



CORTE DEI CONTI

SEZIONE CENTRALE DI CONTROLLO
SULLA GESTIONE DELLE AMMINISTRAZIONI DELLO STATO

CYBERSECURITY

Deliberazione 06 febbraio 2024, n. 17/2024/G



CORTE DEI CONTI



CORTE DEI CONTI

SEZIONE CENTRALE DI CONTROLLO
SULLA GESTIONE DELLE AMMINISTRAZIONI DELLO STATO

CYBERSECURITY

Relatore
Pres. Mauro Orefice

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

SOMMARIO

	Pag.
Deliberazione	7
* * *	
Rapporto	11
1. Premessa	13
2. Misure consequenziali	14
2 a) Bilancio consuntivo per l'anno 2022 dell'Agenzia per la Cybersicurezza	15
2 b) Assestamento al Budget economico per l'anno 2023	21
3. Relazione annuale al Parlamento 2022 dell'ACN	22
4. Avvisi pubblici e rifinanziamenti	25
4 a) Graduatoria per il rifinanziamento dell'Avviso pubblico n. 1 del 2022 ACN	25
4 b) Erogazione di contributi dell'Avviso pubblico n. 5/2022, per l'attivazione di LAP a supporto delle attività di scrutinio tecnologico del CVCN per l'area di accreditamento Software e Network.	27
4 c) Evoluzione del Bando relativo a "60 assunzioni di diplomati per l'information and communication technology (ict)"	28
4 d) Rifinanziamento dell'Avviso pubblico n. 3 del 2022	29
4 e) Avviso n. 6/2023 "a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT". Determina di concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse	31
4 f) Avviso n. 7/2023 "Avviso Pubblico a sportello per l'erogazione di interventi di potenziamento e miglioramento delle capacità cyber degli Organi costituzionali e di rilevanza costituzionale, dei Ministeri, delle Agenzie Fiscali, degli Enti di regolazione dell'attività economica, delle Autorità amministrative indipendenti e degli Enti a struttura associativa"	32
5. Novità intervenute in materia	34
5 a) Linee guida per i soggetti attuatori individuati tramite avvisi pubblici Manuale Operativo	34
5 b) Linee guida per i soggetti attuatori individuati tramite accordi ai sensi dell'art. 5, comma 6, del d.lgs. n. 50/2016 (Accordi Cyber Defence)	34
5 c) Firmato l'Accordo Quadro tra l'Agenzia per la Cybersicurezza Nazionale e la Scuola Nazionale dell'Amministrazione	35
5 d) Protocollo d'Intesa finalizzato alla gestione di procedure di appalto congiunte per l'acquisizione di beni, servizi e lavori, secondo la disciplina di cui al d.lgs. 31 marzo 2023, n. 36.....	36
5 e) Linee guida internazionali sulla sicurezza dell'Intelligenza Artificiale (pubblicate il 27 novembre 2023)	37
5 f) Registro.it (pubblicato il 27 novembre 2027)	38
6. Quadro finanziario.....	39
7. Stato di avanzamento dei milestone e target relativi all'Investimento in esame in relazione alla sua pianificazione per l'anno 2023.....	48
8. Stato di avanzamento dei progetti.	64
9. Conclusioni.....	77

DELIBERAZIONE



CORTE DEI CONTI

SEZIONE CENTRALE DI CONTROLLO SULLA GESTIONE DELLE AMMINISTRAZIONI DELLO STATO

II Collegio

Camera di consiglio del 31 gennaio 2024

Presieduta dal Presidente Mauro Orefice

Composta dai magistrati:

Presidente della Sezione: Mauro OREFICE

Presidente aggiunto della Sezione: Paolo Luigi REBECCHI

Consiglieri: Domenico PECCERILLO, Carmela MIRABELLA, Paola COSA, Carlo PICUNO, Natale Maria Alfonso D'AMICO, Gerardo de MARCO, Paolo ROMANO, Fabia D'ANDREA, Giampiero PIZZICONI, Daniela ALBERGHINI, Giuseppe VICANOLO

Primi Referendari: Paola LO GIUDICE, Salvatore GRASSO, Simonetta INGROSSO

Referendari: Andrea GIORDANO

* * *

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 2023 avente a oggetto *"Cybersecurity"*;

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. 1/2024 con cui i Magistrati sono assegnati a tutti i collegi;

vista l'ordinanza n. 3/2024 prot. n. 375 del 24 gennaio 2024 con la quale il Presidente della Sezione ha convocato il II Collegio per la camera di consiglio del 31 gennaio 2024 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 “Cybersecurity”.

