	**D=(C-B)**	**E=D/B**
Ricavi e proventi per l'attività istituzionale	**101.137.000**	**93.884.000**	**116.812.000**	**22.928.000**	**24%**
contributo ordinario dello Stato	79.141.000	81.381.000	84.897.000	3.516.000	4%
contributi in conto esercizio	21.996.000	12.503.000	31.915.000	19.412.000	155%
altri ricavi e proventi	28.984.000	31.657.000	68.319.000	36.662.000	116%
Totale valore della produzione	**127.746.000**	**125.541.000**	**185.131.000**	**59.590.000**	**47%**
COSTI DELLA PRODUZIONE	**A**	**B**	**C**	**D=(C-B)**	**E=D/B**
per materie prime, sussidiarie, di consumo e di merci	133.000	138.000	357.000	219.000	159%
per servizi	28.332.000	30.100.000	50.803.000	20.703.000	69%
per godimento di beni di terzi	13.764.000	1.527.000	4.430.000	2.903.000	190%
per il personale	55.687.000	57.825.000	55.026.000	-2.799.000	-5%
ammortamenti e svalutazioni	25.749.000	30.797.000	67.459.000	36.662.000	119%
oneri diversi di gestione	1.060.000	1.001.000	1.813.000	812.000	81%
Totale costi della produzione	**124.724.000**	**121.387.000**	**179.887.000**	**58.500.000**	**48%**
DIFFERENZA TRA VALORE E COSTI DELLA PRODUZIONE	**3.021.000**	**4.154.000**	**5.243.000**	**1.089.000**	**26%**

PROVENTI E ONERI FINANZIARI	**A**	**B**	**C**	**D=(C-B)**	**E=D/B**
Interessi passivi ed altri oneri finanziari	0,00	-1.130.000	-2.429.000	1.299.000	115%
Totale proventi ed oneri finanziari	**0,00**	**-1.130.000**	**-2.429.000**	**1.299.000**	**115%**
RISULTATO PRIMA DELLE IMPOSTE	**3.021.000**	**3.023.000**	**2.815.000**	**-208.000**	**-7%**
Imposte di esercizio	3.021.000	3.023.000	2.815.000	-208.000	-7%
AVANZO (DISAVANZO) ECONOMICO	0,00	0,00	0,00	-	-

Dalla tabella di cui sopra si evince che il valore della produzione di 185.131.000 euro, afferente il budget economico per l'anno 2025, presenta un incremento di circa il 47% rispetto alle stime assestate del budget 2024, da attribuire, essenzialmente, secondo quanto affermato nel documento trasmesso dal MEF, ai maggiori contributi statali

unitamente a quelli dell'Unione europea.

Per quanto attiene il dato sui ricavi, per l'esercizio 2025, questi sono rappresentati per la maggior parte dal contributo ordinario da parte dello Stato (84.897.000 euro) e dalla quota di risorse del Fondo per la gestione della cybersicurezza, ai sensi del DPCM 8 luglio 2024 (13.816.000 euro). È stato, altresì, evidenziato che i contributi da parte dell'Unione Europea (18.100.000 euro) presentano un aumento di circa 9.773.000 euro, rispetto alle stime assestate del budget 2024, concernenti le risorse del PNRR e agli introiti attesi dai progetti cofinanziati dall'Unione Europea.

La voce "altri ricavi e proventi", invece, di 68.319.000, euro comprende la quota di contributi pubblici che l'Agenzia destina a investimenti in immobilizzazioni materiali e immateriali (67.459.000 euro) nonché agli introiti attesi per le attività di certificazione (860.000 euro).

È stato poi sottolineato che anche per i costi della produzione, inerenti al budget economico 2025, (di 179.887.000 euro), è stato registrato un incremento di circa il 48% rispetto alle stime assestate del budget 2024. Tali costi risultano costituiti, principalmente, da servizi per 50.803.000 euro (nel 2024, 30.100.000 euro), da oneri per il personale dipendente pari a 55.026.000 euro (nel 2024, 57.825.000 euro), dal godimento di beni di terzi per 4.430.000 euro (nel 2024, 1.527.000 euro) e, infine, da ammortamenti e svalutazioni pari a 67.459.000 euro (nel 2024, 30.797.000 euro).

In tale ambito, appare interessante rilevare un incremento della stima dei costi per servizi (+ 20.703.000 rispetto alle stime assestate del budget 2024), riconducibili a maggiori erogazioni di servizi istituzionali (+ 25.505.000 euro) e a consulenze, collaborazioni e altre prestazioni professionali (+ 6.527.000 euro).

È stato, altresì, evidenziato che nella relazione illustrativa la voce "erogazione di servizi istituzionali", pari a 31.364.000 euro, è rappresentata, soprattutto, da costi inerenti alla manutenzione software e all'assistenza ordinaria (21.088.000 euro), necessari per garantire il corretto funzionamento dei complessi servizi informatici dell'Agenzia. In merito alla voce "consulenze, collaborazioni, altre prestazioni professionali", invece, pari a 13.576.000 euro, la stessa è formata dai servizi professionali di supporto specialistico, di interpretariato e di compensi corrisposti al medico del lavoro e al responsabile della sicurezza sul lavoro, e risulta finanziata quasi interamente da risorse PNRR.

Da quanto emerge dal documento trasmesso, inoltre, il costo del personale, il cui ammontare è pari a 55.026.000 euro, registra una lieve contrazione rispetto alle stime assestate del budget 2024 (-2.799.000 euro), a fronte di una dotazione organica progressivamente incrementata ai sensi del DPCM 4 luglio 2024 (da 400 a 450 unità all'1/1/2025). A tal proposito, nella documentazione fornita è stato evidenziato come la relazione illustrativa fornisca assicurazioni circa la correttezza della previsione, in quanto si è tenuto conto dell'obiettivo volto ad incrementare la consistenza del personale nonché degli oneri complessivi derivanti dagli istituti fissi e variabili della retribuzione applicabili (il trattamento economico è pari a quello in godimento da parte dei dipendenti della Banca d'Italia).

Il MEF, infine specifica che, ai sensi di quanto previsto dall'articolo 2, comma 2, del citato DPCM 4 luglio 2024, la relazione illustrativa presenta una tabella in cui si espone la proiezione della spesa decennale del personale. A tal riguardo il Ministero raccomanda un puntuale monitoraggio della suddetta spesa.

Per quanto attiene poi la voce "ammortamenti e svalutazioni" (pari a 67.459.000 euro) la stessa risulta derivare unicamente dagli ammortamenti dei beni patrimoniali già iscritti nel libro dei cespiti e da quelli relativi agli investimenti programmati nel 2025.

Dalla disamina dei dati effettuata dall'Agenzia circa la gestione finanziaria, risultano stimati interessi passivi pari a 2.429.000 euro, come previsti dal piano di ammortamento del prestito chirografario decennale di 70 milioni di euro acceso con la Cassa Depositi e Prestiti S.p.A. per l'acquisto dell'immobile adibito a sede istituzionale, effettuato nel 2024.

In ordine al budget economico pluriennale 2025-2027 il Ministero dell'Economia e delle Finanze evidenzia che lo stesso presenta previsioni che confermano, negli anni 2026-2027, il pareggio economico pur presentando un moderato incremento dei costi della produzione (nel 2026, 202.968.000 euro; nel 2027, 194.574.000 euro), controbilanciati da stime in aumento dei valori della produzione (nel 2026, 208.339.000 euro; nel 2027, 200.190.000 euro).

Per completezza espositiva, si riportano, altresì, alcuni dati indicati nel documento in esame e afferenti sia al budget degli investimenti, che al budget di cassa.

Per quanto concerne il budget per gli investimenti, le relative previsioni, per l'anno 2025, sono pari a 119.624.000 euro, di cui 95.308.000 euro per le immobilizzazioni

immateriali e 24.316.000 euro per le immobilizzazioni materiali. La succitata previsione che ammonta a 119.624.000 euro sarà finanziata per 72.250.000 euro con le risorse PNRR, mentre le 47.374.000 euro attraverso le risorse proprie (ex articolo 18, decreto-legge n. 82 del 2021).

In tale contesto, particolare rilevanza hanno assunto, tra le voci relative alle immobilizzazioni immateriali, la stima dei costi di ricerca e sviluppo (93.630.000 euro) da finanziare principalmente con le risorse del PNRR (70.000.000 euro).

Per quanto concerne, invece, il budget di cassa per l'anno 2025, la cui predisposizione è riconducibile all'articolo 13 del regolamento di contabilità, le previsioni per i flussi di cassa in entrata ammontano a un totale di 372.558.000 euro, costituiti nello specifico per 371.698.000 euro da entrate di natura contributiva (contributi statali in conto esercizio per 146.087.000 euro; contributi in conto esercizio PNRR e altri fondi europei per 90.350.000 euro; entrate risorse PNRR per trasferimenti ad altre PA per 135.262.00 euro) e per 860.000 euro da entrate di natura non contributive (rimborsi). In merito ai flussi di cassa in uscita la stima ammonta a euro 362.752.000, la cui ripartizione prevede per la parte corrente 243.128.000 euro (di cui si evidenziano 135.262.000 euro per uscite risorse PNRR per trasferimenti ad altre PA, 50.440.000 euro per spese per il personale e 45.653.000 per costi per servizi) e per la parte in conto capitale per euro 119.624.000 (di cui 97.308.000 euro per acquisto di immobilizzazioni immateriali e 22.316.000 euro per acquisto di immobilizzazioni materiali).

6. Quadro contabile.

Come già rappresentato nelle deliberazioni della Corte dei conti adottate nella materia di cui trattasi, ai fini della realizzazione dell'Investimento 1.5 del Piano nazionale di Ripresa e Resilienza, l'Agenzia per la Cybersicurezza nazionale è stata individuata quale soggetto attuatore, mentre il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri, che opera ai sensi del DPCM 15 marzo 2021, risulta essere l'Amministrazione titolare delle relative risorse.

Ai fini di una maggiore comprensione della tematica oggetto del presente capitolo, appare utile ricordare come le attività progettuali sottese all'investimento 1.5 sulla

"Cybersecurity" siano organizzate sulla base di una strutturazione di n. 12 Work Packages (WP), definiti in accordo alla suddivisione del progetto complessivo in tre sotto progetti, quali:

1- Servizi Cyber Nazionali (ambito: da WP 2 a WP 8);

2- Interventi Cyber per le PA (ambito: WP 9 e WP 10);

3- Laboratori di Scrutinio e Certificazione (WP 11 e WP 12).

In ordine alla previsione degli impegni, relativi a ciascun gruppo di attività (WP) per l'investimento in esame, questa Sezione, con nota istruttoria n. 4011, del 4 dicembre del 2024, ha chiesto alle Amministrazioni competenti di fornire il relativo aggiornamento per l'anno 2024.

A tal proposito, il Dipartimento per la trasformazione digitale congiuntamente con l'Agenzia per la cybersicurezza hanno inviato, in data 24 dicembre 2024, una nota contenente le informazioni richieste, unitamente ai relativi allegati.

Gli Enti competenti in sede istruttoria hanno fornito la rappresentazione, in primis, delle previsioni degli importi relativi alle risorse finanziarie impegnate negli anni precedenti e pianificate e impegnate nell'anno in corso, rappresentando, parimenti, la relativa suddivisione per ciascun Work Package (WP) del Piano Operativo di riferimento e rispetto alle modalità attuative adottate ("operazioni a regia" e "operazioni a titolarità").

Seguono, pertanto, le relative tabelle:

Distribuzione WP degli importi impegnati e previsione ulteriori impegni nel 2024

Work Package	Dotazione finanziaria[1]	Importi impegnati anni precedenti (2022 e 2023) titolarità e regia*	Importi impegnati a titolarità nel 2024	Importi impegnati a regia nel 2024	Importi totali impegnati (titolarità + regia) nel 2024	Previsioni ulteriori impegni per il 2024**
WP1 - Project Management	8.000.000,00 €	7.365.007,92 €	158.600,00 €	- €	158.600,00 €	- €
WP2 - Agenzia per la Cybersicurezza Nazionale	55.000.000,00 €	31.641.055,24 €	28.377.257,61 €	- €	28.377.257,61 €	- €
WP3 - HyperSOC	24.000.000,00 €	17.639.875,20 €	7.766.989,92 €	- €	7.766.989,92 €	- €
WP4 - Servizi PSNC e NIS	14.600.000,00 €	10.802.448,77 €	14.839.892,71 €	- €	14.839.892,71 €	- €
WP5 - High Performance Computing e Artificial Intelligence/Machine Learning	32.000.000,00 €	23.844.534,21 €	5.155.619,27 €	- €	5.155.619,27 €	- €
WP6 - Information Sharing and Analysis Center (ISAC)	18.550.000,00 €	7.362.937,94 €	17.426.318,02 €	- €	17.426.318,02 €	- €
WP7 - Rete di Computer Emergency Response Team (CERT)	68.000.000,00 €	30.208.504,92 €	4.861.939,47 €	26.073.494,10 €	30.935.433,57 €	356.508,40 €
WP8 - Ispezioni PSNC e NIS	1.500.000,00 €	537.616,99 €	459.546,45 €	- €	459.546,45 €	- €
WP9 - Interventi di potenziamento cyber per la PA	210.000.000,00 €	96.749.238,59 €	3.462.729,36 €	***100.000.000,00 €	103.462.729,36 €	- €
WP10 - Interventi di potenziamento cyber-defence	150.000.000,00 €	150.000.000,00 €	- €	- €	0,00 €	- €
WP11 - Centro di Valutazione e Certificazione Nazionale (CVCN) e i Centri di Valutazione (CV) di Interno e Difesa	35.350.000,00 €	20.852.398,99 €	4.164.163,73 €	- €	4.164.163,73 €	- €
WP12 - Rete di laboratori di scrutinio e certificazione tecnologica	6.000.000,00 €	4.076.389,65 €	- €	- €	0,00 €	- €
TOTALE	***623.000.000,00 €***	***401.080.008,41 €***	***86.673.056,55 €***	***126.073.494,10 €***	***212.746.550,64 €***	***356.508,40 €***

Distribuzione WP degli importi impegnati e previsione ulteriori impegni nel 2024

Work Package	Dotazione finanziaria[1]	Importi impegnati anni precedenti (2022 e 2023) titolarità	Importi impegnati a titolarità nel 2024	Previsioni ulteriori impegni a titolarità per il 2024
WP1 - Project Management	8.000.000,00 €	7.365.007,92 €	158.600,00 €	- €
WP2 - Agenzia per la Cybersicurezza Nazionale	55.000.000,00 €	31.641.055,24 €	28.377.257,61 €	- €
WP3 - HyperSOC	24.000.000,00 €	17.639.875,20 €	7.766.989,92 €	- €
WP4 - Servizi PSNC e NIS	14.600.000,00 €	10.802.448,77 €	14.839.892,71 €	- €
WP5 - High Performance Computing e Artificial Intelligence/Machine Learning	32.000.000,00 €	23.844.534,21 €	5.155.619,27 €	- €
WP6 - Information Sharing and Analysis Center (ISAC)	18.550.000,00 €	7.362.937,94 €	17.426.318,02 €	- €
WP7 - Rete di Computer Emergency Response Team (CERT)	68.000.000,00 €	1.718.198,42 €	4.861.939,47 €	356.508,40 €
WP8 - Ispezioni PSNC e NIS	1.500.000,00 €	537.616,99 €	459.546,45 €	- €
WP9 - Interventi di potenziamento cyber per la PA	210.000.000,00 €	17.560.124,30 €	3.462.729,36 €	- €
WP10 - Interventi di potenziamento cyber-defence	150.000.000,00 €	- €	- €	- €
WP11 - Centro di Valutazione e Certificazione Nazionale (CVCN) e i Centri di Valutazione (CV) di Interno e Difesa	35.350.000,00 €	2.352.398,99 €	4.164.163,73 €	- €
WP12 - Rete di laboratori di scrutinio e certificazione tecnologica	6.000.000,00 €	60.499,80 €	- €	- €
TOTALE	*623.000.000,00 €*	*120.884.697,78 €*	*86.673.056,55 €*	*356.508,40 €*

Distribuzione WP degli importi impegnati e previsione ulteriori impegni nel 2024

Work Package	Dotazione finanziaria[1]	Importi impegnati anni precedenti (2022 e 2023) regia*	Importi impegnati a regia nel 2024	Previsioni ulteriori impegni a regia per il 2024**
WP1 - Project Management	8.000.000,00 €	- €	- €	- €
WP2 - Agenzia per la Cybersicurezza Nazionale	55.000.000,00 €	- €	- €	- €
WP3 - HyperSOC	24.000.000,00 €	- €	- €	- €
WP4 - Servizi PSNC e NIS	14.600.000,00 €	- €	- €	- €
WP5 - High Performance Computing e Artificial Intelligence/Machine Learning	32.000.000,00 €	- €	- €	- €
WP6 - Information Sharing and Analysis Center (ISAC)	18.550.000,00 €	- €	- €	- €
WP7 - Rete di Computer Emergency Response Team (CERT)	68.000.000,00 €	28.490.306,50 €	26.073.494,10 €	- €
WP8 - Ispezioni PSNC e NIS	1.500.000,00 €	- €	- €	- €
WP9 - Interventi di potenziamento cyber per la PA	210.000.000,00 €	79.189.114,29 €	***100.000.000,00 €	- €
WP10 - Interventi di potenziamento cyber-defence	150.000.000,00 €	150.000.000,00 €	- €	- €
WP11 - Centro di Valutazione e Certificazione Nazionale (CVCN) e i Centri di Valutazione (CV) di Interno e Difesa	35.350.000,00 €	18.500.000,00 €	- €	- €
WP12 - Rete di laboratori di scrutinio e certificazione tecnologica	6.000.000,00 €	4.015.889,85 €	- €	- €
TOTALE	***623.000.000,00 €***	***280.195.310,64 €***	***126.073.494,10 €***	***- €***

In tale sede, è stato, altresì, fatto presente che è stato aggiornato il Piano Operativo, come da secondo atto aggiuntivo all'Accordo sottoscritto in data 28/03/2024, ai sensi dell'art. 5, comma 6, del d. lgs. n. 50 del 2016 per la realizzazione dell'investimento 1.5 – per la Cybersecurity, che sostituisce il precedente Piano Operativo già allegato all'Accordo sottoscritto il 14 dicembre del 2021 tra il Dipartimento per la trasformazione digitale e dall'Agenzia per la Cybersicurezza Nazionale.

Il succitato Piano mira ad enfatizzare le finalità dell'Investimento 1.5, volte a rinforzare le difese cibernetiche, aumentando il grado di resilienza informatica del Paese, con specifica attenzione alle Pubbliche Amministrazioni, anche al fine di fronteggiare sempre più efficacemente la continua evoluzione della minaccia cyber. Ciò sarà realizzato, secondo quanto si apprende dal testo del documento in esame, "anche attraverso la capacità dei sistemi informatici presenti sul nostro territorio di prevedere o rilevare tempestivamente attacchi e incidenti informatici, reagire e ripartire in tempi rapidi, minimizzando i danni con l'obiettivo di rendere il cyberspace nazionale un luogo ideale per i cittadini per conservare i dati più sensibili e per le aziende per ospitare le funzioni chiave per il business".

Dalla documentazione prodotta dal Dipartimento per la trasformazione digitale congiuntamente con l'Agenzia per la cybersicurezza, viene altresì fornito l'aggiornamento sia delle singole spese effettuate nell'anno in corso dal Soggetto attuatore dell'intervento, con separata indicazione per ciascun gruppo di attività (WP) e rispetto alle modalità attuative adottate ("operazioni a regia" e "operazioni a titolarità"), nonché delle spese sostenute negli anni precedenti (aggregati 2022 e 2023).

Si ricorda ancora, così come si evince dalla tabella riportata qui di seguito, che la dotazione finanziaria complessiva di cui all'investimento di che trattasi ammonta ad un totale pari a euro 623.000.000.

Elenco spese Investimento 1.5

Distribuzione sui WP degli importi liquidati

Dati aggiornati al 17.12.2024

Work Package	Dotazione finanziaria1	Importi liquidati anni precedenti (2022 e 2023) titolarità e regia	Importi liquidati a titolarità nel 2024	Importi liquidati a regia nel 2024	Importi totali liquidati
WP1 - Project Management	*8.000.000,00 €*	2.613.452,66 €	1.257.706,37 €	N/A	3.871.159,03 €
WP2 - Agenzia per la Cybersicurezza Nazionale	*55.000.000,00 €*	11.568.141,88 €	10.395.439,27 €	N/A	21.963.581,15 €
WP3 - HyperSOC	*24.000.000,00 €*	7.254.861,61 €	7.246.963,79 €	N/A	14.501.825,40 €
WP4 - Servizi PSNC e NIS	*14.600.000,00 €*	2.235.690,14 €	11.162.892,27 €	N/A	13.398.582,41 €
WP5 - High Performance Computing e Artificial Intelligence/Machine Learning	*32.000.000,00 €*	310.580,56 €	2.474.640,75 €	N/A	2.785.221,31 €
WP6 - Information Sharing and Analysis Center (ISAC)	*18.550.000,00 €*	2.678.665,27 €	5.203.875,58 €	N/A	7.882.540,85 €
WP7 - Rete di Computer Emergency Response Team (CERT)	*68.000.000,00 €*	692.938,60 €	451.657,84 €	1.349.785,16 €	2.494.381,60 €
WP8 - Ispezioni PSNC e NIS	*1.500.000,00 €*	218.565,44 €	89.738,09 €	N/A	308.303,53 €
WP9 - Interventi di potenziamento cyber per la PA	*210.000.000,00 €*	*6.832.685,47 €*	*4.311.770,97 €*	*3.706.005,05 €*	*14.850.461,49 €*
WP10 - Interventi di potenziamento cyber-defence	*150.000.000,00 €*	*14.400.000,00 €*	*N/A*	*32.619.458,91 €*	*47.872.153,38 €*
WP11 - Centro di Valutazione e Certificazione Nazionale (CVCN) e i Centri di Valutazione (CV) di Interno e Difesa	*35.350.000,00 €*	*2.141.278,48 €*	*1.446.117,80 €*	*5.057.251,02 €*	*8.644.647,30 €*
WP12 - Rete di laboratori di scrutinio e certificazione tecnologica	*6.000.000,00 €*	*1.023.462,94 €*	*- €*	*59.608,59 €*	*1.083.071,53 €*
TOTALE	*623.000.000,00 €*	**51.970.323,05 €**	**44.040.802,73 €**	**42.792.108,73 €**	**138.803.234,51 €**

Totale 2024: 86.832.911,46 €

Dalla nota istruttoria trasmessa congiuntamente dalle Amministrazioni interessate, nel mese di dicembre 2024, si acquisiscono anche i dati circa i movimenti dei fondi di cui all'investimento 1.5, concernenti il versamento degli stessi al Dipartimento per la transizione digitale effettuati negli anni 2022-2024.

A tal riguardo, in merito all'investimento sulla "Cybersecurity" è stato rappresentato che a fronte di una dotazione finanziaria complessiva di 623 milioni di euro, alla data del 24 dicembre 2024, sono state trasferite risorse per un totale di euro 207.344.385,07 euro.

Si specifica, che a titolo di anticipazione sono state erogate complessivamente euro 161.980.000. Di tale somma 62,300.000 euro risultano erogati in data 25 marzo 2022, così come già evidenziato nelle deliberazioni precedenti in materia adottate da questa Sezione, e così come riscontrato dalla consultazione dell'applicativo SICR. Trattasi della somma proveniente da risorse comunitarie a fondo perduto in favore del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri, a titolo di anticipo (10 per cento del totale dell'importo dell'Investimento pari a 623 milioni di euro) per l'Accordo che, come Amministrazione titolare dell'investimento in esame, lo stesso ha concluso in data 14 dicembre 2021 con l'Agenzia della Cybersicurezza.

A titolo di anticipazione è stata erogata anche la dotazione finanziaria complessiva di 99.680.000 euro, in data 3 maggio 2024, corrispondente al 16% dell'importo totale dell'investimento in esame, in virtù dell'art. 11 del decreto-legge n. 19, del 2 marzo 2024.

Risultano invece erogati a titolo di rimborso presentato dal Soggetto Attuatore euro 45.364.385,07, a fronte di un totale di 207.344.385,07 euro di risorse già trasferite. A tal proposito, si riportano nel dettaglio le somme a titolo di rimborso presentate dal Soggetto Attuatore, con riferimento all'anno 2024:

- rendiconto di progetto n. 3000028358 pari a 15.109.929,99, erogati in data 24/06/2024;
- rendiconto di progetto n. 3000006362 pari a 2.164.832,86, erogati in data 03/05/2024;
- rendiconto di progetto n. 3000033167 pari a 15.988.309,03, erogati in data 01/07/2024;
- rendiconto di progetto n. 5000031537 pari a 7.066.138,54, erogati in data 23/12/2024.

Per completezza espositiva, si deve indicare anche il titolo di rimborso presentato dal Soggetto attuatore nell'anno 2023, il cui rendiconto di progetto è il n. 3000001478, pari a 5.035.174,65 euro, erogati in data 29/11/2023.

A titolo esemplificativo, si fornisce qui di seguito una tabella riepilogativa dei movimenti di entrata e in uscita della Contabilità Speciale del Dipartimento per la trasformazione digitale, prodotta dagli Enti competenti.

Segue altra tabella contenente i medesimi dati a riscontro di quanto rappresentato dal Dipartimento della trasformazione digitale e dall'Agenzia per la Cybersicurezza, frutto della interrogazione per l'anno 2024, effettuata dalla Sezione, del sistema applicativo Conosco, a disposizione della Corte dei conti.