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:
Direttore 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 06 febbraio 2024

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

RAPPORTO

AGENZIA DELLA CYBERSECURITY NAZIONALE

Sommario: 1. Premessa. – 2. Misure consequenziali – 2. a) Bilancio consuntivo per l'anno 2022 dell'Agenzia per la Cybersicurezza – 2 b) Assestamento al Budget economico per l'anno 2023. – 3. Relazione Annuale al Parlamento 2022 dell'ACN – 4. Avvisi pubblici e rifinanziamenti. – 4 a) Graduatoria per il rifinanziamento dell'Avviso pubblico n. 1 del 2022 ACN. – 4 b) Erogazione di contributi dell'Avviso pubblico n. 5/2022, per l'attivazione di LAP a supporto delle attività di scrutinio tecnologico del CVCN per l'area di accreditamento Software e Network. – 4 c) Evoluzione del Bando relativo a "60 assunzioni di diplomati per l'information and communication technology (ict)". – 4 d) Rifinanziamento dell'Avviso pubblico n. 3 del 2022. – 4 e) Avviso n. 6/2023 "a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT". Determina di concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse. – 4 f) Avviso n. 7/2023 "Avviso Pubblico a sportello per l'erogazione di interventi di potenziamento e miglioramento delle capacità cyber degli Organi costituzionali e di rilevanza costituzionale, dei Ministeri, delle Agenzie Fiscali, degli Enti di regolazione dell'attività economica, delle Autorità amministrative indipendenti e degli Enti a struttura associativa". – 5. Novità intervenute in materia. – 5 a) Linee guida per i soggetti attuatori individuati tramite avvisi pubblici Manuale Operativo. – 5 b) Linee guida per i soggetti attuatori individuati tramite accordi ai sensi dell'art. 5, comma 6, del d.lgs. n. 50/2016 (Accordi Cyber Defence). – 5 c) Firmato l'Accordo Quadro tra l'Agenzia per la Cybersicurezza Nazionale e la Scuola Nazionale dell'Amministrazione. – 5 d) Protocollo d'Intesa finalizzato alla gestione di procedure di appalto congiunte per l'acquisizione di beni, servizi e lavori, secondo la disciplina di cui al d.lgs. 31 marzo 2023, n. 36. – 5 e) Linee guida internazionali sulla sicurezza dell'Intelligenza Artificiale (pubblicate il 27 novembre 2023). – 5 f) Registro.it (pubblicato il 27 novembre 2027). – 6. Quadro finanziario. – 7. Stato di avanzamento dei milestone e target relativi all'Investimento in esame in relazione alla sua pianificazione per l'anno 2023. – 8. Stato di avanzamento dei progetti. – 9. Conclusioni. – Allegato 1.

1. Premessa.

La Sezione centrale di controllo sulla gestione delle Amministrazioni dello Stato con deliberazioni n. 31, del 14 luglio 2022 e n. 5, del 9 febbraio 2023, afferenti all'investimento di cui all'oggetto, ha espletato la funzione di controllo attribuita a questa Corte ai sensi dell'art. 7, comma 7 del decreto-legge n. 77, del 31 maggio 2021, convertito dalla legge 29 luglio 2021, n. 108.

Come già profusamente rappresentato nelle delibere di cui sopra, l'obiettivo sotteso a tale investimento è volto alla tutela degli interessi nazionali nel campo della cybersicurezza. L'Agenzia ha 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 principali compiti dell'Agenzia c'è l'attuazione della Strategia Nazionale di Cybersicurezza, adottata dal Presidente del Consiglio, che contiene gli obiettivi da perseguire entro il 2026.

La misura, giova quindi brevemente ricordare, prevede lo sviluppo di un sistema all'avanguardia che interconnetta strettamente, a livello nazionale e internazionale, il mondo della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia. La nuova Agenzia per la Cybersicurezza Nazionale, altresì, al fine di potenziare la resilienza dell'ecosistema Cyber Nazionale, curerà l'evoluzione dell'infrastruttura e dei servizi per l'attuazione della normativa di riferimento. L'investimento si articola su 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 della Pubblica Amministrazione per la messa in sicurezza dei dati e dei servizi dei cittadini.

L'Agenzia persegue l'attuazione dell'investimento, connettendo il mondo della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia, in stretta sinergia con l'amministrazione titolare, il Dipartimento per la trasformazione digitale (DTD).

Al vertice dell'Agenzia è incardinato 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. Misure conseguenziali

Con nota del 15 febbraio 2023, prot. n. 560 questa Corte ha provveduto ad inviare al Dipartimento per la trasformazione digitale il documento contenente il secondo Rapporto PNRR sull'investimento in esame (deliberazione n. 5, del 9 febbraio 2023), invitando parimenti sia la stessa Amministrazione in quanto titolare del medesimo investimento, sia il Soggetto attuatore a comunicare entro il termine di 4 mesi le misure conseguenziali adottate in esito alle osservazioni formulate nella succitata

deliberazione.

L'Agenzia per la Cybersicurezza ha fatto pervenire, con nota dell'11 settembre 2023, ai sensi dell'art. 11, comma 3, lett. a) del decreto-legge 14 giugno 2021, n. 82, il dpcm recante l'approvazione del bilancio consuntivo per l'anno 2022 dell'Agenzia stessa, per le finalità di cui all'art. 3, comma 4 della legge 14 gennaio 1994, n. 20.

Il soggetto attuatore dell'investimento in esame, inoltre, in data 6 ottobre 2023, ha trasmesso alla Sezione stessa una nota riportante i dati concernenti l'assestamento al Budget economico per l'anno 2023.