All. 3 – Movimentazione fondi Investimento 1.5

Importi liquidati nel corso del 2024

Dati aggiornati al 19.12.2024

Movimentazioni in entrata sulla CS 6288 dal conto MEF 25091 - SERV.CENT.PNRR F.PERD. L178-2

N° Disposizione di Pagamento	Data Disposizione di Pagamento	Causale	Beneficiario	Conto beneficiario	CF/P.Iva	N° Ordine Prelevamento Fondi	Data Ordine Prelevamento Fondi	Cro/Quietanza	Importo OPF (€)
2024061151	05/03/2024	Rimb.man_ ID 3000028358 del 22/02/2024	PRESIDENZA DEL CONSIGLIO DEI MINISTRI/DIPARTIMENT O PER LA TRASFORMAZIONE DIGITALE	CS-348-06288	80188230587	2024001148	06.03.2024	2024000006	15.109.929,99
2024061190	23/04/2024	Rimb. Manuale_ ID 3000006362 del 08/04/2024	PRESIDENZA DEL CONSIGLIO DEI MINISTRI/DIPARTIMENT O PER LA TRASFORMAZIONE DIGITALE	CS-348-06288	80188230587	2024001187	26.04.2024	2024000021	2.164.832,86
2024061188	23/04/2024	Anticipo per Accordo DTD-ACN del 14.12.2021	PRESIDENZA DEL CONSIGLIO DEI MINISTRI/DIPARTIMENT O PER LA TRASFORMAZIONE DIGITALE	CS-348-06288	80188230587	2024001186	26.04.2024	2024000020	99.680.000,00
2024061224	20/06/2024	Rimb. manuale Rend. progetto ID 3000033167 del 04/06/2024	PRESIDENZA DEL CONSIGLIO DEI MINISTRI/DIPARTIMENT O PER LA TRASFORMAZIONE DIGITALE	CS-348-06288	80188230587	2024001222	24.06.2024	2024000039	15.988.309,03
2024061417	13/12/2024	Rimb. manuale Rend. progetto ID 5000031537 del 25/11/2024	PRESIDENZA DEL CONSIGLIO DEI MINISTRI/DIPARTIMENT O PER LA TRASFORMAZIONE DIGITALE	CS-348-06288	80188230587	2024001408	16.12.2024	2024000086	7.066.138,54
								Totale entrata CS 2024	**140.009.210,42**

Movimentazioni in uscita dalla CS 6288 al Soggetto Attuatore

N° Disposizione di Pagamento	Data Disposizione di Pagamento	Causale	Beneficiario	Conto beneficiario	CF/P.Iva	N° Ordine Prelevamento Fondi	Data Ordine Prelevamento Fondi	Cro/Quietanza	Importo OPF (€)
2024420053	07/03/2024	S2RDP014.24_ M1C1 1.5_ACN_rimb.man_ ID 3000028358 del 22/02/2024	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	TU-348-320645	96501130585	2024003771	08/03/2024	70133467013346	15.109.929,99
2024420106	29/04/2024	S2RDP030.24_ M1C1 1.5_ACN_rimb.man_ ID 3000006362 del 08/04/2024	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	TU-348-320645	96501130585	2024007189	30/04/2024	3344717334471	2.164.832,86
2024420107	29/04/2024	Anticipo per Accordo DTD-ACN del 14.12.2021	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	TU-348-320645	96501130585	2024007192	30/04/2024	73344747334474	99.680.000,00
2024420178	25/06/2024	S2RDP046.24 M1C1 1.5 ACN rimb. man ID 3000033167 del 04/06/2024	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	TU-348-320645	96501130585	2024016252	27/06/2024	77251297725129	15.988.309,03
2024420337	17/12/2024	S2RDP0104.24 M1C1 1.5 ACN rimb. man ID 5000031537 del 25/11/2024	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	TU-348-320645	96501130585	2024036648	19/12/2024	89188588918858	7.066.138,54
								Totale uscita CS 2024	**140.009.210,42**

Titoli Contabilità Speciali

Data Movimento	Esercizio	Codice Conto		Tipo Conto	Tesoreria		Numero Titolo CS	Anno Emissione Titolo CS	Tipo Imputazione CS	Cassa Pagatrice	Desc Cassa 76-77-7C-7U	Causale	Titolo CS (RGS)
08/03/2024	2024	000006288	PNRR-DIP TRANSIZIONE DIGITALE	CS	348	ROMA	3771	2024	Competenza	77-Riversamento su T.U.	348 - 000320645 - TU	CUPF84E21007910007Cybersecurity - S2RDP014.24_ M1C1 1.5_ACN_	**15.109.929,99**
30/04/2024	2024	000006288	PNRR-DIP TRANSIZIONE DIGITALE	CS	348	ROMA	7189	2024	Competenza	77-Riversamento su T.U.	348 - 000320645 - TU	CUPF81B21008190007Cybersecurity - S2RDP030.24_ M1C1 1.5_ACN_	**2.164.832,86**
30/04/2024	2024	000006288	PNRR-DIP TRANSIZIONE DIGITALE	CS	348	ROMA	7192	2024	Competenza	77-Riversamento su T.U.	348 - 000320645 - TU	Cybersecurity - S2RDP033.24_ M1C1 1.5_ACN_seconda anticipazi	**99.680.000,00**
27/06/2024	2024	000006288	PNRR-DIP TRANSIZIONE DIGITALE	CS	348	ROMA	16252	2024	Competenza	77-Riversamento su T.U.	348 - 000320645 - TU	CUPF84E21007910007Cybersecurity - S2RDP046.24 M1C1 1.5 ACN_r	**15.988.309,03**
19/12/2024	2024	000006288	PNRR-DIP TRANSIZIONE DIGITALE	CS	348	ROMA	36648	2024	Competenza	77-Riversamento su T.U.	348 - 000320645 - TU	Cybersecurity - S2RDP0104.24 M1C1 1.5ACN Rend mult ID 50000	**7.066.138,54**

Per quanto concerne i progetti a rendiconto, dalla consultazione del cruscotto Monitoraggio Rendiconti di Misura è stato possibile verificare che oltre al progetto a rendiconto (progetto n. 3000001478) concernente i Servizi a supporto dell'Agenzia per la Cybersicurezza Nazionale - Attività di costituzione operativa di ACN e successivo espletamento delle proprie funzioni, di cui si è già dato conto nella precedente relazione e la cui somma erogata in data 29 novembre 2023 ammonta a 5.035.174,65, sono presenti altri 3 progetti a rendiconto per l'anno 2024 a titolarità. A tal riguardo, gli Enti competenti hanno fornito in corso di istruttoria una serie di dati relativi sia ai progetti rendicontati a titolarità, che a quelli a regia. Seguono, pertanto, due diverse tabelle contenti le relative informazioni:

PROGETTI RENDICONTATI - ANNO 2024						
PROGETTI A TITOLARITA'						
ID Rendiconto ReGiS	*Data Rendiconto*	*CUP*	*Contratto – CIG Titolo*	*Titolo Progetto*	*Stato*	*Importo lordo IVA e netto 0,5%*
3000028358	21/02/2024	F84E21007910007	ID 2212 AQ_Cloud_L1 - 89809767D8	Servizi a supporto dell'Agenzia per la Cybersicurezza Nazionale - Attività di costituzione operativa di ACN e successivo espletamento delle proprie funzioni	Approvato dal DTD e rimborsato	15.109.929,99 €
3000006362	03/04/2024	F81B21008190007	ID 2212 AQ_Cloud_L6 - 90031133E1	Servizi a supporto dell'Agenzia per la Cybersicurezza - Governance trasversale del programma	Approvato dal DTD e rimborsato	2.164.832,86 €
3000033167	30/05/2024	F84E21007910007	ID 2212 AQ_Cloud_L1 - 89809767D8	Servizi a supporto dell'Agenzia per la Cybersicurezza Nazionale - Attività di costituzione operativa di ACN e successivo espletamento delle proprie funzioni	Approvato dal DTD e rimborsato	15.988.309,03 €
Totale titolarità					**33.263.071,88 €**	

PROGETTI A REGIA						
ID Rendiconto ReGiS	**Data Rendiconto**	**CUP**	**CLP – Sub Attuatore**	**Titolo Progetto**	**Stato**	**Importo lordo IVA**
5000031537	25/11/2024	G56G21009570006	G56G21009570006 – Guardia di Finanza	Missione digitale	Approvato dal DTD e rimborsato	**700.000,00 €**
		D56G22000410006	D56G22000410006 – Arma dei Carabinieri	Controllo remoto dei nodi		**3.705.713.40 €**
		H86G21005760001	11_WP9_RIST_CORTCOST_3 – Cortecostituzionale	Sala server della corte costituzionale		**325.714,82 €**
		I86G22000280006	22_WP9_RIST_SGPR_1 - Segretariato Generale della Presidenza della Repubblica	Potenziamento rilevamento eventi		**976.639,51 €**
		G84F22000630006	01_WP12_Rist_MEF_1 – Ministero dell'economia e delle finanze	MEFLAB CYSEC		**963,265.64 €**
		C17H22002830006	39_WP_9_rist_Comune_di_Torino – Comune di Torino	Analisi e miglioramento cybersecurity		**133.111,65 €**
		C17H22002840006	41_WP_9_rist_Comune_di_Torino – Comune di Torino	Incremento della consapevolezza del rischio cyber torino		**133.111,62 €**
		J84F22000960006	16_WP_9_rist_Roma_Capitale – Roma Capitale	CYBER STRATEGY DI ROMA CAPITALE		**128.581,90 €**
Totale titolarità					**33.263.071,88 €**	

È stato comunicato che, rispetto alla dotazione finanziaria complessiva dell'investimento, pari a 623.000.000 euro, allo stato si registrano impegni attivi per un totale di circa 613 milioni. Di questi, circa 207 milioni riguardano attività a titolarità e circa 406 milioni riguardano attività a regia. Le spese già sostenute sono pari complessivamente a circa 140 milioni.

7. Stato di avanzamento dei milestone e target relativi all'Investimento in esame in relazione alla sua pianificazione per l'anno 2024

In relazione all'Investimento 1.5, appare utile rappresentare nuovamente le cadenze temporali afferenti gli obiettivi e traguardi (milestone e target) al cui conseguimento sono collegati l'assegnazione delle risorse previste dal Next Generation EU.

Per l'erogazione delle risorse è stato previsto, come primo step, il raggiungimento dei seguenti milestone e target europei entro dicembre 2022:

- Milestone UE (M1C1-5): Creazione della Nuova agenzia nazionale per la sicurezza informatica;
- Milestone UE (M1C1-6): Primo dispiegamento dei servizi nazionali di sicurezza informatica;
- Milestone UE (M1C1-7): Avvio della rete dei laboratori di screening e certificazione della cybersecurity;
- Milestone UE (M1C1-8): Attivazione di un'unità centrale di audit per misure di sicurezza PSNC e NIS;
- Target intermedio UE (M1C1-9): Supporto all'aggiornamento delle misure di sicurezza – 5 strutture di sicurezza adeguate.

Entro dicembre 2024, invece, erano stati fissati i seguenti traguardi:

- Target finale UE (M1C1-19): Supporto all'aggiornamento delle misure di sicurezza – 50 strutture di sicurezza adeguate;
- Milestone UE (M1C1-20): Implementazione completa dei servizi nazionali di sicurezza informatica;

- Milestone UE (M1C1-21): Completamento della rete dei laboratori di screening e certificazione della cybersecurity, Evaluation center;

- Milestone UE (M1C1-22): Piena operatività dell'unità centrale di audit per le misure di sicurezza PSNC e NIS con almeno 30 ispezioni completate.

Nella deliberazione adottata dalla Sezione lo scorso anno, la n. 17 del 6 febbraio 2024, è stata fornita, a titolo esemplificativo, una tabella contenenti i dati estrapolati dal sistema REGIS (aggiornati al 31 dicembre 2023) relativi alle Milestone e Target di rilevanza europea, dalla quale risultavano completati 4 milestone e 1 un target.

Dalla consultazione dell'applicativo Regis, inoltre, componente "Avanzamento M&T" di cui all'investimento 1.5, è stato possibile estrapolare i dati concernenti le Milestone e i Target di rilevanza europea aggiornati al 31 dicembre 2024, nell'ambito dei quali risultano completati sia i 7 milestone che i 2 target. A tal riguardo, si riporta qui di seguito la relativa tabella:

REGIS ATTUAZIONE - AVANZAMENTO MILESTONE & TARGET					
Tipo M/T	**Numero sequenziale (M&T)**	**Testo M&T**	**Data presunto completamento**	**Misura associata**	**Stato avanzamento M&T**
Milestone	M1C1-20	Dispiego integrale dei servizi nazionali di cybersecurity	31.12.2024	M1C1I1.5	**COMPLETATO**
Milestone	M1C1-21	Completamento della rete dei laboratori e dei centri di valutazione per la valutazione e certificazione della cybersecurity	31.12.2024	M1C1I1.5	**COMPLETATO**
Milestone	M1C1-22	Piena operatività dell'unità di audit per le misure di sicurezza PSNC e NIS con il completamento di almeno 30 ispezioni	31.12.2024	M1C1I1.5	**COMPLETATO**
Milestone	M1C1-5	Istituzione della nuova Agenzia per la cybersicurezza nazionale	31.12.2022	M1C1I1.5	**COMPLETATO**
Milestone	M1C1-6	Dispiego iniziale dei servizi nazionali di cybersecurity	31.12.2022	M1C1I1.5	**COMPLETATO**
Milestone	M1C1-7	Avvio della rete dei laboratori di screening e certificazione della cybersecurity	31.12.2022	M1C1I1.5	**COMPLETATO**

Milestone	M1C1-8	Attivazione di un'unità centrale di audit per misure di sicurezza PSNC e NIS	31.12.2022	M1C1I1.5	**COMPLETATO**
Target	M1C1-19	Sostegno al potenziamento delle strutture di sicurezza T2	31.12.2024	M1C1I1.5	**COMPLETATO**
Target	M1C1-9	Sostegno al potenziamento delle strutture di sicurezza T1	31.12.2022	M1C1I1.5	**COMPLETATO**

Per fornire un quadro generale della tematica di cui sopra, appare utile inserire anche una tabella riepilogativa delle varie attività collegate all'investimento in esame in relazione ai diversi target e milestone europei da raggiungere, comprensiva, altresì, sia degli ulteriori step procedurali che delle date programmate ed effettive di inizio e di fine attività. I dati contenuti nella tabella sono il frutto della consultazione effettuata, al 31 dicembre 2024, sul sistema REGIS, componente "Report Cronoprogramma".

Attività	Tipologia attività	Iter procedurale	Stato	Indicatore	Data inizio prevista	Data fine effettiva	Note di dettaglio	Appunti
Adozione atti di organizzazione dell'Agenzia	**Step procedurale**	Approvazione Regolamento	**Completato**		09/12/2021	09/12/2021	Adottati atti di organizzazione dell'Agenzia	Atti di organizzazione dell'Agenzia
Attivazione del CVCN	**Step procedurale**	Attivazione servizi	**Completato**		01/09/2021	30/06/2022	Dal 1/07 è operativo presso l'Agenzia per la Cybersicurezza Nazionale (ACN), il Centro di Valutazione e Certificazione Nazionale. https://www.cybersecitalia.it/perimetro-di-sicurezza-operativo-il-cvcn-per-testare-hardware-e-software-di-5g-cloud/19977/	Dal 1/07 è operativo presso l'Agenzia per la Cybersicurezza Nazionale (ACN), il Centro di Valutazione e Certificazione Nazionale (CVCN). https://www.cybersecitalia.it/perimetro-di-sicurezza-operativo-il-cvcn-per-testare-hardware-e-software-di-5g-cloud/19977/
"Attivazione di un'unità centrale di audit per le misure di sicurezza PSNC e NIS M1C1-8"	**Milestone UE**	Realizzazione delle forniture/acquisizione di beni	**Completato**	**M1C1-8**	01/01/2022	31/12/2022	Definizione del nucleo ispettivo	

Avanzamento attivazione dei Centri di Valutazione di Difesa e Interno	**Step procedurale**	Monitoraggio stato avanzamento target	**Completato**		01/01/2023	31/12/2023	In vista di M1C1-21	Sono state avviate le attività volte all'attivazione dei Centri di Valutazione di Difesa e Interno.Avanzamento dei lavori in linea con i rispettivi Gantt dei piani operativi, con accreditamento previsto entroDicembre 2024 e preliminare attivazione delle capacità dei CV entro ottobre 2024
Avanzamento del sostegno al potenziamento delle strutture di sicurezza T2	**Step procedurale**	Monitoraggio stato avanzamento target	**Completato**		01/01/2023	31/12/2023	in vista di M1C1-19	Sono state avviate le attività relative agli ulteriori interventi di potenziamento delle strutture di sicurezza, con il completamento di circa 27 interventi
Avanzamento nello stato di attivazione dei servizi nazionali di cybersecurity	**Step procedurale**	Monitoraggio stato avanzamento target	**Completato**		01/01/2023	31/12/2023	in vista di M1C1-20	Sono state avviate le attività relative all'attivazione delle squadre di pronto intervento informatico (CERT), del centro nazionale di condivisione e di analisi delle informazioni (ISAC), e dell'HyperSoc nazionale.

Avanzamento nello stato di attivazione della rete dei laboratori e dei centri di valutazione per la valutazione e certificazione della cybersecurity	**Step procedurale**	Monitoraggio stato avanzamento target	**Completato**		01/01/2023	31/12/2023	In vista del conseguimento della Milestone M1C1-21	Sono state avviate le attività volte all'attivazione della rete dei laboratori e dei centri di valutazione per la valutazione e certificazione della cybersecurity.Avviati 7 laboratori con procedura in corso per accreditamento come LAP.
Avanzamento verso la piena operatività dell'unità di audit per le misure di sicurezza PSNC e NIS con il completamento di almeno 15 ispezioni	**Step procedurale**	Monitoraggio stato avanzamento target	**Completato**		01/01/2023	30/06/2024	In vista di M1C1-22	Completate 15 ispezioni in ambito PSNC e NIS, in corso di predisposizione e rendicontazione le ispezioni completate

"Avvio della rete dei laboratori di screening e certificazione della cybersecurity M1C1-7"	**Milestone UE**	Inizio fornitura	**Completato**	**M1C1-7**	01/01/2022	31/12/2022		

"Completamento della rete dei laboratori e dei centri di valutazione per la valutazione e certificazione della cybersecurity M1C1-21"	**Milestone UE**	Realizzazione delle forniture/acquisizione di beni	**Completato**	**M1C1-21**	01/02/2023	31/12/2024	Attivazione di almeno 10 laboratori di screening e certificazione, dei due centri di valutazione (CV), e attivazione del laboratorio di certificazione UE.	
"Dispiego iniziale dei servizi nazionali di cybersecurity M1C1-6"	**Milestone UE**	Realizzazione delle forniture/acquisizione di beni	**Completato**	**M1C1-6**	01/01/2022	31/12/2022	Definizione dell'architettura dettagliata dell'intero ecosistema della cybersecurity nazionale (ovvero un centro nazionale di condivisione e di analisi delle informazioni (ISAC), una rete di squadre di pronto intervento informatico (CERT), un HyperSOC nazionale, il calcolo ad alte prestazioni integrato dagli strumenti di intelligenza artificiale/apprendimento automatico (AI/ML) per analizzare gli incidenti di	

							cybersecurity di portata nazionale)	
"Dispiego integrale dei servizi nazionali di cybersecurity M1C1-20"	**Milestone UE**	Realizzazione delle forniture/acquisizione di beni	**Completato**	**M1C1-20**	01/02/2023	31/12/2024	Attivazione delle squadre di pronto intervento informatico (CERT), la loro interconnessione con il team italiano di risposta agli incidenti di sicurezza informatica (CSIRT) e con il centro nazionale di condivisione e di analisi delle informazioni (ISAC) e l'integrazione di almeno 5 centri operativi di sicurezza (SOC) con l'HyperSOC nazionale, la piena operatività dei servizi di gestione dei rischi di cybersecurity, compresi quelli per l'analisi della catena di	

							approvvigionamento e i servizi di assicurazione contro i rischi informatici.	
Istituzione della nuova Agenzia per la cybersicurezza nazionale M1C1-5	**Milestone UE**	Istituzione Agenzia	**Completato**	**M1C1-5**	31/12/2022	31/12/2022		
Nuove procedure di selezione delle amministrazioni oggetto di intervento	**Step procedurale**	Pubblicazione Avvisi/Bandi	**Completato**		01/01/2023	31/12/2023	Nuovi bandi per Fase 2 potenziamento PA	Nuovi bandi per Fase 2 potenziamento PA: pubblicati da ACN Avvisi 6/2023 e 7/2023

Piena operatività dell'unità di audit per le misure di sicurezza PSNC e NIS con il completamento di almeno 30 ispezioni M1C1-22	**Milestone UE**	Realizzazione delle forniture/acquisizione di beni	**Completato**	**M1C1-22**	01/02/2023	31/12/2024		
Procedure di selezione delle amministrazioni oggetto di intervento	**Step procedurale**	Pubblicazione Avvisi/Bandi	**Completato**		01/01/2022	01/07/2022		Pubblicazione Avvisi di selezione per le amministrazioni oggetto di intervento
Selezione profili professionali	**Step procedurale**	Pubblicazione Avvisi/Bandi	**Completato**		01/09/2021	22/02/2022	Bando di concorso per l'assunzione di 50 unità di personale a tempo indeterminato nei segmenti di Esperto	Pubblicazione del Bando di concorso per l'assunzione di 50 unità di personale a tempo indeterminato nei segmenti di Esperto

"Sostegno al potenziamento delle strutture di sicurezza T1 M1C1-9"	**Target UE**	Verifica raggiungimento Target	**Completato**	**M1C1-9**	01/01/2022	31/12/2022		
"Sostegno al potenziamento delle strutture di sicurezza T2 M1C1-19"	**Target UE**	Verifica raggiungimento Target	**Completato**	**M1C1-19**	01/02/2023	31/12/2024	Almeno 50 interventi di potenziamento effettuati nei settori del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e delle reti e sistemi informativi (NIS). I tipi di intervento riguardano, ad esempio, i centri operativi per la sicurezza (SOC), il miglioramento della difesa dei confini informatici e le capacità interne di monitoraggio e controllo nel rispetto dei requisiti NIS e PSNC. Gli interventi devono riguardare in particolare i settori dell'assistenza sanitaria, dell'energia e	

							dell'ambiente (approvvigionamento di acqua potabile).	

In linea con il traguardo dell'Investimento 1.5 target M1C1-19 - (target finale UE) "Supporto all'aggiornamento delle misure di sicurezza T2 - 50 strutture di sicurezza adeguate entro dicembre 2024" – risulta essere l'avviso pubblico n. 08/2024, alla cui documentazione è possibile accedere attraverso la consultazione del sito istituzionale dell'Agenzia per la Cybersicurezza.

L'Avviso in parola ha ad oggetto la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente a valere sul Piano Nazionale di Ripresa e Resilienza.

La dotazione finanziaria prevista per l'Avviso in esame ammonta complessivamente a € 50.000.000,00, a valere sull'Investimento 1.5 "Cybersecurity" e l'Agenzia si riserva la facoltà di incrementare la dotazione finanziaria dello stesso Avviso.

Nel documento esplicativo viene specificato che ciascun Soggetto partecipante dovrà presentare un progetto finalizzato all'analisi e al potenziamento delle proprie capacità di resilienza cyber in termini di postura di sicurezza, processi e modello organizzativo, competenze e, infine, sistemi e tecnologie abilitanti.

Le attività progettuali finanziabili a valere sul presente Avviso sono, infatti, mirate al miglioramento delle capacità di governo e gestione del rischio cyber, per contrastare uno scenario di minaccia in continua evoluzione, e contestualmente consentire una risposta tempestiva a potenziali attacchi informatici.

È previsto, altresì, che le attività progettuali proposte potranno prevedere uno o più degli interventi di cui ai successivi punti:

1. Governance e programmazione cyber: coordinamento, supervisione e gestione olistica e integrata della cybersecurity attraverso la programmazione strategica di investimenti e iniziative;

2. Gestione del rischio cyber e della continuità operativa: individuazione, valutazione e trattamento sistematico dei rischi associati all'ambito cyber, e implementazione di un piano volto a garantire la resilienza di funzioni e servizi critici in caso di eventi avversi;

3. Gestione e risposta agli incidenti di sicurezza: monitoraggio, identificazione e

gestione degli incidenti cyber, e ripristino dei sistemi impattati;

4. Gestione delle identità digitali e degli accessi logici: governo delle identità e definizione dei permessi di accesso alle risorse al fine di autenticare e autorizzare correttamente persone, gruppi e servizi in base agli attributi specifici e ai principi di "need to know", "least privilege" e "segregation of duties";

5. Sicurezza delle applicazioni, dei dati e delle reti: protezione dell'infrastruttura applicativa e di rete, e regolamentazione dei processi di protezione dei dati riservati, al fine di prevenire l'occorrenza di potenziali incidenti cyber e ridurne gli impatti.

Sono ammessi alla partecipazione ai fini del riconoscimento ed erogazione del contributo in oggetto i grandi Comuni, ovvero i Comuni italiani con una popolazione residente superiore a 100.000 abitanti, i Comuni capoluogo di Regione, le Città Metropolitane, le Agenzie regionali sanitarie, le Aziende ed enti di supporto al Servizio Sanitario Nazionale, le Autorità di sistema portuale, le Autorità del Bacino del Distretto idrografico e le Agenzie regionali per la protezione dell'ambiente.

Si pone in evidenza, che con determina del 23 settembre 2024, unitamente all'approvazione degli elenchi relativi alla graduatoria definitiva, è stata rifinanziata con ulteriori 50.000.000,00 di euro la dotazione finanziaria iniziale complessiva dell'Avviso n. 8/2024, di cui alla determina ACN prot. n. 5959 del 26 febbraio 2024, al fine dello scorrimento della graduatoria dei progetti ammissibili ma parzialmente finanziabili e idonei ma non finanziabili per esaurimento delle risorse disponibili.

Successivamente, con ulteriore determina del 31 dicembre 2024, si è provveduto a rifinanziare con ulteriori 8.000.000,00 di euro la dotazione finanziaria dell'Avviso n. 08/2024, di cui alla determina ACN prot. n. 33707 del 17 ottobre 2024; ciò, al fine dello scorrimento della graduatoria dei progetti ammissibili ma parzialmente finanziabili ed idonei ma non finanziabili per esaurimento delle risorse disponibili, coerentemente con la previsione di cui al paragrafo 4.3 dell'Avviso di che trattasi "l'importo massimo ammissibile a finanziamento è pari a € 1.500.000,00 per Soggetto proponente ivi inclusi tutti i costi diretti, comprensivi di IVA laddove applicabile, e le spese generali qualora valorizzate".

In merito alla graduatoria definitiva a valere sull'Avviso n. 8 del 2024, si riportano in estrema sintesi i relativi dati estrapolati dalle tabelle allegate alla determina di cui sopra:

- Nell'allegato A, risultano finanziati 97 proposte di intervento, per un totale di euro 97.949.498,38;
- Nell'allegato B, le proposte di intervento progettuali parzialmente finanziabili sono 2, per un importo di 2.050.501, 62 euro;
- Negli allegati C e D, sono contenute le proposte di intervento progettuali rispettivamente idonee ma non finanziabili (n. 13 interventi) e quelle non ammesse (3 interventi).

A seguito di diverse interlocuzioni intercorse con l'Agenzia per la cybersicurezza, è stato possibile acquisire specifiche e dettagliate informazioni in merito ai risultati raggiunti con il target M1C1-19 "almeno 50 interventi" di potenziamento cyber entro dicembre 2024. Da quanto appreso in corso di istruttoria, il target risulta essere raggiunto con la realizzazione di 55 interventi, a cui si aggiungono i 7 interventi di potenziamento cyber raggiunti con il Target della M1C1-9, per un totale di 62 complessivi.

Per la realizzazione dei suddetti interventi, l'Agenzia per la cybersicurezza ha espletato quattro procedure selettive, mediante la pubblicazione di Avvisi Pubblici volti al finanziamento di proposte progettuali finalizzate al potenziamento del livello di maturità della gestione del rischio cyber della Pubblica Amministrazione, centrale e locale.

Collegato al target M1C1-19 risulta essere anche l'Avviso n. 8 del 2024 ampiamente descritto in precedenza, i cui progetti finanziati sono imputabili all'anno 2025.

In ordine agli interventi di cui sopra, appare interessate la tabella prodotta dall'Agenzia rappresentativa sia della tipologia di intervento, che delle modalità di attivazione, oltre ad altri elementi utili alla identificazione degli stessi.

Target	Soggetto	ID	Ambito PSNC	Ambito NIS/NIS2	Energia	Sanitario	Ambiente (Approvvigionamento di acqua potabile e gestione dei rifiuti)	Tipologia Intervento	Modalità di attivazione
M1C1-19	Consiglio di Stato	01_CyberDef_Consiglio_di_Stato		X				Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	HyperSOC 1	01_HyperSOC_Energia	X	X	X			Miglioramento delle capacità interne di monitoraggio e controllo	Attivazione servizi ACN
M1C1-19	MISP 1	01_MISP_Multisettore	X	X	X	X	X	Miglioramento della difesa dei confini informatici	Attivazione servizi ACN
M1C1-19	Arma dei Carabinieri	02_CyberDef_Arma_Carabinieri	X					Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	HyperSOC2	02_HyperSOC_Telco	X	X				Miglioramento della difesa dei confini informatici	Attivazione servizi ACN
M1C1-19	Guardia di finanza	03_CyberDef_Guardia_di_finanza	X					Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	Ministero della Giustizia	04_CyberDef_Ministero_Giustizia	X					Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	HyperSOC4	04_HyperSOC_Manufatturiero_Tecnologico	X	X				Miglioramento delle capacità interne di monitoraggio e controllo	Attivazione servizi ACN

M1C1-19	Ministero dell'Ambiente e della sicurezza energetica	05_WP9_A7_MASE + HyperSOC + MISP		X	X		X	Miglioramento della difesa dei confini informatici	Avvisi a Titolarità & Attivazione servizi ACN
M1C1-19	Agenzia delle Dogane e dei Monopoli	05_WP9_Rist_AgDO_1		X				Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Regia
M1C1-19	Regione Piemonte	06_WP_9_rist_Regione Piemonte		X		X	X	Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Regia
M1C1-19	Regione Piemonte	07_WP_9_rist_Regione Piemonte		X			X	Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	Agenzia del Demanio	07_WP9_Rist_AgDEM_1 + AgDem_1		X				Miglioramento della difesa dei confini informatici	Avvisi a Titolarità & Avvisi a Regia
M1C1-19	Camera dei Deputati	08_WP9_Rist_CAM_1 + Camera_1		X				Miglioramento della difesa dei confini informatici	Avvisi a Titolarità & Avvisi a Regia
M1C1-19	Corte Costituzionale	11_WP9_Rist_CORTCOST_3		X				Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	Roma Capitale	14_WP_9_rist_Roma Capitale		X				Realizzazione di Security Operations Center (SOC)	Avvisi a Regia
M1C1-19	Regione Puglia	17_WP_9_rist_Regione Puglia		X		X	X	Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	Ministero dell'Economia e delle Finanze	17_WP9_Rist_MEF_2 + MEF_2 + MEF_3	X					Miglioramento della difesa dei	Avvisi a Titolarità & Avvisi a Regia

								confini informatici	
M1C1-19	Regione Puglia	18_WP_9_rist_Regione Puglia		X		X	X	Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	Regione Calabria	19_WP_9_rist_Regione Calabria		X		X		Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Regia
M1C1-19	Regione Calabria	20_WP_9_rist_Regione Calabria		X		X		Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	Segretariato Generale della Presidenza della Repubblica	22_WP9_Rist_SGPR_1		X				Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	Regione Liguria	23_WP_9_rist_Regione Liguria		X		X		Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Regia
M1C1-19	Ministero degli Affari Esteri e della Cooperazione Internazionale	23_WP9_Rist_MAECI_1 + MAECI_2	X					Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità & Avvisi a Regia
M1C1-19	Regione Liguria	24_WP_9_rist_Regione Liguria		X		X		Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	Ministero dell'ambiente e della sicurezza energetica	26_WP9_Rist_MITE_1 + 27_WP9_Rist_MITE_2		X	X		X	Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	Regione Lombardia	28_WP_9_rist_Regione Lombardia		X		X	X	Miglioramento della difesa dei	Avvisi a Regia

								confini informatici	
M1C1-19	Regione Friuli Venezia Giulia	29_WP_9_rist_Regione Friuli Venezia Giulia		X		X		Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Regia
M1C1-19	Regione Toscana	31_WP_9_rist_Regione Toscana		X		X	X	Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Regia
M1C1-19	Regione Toscana	32_WP_9_rist_Regione Toscana		X		X	X	Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	Regione Lazio	35_WP_9_rist_Regione Lazio		X		X		Miglioramento delle capacità interne di monitoraggio e controllo	Attivazione servizi ACN
M1C1-19	Regione Veneto	36_WP_9_rist_Regione Veneto		X		X	X	Realizzazione di Security Operations Center (SOC)	Avvisi a Regia
M1C1-19	Regione Veneto	37_WP_9_rist_Regione Veneto		X		X	X	Realizzazione di Security Operations Center (SOC)	Avvisi a Regia
M1C1-19	Comune di Messina	42_WP_9_rist_Comune di Messina		X		X		Realizzazione di Security Operations Center (SOC)	Avvisi a Regia
M1C1-19	Comune di Milano	44_WP_9_rist_Comune di Milano		X			X	Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Regia
M1C1-19	Regione Marche	49_WP_9_rist_Regione Marche		X		X		Realizzazione di Security	Avvisi a Regia

								Operations Center (SOC)	
M1C1-19	Regione Lombardia	52_WP_9_rist_Regione Lombardia		X		X		Miglioramento della difesa dei confini informatici	Avvisi a Regia
M1C1-19	Regione Campania	56_WP_9_rist_Regione Campania		X		X		Realizzazione di Security Operations Center (SOC)	Avvisi a Regia
M1C1-19	Regione Emilia Romagna	64_WP_9_rist_Regione Emilia Romagna		X	X	X		Realizzazione di Security Operations Center (SOC)	Avvisi a Regia
M1C1-19	Regione Emilia Romagna	67_WP_9_rist_Regione Emilia Romagna		X	X	X		Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Regia
M1C1-19	Agcom - Autorità per le garanzie nelle comunicazioni	AGCOM_1		X				Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità
M1C1-19	Agenzia nazionale per i servizi sanitari regionali	AGENAS_1		X		X		Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità
M1C1-19	Autorità di regolazione per energia reti e ambiente	ARERA_1		X	X		X	Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità
M1C1-19	Consiglio Superiore della Magistratura	CSM_1	X					Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità

M1C1-19	Dipartimento Protezione Civile	DPC_1 + DPC_2	X					Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità
M1C1-19	Dipartimento dei Vigili del fuoco	DVF_1 + DVF_2 + 15_WP9_Rist_DVF_1	X					Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità & Avvisi a Regia
M1C1-19	Gestore Servizi Energetici	GSE_1		X	X			Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità
M1C1-19	Ministero della Difesa	MD_1	X					Realizzazione di Security Operations Center (SOC)	Avvisi a Titolarità
M1C1-19	Ministero della Difesa	MD_2	X					Realizzazione di Security Operations Center (SOC)	Avvisi a Titolarità
M1C1-19	Ministero della Difesa	MD_3	X					Realizzazione di Security Operations Center (SOC)	Avvisi a Titolarità
M1C1-19	Ministero Della Salute	MDS_2		X		X		Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità
M1C1-19	Ministero delle Imprese e del Made in Italy	MIMIT_2	X					Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità
M1C1-19	MIT	MIT_2	X					Realizzazione di Security Operations Center (SOC)	Avvisi a Titolarità

M1C1-19	Presidenza del Consiglio dei Ministri	PCM_2 + 02_WP9_Rist_PCM_2 + 02_WP9_Rist_PCM_3 + 02_WP9_Rist_PCM_4	X					Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità & Avvisi a Regia
M1C1-19	Senato	Senato_1 + MISP		X				Realizzazione di Security Operations Center (SOC)	Avvisi a Titolarità & Attivazione servizi ACN
			18	**41**	**8**	**23**	**14**		
M1C1-9	Ministero delle Imprese e del Made in Italy	MIMIT 1	X					Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità
M1C1-9	Ministero Della Salute	MDS 1		X		X		Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità
M1C1-9	Ministero Infrastrutture e Trasporti	MIT 1	X					Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità
M1C1-9	Presidenza del Consiglio dei Ministri	PCM 1	X					Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità
M1C1-9	Ministero degli Affari Esteri e della Cooperazione Internazionale	MAECI 1	X					Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Titolarità
M1C1-9	Ministero Economia e Finanze	MEF 1	X					Miglioramento delle capacità interne di	Avvisi a Titolarità

								monitoraggio e controllo	
M1C1-9	Ministero dell'ambiente e della sicurezza energetica	28_WP9_RIST_MITE_3		X	X			Miglioramento delle capacità interne di monitoraggio e controllo	Avvisi a Regia
			23	**43**	**9**	**24**	**14**		

Per quanto attiene invece la milestone M1C1-20 (target finale UE) "Implementazione completa dei servizi nazionali di sicurezza informatica entro dicembre 2024", finalizzata all'attivazione di squadre di pronto intervento informatico (CERT), interconnesse con CSIRT Italia, al fine di contribuire alla gestione dei rischi di cybersicurezza nel Paese, sempre dalla consultazione del sito istituzionale dell'Agenzia è stato possibile visualizzare l'invito a manifestare interesse del 13 giugno 2024, rivolto a tutti i Ministeri individuati ai sensi dell'articolo 2, comma 1, del decreto legislativo del 30 luglio 1999, n. 300, che presentino una manifestazione di interesse con un Piano Operativo rispondente alla Linee guida CSIRT.

Si evidenzia che l'Agenzia, all'esito della manifestazione di interesse, proporrà ai Ministeri interessati che hanno presentato domanda la stipula di un Accordo di collaborazione ex articolo 15 della legge 7 agosto 1990, n. 241, avente ad oggetto la realizzazione di uno CSIRT settoriale, definito secondo il Piano Operativo, da attivare nell'ambito della Missione 1, Componente 1, Investimento 1.5 "Cybersicurezza" del PNRR in coerenza con la milestone M1C1-20. Si aggiunga, altresì, che per l'attivazione degli interventi specifici stabiliti dai Piani Operativi proposti, l'Agenzia ha messo a disposizione un importo complessivo pari a euro 24.000.000,00, da ripartire - fino a concorrenza della dotazione totale, e fatta salva la possibilità di eventuale rifinanziamento del presente invito.

In ordine alle informazioni fornite dagli Enti competenti circa la milestone europea M1C1-20 sul "Dispiego integrale dei servizi cyber nazionali", i WP coinvolti sono dal n. 1 al n. 7.

In tale ambito si inserisce l'Avviso n. 6 - Avviso a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici – la cui disamina è stata già approfondita nella più volta citata deliberazione di questa sezione n. 17 del 2024.

Nell'ambito di tale Avviso, che si rivolge alle Regioni, è previsto il collegamento dei CSIRT regionali con l'Agenzia entro dicembre 2024. A tal proposito dalla documentazione trasmessa dagli Enti competenti in corso di istruttoria è stato possibile

acquisire informazioni approfondite circa lo stato di avanzamento sulla milestone in esame.

In merito alla CSIRT Italia e alla rete di CSIRT Nazionale, di fatti, che consistono in un sistema integrato per la risposta a minacce, incidenti e crisi cyber nazionali, è stato evidenziato che lo stesso si compone del CSIRT Italia (ovvero il Team Italiano di risposta agli incidenti informatici) e la rete di CERT a supporto della constituency nazionale nella gestione di minacce informatiche, ossia eventi di sicurezza monitorati che possono avere un potenziale impatto negativo, nonché di possibili incidenti informatici sui loro sistemi informativi che potrebbero generare situazioni di crisi a livello nazionale.

Tali servizi sono realizzati mediante una stretta collaborazione tra la rete di CERT, la constituency e lo CSIRT Italia come elemento centrale di integrazione anche verso il contesto europeo e internazionale delle omologhe agenzie cyber nazionali.

Nel corso del 2024, si apprende che sono state completate le piattaforme a supporto dello CSIRT Italia e finalizzata l'attivazione di 3 CERT regionali, presso tre regioni, quali Lombardia, Veneto e Toscana.

Nell'ambito della prosecuzione delle attività della presente Misura sarà completata l'attivazione degli altri CERT finanziati.

In merito alla condizionalità della milestone M1C1-20, relativa alla interconnessione delle squadre di pronto intervento informatico (CERT) con il centro nazionale di condivisione e di analisi delle informazioni (ISAC), si riportano i risultati forniti dagli Enti competenti.

L'ISAC Italia, appare utile ricordare, costituisce il servizio di condivisione e analisi, integrato anche con gestione del rischio cyber, che fornisce alla constituency sia informazioni strategiche e operative di alto valore aggiunto, che analisi specialistiche su cyber threat intelligence e analisi settoriali derivanti dalle attività di protezione e risposta di cui ai punti precedenti. Sulla base di tali analisi e attività operative, inoltre, vengono anche fornite alla constituency indicazioni di best-practice e linee guida per permettere il capacity building cyber nella constituency. Tali attività risultano integrate con la gestione del rischio nazionale effettuata dall'ACN, in particolare, anche al fine di prioritizzare nella constituency una sana gestione del rischio cyber, questa anche in attuazione dell'ultima direttiva EU NIS. A tal fine l'Agenzia mette a disposizione un tool di analisi

del rischio che permette la gestione di tale processo in modo continuativo ed efficace.

A fronte di quanto rappresentato, risulta pertanto attivata l'integrazione con i servizi di analisi e condivisione mediante sistemi e piattaforme dell'ISAC nazionale, c.d. ISAC Italia, presso l'ACN.

Per quanto concerne la condizionalità della milestone M1C1-20, relativa alla "integrazione di almeno 5 centri operativi di sicurezza (SOC) con l'HyperSOC nazionale", appare utile ricordare la funzionalità dell'HyperSOC, quale sistema integrato per la protezione degli asset strategici nazionali che fornisce alle organizzazioni pubbliche e private nazionali, la c.d. constituency, servizi a supporto del loro potenziamento delle capacità di monitoraggio e analisi di eventi di sicurezza.

Dalla scheda informativa fornita dal Dipartimento per la trasformazione digitale congiuntamente all'Agenzia per la Cybersicurezza, in corso di istruttoria, è stato evidenziato, in particolare, che il servizio realizzato fornisce alla constituency capacità di monitoraggio e segnalazione di eventi di cybersicurezza di interesse dei loro sistemi informatici e informazioni, permettendo quindi attività di comunicazione di early-warning su scenari cyber di interesse nazionale.

In ordine ai risultati raggiunti, pertanto, risultano attivate tutte le piattaforme informatiche a supporto dell'HyperSOC, sia interne dell'Agenzia che a supporto dell'interconnessione con soggetti esterni, integrando cinque SOC di organizzazioni nazionali.

Per quanto riguarda i risultati connessi alla milestone M1C1-21 "Attivazione di almeno 10 laboratori di screening e certificazione, dei due centri di valutazione (CV), e attivazione del laboratorio di certificazione UE" anche in questo caso gli Enti competenti hanno prodotto una scheda dettagliata, su specifica richiesta della Sezione.

A tal proposito, si apprende che partendo dalla Milestone M1C1-7, nella quale è stata avviata la rete dei laboratori di screening e certificazione della cybersecurity con la costituzione del primo laboratorio realizzato presso il Ministero dell'Economia e delle Finanze, la presente Milestone è stata raggiunta con l'attivazione di un numero complessivo di 10 laboratori e di 2 centri di valutazione (CV).

A tale scopo, occorre ricordare, che l'Agenzia per la cybersicurezza nazionale ha

promosso e attuato diverse iniziative di finanziamento indirizzate sia alla Pubblica Amministrazione che agli Operatori Economici, al fine di costruire e consolidare le capacità nazionali di valutazione e scrutinio tecnologico della sicurezza su beni, sistemi e servizi ICT e sviluppare competenze e capacità specialistiche necessarie a garantire adeguati livelli di cyber resilienza per il paese.

Per quanto attiene alle iniziative verso la Pubblica Amministrazione, l'Agenzia ha stipulato specifici Accordi attuativi con il Ministero dell'Interno e della Difesa, che hanno consentito l'attivazione dei Centri di Valutazione (CV) a supporto del Centro di Valutazione e Certificazione Nazionale (CVCN), istituito presso l'Agenzia. A tale scopo è stato pubblicato l'Avviso Pubblico n. 4/2022, già descritto nelle precedenti deliberazioni esitate da questa Sezione, che ha permesso l'attivazione del primo laboratorio di scrutinio tecnologico nell'ambito della Pubblica Amministrazione.

Per quanto riguarda, invece, le iniziative verso gli Operatori economici, con l'Avviso n. 5/2022., anch'esso ampiamento descritto nelle precedenti deliberazioni della Sezione, è stato possibile estendere, da parte dell'Agenzia, la concessione di finanziamenti per la costituzione ed il potenziamento di laboratori a supporto del CVCN e dei CV, anche ai soggetti privati, portando all'attivazione di ulteriori 9 laboratori di scrutinio tecnologico.

Nella scheda relativa alla milestone in esame, si specifica, altresì, che per attivazione dei laboratori, così come previsto dalle Determinazioni tecniche emanate dal CVCN, si intende il possesso dei seguenti requisiti e delle seguenti capacità:

a) requisiti tecnici e logistici tra cui quelli relativi alla dotazione strumentale per l'esecuzione dei test e alla protezione degli ambienti di test;

b) misure di sicurezza informatica;

c) requisiti di competenza ed esperienza.

Passando ora a trattare lo stato di avanzamento della milestone europea M1C1-22, volta alla "Piena operatività dell'unità di audit per le misure di sicurezza PSNC e NIS con il completamento di almeno 30 ispezioni", è stato posto in evidenza, nella documentazione fornita alla scrivente Sezione, che il percorso intrapreso per la milestone in esame è iniziato con l'attivazione presso l'Agenzia di un'unità centrale ispettiva di audit, la cui realizzazione è collegata alla Milestone M1C1-8.

In tale ambito, è stato evidenziato come l'istituzione dell'Unità Centrale Ispettiva presso l'Agenzia sia avvenuta con l'adozione del DPCM n. 92 del 2022.

Più nello specifico, è necessario rievocare quanto rappresentato nella deliberazione della sezione n. 5 del 2023, in merito alla Milestone M1C1-8, il cui obiettivo di riferimento si prefiggeva il compito di attivare un'unità centrale di ispezione per le misure di sicurezza PSNC e NIS. In tale ambito, si è proceduto all'istituzione dell'organizzazione interna dell'Agenzia responsabile dell'Unità Centrale di Audit per la verifica dell'applicazione delle misure di sicurezza definita nella normativa di riferimento. Inoltre, è stata formalizzata l'attivazione dell'Unità Centrale di Audit tramite la creazione della Divisione Organo Ispettivo e di vigilanza con l'approvazione del Decreto Direttoriale n. 13214, del 14 ottobre 2022.

Si aggiunga, altresì, che nel periodo preso in esame dalla succitata deliberazione il processo di assunzione del personale del Servizio Certificazione e Vigilanza risultava completato. In quel contesto erano stati conclusi i primi processi di reclutamento attraverso il bando di concorso da 50 unità, pubblicato il 22 febbraio 2022, nel cui ambito è stato previsto il reclutamento specifico a valere sul profilo A di n. "15 Esperti per le funzioni tecnico/amministrative di "Certificazione e ispezione" con esperienza nell'applicazione di schemi di certificazione Common Criteria / ITSEC e/o come auditor ISO". Pertanto, nel corso del 2023 è stata pubblicata la Determina di approvazione dalla graduatoria finale per l'assunzione di 15 esperti con funzioni di certificazione e ispezione.

Infine, la piena attivazione dell'Unità Centrale Ispettiva è stata completata attraverso iniziative - di processo, tecnologiche e formative - volte ad abilitare la pianificazione e l'avvio delle attività di verifica e ispezione, a partire dal 14 novembre 2023.

In particolare:

a. è stato definito e formalizzato un sistema di gestione della qualità in conformità alla norma relativa agli Organismi di Ispezione (UNI CEI EN ISO/IEC 17020) al fine di strutturare una logica univoca e coerente per la gestione, documentale e operativa, delle attività ispettive e la definizione efficace di procedure, istruzioni operative, modello e registri funzionali. Tale sistema è inoltre garanzia di imparzialità, indipendenza e riservatezza rispetto alle attività ispettive, nonché di miglioramento continuo dei processi;

b. è stato sviluppato un sistema digitale per supportare la gestione centralizzata delle ispezioni, che richiedono la consultazione, da parte di ispettori opportunamente designati, della documentazione predisposta dai soggetti interessati, nonché la registrazione di tutte le fasi di tali attività;

c. sono stati effettuati percorsi formativi specialistici finalizzati a incrementare e aggiornare il bagaglio di competenze e conoscenze professionali del personale dell'Agenzia preposto allo svolgimento delle ispezioni.

In attuazione, della presente Milestone M1C1-22, pertanto, è stata raggiunta la piena operatività dell'unità di audit per le misure di sicurezza PSNC e NIS attraverso il completamento di 30 ispezioni, alla realizzazione delle quali hanno contribuito le attività appena descritte ai punti a,b e c.

Nella scheda esplicativa delle attività volte al raggiungimento della milestone M1C1-22, in ultimo, viene specificato che nell'ambito dell'organizzazione dell'Agenzia è istituito il Servizio Certificazione e Vigilanza nel quale è incardinato l'Organismo di Verifica e Ispezione. Le attività della omologa Divisione "Organismo di Verifica e Ispezione" sono disciplinate dal DPCM n.92/2022 e dal DPR 54/2021, in ottemperanza dei quali il Manuale di Gestione dell'Unità Centrale Ispettiva definisce l'organizzazione interna e le modalità esecutive delle ispezioni.

In ordine al personale assegnato all'Organismo di Verifica e Ispezione, incaricato dello svolgimento delle attività ispettive, lo stesso ha inoltre condotto specifici percorsi formativi dedicati per l'affinamento delle competenze specialistiche necessarie alle attività ispettive. Congiuntamente, gli strumenti informativi interni permettono agli ispettori le opportune analisi documentali e di dettaglio.

Nell'ambito delle attività svolte dall'Agenzia, nel corso del 2024, si deve segnalare, infine, che sul sito istituzionale l'Agenzia ha pubblicato, in data 8 marzo 2024, l'Avviso pubblico per la ricerca di un immobile in vendita da destinare a sede dell'Agenzia per la cybersicurezza nazionale. A tal proposito, la procedura per l'acquisizione della nuova sede dell'Agenzia si è conclusa in data 6 agosto 2024. Con la sottoscrizione del contratto con la società Colliers si è, infatti, perfezionato l'acquisto dello stabile sito a Roma in corso d'Italia, individuata quale sistemazione logistica di prestigio e di efficienza operativa per tale Organismo.

A seguito di ulteriore richiesta di approfondimenti da parte di questa Sezione in merito ad eventuali scostamenti, rispetto a quanto inizialmente programmato, nel raggiungimento delle milestone e target di cui all'investimento 1.5., l'Agenzia per la cybersicurezza ha esplicitato che non sono stati riscontrati scostamenti nel raggiungimento di quanto inizialmente programmato. E' stato, altresì, rappresentato che, comunque, le Milestone & Target previste a dicembre 2024 sono state aggiornate rispetto all'iniziale versione dell'Investimento 1.5 con la decisione COM(2023) 765 final (il cui annex allegato contiene le versione aggiornate delle Milestone & Target). In particolare, sono state aggiornate dalla Commissione la descrizione delle Milestone:

1) M1C1-19 "Support to the upgrade of security structures T2";
2) M1C1-21 "Completion of the network of cybersecurity screening and certification laboratories, Evaluation Centers".

In relazione alla prima, trattasi di un mero aggiornamento di refusi nel testo, mentre in ordine alla seconda, alla luce dell'assenza di standard di certificazione approvati a livello di EU, è stata tolta dalla precedente versione della Milestone la menzione del "laboratorio di certificazione europea" che non sarebbe allo stato realizzabile per definizione.

8. Relazione annuale al Parlamento 2023.

La Relazione annuale al Parlamento sulle attività svolte dall'Agenzia per la cybersicurezza nazionale (ACN), prevista dal decreto-legge 14 giugno 2021, n. 82 – ampiamente descritta nelle deliberazioni precedenti adottate da questa Sezione in materia - fornisce, in materia di cybersicurezza, una panoramica sulle attività, i dati e le progettualità per il periodo che va dal 1° gennaio al 31 dicembre di ogni anno.

Dal sito istituzionale dell'Agenzia si apprende che il 24 aprile 2024 è stata presentata la Relazione annuale al Parlamento dell'Acn relativa alle attività svolte nel 2023.

La corposa Relazione, composta di 121 pagine, è organizzata in sette sezioni che illustrano il modo in cui l'Agenzia ha operato per il rafforzamento della resilienza cyber del Paese attraverso la protezione degli asset critici nazionali con un approccio sistemico orientato alla prevenzione, gestione e mitigazione del rischio.

Il primo capitolo, dedicato alla Prevenzione e gestione di eventi e incidenti cyber, raccoglie tutti i numeri del Computer Security Response Team Italia dell'Agenzia: analizza gli eventi cibernetici più rilevanti e mette a fuoco le attività connesse alle tensioni geopolitiche in corso. Questo capitolo presenta un focus sugli interventi di ripristino realizzati dal Csirt a supporto delle vittime degli incidenti di strutture pubbliche e dei soggetti nazionali colpiti da questa peculiare forma di interferenza hacker, con numerosi interventi, 1411 casi trattati, 303 incidenti confermati e oltre 20mila segnalazioni. Una parte del capitolo è dedicata, altresì, al tema delle esercitazioni congiunte già realizzate fino alla pianificazione di Cyber Europe 2024 e che coinvolge tutti gli stati membri dell'Unione.

Il secondo capitolo tratta la tematica della Resilienza delle infrastrutture digitali e alla sicurezza tecnologica con un'analisi dello stato del Perimetro di sicurezza nazionale cibernetica (PSNC) e un focus sull'attuazione della Direttiva NIS 2, fino ai temi della certificazione nel mondo digitale e dello Scrutinio tecnologico per il PSNC con le attività ispettive e di verifica connesse. In questa sezione sono descritti, inoltre, i contributi dell'Agenzia a temi di rilievo quali l'esercizio del Golden Power, la Crittografia e la transizione al Cloud.

Il terzo capitolo concerne gli Investimenti PNRR per la cybersicurezza: dal potenziamento della resilienza cyber della Pubblica Amministrazione agli avvisi di finanziamento finalizzati. Il focus è dedicato, in particolare, ai Servizi cyber nazionali e alla costruzione di una rete di CSIRT regionali fino allo stato di avanzamento di HyperSoc, dell'infrastruttura di High Performance Computing, e all'uso di strumenti di IA. La Relazione ha ad oggetto anche i laboratori di scrutinio e certificazione tecnologica: 134 procedimenti CVCN conclusi hanno visto i tecnici dell'Agenzia impegnati nel loro esame.

Il quarto capitolo riguarda la Cooperazione Internazionale, ricostruisce le attività svolte in ambito europeo e internazionale curate dal Servizio Strategie e cooperazione dell'ACN. Sono descritti i numerosi incontri con soggetti omologhi e le attività svolte in costante raccordo con il Ministero degli affari esteri e della cooperazione internazionale. Tra gli elementi qualificanti delle attività bilaterali e multilaterali, uno riguarda la condivisione con la CISA, l'Agenzia cyber degli Stati Uniti, delle valutazioni sul nesso fra

Intelligenza Artificiale e cybersicurezza, in linea con l'indirizzo politico del Presidente del Consiglio dei ministri, che ha consentito l'adesione dell'ACN al documento sulle "Linee guida per uno sviluppo sicuro dell'Intelligenza Artificiale", adottato da agenzie di 18 Paesi.

Il quinto capitolo, dedicato a Ricerca e innovazione, formazione, consapevolezza, presenta i vari programmi industriali, di investimento e di innovazione realizzati, insieme ai programmi di sostegno alla ricerca e alle imprese, in coerenza con l'Agenda per l'Innovazione e la ricerca. Tra le iniziative si segnala in particolare il Cyber Innovation Network, indispensabile a produrre innovazione sicura attraverso il supporto alle start up innovative.

Il sesto capitolo descrive lo stato di attuazione della Strategia Nazionale di cybersicurezza 2022-2026 che evidenza come l'Agenzia abbia svolto nel 2023 un ruolo centrale di indirizzo, coordinamento e monitoraggio nell'attuazione del Piano in raccordo con gli altri soggetti coinvolti con un particolare riferimento all'anticipazione dell'evoluzione della minaccia cyber, alla gestione di possibili scenari di crisi cibernetiche, al conseguimento dell'autonomia strategica nella dimensione cibernetica e al contrasto della disinformazione online.

Nella Relazione, sono state, infine, illustrate le attività di sviluppo della forza lavoro e delle capacità nazionali, tra cui rientra il potenziamento della capacità dell'Agenzia che, nel corso del 2023, ha visto raddoppiare la propria consistenza organica.

Sempre in corso di istruttoria è stato chiesto all'Agenzia di fornire informazioni utili in merito alla Relazione annuale al Parlamento concernenti le attività espletate dall'Agenzia nel 2024, non ancora pubblicata sul sito istituzionale dell'Ente e in via di definizione. In particolare, è stato richiesto di indicare la presenza di eventuali criticità emerse nella gestione delle attività da parte dell'Agenzia che saranno oggetto di esame della Relazione stessa. A tal riguardo, da quanto espresso dall'Ente competente, non sono state rilevate criticità da comunicare.