Ai fini di un aggiornamento puntuale delle informazioni che afferiscono l'investimento di che trattasi, la Sezione ha predisposto e inviato, in data 28 novembre 2023, una nuova nota istruttoria all'Agenzia per la Cybersicurezza, onde poter acquisire tutti gli elementi utili a definire e integrare le informazioni già estrapolate dal sistema REGIS.

2a) Bilancio consuntivo per l'anno 2022 dell'Agenzia per la Cybersicurezza

Il documento fornito dall'Agenzia per la Cybersicurezza, (con precedente comunicazione dell'11 settembre 2023), contenente il bilancio d'esercizio per l'anno 2022, è volto a rappresentare l'insieme degli adempimenti che hanno riguardato l'Agenzia sin dalla sua istituzione ad opera del decreto-legge n. 82 del 2021, con particolare riguardo a tutto quel complesso di attività prodromiche e funzionali al percorso di costruzione e consolidamento dell'Agenzia stessa.

Un'attenzione particolare, dunque, è stata rivolta al quadro normativo di riferimento, concernente sia le procedure interne all'Agenzia, la costituzione degli organi e dei Comitati previsti dal Decreto istitutivo, nonché i bandi di reclutamento del personale necessario all'efficace espletamento di tutte le funzioni.

Nel documento in esame, inoltre, oltre al processo di costruzione di tale istituto, viene posto in evidenza anche il ruolo rivestito dall'Agenzia stessa nel panorama istituzionale "quale attore con competenze specialistiche".

È opportuno ricordare che l'Agenzia per la Cybersicurezza nell'esercizio delle sue funzioni deve adempiere ad alcuni oneri informativi sia nei confronti del Copasir che delle Commissioni parlamentari competenti, ai sensi della legge istitutiva dell'Agenzia

stessa.

In ordine al Copasir (Comitato parlamentare per la sicurezza della repubblica) l'Agenzia deve trasmettere allo stesso il bilancio consuntivo accompagnato dalla relazione della Corte dei conti (ai sensi dell'articolo 11, comma 3, del decreto-legge 14 giugno 2021, n. 82), dando tempestiva e motivata comunicazione dei provvedimenti adottati in materia di dotazione organica (ex articolo 12, comma 5).

In attuazione della norma che prevede il controllo da parte del Copasir, la relazione contenente il bilancio consuntivo dell'Agenzia riporta che nel corso dell'anno 2022 il Direttore generale è stato udito tre volte dal Comitato, mentre ai fini di quanto previsto dall'art. 14 del decreto-legge del 30 giugno 2022 è stata presentata la prima Relazione sulle attività svolte dall'Agenzia nel 2021 in relazione agli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico, così come evidenziato anche da questa Corte nella deliberazione precedente (n. 5, del 9 febbraio 2023).

Nella succitata deliberazione, di fatti, è stato sottolineato che la legge istitutiva dell'Agenzia, nel prevedere precisi oneri informativi nei confronti del Parlamento, ha disposto tra l'altro, che il Presidente del Consiglio dei ministri debba presentare una relazione al Parlamento sulle attività svolte dall'Agenzia nell'anno precedente, fissando il termine di scadenza "ordinario" della relazione al 30 aprile successivo all'anno di riferimento, mentre in sede di prima applicazione è stato previsto un diverso termine di trasmissione al Parlamento (30 novembre 2022).

La Relazione sulla gestione fornita dall'Agenzia per la Cybersicurezza si focalizza anche sull'attività di produzione della normativa interna, la quale è consistita principalmente in provvedimenti del Direttore generale dell'ACN disciplinanti l'organizzazione, nonché l'attività della stessa Agenzia.

Di talché, dalla Relazione di che trattasi si evince che in sede di prima operatività, a fronte delle risorse umane a disposizione, l'Agenzia ha provveduto ad attivare progressivamente Servizi, Divisioni e Strutture di missione, ossia quelle strutture essenziali ai fini dell'efficace svolgimento delle attività prioritarie. Al termine del processo di assunzione nell'anno 2022 l'articolazione della nuova Agenzia ha registrato:

- 5 servizi;

- 16 divisioni, di cui 9 di maggiore complessità, quali articolazioni di livello dirigenziale non generale, in relazione alla particolare delicatezza e rilevanza delle funzioni, che comportano notevoli responsabilità;
- 2 strutture di missione;
- 1 unità a supporto del Vice-Direttore generale;
- 1 Nucleo di progetto.

In tale ambito, dei 7 servizi previsti dal Regolamento di organizzazione e funzionamento adottato dall'Agenzia per la cybersicurezza nazionale (Decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223), 5 risultano quelli attivati nel corso del periodo preso in considerazione dalla Relazione:

- Gabinetto;
- Certificazione e vigilanza;
- Operazioni;
- Programmi industriali, tecnologici, di ricerca e formazione;
- Risorse umane e strumentali.

Dal documento sulla gestione espletata dall'Agenzia nel corso dell'anno 2022 emerge, altresì, l'istituzione sia della Struttura di missione per le relazioni internazionali di carattere strategico volta a consentire l'avvio e l'espansione delle competenze dell'Agenzia in materia di cooperazione internazionale, che della Struttura di missione per lo sviluppo di capacità e competenze in ambito cyber, che costituiscono i fattori abilitanti della Strategia nazionale di cybersicurezza.