9. Stato di avanzamento dei progetti.

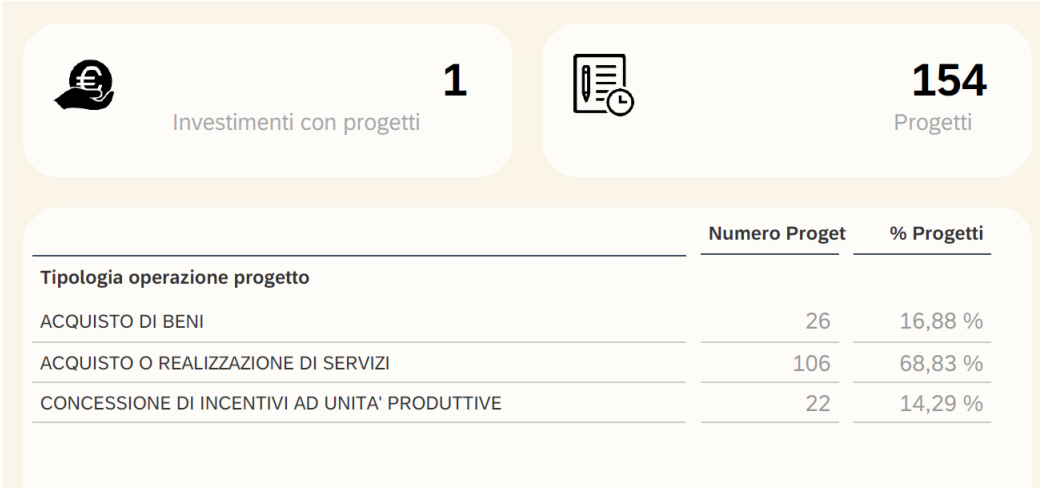
Per quanto concerne lo stato di avanzamento dei progetti coinvolti nell'investimento 1.5, nella succitata nota istruttoria, di dicembre 2024, la Sezione ha chiesto agli Enti

competenti di fornire informazioni dettagliate circa "il numero dei progetti in corso, di quelli non ancora avviati e di quelli già eseguiti, unitamente a quelli che presentano dei ritardi rispetto a quanto programmato per la loro conclusione, indicandone le relative motivazioni e le eventuali criticità".

A riscontro di quanto richiesto gli Enti competenti hanno fornito un documento comprensivo dei progetti attualmente in corso "Lista CUP", unitamente ad una tabella afferente l'"Approfondimento progetti in ritardo".

Nella verifica sullo stato di avanzamento dei progetti si è proceduto, altresì, alla interrogazione del sistema REGIS, dalla cui componente "cruscotto informativo generale – PNRR", nella sezione dedicata ai progetti, è stato possibile ricavare una serie di informazioni concernenti il numero dei progetti in corso, il costo dettagliato dei singoli progetti, nonché lo stato di avanzamento degli stessi.

Dalle informazioni generali estrapolate dal sistema REGIS si premette, in primo luogo, che il numero complessivo dei progetti in corso è pari a 154, dei quali risultano 152 in corso e 2 conclusi. Nell'ambito dei succitati progetti è possibile distinguere 3 tipologie progettuali relativi all'acquisto di beni, all'acquisto o realizzazione di servizi e infine a concessioni di incentivi ad unità produttive.



Tipologia operazione progetto	Numero Proget	% Progetti
ACQUISTO DI BENI	26	16,88 %
ACQUISTO O REALIZZAZIONE DI SERVIZI	106	68,83 %
CONCESSIONE DI INCENTIVI AD UNITA' PRODUTTIVE	22	14,29 %

Dalla componente in esame si evince, altresì, che tra i progetti con i maggiori finanziamenti assegnati se ne individuano 5, dei quali si riportano qui di seguito i rispettivi titoli con il corrispondente ammontare:

- “Attività di costituzione operativa acn”: 192 milioni di euro;
- “Nuove soluzioni basate su integrazioni di sistemi di monitoraggio cibernetico con sistemi C2, potenziamento SCADA e realizzazione centro di valutazione della difesa”: 49 milioni;
- “Intervento creazione dei c-labs e delle unità forense operative del servizio di polizia postale nell'ambito del piano operativo progetto di realizzazione soc, c-lab e ufo, centro valutazione”: 29 milioni di euro;
- “Intervento realizzazione di un nuovo sistema soc a supporto del monitoraggio e mitigazione della minaccia cyber nell'ambito del piano operativo, progetto di realizzazione soc, c-lab e ufo, centro valutazione”: 29 milioni di euro;
- “Sistema di high performance computing pe”: 22 milioni di euro.

A seguito di consultazione dell’applicativo Regis – componente “Cruscotto informativo – progetti” - effettuata al 31 dicembre 2024, si riporta qui di seguito una tabella contenente informazioni sui progetti collegati all’investimento in esame, quali il titolo del progetto, il codice unico progetto, il codice locale di progetto, la data finale prevista per i singoli progetti ed infine il costo ammesso.

Nella tabella, altresì, si riportano tutti i 154 progetti registrati a sistema.

Titolo progetto	Codice CUP	Codice Locale di Progetto (CLP)	Data fine prevista progetto	Costo ammesso progetti*
CSIRT REGIONE MARCHE	B39B23001370006	3_WP7_A6_REGIONE MARCHE	31.12.2025	1,50 milioni EUR
cyber security cert sanita regione abruzzo	C99B22000020006	12_WP_9_RIST_REGIONE ABRUZZO	30.11.2024	1,00 milioni EUR
CYBER STRATEGY DI ROMA CAPITALE	J84F22000960006	16_WP_9_RIST_ROMA CAPITALE	30.11.2024	0,86 milioni EUR
CYBERSICUREZZA SERVIZI ALLE ASP E AO REGIONALI	J69B22000160006	20_WP_9_RIST_REGIONE CALABRIA	23.09.2024	0,90 milioni EUR
GOVERNANCE E AWARENESS PERSONALE ADM	G89B22000340006	06_WP9_RIST_AGDO_2	07.05.2024	1,11 milioni EUR
InnovaPuglia LAP accreditato	J69B22000250006	33_WP12_A5_INNOVAPUGLIA	30.11.2024	0,20 milioni EUR
INTERVENTO CENTRO DI VALUTAZIONE DEL MINISTERO DELL INTERNO NELL'AMBITO DEL PIANO OPERATIVO PROGETTO DI REALIZZAZIONE SOC, C-LAB E UFO, CENTRO VALUTAZIONE	F86G22002220006	F86G22002220006	31.03.2026	9,25 milioni EUR
laboratorio di prova indipendente	F86G23000610006	27_WP12_A5_MPG	15.12.2024	0,20 milioni EUR
Laboratorio Prove Sicurezza IMQ	F46G23000060006	21_WP12_A5_IMQ	15.12.2024	0,03 milioni EUR
LAP NEXT Ingegneria dei Sistemi	F86G23000660004	29_WP12_A5_NEXTINGEGNERIA	31.12.2022	0,19 milioni EUR
PIANO DI CYBERSECURITY AWARENESS	F71B22001250006	73_WP_9_RIST_COMUNE DI VENEZIA	30.11.2024	0,43 milioni EUR
potenziamento del sistema informativo regionale ambientale	E24I22000010005	75_WP_9_RIST_REGIONE SARDEGNA	30.11.2024	1,00 milioni EUR
sicurezza servizi di assistenza sanitaria	B39B22000850006	49_WP_9_RIST_REGIONE MARCHE	30.11.2024	1,00 milioni EUR
sistemi propedeutici cert veneto	H79B22000180001	36_WP_9_RIST_REGIONE VENETO	30.11.2024	1,00 milioni EUR

TECNOLOGIE A MITIGAZIONE DEL RISCHIO CYBER	F76G22000380006	74_WP_9_RIST_COMUNE DI VENEZIA	30.11.2024	0,58 milioni EUR
Accreditamento LAP atsec	F86G23000590006	18_WP12_A5_ATSEC	31.03.2024	0,03 milioni EUR
Acquisto di soluzioni avanzate di cybersecurity	B56G21056820003	B56G21056820003	31.12.2023	1,00 milioni EUR
Adeguamento alle misure previste psnc	J84F22000800001	23_WP9_RIST_MAECI_1	30.09.2023	0,90 milioni EUR
Adeguamento firewall e policy di sicurezza	G36G22000260006	24_WP_9_RIST_REGIONE LIGURIA	30.11.2024	0,98 milioni EUR
Adeguamento Laboratori on-site	F86G23000580006	15_WP12_A5_STONESECURITY	20.11.2024	0,07 milioni EUR
Adozione framework zero trust access	B69B22000320006	50_WP_9_RIST_COMUNE DI NAPOLI	30.11.2024	0,61 milioni EUR
ALAB software and network security	F36G23000050006	35_WP12_A5_ANCHARIA	15.12.2024	0,19 milioni EUR
Ampliamento soc	B59B22000690006	51_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	30.11.2024	0,79 milioni EUR
Analisi della postura cyber genova	B37H22005440006	26_WP_9_RIST_COMUNE DI GENOVA	30.11.2024	0,65 milioni EUR
Analisi della postura di sicurezza catania	D66G22000350006	10_WP_9_RIST_COMUNE DI CATANIA	30.11.2024	1,00 milioni EUR
Analisi e miglioramento cybersecurity della torino	C17H22002830006	39_WP_9_RIST_COMUNE DI TORINO	30.11.2024	1,00 milioni EUR
Analisi e miglioramento dei processi cyber	B46G22015740004	44_WP_9_RIST_COMUNE DI MILANO	30.11.2024	1,00 milioni EUR
APAVELAB	F66G23000110006	19_WP12_A5_APAVEITALIA	15.12.2024	0,16 milioni EUR
Assessment della postura cyber	H79B22000190001	37_WP_9_RIST_REGIONE VENETO	30.06.2024	1,00 milioni EUR
Assessment ed evoluzione della postura cyber	B69B22000330006	53_WP_9_RIST_COMUNE DI NAPOLI	31.10.2024	0,67 milioni EUR
Attivazione CSIRT Abruzzo	C19B23000130006	11_WP7_A6_REGIONE ABRUZZO	31.12.2025	1,50 milioni EUR
Attivazione CSIRT Calabria	J69B23000340006	16_WP7_A6_REGIONE CALABRIA	31.10.2025	1,50 milioni EUR

Attivazione CERT-CSIRT regionale	H19B23000100006	2_WP7_A6_REGIONE VENETO	31.12.2024	1,50 milioni EUR
Attivazione CSIRT Livello Base Molise	D11B23000310006	15_WP7_A6_REGIONE MOLISE	31.12.2025	1,50 milioni EUR
Attivita di costituzione operativa acn	F84E21007910007	F84E21007910007	30.06.2026	192,16 milioni EUR
Beni e servizi per l'infrastruttura telematica dell'arma dei carabinieri	D86G23000030006	D86G23000030006	30.06.2026	20,10 milioni EUR
Bozenasset	B59E22000100006	46_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	30.11.2024	0,46 milioni EUR
Branch office security enforcement	J86G21007170006	02_WP9_RIST_PCM_2	30.11.2024	0,36 milioni EUR
CARDEA - Center of Analysis and Research	F86G23000670004	32_WP12_A5_DIGITALENGINEERING	30.09.2023	0,13 milioni EUR
Centralized threat monitoring	F89B22000150006	26_WP9_RIST_MITE_1	31.12.2023	0,46 milioni EUR
Centro per la cybersicurezza regionale	G36G22000230006	3_WP_9_RIST_REGIONE BASILICATA	30.11.2024	1,00 milioni EUR
Centro per la cybersicurezza regonale ii intervento	G36G22000240006	4_WP_9_RIST_REGIONE BASILICATA	30.11.2024	1,00 milioni EUR
Cert regionale dell'ambito della gestione delle acque	C99B22000030006	13_WP_9_RIST_REGIONE ABRUZZO	30.11.2024	0,75 milioni EUR
CERT TERRITORIALE DELLALTO ADIGE	B59E22000110006	54_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	30.11.2024	0,75 milioni EUR
Client security enforcement	J86G21007160006	04_WP9_RIST_PCM_4	30.11.2024	0,59 milioni EUR
COCY CONSAPEVOLEZZA CYBER	D76G22000390006	8_WP_9_RIST_COMUNE DI PALERMO	30.11.2024	0,99 milioni EUR
Controllo remoto dei nodi	D56G22000410006	D56G22000410006	30.06.2025	3,90 milioni EUR
CSIRT CAMPANIA	B27H23002720006	17_WP7_A6_REGIONE CAMPANIA	31.12.2025	1,50 milioni EUR
CSIRT della Regione Toscana	D11C23000760008	8_WP7_A6_REGIONE TOSCANA	31.12.2025	1,50 milioni EUR
CSIRT LIGURIA	G39B23000090006	1_WP7_A6_REGIONE LIGURIA	31.12.2025	1,50 milioni EUR
CSIRT Provincia autonoma di Trento	C49E23000850006	19_WP7_A6_PROVINCIA AUTONOMA DI TRENTO	31.12.2025	1,50 milioni EUR

CSIRT REGIONE LAZIO	F84F23000230006	4_WP7_A6_REGIONE LAZIO	31.12.2025	1,50 milioni EUR
CSIRT SICILIA	G79B23000220006	18_WP7_A6_REGIONE SICILIA	31.12.2025	1,50 milioni EUR
CSIRT-RAS-PSR - Sardegna	E76G23000110006	12_WP7_A6_REGIONE SARDEGNA	31.12.2024	1,50 milioni EUR
CYBER AWARENESS PA LOCALE DELLA VALLE D'AOSTA	B53E22001890006	71_WP_9_RIST_REGIONE VALLE D'AOSTA	20.11.2024	0,43 milioni EUR
Cyber campania	B66G22017050006	57_WP_9_RIST_REGIONE CAMPANIA	30.11.2024	0,98 milioni EUR
Cyber resilienza e potenziamento dei presidi	B46G22015750004	45_WP_9_RIST_COMUNE DI MILANO	30.11.2024	1,00 milioni EUR
Cyber security assessment enti sanitari lombardia	E87H22002580008	52_WP_9_RIST_REGIONE LOMBARDIA	31.12.2023	1,00 milioni EUR
Cyber strategy & distributed visibility	F89B22000130006	28_WP9_RIST_MITE_3	31.12.2023	0,52 milioni EUR
Cybersecurity framework e tools	H16G22000340006	2_WP_9_RIST_COMUNE DI FIRENZE	30.11.2024	0,99 milioni EUR
Cybersecurity fvg: training&awareness	D21C22001400008	30_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	30.11.2024	0,88 milioni EUR
CYBERSECURITY METROWIDE	H11C22001670006	33_WP_9_RIST_COMUNE DI FIRENZE	30.11.2024	1,00 milioni EUR
CYBERSECURITY POSTURE ASSESSMENT PUGLIA	B31C22001720006	18_WP_9_RIST_REGIONE PUGLIA	30.11.2024	1,00 milioni EUR
Cybersecurity_r_molise	D36G22000250006	70_WP_9_RIST_REGIONE MOLISE	30.11.2024	1,00 milioni EUR
Cybervault per dati mission critical bacino orientale	I67H22002880005	76_WP_9_RIST_REGIONE SICILIA	30.11.2024	1,00 milioni EUR
Deep Cyber	F86G23000560006	8_WP12_A5_DEEPLAB	15.12.2024	0,18 milioni EUR
Definizione delle cyber strategy e formazione cyber security	J94F22001290006	40_WP_9_RIST_COMUNE DI BARI	30.11.2024	0,82 milioni EUR
dipartimento vigili del fuoco upgrade per il potenziamento delle capacita di monitoraggio del rischio cyber	F89B22000160001	15_WP9_RIST_DVF_1	30.09.2024	0,51 milioni EUR

Disaster recovery e buisness continuity	D19B22000420006	31_WP_9_RIST_REGIONE TOSCANA	30.11.2024	1,00 milioni EUR
e-Trace Labs	F86G23000600006	20_WP12_A5_E-TRACE	15.12.2024	0,20 milioni EUR
FORMAZIONE E PROCESSI PER LA CYBERSECURITY	F49B22000100006	38_WP_9_RIST_COMUNE DI MESSINA	30.11.2024	0,72 milioni EUR
Future Ready CS Lab	F86G23000640006	17_WP12_A5_TECNINF	30.11.2023	0,14 milioni EUR
Futuring Technology Center (FTC)	F16G23000170006	23_WP12_A5_TESLY	15.11.2024	0,20 milioni EUR
GDPRSIBAR ATTIVITA DI SICUREZZA SARDEGNA	E24E19000450002	69_WP_9_RIST_REGIONE SARDEGNA	30.11.2024	1,00 milioni EUR
Gestione della qualita e miglioramento dei processi	D19B22000410006	32_WP_9_RIST_REGIONE TOSCANA	30.11.2024	1,00 milioni EUR
Identity and access management csirt puglia	J94F22001300006	27_WP_9_RIST_COMUNE DI BARI	30.11.2024	1,00 milioni EUR
Incremento cultura cyber security ei	D51C22001320006	12_WP9_RIST_DIF_1	20.07.2022	0,12 milioni EUR
Incremento della consapevolezza del rischio cyber torino	C17H22002840006	41_WP_9_RIST_COMUNE DI TORINO	30.11.2024	1,00 milioni EUR
Incremento sicurezza cortecostituzionale	H86G22000180005	09_WP9_RIST_CORTCOST_1	30.11.2024	0,33 milioni EUR
Infrastruttura per bilanciamento worklood	G36G22000250006	23_WP_9_RIST_REGIONE LIGURIA	30.11.2024	1,00 milioni EUR
INFRASTRUTTURA TELEMATICA CENTRALE DEL COMANDO GENERALE DELL'ARMA DEI CARABINIERI VIALE ROMANIA 45 SISTEMI DI INTRUSION DETECTION/PREVENTION	D86G22000440006	D86G22000440006	31.12.2025	2,00 milioni EUR
Innalzamento livello di sicurezza regionale umbra	I64F22000060006	25_WP_9_RIST_REGIONE UMBRIA	30.11.2024	1,00 milioni EUR
INNONATION CYBER SECURITY LAB	F66G23000100006	2_WP12_A5_Innonation	15.12.2024	0,07 milioni EUR
INTELLISYNC LAP	F66G23000120006	22_WP12_A5_INTELLISYNC	15.12.2024	0,14 milioni EUR

Intervento creazione dei c-labs e delle unita forense operative del servizio di polizia postale nell'ambito del piano operativo progetto di realizzazione soc, c-lab e ufo, centro valutazione	F56G22000400006	F56G22000400006	31.03.2026	29,00 milioni EUR
Intervento realizzazione di un nuovo sistema soc a supporto del monitoraggio e mitigazione della minaccia cyber nell'ambito del piano operativo progetto di realizzazione soc, c-lab e ufo, centro valutazione	F86G22002210006	F86G22002210006	31.03.2026	29,00 milioni EUR
LAB IPS	F86G23000620006	3_WP12_A5_IPS	21.05.2024	0,20 milioni EUR
Laboratorio di Prova Secure Network	F46G23000090006	5_WP12_A5_SECURENETWORK	31.12.2023	0,18 milioni EUR
LAP DIGITALPLATFORMS	F86G23000630006	4_WP12_A5_DIGITALPLATFORMS	15.12.2024	0,16 milioni EUR
LAP INNOVERY	F46G23000080006	31_WP12_A5_INNOVERY	15.12.2024	0,20 milioni EUR
LAP SIPAL	F16G23000190006	13_WP12_A5_SIPAL	15.12.2024	0,17 milioni EUR
Licenze e servizi di supporto	H86G20000640006	10_WP9_RIST_CORTCOST_2	30.11.2024	0,39 milioni EUR
Linea progettuale 1 bologna	F31B22001080006	59_WP_9_RIST_COMUNE DI BOLOGNA	30.11.2024	1,00 milioni EUR
Linea progettuale 2 bologna	F31B22001090006	60_WP_9_RIST_COMUNE DI BOLOGNA	30.11.2024	1,00 milioni EUR
MAECI HUMAN FIREWALL	J83E23000060006	24_WP9_RIST_MAECI_2	30.11.2024	0,45 milioni EUR
MEFLAB CYSEC	G84F22000630006	01_WP12_Rist_MEF_1	31.12.2022	1,16 milioni EUR
METROCAGLIARI IT-SECURITY PROGETTO 2	G29B22000280001	79_WP_9_RIST_COMUNE DI CAGLIARI	30.11.2024	1,00 milioni EUR
METROCAGLIARI ITSECURITY PROGETTO 1	G29B21000000006	78_WP_9_RIST_COMUNE DI CAGLIARI	30.11.2024	1,00 milioni EUR
Missione digitale	G56G21009570006	G56G21009570006	29.11.2024	7,00 milioni EUR
Nuclei cyber security proiettabili	D86G21004990006	14_WP9_RIST_DIF_3	30.11.2022	1,33 milioni EUR

Nuove soluzioni basate su integrazione di sistemi di monitoraggio cibernetico con sistemi c2, potenziamento scada e realizzazione centro di valutazione della difesa	D46G21002310006	D46G21002310006	31.03.2026	49,25 milioni EUR
Piano di security awareness regione lazio	F83E22000060006	55_WP_9_RIST_REGIONE LAZIO	30.11.2024	0,77 milioni EUR
Piattaforma soc/epp evoluto	B69B22000310006	48_WP_9_RIST_COMUNE DI NAPOLI	30.11.2024	0,73 milioni EUR
Postazioni di lavoro a rete regionale piemonte	J14F22001110006	6_WP_9_RIST_REGIONE PIEMONTE	30.11.2024	0,98 milioni EUR
Postura di sicurezza awareness adm	G89B22000330006	05_WP9_RIST_AGDO_1	30.09.2024	0,79 milioni EUR
Posture management & attack prevention	F89B22000140006	27_WP9_RIST_MITE_2	31.12.2023	1,02 milioni EUR
Potenziamento CERT Alto Adige	B39E23000040006	13_WP7_A6_PROVINCIA AUTONOMA DI BOLZANO	31.12.2025	1,50 milioni EUR
POTENZIAMENTO CSIRT LOMBARDIA	E47H23001240008	9_WP7_A6_REGIONE LOMBARDIA	31.12.2025	1,50 milioni EUR
Potenziamento CSIRT RAFVG	D21C23000470006	7_WP7_A6_REGIONE FRIULI-VENEZIA GIULIA	31.12.2025	1,50 milioni EUR
Potenziamento Csirt regionale	E31C23001310006	10_WP7_A6_REGIONE EMILIA-ROMAGNA	31.12.2025	1,50 milioni EUR
Potenziamento CSIRT Umbria	I64F23000070006	14_WP7_A6_REGIONE UMBRIA	31.08.2025	1,50 milioni EUR
Potenziamento cyber sanita umbra	I64F22000070006	43_WP_9_RIST_REGIONE UMBRIA	30.11.2024	1,00 milioni EUR
Potenziamento cyber servizi sanitari regionali	E41B22004190006	66_WP_9_RIST_REGIONE EMILIA ROMAGNA	30.11.2024	0,60 milioni EUR
Potenziamento cyber roma capitale	J89B22000540001	14_WP_9_RIST_ROMA CAPITALE	30.11.2024	1,00 milioni EUR
Potenziamento della capacita cyber del trentino	C61B22002620006	22_WP_9_RIST_PROVINCIA AUTONOMA DI TRENTO	30.11.2024	0,95 milioni EUR

Potenziamento della resilienza emiliaromagna	E41B22004200006	67_WP_9_RIST_REGIONE EMILIA ROMAGNA	30.11.2024	0,70 milioni EUR
Potenziamento dello CSIRT Basilicata	G39E23000010001	6_WP7_A6_REGIONE BASILICATA	31.12.2025	1,50 milioni EUR
POTENZIAMENTO DNS SECURITY PER LA PUGLIA	B31C22001730006	17_WP_9_RIST_REGIONE PUGLIA	30.11.2024	1,00 milioni EUR
Potenziamento e rinnovo licenze e supporto sistemistico dei sistemi mcafee di protezione delle reti e sistemi it interforze e delle f.a	D86G21005000006	13_WP9_RIST_DIF_2	30.11.2024	0,54 milioni EUR
Potenziamento e sicurezza degli end-point	D66G22000340006	11_WP_9_RIST_COMUNE DI CATANIA	30.11.2024	1,00 milioni EUR
Potenziamento numero unico emergenza friuli	D66G21003160008	05_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	30.11.2024	0,67 milioni EUR
Potenziamento resilienza cyber valle daosta	B54F22007690006	72_WP_9_RIST_REGIONE VALLE D'AOSTA	30.11.2024	0,92 milioni EUR
POTENZIAMENTO SOC CYBERSECURITY MESSINA	F46G22000690006	42_WP_9_RIST_COMUNE DI MESSINA	30.11.2024	0,85 milioni EUR
Programma di sicurezza e protezione dei dati	E87H22002560008	28_WP_9_RIST_REGIONE LOMBARDIA	30.11.2024	1,00 milioni EUR
RAFFORZAMENTO CSIRT REGIONALE	B34F23009890006	5_WP7_A6_REGIONE PUGLIA	31.12.2025	1,50 milioni EUR
Rafforzamento cyber defence regione lazio	F81C22001910006	34_WP_9_RIST_REGIONE LAZIO	31.10.2024	0,72 milioni EUR
Rafforzamento dei presidi di sicurezza roma capitale	J89B22000550001	15_WP_9_RIST_ROMA CAPITALE	30.11.2024	0,15 milioni EUR
Rafforzamento dei processi cybersicurezza marche	B39B22000840001	47_WP_9_RIST_REGIONE MARCHE	30.11.2024	1,00 milioni EUR
Realizzazione csirt emiliaromagna	E44F22005970006	64_WP_9_RIST_REGIONE EMILIA ROMAGNA	30.11.2024	0,70 milioni EUR
Reggiocyber (rc)	H36G22000100006	62_WP_9_RIST_COMUNE DI REGGIO CALABRIA	30.09.2024	1,00 milioni EUR
REGIONE FRIULI VENEZIA GIULIA CYBER INIZIATIVE	D21C22001380008	29_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	30.06.2023	0,33 milioni EUR

RESILIENZA CIBERNETICA COMUNE DI VENEZIA	F71B22001240006	58_WP_9_RIST_COMUNE DI VENEZIA	30.11.2024	0,24 milioni EUR
Resilienza cyber agenzia del demanio	E84I22000000006	07_WP9_RIST_AGDEM_1	30.11.2022	0,28 milioni EUR
Resilienza cyber comune di palermo	D76G22000400006	9_WP_9_RIST_COMUNE DI PALERMO	30.11.2024	1,00 milioni EUR
Resilienza cyber per la provincia autonoma di trento	C64F22000320006	21_WP_9_RIST_PROVINCIA AUTONOMA DI TRENTO	31.10.2024	0,76 milioni EUR
SABABA SECURITY LABORATORIO	F46G23000070006	30_WP12_A5_SABABA	15.12.2024	0,17 milioni EUR
SEA_LAP	F86G23000570006	12_WP12_A5_SISTEMI&AUTOMAZIONE	15.12.2024	0,20 milioni EUR
Security enforcement regione lazio	F84F22000850006	35_WP_9_RIST_REGIONE LAZIO	30.11.2024	0,51 milioni EUR
Security monitoring identity governance	G86G22000230006	17_WP9_RIST_MEF_2	30.11.2024	2,00 milioni EUR
Servizi a supporto dell'agenzia per la cybersicurezza - governance trasversale del programma	F81B21008190007	F81B21008190007	30.06.2026	3,79 milioni EUR
Sicurezza perimetro rete camera	D86G21004980006	08_WP9_RIST_CAM_1	31.12.2023	1,10 milioni EUR
Sicurezza dati ministero di giustizia	J51B22001240006	J51B22001240006	30.09.2025	5,00 milioni EUR
SICUREZZA ENDPOINT RTRS	G66G22000200008	65_WP_9_RIST_REGIONE SICILIA	30.09.2024	0,01 milioni EUR
SICUREZZA PERIMETRO INTERNO RTRS	G66G22000190008	63_WP_9_RIST_REGIONE SICILIA	30.12.2024	1,00 milioni EUR
Sinfonia	B66G22017040006	56_WP_9_RIST_REGIONE CAMPANIA	30.09.2024	0,97 milioni EUR
SISTEMA DI HIGH PERFORMANCE COMPUTING PE	F66G24000010006	F66G24000010006	01.06.2025	21,90 milioni EUR
Sistemi di discovery automatica di cose connesse alla rete dellarma dei carabinieri	D86G22000450006	D86G22000450006	30.06.2026	7,00 milioni EUR
SONIC	F86G23000650006	28_WP12_A5_HERMESBAY	15.12.2023	0,16 milioni EUR
Strategia cyber per la regione calabria	J69B22000170006	19_WP_9_RIST_REGIONE CALABRIA	30.12.2023	0,96 milioni EUR

SW HW DATACENTER ARMA	D86G22000490006	D86G22000490006	30.06.2026	6,00 milioni EUR
Transizione digitale e servizi sicuri	J14F22001120006	7_WP_9_RIST_REGIONE PIEMONTE	30.11.2024	1,00 milioni EUR
User account security enforcement	J86G21007150006	03_WP9_RIST_PCM_3	30.11.2024	1,04 milioni EUR
TOTALE				**50.900.000,00 EUR**

In corso di istruttoria il Dipartimento per la trasformazione digitale, nella nota congiunta con l'Agenzia per la cybersicurezza, ha fornito, su richiesta della scrivente Sezione, una tabella comprensiva dei dati significativi dei 154 progetti legati all'investimento di che trattasi, riportante una colonna con lo stato attuale dei progetti stessi. Dalla stessa si evince che a fronte dei 154 progetti di cui sopra, solo 2 sono stati conclusi.

Inoltre, a seguito di diverse interlocuzioni intercorse con l'Agenzia, è stato possibile apprendere che per diversi progetti legati ad alcuni avvisi, che dovevano essere completati entro dicembre 2024, è stata chiesta una proroga.

A tal proposito, si riporta una tabella prodotta dagli Enti competenti dove sono evidenziati la tipologia degli avvisi interessati dalle richieste di proroga, unitamente alle relative descrizioni, in cui si pongono in evidenza le determine con cui sono state autorizzate le proroghe e a seguito delle quali i cronoprogrammi dei progetti da modificare sono ancora oggetto di valutazione da parte dell'Agenzia e non sono ancora visibili dal sistema Regis.

Pertanto, nelle pagine seguenti sono riportate le tabelle fornite dagli Enti competenti concernenti il quadro dettagliato dei progetti attualmente in corso "Lista CUP" e l'"Approfondimento progetti in ritardo". In merito alla Lista CUP, si rappresenta che i CUP di progetti finanziati di cui all'Avviso n. 8/2024 risultano già finanziati con giusta determina ma non ancora caricati su ReGiS.

Segue, in primis, la tabella "Lista CUP" dei 154 progetti:

Piano	Amministrazione	Codice Misura	Codice Unico Progetto	Codice Locale Progetto	Descr. Titolo Progetto	Denominazione	Stato
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F81B21008190007	F81B21008190007	SERVIZI A SUPPORTO DELL'AGENZIA PER LA CYBERSICUREZZA - GOVERNANCE TRASVERSALE DEL PROGRAMMA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F84E21007910007	F84E21007910007	ATTIVITA DI COSTITUZIONE OPERATIVA ACN	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F56G22000400006	F56G22000400006	INTERVENTO CREAZIONE DEI C-LABS E DELLE UNITA FORENSE OPERATIVE DEL SERVIZIO DI POLIZIA POSTALE NELL'AMBITO DEL PIANO OPERATIVO PROGETTO DI REALIZZAZIONE SOC, C-LAB E UFO, CENTRO VALUTAZIONE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G22002220006	F86G22002220006	INTERVENTO CENTRO DI VALUTAZIONE DEL MINISTERO DELL INTERNO NELL'AMBITO DEL PIANO OPERATIVO PROGETTO DI REALIZZAZIONE SOC, C-LAB E UFO, CENTRO VALUTAZIONE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G22002210006	F86G22002210006	INTERVENTO REALIZZAZIONE DI UN NUOVO SISTEMA SOC A SUPPORTO DEL MONITORAGGIO E MITIGAZIONE DELLA MINACCIA CYBER NELL'AMBITO DEL PIANO OPERATIVO PROGETTO DI REALIZZAZIONE SOC, C-LAB E UFO, CENTRO VALUTAZIONE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D46G21002310006	D46G21002310006	NUOVE SOLUZIONI BASATE SU INTEGRAZIONE DI SISTEMI DI MONITORAGGIO CIBERNETICO CON SISTEMI C2, POTENZIAMENTO SCADA E REALIZZAZIONE CENTRO DI VALUTAZIONE DELLA DIFESA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G56G21009570006	G56G21009570006	MISSIONE DIGITALE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B56G21056820003	B56G21056820003	ACQUISTO DI SOLUZIONI AVANZATE DI CYBERSECURITY	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J51B22001240006	J51B22001240006	SICUREZZA DATI MINISTERO DI GIUSTIZIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D56G22000410006	D56G22000410006	CONTROLLO REMOTO DEI NODI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D86G22000490006	D86G22000490006	SW HW DATACENTER ARMA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	E84I22000000006	07_WP9_RIST_AGDEM_1	RESILIENZA CYBER AGENZIA DEL DEMANIO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G89B22000330006	05_WP9_RIST_AGDO_1	POSTURA DI SICUREZZA AWARENESS ADM	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G89B22000340006	06_WP9_RIST_AGDO_2	GOVERNANCE E AWARENESS PERSONALE ADM	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D86G21004980006	08_WP9_RIST_CAM_1	SICUREZZA PERIMETRO RETE CAMERA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	H86G20000640006	10_WP9_RIST_CORTCOST_2	LICENZE E SERVIZI DI SUPPORTO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	H86G21005760001	11_WP9_RIST_CORTCOST_3	SALA SERVER DELLA CORTE COSTITUZIONALE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	CONCLUSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	H86G22000180005	09_WP9_RIST_CORTCOST_1	INCREMENTO SICUREZZA CORTECOSTITUZIONALE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J84F22000800001	23_WP9_RIST_MAECI_1	ADEGUAMENTO ALLE MISURE PREVISTE PSNC	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G86G22000230006	17_WP9_RIST_MEF_2	SECURITY MONITORING IDENTITY GOVERNANCE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D86G21004990006	14_WP9_RIST_DIF_3	NUCLEI CYBER SECURITY PROIETTABILI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D51C22001320006	12_WP9_RIST_DIF_1	INCREMENTO CULTURA CYBER SECURITY EI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F89B22000130006	28_WP9_RIST_MITE_3	CYBER STRATEGY & DISTRIBUTED VISIBILITY	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F89B22000140006	27_WP9_RIST_MITE_2	POSTURE MANAGEMENT & ATTACK PREVENTION	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F89B22000150006	26_WP9_RIST_MITE_1	CENTRALIZED THREAT MONITORING	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J86G21007150006	03_WP9_RIST_PCM_3	USER ACCOUNT SECURITY ENFORCEMENT	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J86G21007160006	04_WP9_RIST_PCM_4	CLIENT SECURITY ENFORCEMENT	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J86G21007170006	02_WP9_RIST_PCM_2	BRANCH OFFICE SECURITY ENFORCEMENT	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	I86G22000280006	22_WP9_RIST_SGPR_1	POTENZIAMENTO RILEVAMENTO EVENTI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	CONCLUSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G84F22000630006	01_WP12_Rist_MEF_1	MEFLAB CYSEC	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D86G22000440006	D86G22000440006	INFRASTRUTTURA TELEMATICA CENTRALE DEL COMANDO GENERALE DELL'ARMA DEI CARABINIERI VIALE ROMANIA 45 SISTEMI DI INTRUSION DETECTION/PREVENTION	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D86G22000450006	D86G22000450006	SISTEMI DI DISCOVERY AUTOMATICA DI COSE CONNESSE ALLA RETE DELLARMA DEI CARABINIERI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D86G23000030006	D86G23000030006	BENI E SERVIZI PER L'INFRASTRUTTURA TELEMATICA DELL'ARMA DEI CARABINIERI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F89B22000160001	15_WP9_RIST_DVF_1	DIPARTIMENTO VIGILI DEL FUOCO UPGRADE PER IL POTENZIAMENTO DELLE CAPACITA DI MONITORAGGIO DEL RISCHIO CYBER	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J14F22001120006	7_WP_9_rist_Regione Piemonte	TRANSIZIONE DIGITALE E SERVIZI SICURI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B46G22015750004	45_WP_9_RIST_COMUNE DI MILANO	CYBER RESILIENZA E POTENZIAMENTO DEI PRESIDI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B46G22015740004	44_WP_9_RIST_COMUNE DI MILANO	ANALISI E MIGLIORAMENTO DEI PROCESSI CYBER	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	H79B22000190001	37_WP_9_RIST_REGIONE VENETO	ASSESSMENT DELLA POSTURA CYBER	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J69B22000170006	19_WP_9_RIST_REGIONE CALABRIA	STRATEGIA CYBER PER LA REGIONE CALABRIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	E44F22005970006	64_WP_9_RIST_REGIONE EMILIA ROMAGNA	REALIZZAZIONE CSIRT EMILIAROMAGNA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D66G21003160008	05_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	POTENZIAMENTO NUMERO UNICO EMERGENZA FRIULI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D36G22000250006	70_WP_9_RIST_REGIONE MOLISE	CYBERSECURITY_R_MOLISE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	E41B22004200006	67_WP_9_RIST_REGIONE EMILIA ROMAGNA	POTENZIAMENTO DELLA RESILIENZA EMILIAROMAGNA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	C61B22002620006	22_WP_9_RIST_PROVINCIA AUTONOMA DI TRENTO	POTENZIAMENTO DELLA CAPACITA CYBER DEL TRENTINO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F84F22000850006	35_WP_9_RIST_REGIONE LAZIO	SECURITY ENFORCEMENT REGIONE LAZIO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F81C22001910006	34_WP_9_RIST_REGIONE LAZIO	RAFFORZAMENTO CYBER DEFENCE REGIONE LAZIO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D76G22000390006	8_WP_9_RIST_COMUNE DI PALERMO	COCY CONSAPEVOLEZZA CYBER	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B66G22017040006	56_WP_9_RIST_REGIONE CAMPANIA	SINFONIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G66G22000190008	63_WP_9_RIST_REGIONE SICILIA	SICUREZZA PERIMETRO INTERNO RTRS	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B59E22000100006	46_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	BOZENASSET	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B31C22001720006	18_WP_9_RIST_REGIONE PUGLIA	CYBERSECURITY POSTURE ASSESSMENT PUGLIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B31C22001730006	17_WP_9_RIST_REGIONE PUGLIA	POTENZIAMENTO DNS SECURITY PER LA PUGLIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	I67H22002880005	76_WP_9_RIST_REGIONE SICILIA	CYBERVAULT PER DATI MISSION CRITICAL BACINO ORIENTALE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F49B22000100006	38_WP_9_RIST_COMUNE DI MESSINA	FORMAZIONE E PROCESSI PER LA CYBERSECURITY	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B59E22000110006	54_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	CERT TERRITORIALE DELLALTO ADIGE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G36G22000250006	23_WP_9_RIST_REGIONE LIGURIA	INFRASTRUTTURA PER BILANCIAMENTO WORKLOOD	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F46G22000690006	42_WP_9_RIST_COMUNE DI MESSINA	POTENZIAMENTO SOC CYBERSECURITY MESSINA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F31B22001080006	59_WP_9_RIST_COMUNE DI BOLOGNA	LINEA PROGETTUALE 1 BOLOGNA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D66G22000350006	10_WP_9_RIST_COMUNE DI CATANIA	ANALISI DELLA POSTURA DI SICUREZZA CATANIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	H11C22001670006	33_WP_9_RIST_COMUNE DI FIRENZE	CYBERSECURITY METROWIDE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B69B22000330006	53_WP_9_RIST_COMUNE DI NAPOLI	ASSESSMENT ED EVOLUZIONE DELLA POSTURA CYBER	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F31B22001090006	60_WP_9_RIST_COMUNE DI BOLOGNA	LINEA PROGETTUALE 2 BOLOGNA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J14F22001110006	6_WP_9_RIST_REGIONE PIEMONTE	POSTAZIONI DI LAVORO A RETE REGIONALE PIEMONTE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	C17H22002830006	39_WP_9_RIST_COMUNE DI TORINO	ANALISI E MIGLIORAMENTO CYBERSECURITY DELLA TORINO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B54F22007690006	72_WP_9_RIST_REGIONE VALLE D'AOSTA	POTENZIAMENTO RESILIENZA CYBER VALLE DAOSTA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	H16G22000340006	2_WP_9_RIST_COMUNE DI FIRENZE	CYBERSECURITY FRAMEWORK E TOOLS	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J94F22001300006	27_WP_9_RIST_COMUNE DI BARI	IDENTITY AND ACCESS MANAGEMENT CSIRT PUGLIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	C17H22002840006	41_WP_9_RIST_COMUNE DI TORINO	INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER TORINO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J94F22001290006	40_WP_9_RIST_COMUNE DI BARI	DEFINIZIONE DELLE CYBER STRATEGY E FORMAZIONE CYBER SECURITY	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G29B21000000006	78_WP_9_RIST_COMUNE DI CAGLIARI	METROCAGLIARI ITSECURITY PROGETTO 1	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	H79B22000180001	36_WP_9_RIST_REGIONE VENETO	SISTEMI PROPEDEUTICI CERT VENETO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	E24E19000450002	69_WP_9_RIST_REGIONE SARDEGNA	GDPRSIBAR ATTIVITA DI SICUREZZA SARDEGNA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J84F22000960006	16_WP_9_RIST_ROMA CAPITALE	CYBER STRATEGY DI ROMA CAPITALE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D19B22000410006	32_WP_9_RIST_REGIONE TOSCANA	GESTIONE DELLA QUALITA E MIGLIORAMENTO DEI PROCESSI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B37H22005440006	26_WP_9_RIST_COMUNE DI GENOVA	ANALISI DELLA POSTURA CYBER GENOVA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	H36G22000100006	62_WP_9_RIST_COMUNE DI REGGIO CALABRIA	REGGIOCYBER (RC)	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B39B22000840001	47_WP_9_RIST_REGIONE MARCHE	RAFFORZAMENTO DEI PROCESSI CYBERSICUREZZA MARCHE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G36G22000240006	4_WP_9_RIST_REGIONE BASILICATA	CENTRO PER LA CYBERSICUREZZA REGONALE II INTERVENTO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J89B22000540001	14_WP_9_RIST_ROMA CAPITALE	POTENZIAMENTO CYBER ROMA CAPITALE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	C99B22000020006	12_WP_9_RIST_REGIONE ABRUZZO	CYBER SECURITY CERT SANITA REGIONE ABRUZZO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F71B22001240006	58_WP_9_RIST_COMUNE DI VENEZIA	RESILIENZA CIBERNETICA COMUNE DI VENEZIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	E87H22002580008	52_WP_9_RIST_REGIONE LOMBARDIA	CYBER SECURITY ASSESSMENT ENTI SANITARI LOMBARDIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	E87H22002560008	28_WP_9_RIST_REGIONE LOMBARDIA	PROGRAMMA DI SICUREZZA E PROTEZIONE DEI DATI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	I64F22000070006	43_WP_9_RIST_REGIONE UMBRIA	POTENZIAMENTO CYBER SANITA UMBRA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J83E23000060006	24_WP9_RIST_MAECI_2	MAECI HUMAN FIREWALL	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G36G22000230006	3_WP_9_RIST_REGIONE BASILICATA	CENTRO PER LA CYBERSICUREZZA REGIONALE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D76G22000400006	9_WP_9_RIST_COMUNE DI PALERMO	RESILIENZA CYBER COMUNE DI PALERMO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D66G22000340006	11_WP_9_RIST_COMUNE DI CATANIA	POTENZIAMENTO E SICUREZZA DEGLI END-POINT	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	C99B22000030006	13_WP_9_RIST_REGIONE ABRUZZO	CERT REGIONALE DELL'AMBITO DELLA GESTIONE DELLE ACQUE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J89B22000550001	15_WP_9_RIST_ROMA CAPITALE	RAFFORZAMENTO DEI PRESIDI DI SICUREZZA ROMA CAPITALE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J69B22000160006	20_WP_9_RIST_REGIONE CALABRIA	CYBERSICUREZZA SERVIZI ALLE ASP E AO REGIONALI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	C64F22000320006	21_WP_9_RIST_PROVINCIA AUTONOMA DI TRENTO	RESILIENZA CYBER PER LA PROVINCIA AUTONOMA DI TRENTO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G36G22000260006	24_WP_9_RIST_REGIONE LIGURIA	ADEGUAMENTO FIREWALL E POLICY DI SICUREZZA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	I64F22000060006	25_WP_9_RIST_REGIONE UMBRIA	INNALZAMENTO LIVELLO DI SICUREZZA REGIONALE UMBRA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D19B22000420006	31_WP_9_RIST_REGIONE TOSCANA	DISASTER RECOVERY E BUISNESS CONTINUITY	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B69B22000310006	48_WP_9_RIST_COMUNE DI NAPOLI	PIATTAFORMA SOC/EPP EVOLUTO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B39B22000850006	49_WP_9_RIST_REGIONE MARCHE	SICUREZZA SERVIZI DI ASSISTENZA SANITARIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B69B22000320006	50_WP_9_RIST_COMUNE DI NAPOLI	ADOZIONE FRAMEWORK ZERO TRUST ACCESS	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B59B22000690006	51_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	AMPLIAMENTO SOC	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B66G22017050006	57_WP_9_RIST_REGIONE CAMPANIA	CYBER CAMPANIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G66G22000200008	65_WP_9_RIST_REGIONE SICILIA	SICUREZZA ENDPOINT RTRS	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	E41B22004190006	66_WP_9_RIST_REGIONE EMILIA ROMAGNA	POTENZIAMENTO CYBER SERVIZI SANITARI REGIONALI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B53E22001890006	71_WP_9_RIST_REGIONE VALLE D'AOSTA	CYBER AWARENESS PA LOCALE DELLA VALLE D'AOSTA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F71B22001250006	73_WP_9_RIST_COMUNE DI VENEZIA	PIANO DI CYBERSECURITY AWARENESS	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F76G22000380006	74_WP_9_RIST_COMUNE DI VENEZIA	TECNOLOGIE A MITIGAZIONE DEL RISCHIO CYBER	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	E24I22000010005	75_WP_9_RIST_REGIONE SARDEGNA	POTENZIAMENTO DEL SISTEMA INFORMATIVO REGIONALE AMBIENTALE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G29B22000280001	79_WP_9_RIST_COMUNE DI CAGLIARI	METROCAGLIARI IT-SECURITY PROGETTO 2	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F66G23000100006	2_WP12_A5_Innonation	INNONATION CYBER SECURITY LAB	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D86G21005000006	13_WP9_RIST_DIF_2	POTENZIAMENTO E RINNOVO LICENZE E SUPPORTO SISTEMISTICO DEI SISTEMI MCAFEE DI PROTEZIONE DELLE RETI E SISTEMI IT INTERFORZE E DELLE F.A	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D21C22001380008	29_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	REGIONE FRIULI VENEZIA GIULIA CYBER INIZIATIVE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D21C22001400008	30_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	CYBERSECURITY FVG: TRAINING&AWARENESS	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F83E22000060006	55_WP_9_RIST_REGIONE LAZIO	PIANO DI SECURITY AWARENESS REGIONE LAZIO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F66G24000010006	F66G24000010006	SISTEMA DI HIGH PERFORMANCE COMPUTING PE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G39B23000090006	1_WP7_A6_REGIONE LIGURIA	CSIRT LIGURIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	H19B23000100006	2_WP7_A6_REGIONE VENETO	ATTIVAZIONE CERT-CSIRT REGIONALE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B39B23001370006	3_WP7_A6_REGIONE MARCHE	CSIRT REGIONE MARCHE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F84F23000230006	4_WP7_A6_REGIONE LAZIO	CSIRT REGIONE LAZIO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G39E23000010001	6_WP7_A6_REGIONE BASILICATA	"POTENZIAMENTO DELLO CSIRT BASILICATA"	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D11C23000760008	8_WP7_A6_REGIONE TOSCANA	CSIRT DELLA REGIONE TOSCANA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	E47H23001240008	9_WP7_A6_REGIONE LOMBARDIA	POTENZIAMENTO CSIRT LOMBARDIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	E31C23001310006	10_WP7_A6_REGIONE EMILIA-ROMAGNA	POTENZIAMENTO CSIRT REGIONALE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	C19B23000130006	11_WP7_A6_REGIONE ABRUZZO	ATTIVAZIONE CSIRT ABRUZZO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	E76G23000110006	12_WP7_A6_REGIONE SARDEGNA	CSIRT-RAS-PSR - SARDEGNA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	I64F23000070006	14_WP7_A6_REGIONE UMBRIA	POTENZIAMENTO CSIRT UMBRIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D11B23000310006	15_WP7_A6_REGIONE MOLISE	ATTIVAZIONE CSIRT LIVELLO BASE MOLISE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J69B23000340006	16_WP7_A6_REGIONE CALABRIA	"ATTIVAZIONE CSIRT CALABRIA"	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B27H23002720006	17_WP7_A6_REGIONE CAMPANIA	CSIRT – CAMPANIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	G79B23000220006	18_WP7_A6_REGIONE SICILIA	CSIRT SICILIA	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	C49E23000850006	19_WP7_A6_PROVINCIA AUTONOMA DI TRENTO	CSIRT PROVINCIA AUTONOMA DI TRENTO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B39E23000040006	13_WP7_A6_PROVINCIA AUTONOMA DI BOLZANO	"POTENZIAMENTO CERT ALTO ADIGE"	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	B34F23009890006	5_WP7_A6_REGIONE PUGLIA	RAFFORZAMENTO CSIRT REGIONALE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	D21C23000470006	7_WP7_A6_REGIONE FRIULI-VENEZIA GIULIA	POTENZIAMENTO CSIRT RAFVG	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G23000630006	4_WP12_A5_DIGITALPLATFORMS	LAP DIGITALPLATFORMS	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G23000620006	3_WP12_A5_IPS	LAB IPS	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G23000580006	15_WP12_A5_STONESECURITY	ADEGUAMENTO LABORATORI ON-SITE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G23000560006	8_WP12_A5_DEEPLAB	DEEP CYBER	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G23000590006	18_WP12_A5_ATSEC	ACCREDITAMENTO LAP ATSEC	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G23000640006	17_WP12_A5_TECNINF	FUTURE READY CS LAB	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F46G23000090006	5_WP12_A5_SECURENETWORK	LABORATORIO DI PROVA SECURE NETWORK	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G23000570006	12_WP12_A5_SISTEMI&AUTOMAZIONE	SEA_LAP	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F66G23000110006	19_WP12_A5_APAVEITALIA	APAVELAB	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F16G23000190006	13_WP12_A5_SIPAL	LAP SIPAL	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G23000600006	20_WP12_A5_E-TRACE	E-TRACE LABS	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F46G23000060006	21_WP12_A5_IMQ	LABORATORIO PROVE SICUREZZA IMQ	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F16G23000170006	23_WP12_A5_TESLY	FUTURING TECHNOLOGY CENTER (FTC)	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F66G23000120006	22_WP12_A5_INTELLISYNC	INTELLISYNC LAP	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G23000660004	29_WP12_A5_NEXTINGEGNERIA	LAP NEXT INGEGNERIA DEI SISTEMI	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G23000610006	27_WP12_A5_MPG	LABORATORIO DI PROVA INDIPENDENTE	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F46G23000070006	30_WP12_A5_SABABA	SABABA SECURITY LABORATORIO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G23000650006	28_WP12_A5_HERMESBAY	SONIC	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F46G23000080006	31_WP12_A5_INNOVERY	LAP INNOVERY	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F86G23000670004	32_WP12_A5_DIGITALENGINEERING	CARDEA - CENTER OF ANALYSIS AND RESEARCH	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	J69B22000250006	33_WP12_A5_INNOVAPUGLIA	INNOVAPUGLIA LAP ACCREDITATO	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO
PIANO NAZIONALE RIPRESA E RESILIENZA	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE	M1C1I1.5	F36G23000050006	35_WP12_A5_ANCHARIA	ALAB SOFTWARE AND NETWORK SECURITY	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	IN CORSO

Qui di seguito la tabella contenente i dati dei progetti, forniti dal Dipartimento per la trasformazione digitale, congiuntamente con l'Agenzia per la cybersicurezza, concernenti l'Avviso n. 8, già ampiamento descritto in precedenza.