Rileva, inoltre, l'informazione concernente il provvedimento adottato dal Direttore generale dell'Agenzia il 14 giugno 2022, su deliberazione del Comitato di Vertice, sotto la Presidenza dell'Autorità delegata, con il quale è stato nominato il Collegio dei Revisori dei conti, quale organo di controllo dell'Agenzia.

Nel documento in esame viene posto in rilievo, altresì, l'istituzione di un Comitato tecnico-scientifico, previsto dall'art. 7, comma 1-bis del decreto istitutivo dell'Agenzia (decreto-legge 14 giugno 2021, n. 82), i cui caratteri e funzioni sono state ben esplicitati dal Regolamento di organizzazione e funzionamento dell'Agenzia stessa (decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223).

A tal riguarda, l'art. 11 del citato regolamento disciplina al comma 1 l'istituto del Comitato tecnico-scientifico, il quale si presenta con "funzioni di consulenza e proposta, volto a promuovere la collaborazione con il sistema dell'università e della ricerca e con il sistema produttivo nazionale, nonché a supportare le iniziative pubblico-private in materia di cybersicurezza". Al Comitato possono essere sottoposte, oltre alle questioni in materia di sviluppo di competenze, innovazione, partecipazione a programmi e progetti di cybersicurezza nazionali ed internazionali, di comunicazione e promozione della consapevolezza in materia di cybersicurezza, di formazione e qualificazione delle risorse umane, nonché le questioni afferenti al Centro nazionale di coordinamento, ogni altra tematica individuata dal direttore generale.

Il successivo comma 2 dispone che il Comitato deve essere presieduto dal Direttore generale, ovvero dal Vice-direttore generale o da un dirigente dell'Agenzia ove delegati, e i suoi componenti devono essere scelti tra:

- a) il personale dell'Agenzia in numero non superiore a quattro;
- b) quattro dirigenti, preferibilmente individuati tra quelli chiamati a riferire in via immediata e diretta al vertice gerarchico, in rappresentanza dell'industria operativa negli ambiti di attività dell'Agenzia, comprese le piccole e medie imprese;
- c) quattro professori universitari ordinari o equivalenti, in rappresentanza del sistema dell'università e della ricerca;
- d) un esponente di associazioni del settore della sicurezza delle aziende strategiche del Paese.

Sulla scorta di quanto disposto, i componenti del Comitato tecnico-scientifico sono stati nominati con dpcm del 15 giugno 2022, sentito il Comitato di vertice dell'Agenzia, su proposta del Direttore generale. A tal proposito, sulla pagina istituzionale dell'Agenzia si apprende che i membri del Comitato "possiedono comprovata qualificazione tecnologica, scientifica e professionale negli ambiti di attività dell'Agenzia, in particolare nel contesto della definizione, progettazione, dell'attuazione e della gestione di progetti di ricerca e sviluppo tecnologico, industriale e scientifico, nei campi, tra gli altri, del quantum computing, dell'intelligenza artificiale e della robotica, della crittografia, dell'Internet of Things, delle reti e del software,

nonché negli ambiti della formazione e qualificazione delle risorse umane, della promozione e diffusione della cultura della cybersicurezza”.

In tale contesto, sono stati nominati in rappresentanza dell'industria operativa negli ambiti di attività dell'Agenzia, comprese le piccole e medie imprese:

- L'Amministratore Delegato della Elettronica SpA e Presidente della Cy4Gate SpA.
- Il Global Lead di Accenture Security;
- Il Chief IT Digital & Innovation Officer di Intesa Sanpaolo SpA.
- Il Chief Technology & Innovation Officer del gruppo Leonardo SpA.

In rappresentanza del sistema dell'università e della ricerca, invece, sono stati nominati:

- Un Direttore dell'Istituto di informatica e telematica del Consiglio Nazionale delle Ricerche e responsabile del Registro.it.,
- L'IBM Fellow, Vice-President Europa e Africa nonché Direttore del Laboratorio di Ricerca IBM di Zurigo e Global Research VP IBM in Security e in Future of computing;
- Il Professore emerito, Vice-Presidente della Università LUISS Guido Carli e Direttore della Scuola Nazionale dell'Amministrazione;
- Professore ordinario di Ingegneria Informatica del Politecnico di Milano, nonché dal 2015 Prorettore vicario con delega alla ricerca.

In qualità di esponente di associazioni del settore della sicurezza delle aziende strategiche del Paese, infine, è stato nominato il Presidente pro tempore dell'Associazione Italiana Professionisti della Security Aziendale (AIPSA), in ragione delle competenze professionali e in rappresentanza delle oltre 800 aziende e persone operanti nei diversi ambiti specialistici della sicurezza in azienda.