	Codice Unico Progetto	*Codice Locale Progetto*	*Descr. Titolo Progetto*
1	H66G24000010006	1_WP9_A8_Città Metropolitana di Napoli	METRO CYBER NAPOLI
2	B79B24000050006	10_WP9_A8_Autorità di Sistema Portuale del Mare di Sardegna	Implementazione di un modello tecnico organizzativo di cybersecurity aziendale
3	F36G24000050002	102_WP9_A8_Autorità di Sistema Portuale del Mar Ligure Orientale	INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBERSECURITY DEL SISTEMA PORTUALE DELLA SPEZIA E MARINA DI CARRARA
4	B39B24000140006	103_WP9_A8_Città Metropolitana di Reggio Calabria	CMDRC SECURITY
5	H31B24000030006	104_WP9_A8_Agenzia Regionale per la Protezione dell'Ambiente della Basilicata – ARPAB	ARPAB Security
6	I76G24000090006	105_WP9_A8_Agenzia Regionale Protezione Ambiente Marche – ARPAM	Rafforzamento dei processi e dei sistemi relativi alla cybersecurity
7	J26G24000010006	106_WP9_A8_Comune di Pescara	Potenziamento Cybersicurezza Comune di Pescara
8	B19B24000070006	107_WP9_A8_Città Metropolitana di Firenze	CyberMetroFI – Potenziamento di servizi e infrastrutture Cyber della Città Metropolitana di Firenze
9	E39E24000010006	111_WP9_A8_Comune di Piacenza	Potenziamento della resilienza cyber del Comune di Piacenza
10	H31B24000020001	112_WP9_A8_Agenzia Regionale Sanitaria Marche	Rafforzamento della sicurezza cibernetica dei sistemi critici sanitari della Regione Marche
11	G71F24000090006	113_WP9_A8_Autorità di Bacino Distrettuale delle Alpi Orientali	Potenziamento della resilienza cyber dell'Autorità di Bacino distrettuale delle Alpi Orientali
12	B31B24000140006	114_WP9_A8_Comune di Potenza	CyberShield: Progetto di Sicurezza Informatica e Difesa Digitale
13	J26G23000250006	115_WP9_A8_Città Metropolitana di Cagliari	POTENZIAMENTO CYBERSECURITY
14	I57H24000740006	116_WP9_A8_Comune di Salerno	POTENZIAMENTO GOVERNANCE E PROGRAMMAZIONE CYBER, PROCESSI DI SICUREZZA, GESTIONE DEL RISCHIO CYBER E CONTINUITÀ OPERATIVA
15	I69B24000080006	117_WP9_A8_Azienda Regionale dell'Emergenza e	POTENZIAMENTO RESILIENZA CYBER - AREUS

		Urgenza della Sardegna – AREUS	
16	G27H24000530004	118_WP9_A8_Agenzia Sanitaria Regionale – Abruzzo	Potenziamento Controlli Cyber ASR
17	J31I24000030006	119_WP9_A8_Autorità di Sistema Portuale del Mar Tirreno Centro Settentrionale	PROGETTO DI RESILIENZA 1.5 PER L'ADEMPIMENTO DELLE MISURE DI SICUREZZA
18	I51F24000040006	12_WP9_A8_Agenzia Regionale per la Protezione dell'Ambiente della Calabria – ARPACAL	ARPACAL Cyber Defense for Environment and Health
19	E64F24000280006	121_WP9_A8_Agenzia Regionale per la Protezione dell'Ambiente della Campania – ARPAC	Assessment e potenziamento della resilienza cyber di ARPAC
20	D87H24001050006	122_WP9_A8_Autorità di Bacino Distrettuale dell'Appennino Centrale	Realizzazione di interventi di potenziamento della resilienza cyber dell'Autorità di Bacino Distrettuale dell'Appennino Centrale
21	F96G24000080001	13_WP9_A8_Comune di Trieste	ADEGUAMENTO SICUREZZA INFORMATICA
22	I46G24000000006	14_WP9_A8_Città Metropolitana di Milano	COMPREHENSIVE CYBERSECURITY CITTÀ METROPOLITANA MILANO
23	D66G24000040006	95_WP9_A8_Comune di Trento	Intervento cyber security e resilienza Comune di Trento
24	H19B24000040006	78_WP9_A8_Comune di Bergamo	Bergamo CyberSec360
25	D66G23000210006	18_WP9_A8_Città Metropolitana di Catania	Città Metropolitana di Catania Sicura
26	C81B24000100006	19_WP9_A8_Comune di Brescia	POTENZIAMENTO DI SERVIZI E INFRASTRUTTURE DI SICUREZZA INFORMATICA PER COMUNE DI BRESCIA
27	D57H24000980005	20_WP9_A8_Autorità di Sistema Portuale del Mare Ionio	POTENZIAMENTO DELLA RESILIENZA CYBER DEL PORTO DI TARANTO
28	B24F24000540006	21_WP9_A8_Comune di Latina	POTENZIAMENTO DELLA RESILIENZA CYBER DEL COMUNE DI LATINA
29	J81B24000320001	23_WP9_A8_Comune di Reggio Emilia	PIANO DI POTENZIAMENTO DELLA SICUREZZA INFORMATICA
30	C36G24000020006	24_WP9_A8_Città Metropolitana di Bologna	Cyber_In_BO
31	E66G24000000005	26_WP9_A8_Agenzia Regionale per la Protezione dell'Ambiente del Friuli-Venezia Giulia – ARPAFVG	SICUREZZA INFORMATICA ARPA FVG
32	J46G24000020006	54_WP9_A8_Comune di Livorno	Livorno Cyber Resilience: Potenziamento dell'Infrastruttura Cyber dell'Ente Attraverso Strategie di Formazione, Sensibilizzazione, Rilevamento, Monitoraggio, Risposta e Ripristino
33	F19B23000110006	29_WP9_A8_Comune di Novara	No.V.A.R.A. Presidium IT Securitatis (Novara Vulnerability Assessment Risk Analysis)
34	E76G24000010001	3_WP9_A8_Agenzia Regionale per la Protezione dell'Ambiente della Sicilia – ARPA SICILIA	ARES – ARPA Resilient Environment Security
35	J41F24000100006	30_WP9_A8_Agenzia Regionale per la Protezione dell'Ambiente dell'Umbria – ARPA UMBRIA	Cybersecurity Arpa Umbria

36	F46G24000040006	31_WP9_A8_Agenzia Regionale Emergenza Urgenza – Lombardia	AREU Sicura
37	B36G24000030006	32_WP9_A8_Agenzia Regionale per la Protezione dell'Ambiente Ligure – ARPAL	CYBER ARPAL
38	G96G23000210006	34_WP9_A8_Comune di Giugliano in Campania	Istituzione della Funzione Operativa di Resilienza Cibernetica Evoluta (FORCE)
39	D69B24000000006	37_WP9_A8_Comune di Catanzaro	Potenziamento della resilienza cyber del Comune di Catanzaro
40	G69B24000020006	38_WP9_A8_Autorità di Sistema Portuale del Mar Tirreno Centrale	CyberADSP_2024
41	D56G23000420006	39_WP9_A8_Agenzia Regionale di Sanità – Regione Toscana	Potenziamento resilienza cyber di ARS Toscana
42	E56G23000090006	4_WP9_A8_Comune di Taranto	Potenziamento postura di cybersecurity rispetto agli accessi di utenti ed apparati alla rete dei servizi comunali
43	J36G23000230006	50_WP9_A8_Agenzia Regionale per la Prevenzione, l'Ambiente e l'Energia dell'Emilia-Romagna – ARPAE	Potenziamento della capacità di identificazione e risposta ai rischi cyber
44	E29B24000000006	43_WP9_A8_Azienda Regionale di Coordinamento per la Salute – ARCS	Miglioramento della postura di sicurezza cyber nel perimetro aziendale
45	H56G24000030006	44_WP9_A8_Autorità di Bacino Distrettuale dell'Appennino Settentrionale	POTENZIAMENTO RESILIENZA CYBER – ADAS
46	I26G24000030006	45_WP9_A8_Agenzia Regionale per la Protezione dell'Ambiente della Sardegna – ARPAS	ARPAS4SEC
47	C96G24000010006	46_WP9_A8_Comune di Perugia	Perugia Data Safe
48	J16G24000030006	47_WP9_A8_ Agenzia Regionale per la Prevenzione e Protezione Ambientale del Veneto – ARPAV	ARPAV CYBERSICURA - Incremento del livello di sicurezza informatica e della resilienza dell'Ente ad eventuali attacchi informatici
49	C99B24000010006	49_WP9_A8_Città Metropolitana di Bari	PROGRAMMA DI POTENZIAMENTO CYBER DELLA CITTÀ METROPOLITANA DI BARI
50	B76G24000040006	5_WP9_A8_Comune di Foggia	CyberSec Foggia – Implementazione di misure di Cybersecurity per il potenziamento dei sistemi IT Comunali
51	B76G21063570006	42_WP9_A8_Comune di Ferrara	Strumenti e servizi per l'irrobustimento della postura di sicurezza e l'efficace gestione degli incidenti
52	I99B24000040006	51_WP9_A8_Comune di Parma	L'evoluzione della cyber security a 360°. Dalla formazione alle tecnologie innovative
53	D79B24000140006	52_WP9_A8_Città Metropolitana di Palermo	Cyber security e Resilienza nella Città Metropolitana di Palermo
54	G76G24000060006	53_WP9_A8_Agenzia Regionale per la Protezione dell'Ambiente della Valle d'Aosta – ARPAVDA	Interventi di potenziamento della resilienza cyber – PA
55	C91B24000110006	28_WP9_A8_Comune di Rimini	MUNICIPALITY CYBERSECURITY AS A NEW PARADIGM

56	I76G24000060006	55_WP9_A8_Autorità di Sistema Portuale del Mare di Sicilia Occidentale	Interventi di potenziamento della resilienza cyber dell'Autorità di Sistema Portuale del Mare di Sicilia Occidentale
57	F36G24000060006	58_WP9_A8_Città Metropolitana Roma Capitale	Potenziamento di servizi e infrastrutture per Città Metropolitana di Roma Capitale
58	E39B24000020006	6_WP9_A8_Comune di Ancona	SecurityAN
59	B51C24000130006	60_WP9_A8_Comune di Monza	POTENZIAMENTO DELLA RESILIENZA CYBER DEL COMUNE DI MONZA
60	B79B21002230006	62_WP9_A8_Città Metropolitana di Venezia	CYBERMET – Cybersecurity Metropolitana
61	F91B24000140005	65_WP9_A8_Autorità di Bacino Distrettuale del Fiume Po	Miglioramento della Sicurezza Informatica all'interno dell'Autorità di Bacino Distrettuale del fiume Po
62	C96G23000250006	66_WP9_A8_Autorità di Sistema Portuale del Mare Adriatico Orientale	Porto Digitale Resiliente - PODRES
63	D36G24000030006	67_WP9_A8_Comune di Campobasso	Cyber Sentinel: rafforzare le infrastrutture comunali contro le minacce informatiche
64	B41F24000050006	69_WP9_A8_Autorità di Sistema Portuale del Mar Tirreno Settentrionale	Potenziamento resilienza cyber AdSP MTS
65	J86G23000390008	7_WP9_A8_Agenzia Regionale Emergenza Sanitaria ARES 118	Concessione e la relativa Convenzione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del d.l. n. 179 del 2012, ai sensi degli artt. 164, 165, 179, 180, comma 3 e 183, comma 15 del d.lgs. 18 aprile 2016, n. 50 e successive modificazioni o integrazioni avente ad oggetto l'affidamento in concessione dei servizi infrastrutturali e applicativi in cloud per la gestione di dati sensibili - "Polo Strategico Nazionale". Migrazione della struttura informatica di ARES 118 al Cloud del PSN nell'ambito del Piano Nazionale di Ripresa e Resilienza "Obiettivi Italia Digitale 2026" – "Obiettivo 3 – Cloud e Infrastrutture digitali". Approvazione del piano di migrazione e delle relative attività propedeutiche necessarie all'assolvimento dello stesso per le quali saranno effettuate specifiche delibere.
66	J37H24000670006	70_WP9_A8_Autorità di Sistema Portuale del Mare Adriatico Centrale	ADSPMAC CYBER
67	J91F23001330001	71_WP9_A8_Agenzia Regionale Strategica per la Salute e il Sociale – A.Re.S.S.	Potenziamento capacità cyber AReSS Puglia
68	J19B24000020001	73_WP9_A8_Città Metropolitana di Torino	CyberMetro

69	B37H24000910006	75_WP9_A8_Comune di Vicenza	Vicenza (cyber)sicura rinforziamo la difesa digitale della nostra città
70	D41B20001480006	77_WP9_A8_Città Metropolitana di Genova	Cyber-CMGE
71	C39B22000090006	17_WP9_A8_Autorità di Sistema Portuale del Mar Ligure Occidentale	Interventi a supporto della consapevolezza e della postura nel rischio cyber per la resilienza di un sistema portuale complesso
72	I97H24000290006	8_WP9_A8_Agenzia Regionale per la Prevenzione e la Protezione dell'Ambiente – ARPA Puglia	Cyber ARPA Puglia – Progettazione e realizzazione di misure di sicurezza per il potenziamento della resilienza cyber dei sistemi di monitoraggio ambientale
73	C69B24000050001	80_WP9_A8_Comune di Ravenna	PROGRAMMA DI POTENZIAMENTO CYBER DEL COMUNE DI RAVENNA
74	E19B24000020006	87_WP9_A8_Agenzia Regionale per la Protezione Ambientale della Toscana – ARPAT	ARPAT-Interventi di potenziamento della resilienza cyber
75	C61B24000080006	89_WP9_A8_Autorità di Sistema Portuale del Mare Adriatico Centro Settentrionale	MACSecurity
76	H96G24000050006	90_WP9_A8_Comune di Padova	P@CYBER
77	I16G24000040006	92_WP9_A8_Agenzia Regionale per la Protezione dell'Ambiente del Lazio – ARPA LAZIO	Potenziamento di servizi e infrastrutture di sicurezza per ARPA Lazio
78	C66G24000050006	94_WP9_A8_Comune di Aosta	Potenziamento della resilienza Cyber per il Comune di Aosta
79	C39E24000160006	15_WP9_A8_Comune di Prato	Miglioramento postura di sicurezza del Comune di Prato
80	F71C24000010006	98_WP9_A8_Autorità di Sistema Portuale del Mare Adriatico Settentrionale	POTENZIAMENTO DELLE CAPACITA' DI SICUREZZA INFORMATICA E INNOVAZIONE NEI PORTI DI VENEZIA E CHIOGGIA
81	I36G24000020006	99_WP9_A8_Comune di Verona	Progetto di potenziamento cybersecurity strategica e operativa

Per quanto concerne i dati forniti dal Dipartimento per la trasformazione digitale, congiuntamente con l'Agenzia per la cybersicurezza, in relazione al monitoraggio sull'avanzamento dei progetti e sugli eventuali scostamenti di cui si è fatto cenno nelle pagine precedenti, si riporta qui di seguito una tabella esplicativa dalla quale si evince la presenza di disallineamenti nel sistema Regis, la cui giustificazione si rinviene nelle note ivi contenute.

Tipologia Avviso	Riscontro
Avviso n. 01/2022	Con Determina prot. ACN n. 0037953 del 20-11-2024 è stata autorizzata la possibilità di prorogare il termine di completamento degli interventi al 30.06.2025. A fronte di tale determina sono state trasmesse e sono parzialmente ancora in valutazione richieste di modifica dei cronoprogrammi dei progetti, le quali, verificate dall'Agenzia, saranno visibili sul sistema ReGiS che ad oggi, pertanto, presenta ancora le precedenti scadenze e non tiene conto di eventuali disimpegni/rinunce del periodo di riferimento e che saranno visibili secondo l'iter di implementazione del sistema.
Avviso n. 03/2022	Con Determina prot. ACN n. 0037953 del 20-11-2024 è stata autorizzata la possibilità di prorogare il termine di completamento degli interventi al 30.06.2025. A fronte di tale determina sono state trasmesse e sono parzialmente ancora in valutazione richieste di modifica dei cronoprogrammi dei progetti, le quali, verificate dall'Agenzia, saranno visibili sul sistema ReGiS che ad oggi, pertanto, presenta ancora le precedenti scadenze e non tiene conto di eventuali disimpegni/rinunce del periodo di riferimento e che saranno visibili secondo l'iter di implementazione del sistema.
Avviso n. 05/2023	Con Determina prot. ACN n. 033725 del 17-10-2024 è stato modificato il termine del 30.09.2025 come segue: *(…) per quanto riguarda il contributo alla milestone ovvero la trasmissione dell'attestazione relativa all'attivazione del laboratorio sulla base del modello "Dichiarazione attivazione laboratorio" entro la data del 15 dicembre 2024; per quanto riguarda la chiusura delle attività e presentazione della rendicontazione finale delle spese, non oltre la data 30 settembre 2025.* A fronte di tale determina sono state trasmesse e sono parzialmente ancora in valutazione richieste di modifica dei cronoprogrammi dei progetti, le quali, verificate dall'Agenzia, saranno visibili sul sistema ReGiS che ad oggi, pertanto, presenta ancora le precedenti scadenze e non tiene conto di eventuali disimpegni/rinunce del periodo di riferimento e che saranno visibili secondo l'iter di implementazione del sistema. In verifica la puntuale ricezione al 15. dicembre 2024 delle Dichiarazioni.
Avviso n. 06/2023	In corso di valutazione le richieste di modifica attinenti in particolare alle proroghe per le attività amministrativo-contabili , le quali, verificate dall'Agenzia, saranno visibili sul sistema ReGiS secondo le scadenze di monitoraggio consuete (entro il 10° giorno del mese successivo all'approvazione). In valutazione la possibilità di procedere ad analoga proroga come per gli Avvisi 1 e 3.
Cyber Defence	In corso di valutazione le Domande di rimborso presentate dai soggetti sub-attuatori, il sistema ReGiS, come da intese con l'Amministrazione Titolare, sarà alimentato a chiusura delle procedure di controllo sostanziale effettuate dall'ACN.

Nella tabella suindicata, si evidenzia, in particolare, la determina adottata dall'Agenzia per la Cybersicurezza del 20 novembre 2024, n. 0037953, che si riferisce all'Avviso pubblico n. 01/2022 (approvato con determina ACN prot. n. 1816 del 02 marzo 2022) e all'Avviso pubblico n. 03/2022 (approvato con determina ACN prot. n. 10220 del 29 luglio 2022).

Nella succitata determina sono richiamati nelle premesse il paragrafo 1.2 dei menzionati Avvisi Pubblici n. 01/2022 e n. 03/2022, ai sensi del quale "la rendicontazione di Milestone e Target non è necessariamente legata all'avanzamento finanziario del Progetto" e che, conseguentemente, le attività amministrative e rendicontazione

finanziaria delle spese sostenute non rilevano ai fini del conseguimento del target.

Nella determina emerge, altresì, che a seguito delle richieste pervenute dai Soggetti attuatori ammessi a finanziamento in merito all'opportunità necessità di una proroga della scadenza prevista al 30 novembre 2024 per il completamento degli adempimenti connessi alla rendicontazione del finanziamento e dell'inoltro della domanda di rimborso a saldo, nonché per il completamento di alcune delle attività previste, l'Agenzia – ravvisata l'opportunità di prorogare, previa valutazione positiva da parte dell'Agenzia stessa di una specifica richiesta di modifica progettuale, il termine di conclusione dei progetti, fermo restando il suddetto allineamento alle finalità dell'Investimento 1.5 – ha ritenuto di modificare gli Avvisi n. 1 e n. 3, consentendo di prorogare il termine di completamento degli interventi al 30 giugno 2025.

Nella stessa direzione la determina adottata dall'Agenzia il 17 ottobre 2024, che si riferisce all'Avviso pubblico n. 5 - collegato alla milestone M1C1-21 "Completamento della rete dei laboratori e dei centri di valutazione per la valutazione e certificazione della cybersecurity" entro dicembre 2024 – dalla quale si apprende che la stessa ha ravvisato l'opportunità di prevedere una proroga dei termini di conclusione dei progetti in relazione alle attività amministrative e rendicontazione finanziaria delle spese sostenute, fermo restando il termine per la presentazione della documentazione attestante l'attivazione dei laboratori di scrutinio e analisi software. Termine pertanto prorogato fino al 30 settembre 2025.

Si riporta, infine, una tabella con i dati più significativi dei 120 progetti che presentano dei ritardi, estrapolata da una tabella excel, fornita in corso di istruttoria dagli Enti competenti, in cui sono indicati anche gli Avvisi collegati ai singoli progetti:

	Avviso di riferimento	Codice Locale Progetto	Stato CUP	Stato Avanzamento Progetto	Titolo Progetto	Sintesi Progetto	Descrizione Tipo Aiuto	Data Fine Progetto Prevista
1	avviso_1_2022	06_WP9_RIST_AGDO_2	Attivo	In Corso	GOVERNANCE E AWARENESS PERSONALE ADM	IL SISTEMA INFORMATIVO (SI) ADM PARTE INTEGRANTE DEL SI DELLA FISCALIT . LINTERVENTO CONCERNE I SETTORI DOGANE E MONOPOLI GOVERNATI PRESSO LA DIREZIONE GENERALE DI ROMA E LE 300 STRUTTURE TERRITORIALI.*INTERO TERRITORIO NAZIONALE*INTERVENTO 2: RESI	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	07/05/2024
2	avviso_1_2022	12_WP9_RIST_DIF_1	Attivo	In Corso	Incremento cultura cyber security ei	RETE INFORMATICA DELL'ESERCITO ITALIANO*STATO MAGGIORE ESERCITO - COMANDO TRASMISSIONI-REPARTO SICUREZZA CIBERNETICA DELL EI*SVILUPPO DI UN'APPLICAZIONE SW PER ADDESTRARE IL PERSONALE ALLE TEMATICHE DI SICUREZZA CYBER PER INCREMENTARE LA CONSAPEVOLEZZA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	20/07/2022
3	avviso_1_2022	23_WP9_RIST_MAECI_1	Attivo	In Corso	Adeguamento alle misure previste psnc	MAECI - DGAI UFFICIO VIII MINISTERO AFFARI ESTERI*PIAZZA DELLA FARNESINA 1*PERCORSO DI TRASFORMAZIONE DIGITALE IN MATERIA DI PROTEZIONE DEI SISTEMI INFORMATIVI CHE	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/09/2023

						EVIDENZI ELEMENTI UTILI PER COLMARE EVENTUALI AREE DI CRITICIT DI NATURA CIBERNETICA		
4	avviso_1_2022	05_WP9_RIST_AGDO_1	Attivo	In Corso	Postura di sicurezza awareness adm	IL SISTEMA INFORMATIVO (SI) ADM PARTE INTEGRANTE DEL SI DELLA FISCALIT . L INTERVENTO CONCERNE I SETTORI DOGANE E MONOPOLI GOVERNATI PRESSO LA DIREZIONE GENERALE DI ROMA E LE 300 STRUTTURE TERRITORIALI.*INTERO TERRITORIO NAZIONALE*INTERVENTO 1:RESILIENZ	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/09/2024
5	avviso_1_2022	15_WP9_RIST_DVF_1	Attivo	In Corso	DIPARTIMENTO VIGILI DEL FUOCO UPGRADE PER IL POTENZIAMENTO DELLE CAPACITA DI MONITORAGGIO DEL RISCHIO CYBER	MINISTERO DELL'INTERNO-DIPARTIMENTO VIGILI DEL FUOCO SOCCORSO PUBBLICO E DIFESA CIVILE-DIREZIONE CENTRALE PER LE RISORSE LOGISTICHE E STRUMENTALI-UFFICIO PER I SERVIZI INFORMATICI MINISTERO DELL'INTERNO*VIA CAVOUR 5*UPGRADE PER IL POTENZIAMENTO DELLE CAP	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/09/2024
6	avviso_1_2022	07_WP9_RIST_AGDEM_1	Attivo	In Corso	Resilienza cyber agenzia del demanio	SISTEMA INFORMATIVO AGENZIA DEL DEMANIO*VIA BARBERINI 38*REALIZZAZIONE SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2022

7	avviso_1_2022	14_WP9_RIST_DIF_3	Attivo	In Corso	Nuclei cyber security proiettabili	RETE INFORMATICA DELL'ESERCITO ITALIANO*STATO MAGGIORE ESERCITO - COMANDO TRASMISSIONI-REPARTO SICUREZZA CIBERNETICA DELL EI*SIEM TATTICI PER EI PER AMMODERNAMENTO EQUIPAGGIAMENTO PER NUCLEI CYBER SECURITY PROIETTABILI	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2022
8	avviso_1_2022	13_WP9_RIST_DIF_2	Attivo	In Corso	Potenziamento e rinnovo licenze e supporto sistemistico dei sistemi mcafee di protezione delle reti e sistemi it interforze e delle f.a	STATO MAGGIORE DIFESA - COMANDO PER LE OPERAZIONI IN RETE (COR) - ROMA*VIA STRESA 31/B*POTENZIAMENTO E RINNOVO LICENZE E SUPPORTO SISTEMISTICO DEI SISTEMI MCAFEE DI PROTEZIONE DELLE RETI E SISTEMI IT CLASSIFICATI E NON CLASSIFICATI INTERFORZE E DELLE F.A.	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
9	avviso_1_2022	03_WP9_RIST_PCM_3	Attivo	In Corso	User account security enforcement	PRESIDENZA DEL CONSIGLIO DEI MINISTRI*PIAZZA COLONNA 370*PASSAGGIO DA CREDENZIALI DI ACCESSO STANDARD A DOPPIA CHIAVE DI AUTENTICAZIONE	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
10	avviso_1_2022	09_WP9_RIST_CORTCOST_1	Attivo	In Corso	Incremento sicurezza cortecostituzionale	SEGRETERIA GENERALE CORTE COSTITUZIONALE*PIAZZA QUIRINALE*INCREMENTO DELLA SICUREZZA DELLA CORTE COSTITUZIONALE CONTRO ATTACCHI CYBER	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
11	avviso_1_2022	04_WP9_RIST_PCM_4	Attivo	In Corso	Client security enforcement	PRESIDENZA DEL CONSIGLIO DEI MINISTRI*PIAZZA COLONNA 370*CLIENT SECURITY ENFORCEMENT	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

12	avviso_1_2022	02_WP9_RIST_PCM_2	Attivo	In Corso	Branch office security enforcement	PRESIDENZA DEL CONSIGLIO DEI MINISTRI*PIAZZA COLONNA 370*BRANCH OFFICE SECURITY ENFORCEMENT	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
13	avviso_1_2022	24_WP9_RIST_MAECI_2	Attivo	In Corso	MAECI HUMAN FIREWALL	MAECI HUMAN FIREWALL*CORSI PER PERSONALE MAECI SU CYBERSICUREZZA*MODALIT FORMATIVA (E.LEARNING) E ADDESTRATIVA. IL PERCORSO FORMATIVO ARTICOLATO IN 24 MODULI MULTI-LINGUE. IL SERVIZIO SIA NELLA MODALIT FORMATIVA SIA NELLA MODALIT ADDESTRATIVA VIENE E	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
14	avviso_1_2022	17_WP9_RIST_MEF_2	Attivo	In Corso	Security monitoring identity governance	MINISTERO DELL'ECONOMIA E DELLE FINANZE*VIA XX SETTEMBRE 97*PIATTAFORMA DI MONITORAGGIO E DIFESA CONTRO LE MINACCE CYBER BASATA SU INTELLIGENZA ARTIFICIALE-PIATTAFORMA PER UNA GESTIONE AVANZATA DEL CICLO DI VITA DELLE UTENZE - AUTENTICAZIONE AVANZATA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
15	avviso_1_2022	10_WP9_RIST_CORTCOST_2	Attivo	In Corso	Licenze e servizi di supporto	SEGRETERIA GENERALE CORTE COSTITUZIONALE*PIAZZA QUIRINALE*ACQUISIZIONE DI NUOVI SERVIZI E STRUMENTI (LICENZE E SERVIZI DI SUPPORTO) PER IL MIGLIORAMENTO DELLA SICUREZZA LOGICA DELLE POSTAZIONI DI LAVORO E DEI SERVER	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
16	avviso_1_2022	08_WP9_RIST_CAM_1	Attivo	In Corso	Sicurezza perimetro rete camera	CENTRO ELABORAZIONE DATI E RETE DATI DELLA CAMERA DEI DEPUTATI*PIAZZA DEL PARLAMENTO 19-24*APPARATI	INTERVENTO CHE NON COSTITUISCE	31/12/2023

						DI RETE E PER LA SICUREZZA INFORMATICA	AIUTO DI STATO	
17	avviso_1_2022	28_WP9_RIST_MITE_3	Attivo	In Corso	Cyber strategy & distributed visibility	MINISTERO DELLA TRANSIZIONE ECOLOGICA*VIA CRISTOFORO COLOMBO 44*MISURE DI POTENZIAMENTO DELLA SICUREZZA INFORMATICA_PROGETTO 1 CYBER STRATEGY & DISTRIBUTED VISIBILITY	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	31/12/2023
18	avviso_1_2022	26_WP9_RIST_MITE_1	Attivo	In Corso	Centralized threat monitoring	MINISTERO DELLA TRANSIZIONE ECOLOGICA_DG ITC*VIA CRISTOFORO COLOMBO 44*MISURE DI POTENZIAMENTO DELLA SICUREZZA INFORMATICA_PROGETTO 3 CENTRALIZED THREAT MONITORING	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	31/12/2023
19	avviso_1_2022	27_WP9_RIST_MITE_2	Attivo	In Corso	Posture management & attack prevention	MINISTERO DELLA TRANSIZIONE ECOLOGICA_DG ITC*VIA CRISTOFORO COLOMBO 44*MISURE DI POTENZIAMENTO DELLA SICUREZZA INFORMATICA_PROGETTO 2 POSTURE MANAGEMENT AND ATTACK PREVENTION	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	31/12/2023
20	avviso_3_2022	71_WP_9_RIST_REGIONE VALLE D'AOSTA	Attivo	In Corso	CYBER AWARENESS PA LOCALE DELLA VALLE D'AOSTA	CYBER AWARENESS E FORMAZIONE SPECIALISTICA PER LA PA LOCALE DELLA VALLE D'AOSTA*CORSO PER MIGLIORARE LA CONSAPEVOLEZZA SUI RISCHI INFORMATICI (CYBERSECURITY) DEI DIPENDENTI DELLA PA LOCALE*CORSI ON LINE A TUTTI I DIPENDENTI DELLE PA COINVOLTE E CORSI SPEC	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	20/11/2024

21	avviso_3_2022	20_WP_9_RIST_REGIONE CALABRIA	Attivo	In Corso	CYBERSICUREZZA SERVIZI ALLE ASP E AO REGIONALI	RAFFORZAMENTO CYBER SICUREZZA E DATA PROTECTION DEI SISTEMI E DEI PROCESSI CONNESSI ALL'EROGAZIONE DEI SERVIZI DELLA REGIONE CALABRIA ALLE ASP E AO REGIONALI*VIA LOC GERMANETO*INTERVENTO DI CYBER SICUREZZA RELATIVO AL MONDO SANITARIO DELLA REGIONE CALABRI	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	23/09/2024
22	avviso_3_2022	29_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	Attivo	In Corso	REGIONE FRIULI VENEZIA GIULIA CYBER INIZIATIVE	REGIONE FRIULI VENEZIA GIULIA*PIAZZA UNIT D'ITALIA 1 - TRIESTE*REALIZZAZIONE DI SISTEMI PER LA CYBERSECURITY DELL'AMMINISTRAZIONE REGIONALE	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/06/2023
23	avviso_3_2022	37_WP_9_RIST_REGIONE VENETO	Attivo	In Corso	Assessment della postura cyber	REGIONE DEL VENETO DIREZIONE ICT E AGENDA DIGITALE*VIA PACINOTTI N. 4*SERVIZI DI ASSESSMENT PER LA CYBER SECURITY.	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/06/2024
24	avviso_3_2022	65_WP_9_RIST_REGIONE SICILIA	Attivo	In Corso	SICUREZZA ENDPOINT RTRS	SICUREZZA ENDPOINT RTRS*REGIONE SICILIA*APPLICATIVI DI SICUREZZA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/09/2024
25	avviso_3_2022	56_WP_9_RIST_REGIONE CAMPANIA	Attivo	In Corso	Sinfonia	SINFONIA SICUREZZA*VIA DON BOSCO 9/E*SINFONIA SICUREZZA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/09/2024

26	avviso_3_2022	62_WP_9_RIST_COMUNE DI REGGIO CALABRIA	Attivo	In Corso	Reggiocyber (rc)	UPI COMUNICAZIONE PARTECIPAZIONE TRANSIZIONE DIGITALE E QUALIT DEI PROCESSI E SERVIZI FONDI SIE E PNRR PON METRO E POC METRO*TERRITORIO COMUNALE DI REGGIO CALABRIA*POTENZIAMENTO DELLA RESILIENZA CYBER: MIGLIORAMENTO DEI PROCESSI E DELL ORGANIZZAZIONE D	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/09/2024
27	avviso_3_2022	60_WP_9_RIST_COMUNE DI BOLOGNA	Attivo	In Corso	Linea progettuale 2 bologna	ENTI AREA METROPOLITANA DI BOLOGNA-PNRR INTERVENTI IN RISPOSTA ALL'AVVISO M1C1 ASSE 1 INVESTIMENTO 1.5 CYBERSECURITY *COMUNE DI BOLOGNA*INTERVENTI PER IL RAFFORZAMENTO DELLE DIFESE CIBERNETICHE. ATTIVAZIONE DEL SISTEMA DI MONITORAGGIO E PROTEZIONE DELLE	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
28	avviso_3_2022	30_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	Attivo	In Corso	Cybersecurity fvg: training&awareness	REGIONE FRIULI VENEZIA GIULIA*PIAZZA UNIT D'ITALIA 1 - TRIESTE*INTERVENTI INFO/FORMATIVI RELATIVI ALLA CYBERSECURITY	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
29	avviso_3_2022	59_WP_9_RIST_COMUNE DI BOLOGNA	Attivo	In Corso	Linea progettuale 1 bologna	ENTI AREA METROPOLITANA DI BOLOGNA-PNRR INTERVENTI IN RISPOSTA ALL'AVVISO M1C1 ASSE 1 INVESTIMENTO 1.5 CYBERSECURITY *COMUNE DI BOLOGNA*INTERVENTI PER IL RAFFORZAMENTO DELLE DIFESE CIBERNETICHE. ANALISI DELLA SICUREZZA PREDISPOSIZIONE DEL PIANO DEGLI I	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

30	avviso_3_2022	50_WP_9_RIST_COMUNE DI NAPOLI	Attivo	In Corso	Adozione framework zero trust access	SISTEMI INFORMATIVI DELLE ORGANIZZAZIONI COINVOLTE NEL PROGETTO.*VIA ADRIANO 40 NAPOLI*REALIZZAZIONE DI PIATTAFORME PER IL CONTINUOUS VULNERABILITY MANAGEMENT EVOLUTO FINALIZZATE ALLA RILEVAZIONE PRECOCE DELLE VULNERABILIT E DELLE MINACCE CYBER IMPLEM	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
31	avviso_3_2022	48_WP_9_RIST_COMUNE DI NAPOLI	Attivo	In Corso	Piattaforma soc/epp evoluto	SISTEMI INFORMATIVI DELLE ORGANIZZAZIONI COINVOLTE NEL PROGETTO.*VIA ADRIANO 40 NAPOLI*REALIZZAZIONE DI UNA PIATTAFORMA DI SECURITY OPERATION NELLE AREE DELL INCIDENT DETECTION E DELL INCIDENT RESPONSE ATTRAVERSO L ADOZIONE DI STRUMENTI DI EPP EVOLUTI P	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
32	avviso_3_2022	31_WP_9_RIST_REGIONE TOSCANA	Attivo	In Corso	Disaster recovery e buisness continuity	REGIONE TOSCANA - GIUNTA REGIONALE - DIREZIONE SISTEMI INFORMATIVI INFRASTRUTTURE TECNOLOGICHE E INNOVAZIONE - SETTORE SISTEMA INFORMATIVO ARCHITETTURA APPLICATIVA E CYBERSECURITY*VIA DI NOVOLI 26*ASSESSMENT CATALOGO DEGLI ASSET PER DISASTER RECOVERY	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
33	avviso_3_2022	66_WP_9_RIST_REGIONE EMILIA ROMAGNA	Attivo	In Corso	Potenziamento cyber servizi sanitari regionali	PROGETTO 2: POTENZIAMENTO DELLA RESILIENZA CYBER DELLE INFRASTRUTTURE DEI SERVIZI SANITARI REGIONALI*VIALE A. MORO 52*EROGAZIONE DI SERVIZI SPECIALISTICI E ACQUISIZIONE DI LICENZE PER IL POTENZIAMENTO DELLA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

						RESILIENZA CYBER DELLE INFRASTRUTTURE DEI SERVIZ		
34	avviso_3_2022	79_WP_9_RIST_COMUNE DI CAGLIARI	Attivo	In Corso	METROCAGLIARI IT-SECURITY PROGETTO 2	BENI E SERVIZI IT SECURITY PER SERVIZIO SMART CITY E INNOVAZIONE TECNOLOGICA*PIAZZA ALCIDE DE GASPERI 2*POTENZIAMENTO DELLA RESILIENZA GLI ATTACCHI CYBER - PROGETTO 2	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
35	avviso_3_2022	76_WP_9_RIST_REGIONE SICILIA	Attivo	In Corso	Cybervault per dati mission critical bacino orientale	REGIONE SICILIA AZIENDE SANITARIE E OSPEDALIERE BACINO ORIENTALE*REGIONE SICILIA - BACINO ORIENTALE*MIGLIORAMENTO DEI PROCESSI E DELLORGANIZZAZIONE DI GESTIONE DELLA CYBERSECURITY SVILUPPO DI NUOVI SISTEMI PER LA MITIGAZIONE DEL RISCHIO CYBER SICILIA ORI	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
36	avviso_3_2022	64_WP_9_RIST_REGIONE EMILIA ROMAGNA	Attivo	In Corso	Realizzazione csirt emiliaromagna	PROGETTO 1: REALIZZAZIONE CSIRT REGIONE EMILIA-ROMAGNA (CSIRT-RER)*VIALE A. MORO 52*EROGAZIONE DI SERVIZI PROFESSIONALI E ACQUISIZIONE DI LICENZE PER L OPERATIVIT DEL CSIRT DELLA REGIONE EMILIA-ROMAGNA (CSIRT-RER)	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

37	avviso_3_2022	15_WP_9_RIST_ROMA CAPITALE	Attivo	In Corso	Rafforzamento dei presidi di sicurezza roma capitale	ROMA CAPITALE DIPARTIMENTO DI CYBERSECURITY E SICUREZZA*VIA DELLA PREVIDENZA SOCIALE 20 00144 ROMA*RAFFORZAMENTO DEI PRESIDI DI SICUREZZA ROMA CAPITALE	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
38	avviso_3_2022	67_WP_9_RIST_REGIONE EMILIA ROMAGNA	Attivo	In Corso	Potenziamento della resilienza emiliaromagna	PROGETTO 3: POTENZIAMENTO DELLA RESILIENZA E DELLA GESTIONE DEL RISCHIO CYBER DI REGIONE EMILIA-ROMAGNA*VIALE A. MORO 52*EROGAZIONE SERVIZI PROFESSIONALI E ACQUISIZIONE SERVIZI E LICENZE PER IL POTENZIAMENTO DELLA RESILIENZA E DELLA GESTIONE DEL RISCHIO C	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
39	avviso_3_2022	70_WP_9_RIST_REGIONE MOLISE	Attivo	In Corso	Cybersecurity_r_molise	PIANO NAZIONALE DI RIPRESA E RESILIENZA MISSIONE 1 COMPONENTE 1 INVESTIMENTO 1.5 CYBERSECURITY M1C1I1.5*VIA GENOVA 11*PRIMO DIPARTIMENTO DELLA GIUNTA REGIONALE. UFFICIO RTD	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
40	avviso_3_2022	78_WP_9_RIST_COMUNE DI CAGLIARI	Attivo	In Corso	METROCAGLIARI ITSECURITY PROGETTO 1	BENI E SERVIZI IT SECURITY PER SERVIZIO SMART CITY E INNOVAZIONE TECNOLOGIA*PIAZZA ALCIDE DE GASPERI 2*POTENZIAMENTO DELLA RESILIENZA GLI ATTACCHI CYBER - PROGETTO 1	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

41	avviso_3_2022	36_WP_9_RIST_REGIONE VENETO	Attivo	In Corso	sistemi propedeutici cert veneto	REGIONE DEL VENETO DIREZIONE ICT E AGENDA DIGITALE*VIA PACINOTTI N. 4*SERVIZI DI RACCOLTA AGGREGAZIONE ANALISI DEI DATI AI FINI DELLA CYBER SECURITY SERVIZI DI ANALISI DI PREVENZIONE DEGLI ATTACCHI AI SISTEMI INFORMATIVI REALIZZAZIONE DI UN CENTRO DI	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
42	avviso_3_2022	14_WP_9_RIST_ROMA CAPITALE	Attivo	In Corso	Potenziamento cyber roma capitale	ROMA CAPITALE - DIPARTIMENTO DI CYBERSECURITY E SICUREZZA*VIA DELLA PREVIDENZA SOCIALE 20 00144 ROMA*SOLUZIONI PER IL POTENZIAMENTO DELLA PREVENZIONE RILEVAZIONE GESTIONE DEGLI INCIDENTI (RISPOSTA AUTOMATIZZATA)	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
43	avviso_3_2022	69_WP_9_RIST_REGIONE SARDEGNA	Attivo	In Corso	GDPRSIBAR ATTIVITA DI SICUREZZA SARDEGNA	GDPR-SIBAR. PROGETTO PER LA REALIZZAZIONE DI ATTIVITA DI SICUREZZA APPLICATIVA ED INFRASTRUTTURALE NELL AMBITO DEL SISTEMA INFORMATIVO DI BASE DELL AMMINISTRAZIONE REGIONALE SIBAR IN ATTUAZIONE DEL GDPR*VIA POSADA 1*SERVIZI DI ADEGUAMENTO AL GDPR DEL SIS	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
44	avviso_3_2022	45_WP_9_RIST_COMUNE DI MILANO	Attivo	In Corso	Cyber resilienza e potenziamento dei presidi	SISTEMA DI SICUREZZA DEL COMUNE DI MILANO CYBERSECURITY - PIANO DELLA SICUREZZA INTEGRATO*VIA G. B. VICO 18*PROGETTO PIANO DELLA SICUREZZA INTEGRATO - MIGLIORAMENTO DELLA CONSAPEVOLEZZA DELLE PERSONE PROGETTAZIONE E	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

						SVILUPPO DI NUOVI SISTEMI PER LA MITIG		
45	avviso_3_2022	38_WP_9_RIST_COMUNE DI MESSINA	Attivo	In Corso	FORMAZIONE E PROCESSI PER LA CYBERSECURITY	PP.AA. - POTENZIAMENTO RESILIENZA CYBER*PIAZZA UNIONE EUROPEA 1*ANALISI DELLA POSTURA DI SICUREZZA MIGLIORAMENTO DEI PROCESSI E DELL'ORGANIZZAZIONE DI GESTIONE DELLA CYBER SECURITY MIGLIORAMENTO DELLA CONSAPEVOLEZZA DELLE PERSONE PROGETTAZIONE E SVILUP	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
46	avviso_3_2022	32_WP_9_RIST_REGIONE TOSCANA	Attivo	In Corso	Gestione della qualita e miglioramento dei processi	REGIONE TOSCANA - GIUNTA REGIONALE - DIREZIONE SISTEMI INFORMATIVI INFRASTRUTTURE TECNOLOGICHE E INNOVAZIONE - SETTORE SISTEMA INFORMATIVO ARCHITETTURA APPLICATIVA E CYBER SECURITY*VIA DI NOVOLI 26*GESTIONE DELLA QUALIT E MIGLIORAMENTO DEI PROCESSI C	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
47	avviso_3_2022	44_WP_9_RIST_COMUNE DI MILANO	Attivo	In Corso	Analisi e miglioramento dei processi cyber	SISTEMA DI SICUREZZA DEL COMUNE DI MILANO CYBERSECURITY - PIANO DELLA SICUREZZA INTEGRATO*VIA G. B. VICO 18*PROGETTO PIANO DELLA SICUREZZA INTEGRATO - ANALISI POSTURA DELLA SICUREZZA E PIANO DI POTENZIAMENTO	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

						MIGLIORAMENTO DEI PROCESSI E DELL ORGANIZZAZIO		
48	avviso_3_2022	75_WP_9_RIST_REGIONE SARDEGNA	Attivo	In Corso	potenziamento del sistema informativo regionale ambientale	SISTEMA INFORMATIVO REGIONALE AMBIENTALE (S.I.R.A.) DELLA SARDEGNA*VIA ROMA 80*PROGETTAZIONE E SVILUPPO DI NUOVI SISTEMI PER LA MITIGAZIONE DEL RISCHIO CYBER	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
49	avviso_3_2022	57_WP_9_RIST_REGIONE CAMPANIA	Attivo	In Corso	Cyber campania	CYBER CAMPANIA*VIA DON BOSCO 9/E NAPOLI*CYBER CAMPANIA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
50	avviso_3_2022	11_WP_9_RIST_COMUNE DI CATANIA	Attivo	In Corso	Potenziamento e sicurezza degli end-point	POTENZIAMENTO E MESSA IN SICUREZZA DEGLI END-POINT*PIAZZA SAN DOMENICO N. 34*POTENZIAMENTO E MESSA IN SICUREZZA DEGLI END-POINT	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
51	avviso_3_2022	27_WP_9_RIST_COMUNE DI BARI	Attivo	In Corso	Identity and access management csirt puglia	IDENTITY AND ACCESS MANAGEMENT E MODELLO DI INTEGRAZIONE AL SERVIZIO DI CSIRT OFFERTO DALLA REGIONE PUGLIA*CORSO VITTORIO EMANUELE II 143*ANALISI E VALUTAZIONI TECNOLOGICHE PER LA REALIZZAZIONE DI UN SISTEMA DI GESTIONE DELLE IDENTIT E DEI RUOLI E PROCE	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

52	avviso_3_2022	40_WP_9_RIST_COMUNE DI BARI	Attivo	In Corso	Definizione delle cyber strategy e formazione cyber security	CYBER SECURITY POSTURE ASSESSMENT DEFINIZIONE DELLE CYBER STRATEGY E FORMAZIONE IN MATERIA DI CYBER SECURITY*CORSO VITTORIO EMANUELE II 143*IL PROGETTO PREVEDE ATTIVIT DI ANALISI DI PROGETTAZIONE DI RILASCIO SERVIZIE DI FORMAZIONE PER DESCRIVERE LO	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
53	avviso_3_2022	16_WP_9_RIST_ROMA CAPITALE	Attivo	In Corso	CYBER STRATEGY DI ROMA CAPITALE	ROMA CAPITALE DIPARTIMENTO CYBERSECURITY E SICUREZZA*VIA DELLA PREVIDENZA SOCIALE 20 00144 ROMA*CYBER SECURITY POSTURE ASSESSMENT DEFINIZIONE DELLE CYBER STRATEGY DI ROMA CAPITALE E VULNERABILITY ASSESSMENT E PENETRATION	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
54	avviso_3_2022	47_WP_9_RIST_REGIONE MARCHE	Attivo	In Corso	Rafforzamento dei processi cybersicurezza marche	RAFFORZAMENTO DEI PROCESSI E DELLE PROCEDURE RELATIVE ALLA CYBERSICUREZZA SERVIZI EROGATI TRAMITE L INFRASTRUTTURA CLOUD REGIONALE*VIA TIZIANO 44 - 60125 ANCONA*SERVIZI RELATIVI AL RAFFORZAMENTO DEI PROCESSI E DELLE PROCEDURE RELATIVE ALLA CYBERSICUREZZA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
55	avviso_3_2022	12_WP_9_RIST_REGIONE ABRUZZO	Attivo	In Corso	cyber security cert sanita regione abruzzo	INFRASTRUTTURA A SUPPORTO DELLA CYBER SECURITY PER IL CERT REGIONALE NELL'AMBITO DELLA SANIT *REGIONE ABRUZZO*INFRASTRUTTURE DI SICUREZZA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

56	avviso_3_2022	43_WP_9_RIST_REGIONE UMBRIA	Attivo	In Corso	Potenziamento cyber sanita umbra	DATA CENTER REGIONALE UNITARIO (DCRU) DATA CENTER AZIENDA OSPEDALIERA DI PERUGIA DATA CENTER AZIENDA OSPEDALIERA DI TERNI DATA CENTER AZIENDA USLUMBRIA1 DATA CENTER AZIENDA USLUMBRIA2*AZIENDE SANITARIE UMBRIA*PROGETTAZIONE CONFIGURAZIONE E SUPPORT	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
57	avviso_3_2022	13_WP_9_RIST_REGIONE ABRUZZO	Attivo	In Corso	Cert regionale dell'ambito della gestione delle acque	INFRASTRUTTURA A SUPPORTO DELLA CYBER SECURITY PER IL CERT REGIONALE NELL'AMBITO DELLA GESTIONE DELLE ACQUE*REGIONE ABRUZZO*INFRASTRUTTURE DI SICUREZZA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
58	avviso_3_2022	25_WP_9_RIST_REGIONE UMBRIA	Attivo	In Corso	Innalzamento livello di sicurezza regionale umbra	REGIONE UMBRIA - SERVIZIO SISTEMA INFORMATIVO REGIONALE INFRASTRUTTURE DIGITALI E SOCIET IN HOUSE PUNTOZERO SCARL*CORSO VANNUCCI 96*INNALZAMENTO LIVELLO DI SICUREZZA DELL INFRASTRUTTURA TECNOLOGICA REGIONALE UMBRA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
59	avviso_3_2022	49_WP_9_RIST_REGIONE MARCHE	Attivo	In Corso	sicurezza servizi di assistenza sanitaria	MIGLIORAMENTO DELLA SICUREZZA CON COINVOLGIMENTO DEI SERVIZI DI ASSISTENZA SANITARIA*VIA TIZIANO N. 44 - 60125 ANCONA*MIGLIORAMENTO DELLA SICUREZZA CON COINVOLGIMENTO DEI SERVIZI DI ASSISTENZA SANITARIA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

60	avviso_3_2022	23_WP_9_RIST_REGIONE LIGURIA	Attivo	In Corso	Infrastruttura per bilanciamento worklood	DATA CENTER REGIONE LIGURIA*VIA SCARSELLINI N. 42*IMPLEMENTAZIONE DELL'INFRASTRUTTURA DI SICUREZZA CIBERNETICA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
61	avviso_3_2022	42_WP_9_RIST_COMUNE DI MESSINA	Attivo	In Corso	POTENZIAMENTO SOC CYBERSECURITY MESSINA	PP.AA. - POTENZIAMENTO RESILIENZA CYBER*PIAZZA UNIONE EUROPEA 1*ANALISI DELLA POSTURA DI SICUREZZA E RELATIVO PIANO DI POTENZIAMENTO E PROGETTAZIONE E SVILUPPO DI NUOVI SISTEMI PER LA MITIGAZIONE DEL RISCHIO CYBER	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
62	avviso_3_2022	39_WP_9_RIST_COMUNE DI TORINO	Attivo	In Corso	Analisi e miglioramento cybersecurity della torino	SISTEMI INFORMATIVI - CYBERSECURITY*VIA MEUCCI 4*ANALISI DELLA POSTURA DI SICUREZZA E MIGLIORAMENTO NELLA GESTIONE DEI PROCESSI LEGATI ALLA CYBERSECURITY DELLA CITT DI TORINO	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
63	avviso_3_2022	2_WP_9_RIST_COMUNE DI FIRENZE	Attivo	In Corso	Cybersecurity framework e tools	COMUNE DI FIRENZE - DIREZIONE SISTEMI INFORMATIVI*VIA REGINALDO GIULIANI 250*STRUMENTI HW E SW PER LA CYBERSECURITY	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
64	avviso_3_2022	41_WP_9_RIST_COMUNE DI TORINO	Attivo	In Corso	Incremento della consapevolezza del rischio cyber torino	SISTEMI INFORMATIVI - CYBERSECURITY*VIA MEUCCI 4*CYBERSECURITY: INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER E SVILUPPO NUOVI SISTEMI PER LA MITIGAZIONE DEL RISCHIO NELLA CITT DI TORINO	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
65	avviso_3_2022	26_WP_9_RIST_COMUNE DI GENOVA	Attivo	In Corso	Analisi della postura cyber genova	CITT METROPOLITANA DI GENOVA*VIA GARIBALDI 9*IL POTENZIAMENTO DELLA RESILIENZA CYBER RISPETTO ALLE TRE COMPONENTI CHIAVE:	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

						TECNOLOGIE PROCESSI E PERSONE		
66	avviso_3_2022	72_WP_9_RIST_REGIONE VALLE D'AOSTA	Attivo	In Corso	Potenziamento resilienza cyber valle daosta	DATACENTER UNICO REGIONALE AD USO DEGLI ENTI LOCALI DEL TERRITORIO REGIONALE E RELATIVA INFRASTRUTTURA DI RETE REGIONALE*PIAZZA DEFFEYES 1 AOSTA*ANALISI DELLA POSTURA DI SICUREZZA E PIANO DI POTENZIAMENTO MIGLIORAMENTO DEI PROCESSI E DELL'ORGANIZZAZIONE	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
67	avviso_3_2022	7_WP_9_rist_Regione Piemonte	Attivo	In Corso	Transizione digitale e servizi sicuri	SOTTOINSIEME DI SERVIZI APPLICATIVI DEL SISTEMA INFORMATIVO REGIONALE*REGIONE PIEMONTE*ANALISI REVISIONE E PROGETTAZIONE DELLA SICUREZZA DI UN SOTTOINSIEME DI SERVIZI APPLICATIVI DEL SISTEMA INFORMATIVO REGIONALE: PROCEDURE DI SICUREZZA DEI SERVIZI PERC	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
68	avviso_3_2022	35_WP_9_RIST_REGIONE LAZIO	Attivo	In Corso	Security enforcement regione lazio	REGIONE LAZIO*VIA R. R. GARIBALDI 7 00154 ROMA*MIGLIORAMENTO DEI PROCESSI E DELL'ORGANIZZAZIONE DI GESTIONE DELLA CYBERSICUREZZA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

69	avviso_3_2022	18_WP_9_RIST_REGIONE PUGLIA	Attivo	In Corso	CYBERSECURITY POSTURE ASSESSMENT PUGLIA	REGIONE PUGLIA - UFFICIO TRANSIZIONE DIGITALE TUTTE LE AGENZIE REGIONALI INNOVAPUGLIA PUGLIA SVILUPPO ASL REGIONALI*REGIONE PUGLIA*CYBERSECURITY POSTURE ASSESSMENT E SECURITY AWARENESS TRAINING PER MIGLIORARE LA CONSAPEVOLEZZA DEGLI UTENTI SU TEMI D	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
70	avviso_3_2022	17_WP_9_RIST_REGIONE PUGLIA	Attivo	In Corso	POTENZIAMENTO DNS SECURITY PER LA PUGLIA	REGIONE PUGLIA - UFFICIO TRANSIZIONE DIGITALE TUTTE LE AGENZIE REGIONALI INNOVAPUGLIA PUGLIA SVILUPPO ASL REGIONALI*REGIONE PUGLIA*POTENZIAMENTO DELLA INFRASTRUTTURA DI DNS SECURITY PER LA REGIONE PUGLIA LE AZIENDE SANITARIE LOCALI LE AGENZIE REGIO	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
71	avviso_3_2022	33_WP_9_RIST_COMUNE DI FIRENZE	Attivo	In Corso	CYBERSECURITY METROWIDE	COMUNE DI FIRENZE - DIREZIONE SISTEMI INFORMATIVI*VIA REGINALDO GIULIANI 250*LICENZE E SISTEMI CYBERSECURITY	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
72	avviso_3_2022	6_WP_9_RIST_REGIONE PIEMONTE	Attivo	In Corso	Postazioni di lavoro a rete regionale piemonte	POSTAZIONI DI LAVORO DELLA REGIONE PIEMONTE E INFRASTRUTTURA DI RETE REGIONALE*REGIONE PIEMONTE*ANALISI REVISIONE E POTENZIAMENTO DEL PERIMETRO DI SICUREZZA RIFERITO A POSTAZIONI DI LAVORO E RETE REGIONALE IN RELAZIONE SIA ALLE PROCEDURE DI GESTIONE DEL	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

73	avviso_3_2022	54_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	Attivo	In Corso	CERT TERRITORIALE DELLALTO ADIGE	PROVINCIA AUTONOMA DI BOLZANO RIPARTIZIONE 9. INFORMATICA*TUTTA LA PROVINCIA DI BOLZANO*CREAZIONE DEL CERT DELL'ALTO ADIGE	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
74	avviso_3_2022	46_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	Attivo	In Corso	Bozenasset	PROVINCIA AUTONOMA DI BOLZANO RIPARTIZIONE 9. INFORMATICA*PROVINCIA DI BOLZANO*PIANO DI POTENZIAMENTO IN CYBERSECURITY	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
75	avviso_3_2022	8_WP_9_RIST_COMUNE DI PALERMO	Attivo	In Corso	COCY CONSAPEVOLEZZA CYBER	COCY - MIGLIORAMENTO DELLA CONSAPEVOLEZZA E DELLA SICUREZZA CYBER*TERRITORIO PROVINCIALE*ANALISI DELLA POSTURA DI SICUREZZA E PIANO DI POTENZIAMENTO MIGLIORAMENTO DEI PROCESSI DELLA CYBERSECURITY E DELLA CONSAPEVOLEZZA DELLE PERSONE NUOVI SISTEMI PER L	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
76	avviso_3_2022	22_WP_9_RIST_PROVINCIA AUTONOMA DI TRENTO	Attivo	In Corso	Potenziamento della capacita cyber del trentino	POTENZIAMENTO DELLE CAPACIT CYBER DEL TRENTINO A SUPPORTO DELLA TRASFORMAZIONE DIGITALE SICURA DELLA PA*PIAZZA DANTE 15*SERVIZIO DI DIFFUSIONE DELLA CULTURA DELLA SICUREZZA CIBERNETICA SERVIZI PER LA PROTEZIONE DELLE INFRASTRUTTURE DIGITALI PROVINCIALI	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