Al Comitato, inoltre, anche in un'ottica di realizzazione delle 82 misure previste dalla Strategia Nazionale per la Cybersicurezza 2022-2026 adottata dal Presidente del Consiglio il 17 maggio 2022, potranno essere sottoposte questioni in materia di sviluppo di competenze, innovazione, partecipazione a programmi e progetti di

cybersicurezza nazionali ed internazionali, comunicazione e promozione della consapevolezza in materia di cybersicurezza, formazione e qualificazione delle risorse umane, nonché questioni afferenti al Centro nazionale di coordinamento in cybersecurity.

La Relazione fornita dall'Agenzia sul bilancio d'esercizio 2022 pone l'accento anche sul ruolo fondamentale svolto dalla Strategia Nazionale di Cybersicurezza 2022-2026 e sull'annesso Piano di Implementazione; documenti adottati il 17 maggio 2022 e pubblicati il giorno 25 di quello stesso mese e di cui questa Sezione ha profusamente discusso nelle precedenti deliberazioni dedicate all'Agenzia per la Cybersicurezza (deliberazioni n. 31, del 14 luglio 2022 e n. 5, del 9 febbraio 2023).

In merito alla gestione economica, finanziaria e patrimoniale dell'Agenzia illustrata nel documento in esame viene sottolineato quanto già rappresentato da questa Sezione nell'ultima deliberazione più volte citata, dal contenuto della quale si evince che nell'ambito dei 623 milioni di finanziamento PNRR assegnati all'investimento 1.5 "Cybersecurity", l'Agenzia ha acquistato a titolo di anticipazione la somma di 62,3 milioni di euro, equivalenti al 10 per cento dell'importo totale. Dalle risultanze finali il bilancio 2022 redatto dall'Agenzia ha registrato un utile di 21, 706 milioni di euro e nel documento è stato osservato che, trattandosi del primo anno di attività dell'Agenzia, nel corso dell'esercizio si è dovuto necessariamente coniugare la costruzione della nuova organizzazione, nei termini ben delineati nel documento stesso, con il pieno assolvimento dei compiti istituzionali ad essa affidati.

Altro dato interessante che si rileva dalla Relazione sul bilancio di esercizio dell'Agenzia attiene la materia della prevenzione della corruzione e della trasparenza e dell'adozione del piano anticorruzione, definita col provvedimento del 23 gennaio 2023, ai sensi dell'art. 1, comma 8 della legge n. 190 del 2012, dal quale emergono gli obiettivi strategici in materia di corruzione.

Le misure di prevenzione previste nel succitato provvedimento, dunque, "sono volte a creare un ambiente sfavorevole alla corruzione attraverso l'individuazione di idonei presidi per la gestione del rischio di corruzione, la diffusione della cultura della *compliance*, la sensibilizzazione e la responsabilizzazione del personale, l'elaborazione di procedure che favoriscono meccanismi di segnalazione di condotte illecite

(whistleblowing)”.

In tale contesto, il Direttore generale dell’Agenzia il 31 marzo 2023 ha approvato il Piano triennale di prevenzione della corruzione e della trasparenza 2023-2025. Il Piano è stato elaborato, da quanto rappresentato nel documento, in modo tale da promuovere l’innovazione, l’efficienza organizzativa e la trasparenza, valorizzare la dimensione di valore pubblico delle misure di prevenzione della corruzione e della trasparenza, monitorare il costante utilizzo degli strumenti e delle misure previste in materia, nonché assicurare la formazione del personale ed il relativo aggiornamento.

2 b) Assestamento al Budget economico per l’anno 2023.

Come accennato in precedenza, nel mese di ottobre 2023 alla Sezione è pervenuta una nota da parte del Ministero dell’Economia e delle Finanze afferente il provvedimento di assestamento al budget economico annuale 2023, adottato dal Direttore Generale dell’Agenzia per la Cybersicurezza con delibera prot. n. 20908 del 1° agosto 2023, ai sensi dell’articolo 14 del DPCM 9 dicembre 2021, n. 222, concernente “Regolamento di contabilità dell’Agenzia per la cybersicurezza nazionale”.

Dalle risultanze di tale provvedimento sono stati registrati “minori ricavi per 16.311.000 euro per effetto, principalmente, della riduzione registrata nella voce “contributo ordinario dello Stato” (-1.250.00 euro) e nella voce “contributi da altri enti pubblici” (- 20.686.000 euro), in parte compensata dagli aumenti derivanti dal contributo in conto esercizio da parte dello Stato (+1.000.000 euro) ai sensi dell’articolo 1, comma 899, della legge n. 197/2022 e da altri ricavi e proventi (+ 4.625.000 euro).”

Nella nota si legge, altresì, che “similmente, anche i costi della produzione rilevano una diminuzione di 16.311.000 euro, da attribuire alla riduzione registrata nei costi per servizi (-27.579.000 euro) e altri accantonamenti (-400.000 euro). Si registrano, invece, aumenti nelle voci di costi relativi a materie prime (+20.000 euro), godimento di beni di terzi (+6.872.000 euro), ammortamenti e svalutazioni (+4.625.000 euro) e oneri diversi di gestione (+ 151.000 euro).

Da tali variazioni compensative, pertanto, ne deriva che il valore e il costo della produzione si assestano, rispettivamente, a 102.978.000 euro e a 100.555.000 euro, confermando il pareggio economico previsto in sede di approvazione del budget 2023.

3. Relazione annuale al Parlamento 2022 dell'ACN.

La seconda Relazione annuale dell'Agenzia per la cybersicurezza nazionale, prevista dal decreto-legge 14 giugno 2021, n. 82, ai fini dell'assolvimento di precisi oneri informativi nei confronti del Parlamento, è stata presentata allo stesso a giugno 2023. La legge istitutiva dell'Agenzia, infatti, prevede, così come già rappresentato nella deliberazione della sezione licenziata nel mese di febbraio 2023, che il Presidente del Consiglio dei ministri presenti una relazione al Parlamento sulle attività svolte dall'Agenzia nell'anno precedente entro il termine ordinario di scadenza fissato al 30 aprile successivo all'anno di riferimento, ai sensi dell'art. 14, comma 1, del decreto medesimo.

La relazione annuale offre una panoramica generale sulle attività, dati e progettualità espletati dall'Agenzia nel corso dell'anno di riferimento, mostrando il processo di maturazione della stessa che ha portato tale Istituto 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.

Tale documento descrive compiutamente l'intenso lavoro svolto dall'Agenzia a tutela degli interessi nazionali nel campo della cybersicurezza, dialogando costantemente con le Amministrazioni che compongono l'architettura nazionale, incoraggiando, parimenti, 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 lavoro, si legge altresì, è stato compiuto lavorando 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 tale ottica, a seguito di una accurata disamina del documento di che trattasi, appare utile focalizzare l'attenzione sul ruolo svolto dalle articolazioni tecnico-operative dell'Agenzia, con particolare riferimento in primis al CSIRT Italia. Tali articolazioni, nell'ambito delle funzioni istituzionali attribuite dalla legge – che

includono sia attività di natura proattiva, finalizzate al monitoraggio e all'identificazione precoce della minaccia cibernetica, sia di natura reattiva, volte alla mitigazione dei rischi e al contenimento degli impatti sulle infrastrutture digitali nazionali derivanti dagli incidenti cibernetici – hanno adottato processi tecnici e analitici per la raccolta e la valorizzazione, in chiave di protezione, delle informazioni relative ad eventi malevoli o potenziali tali.

In tale ambito, appare utile riportare qui di seguito la tabella riportata all'interno della Relazione in esame concernente la definizione dei concetti utilizzati, nonché la descrizione sintetica della metodologia alla base del lavoro operativo svolto dall'Agenzia.

BOX 1

DEFINIZIONI E METODOLOGIA

È utile definire i concetti utilizzati e fornire una breve descrizione della metodologia che è alla base del lavoro operativo svolto dall'Agenzia, con particolare riferimento alla modalità di rilevazione di eventi e incidenti cibernetici e alla loro successiva trattazione.

DEFINIZIONI

	Segnalazione le comunicazioni previste per legge per i soggetti appartenenti al Perimetro di sicurezza nazionale cibernetica, per gli Operatori di Servizi Essenziali e Fornitori di Servizi Digitali (Direttiva NIS), e per gli operatori di comunicazione (D.M. Telco). Le Segnalazioni vengono trattate direttamente come eventi cyber
	Comunicazione ricevuta <i>e-mail</i> ricevute dal CSIRT Italia relative ad informazioni contenenti profili di natura <i>cyber</i> anche generiche, sottoposte a valutazione preliminare per determinare l'apertura di <i>case</i> o meno
	Asset potenzialmente compromessi sistemi o servizi esposti su Internet da soggetti italiani, rilevati dalle attività di monitoraggio proattivo e per i quali vengono inviate specifiche comunicazioni
	Triage la fase in cui gli operatori analizzano le segnalazioni, le comunicazioni ricevute e ogni possibile evento <i>cyber</i> di cui il CSIRT Italia viene a conoscenza, anche a seguito di attività di monitoraggio proattivo, al fine di identificare i potenziali impatti e classificare quindi l'informazione come evento <i>cyber</i> e proseguire o meno con le ulteriori fasi di trattazione
	Case un avvenimento d'interesse per il CSIRT Italia, opportunamente approfondito al fine di identificare il possibile impatto e valutare la necessità di azioni di resilienza. I <i>case</i> possono diventare eventi cyber
	Evento cyber un <i>case</i> con potenziale impatto su almeno un soggetto nazionale, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, CSIRT Italia dirama <i>alert</i> e/o supporta, eventualmente anche in loco, i soggetti colpiti. Qualora fosse confermato l'impatto dalla vittima, l'evento <i>cyber</i> viene considerato incidente
	Richieste di informazioni richieste effettuate dal CSIRT Italia al soggetto potenzialmente impattato da un evento <i>cyber</i> per acquisire ulteriori elementi, come ad esempio la conferma di una possibile compromissione (e la conseguente classificazione dell'evento <i>cyber</i> quale incidente)

	Comunicazione inviata <i>alert</i> , anche massivi, inviati a Pubbliche Amministrazioni e soggetti privati potenzialmente interessati da eventi cyber
	Constituency l'insieme dei soggetti nei confronti dei quali il CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta al fine di prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici
	Portale di <i>collaboration</i> il portale di <i>collaboration</i> è riservato ai membri della <i>constituency</i> del CSIRT Italia e costituisce lo strumento privilegiato per favorire lo scambio di informazioni tecniche specifiche con i soggetti accreditati
	Portale pubblico è il sito web del CSIRT Italia accessibile all'intera comunità