77	avviso_3_2022	05_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	Attivo	In Corso	Potenziamento numero unico emergenza friuli	NUE112 CENTRALE UNICA DI RISPOSTA PER IL FRIULI VENEZIA GIULIA SITA IN PALMANOVA*VIA NATISONE 43*POTENZIAMENTO DELLA RESILIENZA CYBER DEL NUMERO UNICO DI EMERGENZA (NUE112)DELLA CENTRALE UNICA DI RISPOSTA (CUR) DEL FRIULI VENEZIA GIULIA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
78	avviso_3_2022	28_WP_9_RIST_REGIONE LOMBARDIA	Attivo	In Corso	Programma di sicurezza e protezione dei dati	UNIT ORGANIZZATIVA SEMPLIFICAZIONE TRASFORMAZIONE DIGITALE E SISTEMI INFORMATIVI PROGETTO: PROGRAMMA DI SICUREZZA E PROTEZIONE DEI DATI*PIAZZA CITT DI LOMBARDIA 1 MILANO*INTERVENTI PER LA GESTIONE DEL RISCHIO COMPLIANCE E PROTEZIONE DEI DATI. I BENE	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
79	avviso_3_2022	10_WP_9_RIST_COMUNE DI CATANIA	Attivo	In Corso	Analisi della postura di sicurezza catania	ANALISI DELLA POSTURA DI SICUREZZA PROGETTAZIONE E IMPLEMENTAZIONE DEL POTENZIAMENTO DEL LIVELLO DI PROTEZIONE*PIAZZA SAN DOMENICO N. 34*ANALISI DELLA POSTURA DI SICUREZZA PROGETTAZIONE E IMPLEMENTAZIONE DEL POTENZIAMENTO DEL LIVELLO DI PROTEZIONE	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

80	avviso_3_2022	9_WP_9_RIST_COMUNE DI PALERMO	Attivo	In Corso	Resilienza cyber comune di palermo	RECYPA -RESILIENZA CYBER DELLE INFRASTRUTTURE DEL COMUNE DI PALERMO*TERRITORIO PROVINCIALE*MIGLIORAMENTO DELLA CONSAPEVOLEZZA E DELLA SICUREZZA CYBER ANALISI DELLA POSTURA DI SICUREZZA E PIANO DI POTENZIAMENTO MIGLIORAMENTO DEI PROCESSI DELLA CYBERSECU	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
81	avviso_3_2022	3_WP_9_RIST_REGIONE BASILICATA	Attivo	In Corso	Centro per la cybersicurezza regionale	CENTRO REGIONALE PER LA CYBERSECURITY .*VIA VINCENZO VERRASTRO 4 - 85100 POTENZA*HARDWARE E SOFTWARE PER LA GESTIONE DELLA CYBERSECURITY REGIONALE.	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
82	avviso_3_2022	24_WP_9_RIST_REGIONE LIGURIA	Attivo	In Corso	Adeguamento firewall e policy di sicurezza	DATA CENTER REGIONE LIGURIA*VIA SCARSELLINI N. 42*ADEGUAMENTO DELL'INFRASTRUTTURA FIREWALL E FIREWALL ORCHESTRATOR	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
83	avviso_3_2022	73_WP_9_RIST_COMUNE DI VENEZIA	Attivo	In Corso	PIANO DI CYBERSECURITY AWARENESS	RESILIENZA CIBERNETICA COMUNE DI VENEZIA PIANO DI CYBERSECURITY AWARENESS*SAN MARCO 4136 CAP. 30100*SERVIZI DI PROGETTAZIONE E SUPPORTO PER IL MIGLIORAMENTO DELLA CYBERSECURITY AWARENESS	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
84	avviso_3_2022	74_WP_9_RIST_COMUNE DI VENEZIA	Attivo	In Corso	TECNOLOGIE A MITIGAZIONE DEL RISCHIO CYBER	RESILIENZA CIBERNETICA COMUNE DI VENEZIA NUOVE TECNOLOGIE DI SICUREZZA A MITIGAZIONE DEL RISCHIO CYBER*SAN MARCO 4136 CAP. 30100*PIATTAFORME HARDWARE E SOFTWARE PER	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

						LA CYBER SICUREZZA E RELATIVI SERVIZI		
85	avviso_3_2022	51_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	Attivo	In Corso	Ampliamento soc	PROVINCIA AUTONOMA DI BOLZANO RIPARTIZIONE 9. INFORMATICA*ALTO ADIGE*AMPLIAMENTO E OTTIMIZZAZIONE DELLA CAPACIT DI MONITORAGGIO DEL SECURITY OPERATION CENTER	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
86	avviso_3_2022	58_WP_9_RIST_COMUNE DI VENEZIA	Attivo	In Corso	RESILIENZA CIBERNETICA COMUNE DI VENEZIA	RESILIENZA CIBERNETICA COMUNE DI VENEZIA MATURITY ASSESSMENT E PIANO DI MIGLIORAMENTO*SAN MARCO 4136 CAP. 30100*SERVIZI DI ANALISI DELLA POSTURA DI SICUREZZA DEL SISTEMA INFORMATIVO DEL COMUNE DI VENEZIA E SERVIZI DI PROGETTAZIONE DEL PIANO DI MIGLIORA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
87	avviso_3_2022	4_WP_9_RIST_REGIONE BASILICATA	Attivo	In Corso	Centro per la cybersicurezza regionale ii intervento	CENTRO REGIONALE PER LA CYBERSECURITY - II INTERVENTO*VIA VINCENZO VERRASTRO 4 - 85100 POTENZA*HARDWARE E SOFTWARE PER LA GESTIONE DELLA CYBERSECURITY REGIONALE.	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024
88	avviso_3_2022	55_WP_9_RIST_REGIONE LAZIO	Attivo	In Corso	Piano di security awareness regione lazio	PIANO DI SECURITY AWARENESS REGIONE LAZIO*CORSO RIVOLTO AI DIPENDENTI REGIONALI PER LA SECURITY AWARENESS*DAL 01.01.2023 AL 30.11.2024	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/11/2024

89	avviso_3_2022	19_WP_9_RIST_REGIONE CALABRIA	Attivo	In Corso	Strategia cyber per la regione calabria	STRATEGIA CYBER PER LA REGIONE CALABRIA*VIALE EUROPA*ATTIVIT ATTE A RAFFORZARE LA CYBERSICUREZZA DI PROCESSI SISTEMI E DELLE APPLICAZIONI MAGGIORMENTE CRITICHE UTILIZZATE DAI DIPARTIMENTI DELLA REGIONE CALABRIA NONCH DALLE AZIENDE SANITARIE PROVINCIALI	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/12/2023
90	avviso_3_2022	63_WP_9_RIST_REGIONE SICILIA	Attivo	In Corso	SICUREZZA PERIMETRO INTERNO RTRS	SICUREZZA PERIMETRO INTERNO RTRS*REGIONE SICILIA*APPARATI DI SICUREZZA E RELATIVI SOFTWARE	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	30/12/2024
91	avviso_3_2022	53_WP_9_RIST_COMUNE DI NAPOLI	Attivo	In Corso	Assessment ed evoluzione della postura cyber	SISTEMI INFORMATIVI DELLE ORGANIZZAZIONI COINVOLTE NEL PROGETTO.*VIA ADRIANO 40 NAPOLI*ATTIVIT DI SICUREZZA PER LA VALUTAZIONE DELLA CYBER MATURITY ATTUALE E SUCCESSIVO MIGLIORAMENTO PER IL POTENZIAMENTO DELLA RESILIENZA CYBER ATTIVIT DI VULNERABILITY	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	31/10/2024
92	avviso_3_2022	21_WP_9_RIST_PROVINCIA AUTONOMA DI TRENTO	Attivo	In Corso	Resilienza cyber per la provincia autonoma di trento	L INTERVENTO PROPOSTO RIGUARDER I SERVIZI APPLICATIVI IN GESTIONE NELL AMBITO DEL SISTEMA INFORMATIVO ELETTRONICO DELLA PROVINCIA AUTONOMA DI TRENTO E I RELATIVI SERVIZI INFRASTRUTTURALI.*PIAZZA DANTE 15*SERVIZI PER ANALIZZARE E DEFINIRE LE EVOLUZIONI S	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	31/10/2024

93	avviso_3_2022	34_WP_9_RIST_REGIONE LAZIO	Attivo	In Corso	Rafforzamento cyber defence regione lazio	REGIONE LAZIO*VIA R. R. GARIBALDI 7 00154 ROMA*PIATTAFORME DI MONITORAGGIO CYBERSICUREZZA	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	31/10/2024
94	avviso_3_2022	52_WP_9_RIST_REGIONE LOMBARDIA	Attivo	In Corso	Cyber security assessment enti sanitari lombardia	UO SISTEMI INFORMATIVI E SANITA' DIGITALE PROGETTO: CYBER SECURITY ASSESSMENT & REMEDIATION ENTI SANITARI*PIAZZA CITT DI LOMBARDIA 1*L'INTERVENTO HA PER OGGETTO LA PROGETTAZIONE E SVILUPPO DI NUOVI SISTEMI PER LA MITIGAZIONE DEL RISCHIO CYBER E IL M	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	31/12/2023
95	avviso_5_2022	23_WP12_A5_TESLY	Attivo	In Corso	Futuring Technology Center (FTC)	TELSY S.P.A.*REALIZZAZIONE LABORATORIO DI PROVA*CORSO SVIZZERA 185		15/11/2024
96	avviso_5_2022	28_WP12_A5_HERMESBAY	Attivo	In Corso	SONIC	HERMES BAY SRL*REALIZZAZIONE LABORATORIO DI PROVA*VIA LUCA GAURICO 257		15/12/2023
97	avviso_5_2022	8_WP12_A5_DEEPLAB	Attivo	In Corso	Deep Cyber	DEEP LAB S.R.L.*REALIZZAZIONE LABORATORIO DI PROVA*VIA NAZIONALE 60		15/12/2024
98	avviso_5_2022	4_WP12_A5_DIGITALPLATFORMS	Attivo	In Corso	LAP DIGITALPLATFORMS	DIGITALPLATFORMS S.P.A.*REALIZZAZIONE LABORATORIO DI PROVA*VIA NOALE 351		15/12/2024
99	avviso_5_2022	12_WP12_A5_SISTEMI&AUTOMAZIONE	Attivo	In Corso	SEA_LAP	SISTEMI & AUTOMAZIONE S.P.A.*REALIZZAZIONE LABORATORIO DI PROVA*VIA SANTE BARGELLINI 4		15/12/2024

100	avviso_5_2022	31_WP12_A5_INNOVERY	Attivo	In Corso	LAP INNOVERY	INNOVERY S.P.A.*REALIZZAZIONE LABORATORIO DI PROVA*QUATTRO PALAZZINA A6		15/12/2024
101	avviso_5_2022	30_WP12_A5_SABABA	Attivo	In Corso	SABABA SECURITY LABORATORIO	SABABA SECURITY S.P.A.*REALIZZAZIONE LABORATORIO DI PROVA*PIAZZA TRE TORRI 2		15/12/2024
102	avviso_5_2022	27_WP12_A5_MPG	Attivo	In Corso	laboratorio di prova indipendente	MPG SYSTEM S.R.L.*REALIZZAZIONE LABORATORIO DI PROVA*PIAZZA FERNANDO DE LUCIA 35		15/12/2024
103	avviso_5_2022	2_WP12_A5_Innonation	Attivo	In Corso	INNONATION CYBER SECURITY LAB	INNONATION S.R.L*REALIZZAZIONE LABORATORIO DI PROVA*VIA RUILIO 18/20	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	15/12/2024
104	avviso_5_2022	22_WP12_A5_INTELLISYNC	Attivo	In Corso	INTELLISYNC LAP	INTELLISYNC S.R.L.*REALIZZAZIONE LABORATORIO DI PROVA*VIA SCLAFANI 40B		15/12/2024
105	avviso_5_2022	20_WP12_A5_E-TRACE	Attivo	In Corso	e-Trace Labs	E-TRACE S.R.L.*REALIZZAZIONE LABORATORIO DI PROVA*VIA PARAGUAY 5		15/12/2024
106	avviso_5_2022	13_WP12_A5_SIPAL	Attivo	In Corso	LAP SIPAL	SIPAL S.P.A.*REALIZZAZIONE LABORATORIO DI PROVA*CORSO VITTORIO EMANUELE II 178		15/12/2024
107	avviso_5_2022	19_WP12_A5_APAVEITALIA	Attivo	In Corso	APAVELAB	APAVE ITALIA CPM S.R.L.*REALIZZAZIONE LABORATORIO DI PROVA*VIA ARTIGIANI 63		15/12/2024
108	avviso_5_2022	35_WP12_A5_ANCHARIA	Attivo	In Corso	ALAB software and network security	ANCHARIA S.R.L.*REALIZZAZIONE LABORATORIO DI PROVA*VIA BRECCE BIANCHE 12		15/12/2024

109	avviso_5_2022	21_WP12_A5_IMQ	Attivo	In Corso	Laboratorio Prove Sicurezza IMQ	IMQ S.P.A.*REALIZZAZIONE LABORATORIO DI PROVA*VIA QUINTILIANO MARCO FABIO 43		15/12/2024
110	avviso_5_2022	15_WP12_A5_STONESECURITY	Attivo	In Corso	Adeguamento Laboratori on-site	STONE SECURITY S.R.L.*REALIZZAZIONE LABORATORIO DI PROVA*VIA VALENTINO MAZZOLA 38		20/11/2024
111	avviso_5_2022	3_WP12_A5_IPS	Attivo	In Corso	LAB IPS	IPS S.P.A.*REALIZZAZIONE LABORATORIO DI PROVA*VIA DELLA GIULIANA 82		21/05/2024
112	avviso_5_2022	32_WP12_A5_DIGITALENGINEERING	Attivo	In Corso	CARDEA - Center of Analysis and Research	DIGITAL ENGINEERING S.R.L.-NEXT SOFTWARE GENERATION*REALIZZAZIONE LABORATORIO DI PROVA*VIA DELL'ACQUEDOTTO PAOLO 80		30/09/2023
113	avviso_5_2022	17_WP12_A5_TECNINF	Attivo	In Corso	Future Ready CS Lab	TECNINF S.P.A.*REALIZZAZIONE LABORATORIO DI PROVA*VIA MOSCA 52		30/11/2023
114	avviso_5_2022	33_WP12_A5_INNOVAPUGLIA	Attivo	In Corso	InnovaPuglia LAP accreditato	CREAZIONE DI UN LABORATORIO ACCREDITATO DI PROVA*STRADA PROV. PER CASAMASSIMA KM 3*ACQUISIZIONE DI STRUMENTAZIONE PER VULNERABILITY ASSESSMENT		30/11/2024
115	avviso_5_2022	18_WP12_A5_ATSEC	Attivo	In Corso	Accreditamento LAP atsec	ATSEC INFORMATION SECURITY S.R.L.*REALIZZAZIONE LABORATORIO DI PROVA*PIAZZA DELLE BELLE ARTI 3		31/03/2024
116	avviso_5_2022	29_WP12_A5_NEXTINGEGNERIA	Attivo	In Corso	LAP NEXT Ingegneria dei Sistemi	NEXT INGEGNERIA DEI SISTEMI S.P.A.*REALIZZAZIONE LABORATORIO DI PROVA*VIA GIACOMO PERONI 452		31/12/2022

117	avviso_5_2022	5_WP12_A5_SECURENETWORK	Attivo	In Corso	Laboratorio di Prova Secure Network	SECURE NETWORK S.R.L.*REALIZZAZIONE LABORATORIO DI PROVA*PIAZZA GENERALE ARMANDO DIAZ 6		31/12/2023
118	avviso_6_2023	14_WP7_A6_REGIONE UMBRIA	Attivo	In Corso	Potenziamento CSIRT Umbria	REGIONE UMBRIA - SERVIZIO SISTEMA INFORMATIVO REGIONALE INFRASTRUTTURE DIGITALI E SOCIET IN HOUSE PUNTOZERO SCARL*CORSO VANNUCCI 96*POTENZIAMENTO CSIRT UMBRIA		31/08/2025
119	CyberDefence_CS	B56G21056820003	Attivo	In Corso	Acquisto di soluzioni avanzate di cybersecurity	GIUSTIZIA AMMINISTRATIVA*VIA MONTE DI PIETA' 33*DECEPTIVE BYTES SPC CLOUD LOTTO 2 FW PERIMETRALI FW PERIMETRALI (UNA TANTUM)FW PERIMETRALI (SITE PREPARATION)	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	31/12/2023
120	CyberDefence_GF	G56G21009570006	Attivo	In Corso	Missione digitale	REPARTI DEL CORPO DELLA GUARDIA DI FINANZA*REPARTI DEL CORPO DELLA GUARDIA DI FINANZA*IMPLEMENTAZIONE DELLA SICUREZZA INFORMATICA DEL CORPO (CYBERSECURITY)	INTERVENTO CHE NON COSTITUISCE AIUTO DI STATO	29/11/2024

10. Monitoraggio effettuato dall'Agenzia per la Cybersicurezza sulle attività di attuazione degli interventi da parte delle pubbliche amministrazioni, quali soggetti sub-attuatori, nonché le eventuali criticità riscontrate da parte delle stesse Amministrazioni.

Nelle diverse interlocuzioni intercorse con l'Agenzia per la Cybersicurezza, la Sezione ha voluto approfondire la tematica afferente il monitoraggio effettuato dall'Agenzia per la Cybersicurezza sulle attività di attuazione degli interventi da parte delle pubbliche amministrazioni, quali soggetti sub-attuatori, nonché le eventuali criticità riscontrate da parte delle stesse Amministrazioni.

A riscontro di quanto richiesto l'Agenzia ha precisato che, nell'ambito dell'Investimento 1.5, è stata prevista la selezione di progetti a titolarità di altri soggetti sub-attuatori che sono stati responsabili dell'avvio, dell'attuazione e della funzionalità dei singoli interventi di competenza, nonché della regolarità delle procedure e delle spese rendicontate a valere sulle risorse del PNRR, oltre al monitoraggio circa il conseguimento dei valori definiti per gli indicatori associati ai propri progetti.

A tal proposito, in attuazione delle Linee Guida per i Soggetti Attuatori dell'Amministrazione Titolare dell'Investimento e delle Linee Guida per la realizzazione dei Progetti PNRR del MEF, l'Agenzia ha richiesto al Soggetto sub-attuatore le informazioni di competenza secondo modalità definite dal "Manuale Operativo - Linee guida per i soggetti attuatori individuati tramite avvisi pubblici".

Nel dettaglio, l'Agenzia ha acquisito, attraverso la trasmissione di relazioni periodiche bimestrali, specifiche informazioni relative a:

- tempi previsti e realizzati in merito all'attività progettuale, con eventuali dettagli su scostamenti tra tempi previsti e realizzati e specifiche indicazioni delle motivazioni di eventuale ritardo;
- stato di avanzamento della attività previste dal progetto;
- pertinenza delle spese per il conseguimento delle attività;
- eventuali variazioni verificatesi durante l'implementazione dell'intervento;
- principali problemi riscontrati di carattere tecnico o gestionale e le relative azioni che si intendono adottare per annullare gli eventuali scostamenti e la relativa tempistica;

- obiettivi raggiunti.

È stato quindi asserito che le informazioni di monitoraggio sono valutate dall'Agenzia e utilizzate nell'ambito dei controlli formali e sostanziali sulle domande di rimborso presentate dai soggetti sub-attuatori.

8. Conclusioni.

Nel corso del 2024 il quadro normativo e regolamentare dell'Agenzia per la cybersicurezza è stato in costante evoluzione, sia per rispondere alle sollecitazioni dell'Unione Europea nel realizzare un sistema coordinato di potenziamento del sistema cyber del Paese, con il recepimento della Direttiva (UE) 2022/2555 (NIS 2) per mezzo del decreto legislativo 4 settembre 2024 n. 138, nonché per consentire una maggiore operatività della stessa Agenzia in ordine agli aspetti strumentali e funzionali per la realizzazione delle attività strettamente legate alla difesa informatica del Paese.

Le attività dell'Agenzia, nel corso del 2024, sono state finalizzate alla costruzione di un sistema di protezione sempre più allargato nei settori strategici pubblici e privati per consentire risposte adeguate in materia di cybersicurezza. In particolare, il 26 novembre 2024 è stata firmata dal Direttore dell'ACN la prima determina attuativa relativa gli obblighi della NIS2, con la quale è stata stabilita la creazione di una piattaforma digitale per la registrazione dei "soggetti NIS" (enti pubblici e privati tenuti a registrarsi entro il 28 febbraio 2025) attraverso un "punto di contatto", ovvero una persona fisica designata responsabile delle comunicazioni e degli adempimenti per ciascun ente. Inoltre, è stata prevista una finestra di implementazione differenziata: 9 mesi per le notifiche e 18 mesi per le misure di sicurezza, che decorreranno dalla data di consolidamento dell'elenco dei soggetti NIS (fine marzo 2025).

Anche il ruolo di monitoraggio e supporto affidato all'Agenzia verso le pubbliche amministrazioni prevede una costante implementazione nei rapporti, in particolare nello scambio di informazioni e di accordi di collaborazione. Ciò, è stato di rilevante importanza a fronte di un ritardo che si riscontra nelle pubbliche amministrazioni nel dotarsi di sistemi informatici e di sviluppo digitale resilienti e sicuri da attacchi informatici finalizzati a mettere in crisi i servizi operativi necessari allo svolgimento corretto e sicuro dei servizi pubblici essenziali.

Sempre nel corso del 2024, l'Agenzia ha acquisito le necessarie risorse umane ampliando, nel rispetto delle disposizioni legislative, la propria dotazione organica utilizzando anche lo strumento della mobilità con l'inserimento nei propri ruoli del personale già comandato dalle pubbliche amministrazioni nella prima fase attuativa.

Per quanto concerne il personale, inoltre, per il periodo di tempo preso in considerazione nel Report di che trattasi (anno 2024), si apprende, per le vie brevi, che sono state eseguite le procedure per la stabilizzazione di 20 comandati. In relazione alle assunzioni, invece, sono state espletate delle procedure concorsuali (per le categorie protette, coordinatori e 3 Esperti), a seguito delle quali sono entrati nei ruoli 51 lavoratori.

A tali numeri, comunque, se ne aggiungeranno altri nell'arco del 2025, in quanto la dotazione organica non risulta allo stato attuale ancora completa.

Da segnalare, altresì, nel corso del 2024, l'Avviso pubblico per la ricerca di un immobile in vendita da destinare a sede dell'Agenzia per la cybersicurezza nazionale, la cui procedura si è perfezionata, in data 6 agosto 2024, con la sottoscrizione del contratto con la società Colliers, volto all'acquisto dello stabile sito a Roma in corso d'Italia, individuata quale sistemazione logistica di prestigio e di efficienza operativa per tale Organismo.

Quanto alle attività di approvvigionamento di beni e servizi informatici, si sottolinea il fondamentale ruolo della stazione appaltante, che dovrà tenere conto degli elementi delle offerte, affinché le stesse assicurino che il bene o servizio offerto posseggano gli "elementi essenziali di cybersicurezza" di cui all'art. 14, della legge 28 giugno 2024, n. 90. Inoltre, nel corso delle predette attività di approvvigionamento dovranno essere previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi che sono parte di accordi di collaborazione con l'Unione europea o con la NATO.

Da rilevare, anche, l'aggiornamento del Piano Operativo aggiuntivo all'Accordo sottoscritto in data 28 marzo 2024, ai sensi dell'art. 5, comma 6, del d.lgs. n. 50 del 2016, in sostituzione del precedente sottoscritto in data 14 dicembre 2021, tra il Dipartimento per la trasformazione digitale e l'ACN. Tale Piano mira a realizzare l'investimento 1.5 – per la Cybersecurity e, in particolare, a rinforzare le difese cibernetiche, aumentando il grado di resilienza del Paese, con particolare attenzione alla Pubblica Amministrazione,

anche per fronteggiare con maggiore efficacia la continua evoluzione della minaccia cyber.

Dalla documentazione prodotta dal Dipartimento per la trasformazione digitale si evince che, a fronte di una dotazione finanziaria complessiva dell'Investimento 1.5 - Cybersecurity pari a euro 623.000.000,00, alla data del 24 dicembre 2024, sono state trasferite risorse per un totale di euro 207.334.385,07.

Per quanto riguarda lo stato di avanzamento delle milestone e dei target relativi all'Investimento 1.5, nel periodo preso in esame, dalla consultazione dell'applicativo Regis, componente "Avanzamento M&T", è stato possibile verificare il raggiungimento dei traguardi relativi ad un target e alle 3 milestone ampiamente descritte in Relazione, così come anche confermato in corso di istruttoria dagli Enti competenti.

Dalla disamina sullo stato di avanzamento dei progetti in corso è emerso, dalle informazioni generali estrapolate dal sistema REGIS e confermate dalla documentazione prodotta dall'Agenzia, che il numero complessivo dei progetti in corso è pari a 154, dei quali 152 risultano in corso e solamente 2 conclusi.

Altro dato emerso nel corso del monitoraggio sull'avanzamento dei progetti e sugli scostamenti di cui si è fatto cenno nei capitoli precedenti riguarda un disallineamento tra il cronoprogramma dei progetti e lo stato di realizzazione degli stessi nel periodo preso in esame (anno 2024). Disallineamento emerso anche dal confronto con i dati inseriti nell'applicativo Regis.

A tal riguardo, gli enti competenti hanno fornito elementi di approfondimenti sui progetti in ritardo e sui relativi avvisi oggetto di richiesta di specifiche proroghe in ordine alla loro conclusione, evidenziando le determine con cui sono state autorizzate tali proroghe e a seguito delle quali i cronoprogrammi dei progetti da modificare sono ancora oggetto di valutazione da parte dell'Agenzia e non sono ancora visibili dal sistema Regis.

In ragione di quanto rappresentato, si raccomanda agli Enti competenti di monitorare sullo stato di realizzazione dei progetti sottesi alla misura in esame, affinché siano poste in essere tutte le misure organizzative e funzionali per recuperare il predetto disallineamento entro il 2025, e comunque entro i termini fissati dai rispettivi cronoprogrammi, sottolineando parimenti che comunque non emergono difficoltà sostanziali e criticità nel raggiungimento degli obiettivi da parte dell'Agenzia.

Si apprende, infine, che, rispetto alla dotazione finanziaria complessiva dell'investimento, pari a 623.000.000 euro, allo stato si registrano impegni attivi per un totale di circa 613 milioni. Di questi, circa 207 milioni riguardano attività a titolarità e circa 406 milioni riguardano attività a regia, mentre le spese già sostenute risultano pari, a decorrere dal 2022, complessivamente a circa 140 milioni.

Inoltre, le spese sostenute nel 2024 ammontano a euro 86.832.911, 46, mentre nell'anno 2023 erano stati spesi, così come risulta dalla precedente deliberazione di questa sezione, 40.063.048 milioni.

Se ne ricava, pertanto, che nell'ambito degli interventi sottesi all'investimento in esame, nell'arco di tempo preso in considerazione, non tutte le risorse disponibili risultano impiegate nell'ambito delle finalità proprie dell'Agenzia, così come era stato notato nella pregressa deliberazione, tenendo sempre ben presente che la realizzazione dei progetti in esame copre un arco temporale ampio, con scadenze ricadenti fino al 2026.

CORTE DEI CONTI - CENTRO UNICO PER LA FOTORIPRODUZIONE E LA STAMPA - ROMA