METODOLOGIA

	CSIRT Italia, articolazione tecnico-operativa dell'Agenzia, è <i>hub</i> nazionale delle notifiche obbligatorie e volontarie di incidenti previste per legge (Perimetro di sicurezza nazionale cibernetica, Direttiva NIS, D.M. Telco). Collaziona, altresì, informazioni provenienti da fonti aperte e commerciali nonché da altre articolazioni omologhe nazionali e internazionali, che le condividono di iniziativa o in base ad accordi di collaborazione. Queste informazioni costituiscono un ampio cono di visibilità di cui l'Agenzia dispone sullo stato della minaccia <i>cyber</i> a danno del sistema Paese e forniscono all'Agenzia, dal punto di vista qualitativo, un quadro strutturato delle minacce e del livello di esposizione dei soggetti nazionali. Dal punto di vista quantitativo, al fine di intercettare quei fenomeni che non emergono a seguito di obblighi di legge o nell'ambito più ampio delle attività tecniche svolte, l'Agenzia sta ampliando il citato cono di visibilità attraverso l'attuazione di un programma teso a formalizzare la collaborazione con soggetti pubblici e privati, per rafforzare lo scambio di informazioni e realizzare sinergie per la protezione dalla minaccia <i>cyber</i> (vds. Cap. 3.5) nonché attraverso la progettazione ed implementazione dei servizi <i>cyber</i> nazionali (HyperSOC, ISAC, Rete CERT, vds. Cap. 3.6). Tutte le informazioni collazionate vengono studiate e valorizzate dagli operatori del CSIRT Italia, i quali nella fase di <i>triage</i> le analizzano e classificano come eventi <i>cyber</i>; per ognuno di questi vengono esperite una serie di attività a seconda del soggetto impattato e del tipo di evento. In particolare, il CSIRT Italia: ■ approfondisce le informazioni a disposizione, analizzando i contenuti anche dal punto di vista strettamente tecnico quale lo studio dei <i>malware</i>, valutando il rischio d'impatto sistemico di vulnerabilità e incidenti; ■ se necessario invia richieste di informazioni ai soggetti; ■ fornisce supporto da remoto o <i>in loco</i> ai soggetti impattati; ■ invia comunicazioni ai soggetti impattati oppure a tutti i soggetti potenzialmente impattati dall'evento <i>cyber</i>; ■ pubblica <i>alert</i> o bollettini. Si noti che un evento <i>cyber</i> viene considerato incidente solo qualora l'impatto fosse confermato dalla vittima a seguito del supporto diretto ovvero in risposta a una richiesta di informazioni da parte del CSIRT Italia.
--	---

In ordine a tale metodologia, è stato evidenziato che le informazioni oggetto di interesse in questo campo sono state raccolte utilizzando, oltre le segnalazioni indirizzate al CSIRT Italia dalla constituency di riferimento, anche le fonti pubblicamente disponibili e fonti non pubbliche, ma reperibili nell'ambito dell'attività di cooperazione con articolazioni tecniche di altre Amministrazioni ed enti nazionali, omologhe Agenzie estere e internazionali, nonché provider di sicurezza.

Sulla scorta di quanto detto, l'Agenzia ha avviato una intensa attività di alerting e divulgazione sui principali rischi, sia in chiave pubblica, sia tramite comunicazioni puntuali ai soggetti direttamente esposti alle minacce.

Inoltre, un focus particolare in tale ambito è stato dedicato alle attività volte ad elevare il livello di allerta degli operatori pubblici e privati rispetto al rischio cyber

derivante dalla situazione internazionale.

A causa del noto conflitto bellico tra Russia e Ucraina, l'Agenzia ha intensificato la sua attività, determinando una crescita delle comunicazioni verso i soggetti della *constituency*, tanto che, nel periodo compreso tra il 26 febbraio e il 29 marzo 2022, sono state rilevate circa 19.500 comunicazioni inviate, dirette prevalentemente a *soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica*.

Nella Relazione è stato, altresì, evidenziato l'attività svolta dall'Agenzia tesa a condividere elementi informativi tecnici (Indicatori di Compromissione), al fine di sensibilizzare la *constituency* relativamente a possibili attacchi di tipo DDoS, la cui incidenza straordinaria, osservata a maggio 2022, lasciava ipotizzare che detti attacchi, nell'ambito di un conflitto ibrido, potessero essere una conseguenza del sostegno italiano all'Ucraina in ambito UE e NATO.

L'analisi di tali eventi ha consentito al CSIRT Italia di "identificare le peculiari metodologie utilizzate per condurre tali attacchi, in relazione ai quali sono stati pubblicati, in una sezione dedicata del sito web istituzionale, gli elementi informativi e operativi necessari per la pianificazione delle attività di mitigazione sui rischi cyber connessi".

Dal documento in esame, inoltre, emerge anche l'attività espletata dall'Agenzia per la Cybersicurezza volta alla gestione dei bandi e degli avvisi pubblici avviati nell'anno di riferimento, e di cui si è già parlato nelle precedenti deliberazioni adottate dalla sezione in materia, per potenziare i progetti rivolti alle pubbliche amministrazioni sia a livello centrale che locale.

4. Avvisi pubblici e rifinanziamenti.

4 a) Graduatoria per il rifinanziamento dell'Avviso pubblico n. 1 del 2022 ACN

L'Agenzia per la Cybersicurezza Nazionale con comunicazione del 30 maggio 2023, apposta sul relativo sito istituzionale, ha segnalato che si è provveduto ad incrementare la dotazione finanziaria di cui all'Avviso 1 del 2022 dedicato al potenziamento cyber delle Amministrazioni centrali.

Appare utile ricordare brevemente che l'Avviso in parola, di cui si è già parlato

nelle citate deliberazioni adottate in precedenza da questa Sezione nella materia di che trattasi, si era posto come obiettivo quello di contribuire - in attuazione dell'Investimento 1.5 "Cybersecurity" della Missione 1, Componente 1 del PNRR - al potenziamento del livello di maturità delle capacità cyber dei sistemi, delle infrastrutture e dei processi volti alla messa in sicurezza dei dati e dei servizi dei cittadini, nonché di incrementare le competenze specialistiche necessarie a garantire adeguati livelli di resilienza cyber degli Organi Costituzionali e di rilievo Costituzionale, delle Agenzie Fiscali e delle Amministrazioni facenti parte del Nucleo per la cybersicurezza.

Si evidenzia, altresì, che i traguardi e gli obiettivi dell'Avviso 1/2022 da perseguire nell'ambito dell'Investimento 1.5, collegati agli interventi di potenziamento della resilienza cyber per la PA, corrispondono nello specifico a:

- M1C1-9 (target intermedio UE) "Supporto all'aggiornamento delle misure di sicurezza - 5 strutture di sicurezza adeguate entro dicembre 2022";
- M1C1-19 (target finale UE) "Supporto all'aggiornamento delle misure di sicurezza - 50 strutture di sicurezza adeguate entro dicembre 2024".

All'esito dell'espletamento della procedura la graduatoria definitiva dell'Avviso n. 1 del 2022, che determinava l'ammissione a finanziamento di 20 progetti presentati da 12 Pubbliche Amministrazioni centrali, allocando l'intera dotazione finanziaria pari a 15 milioni a valere sul Piano Nazionale di Ripresa e Resilienza Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity", era stata pubblicata nel corso del mese di settembre 2022.

Con la determina del 23 maggio 2023 dell'Agenzia, pubblicata sul relativo sito istituzionale, si è disposto di prorogare al 30 novembre 2024 il termine ultimo ammissibile dei cronoprogrammi dei progetti non ancora completati a dicembre 2022, al fine di contribuire al raggiungimento del target M1C1-19 e di disimpegnare, parimenti, la somma pari a euro 652.946,54, inizialmente destinata al finanziamento del progetto "Adeguamento alle misure previste dal PSNC presentato dal Ministero degli Affari Esteri e della Cooperazione Internazionale", il quale ha richiesto all'Agenzia una diminuzione del finanziamento inizialmente concesso per un importo maggiore pari a euro 1.549.400,00.

Con la determina in esame si è stabilito anche di stanziare ulteriori euro 501.860,43 per il rifinanziamento dell'Avviso n. 01, somma che si aggiunge a quella disimpegnata di euro 652.946,54 e il cui importo complessivo pari a euro 1.154.806,97 andrà, pertanto, a finanziare i progetti che, valutati positivamente, non sono stati finanziati per esaurimento delle risorse a valere sull'Avviso in parola.

Sulla pagina istituzionale dell'Agenzia, quindi, si comunica che a seguito di aggiornamento della graduatoria finale il rifinanziamento di cui sopra consente di ampliare a 22 il numero di progetti finanziati, presentati dalle 12 Amministrazioni che hanno partecipato all'Avviso.

L'Agenzia per la Cybersicurezza, nel corso dell'istruttoria, ha rappresentato che, nell'ambito dell'Avviso di cui si tratta, è stata completata la firma degli Atti d'Obbligo dei progetti ammessi con rifinanziamento che ha previsto l'incremento della dotazione finanziaria.

4 b) Rifinanziamento dell'Avviso pubblico n. 3 del 2022

L'Avviso n. 3 del 2022, di cui si è diffusamente parlato nella deliberazione n. 5 del 2023 adottata da questa Sezione, si pone come obiettivo, in attuazione dell'investimento 1.5 Cybersecurity, quello di contribuire al potenziamento del livello di maturità delle capacità cyber dei sistemi per la messa in sicurezza dei dati e dei servizi dei cittadini, nonché di irrobustire le competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza per le Regioni, per i Comuni capoluogo facenti parte di Città metropolitane e per le Province autonome.

Si ricorda che i traguardi e gli obiettivi da perseguire sottesi all'Investimento 1.5 di cui all'Avviso di cui si tratta sono collegati agli investimenti di potenziamento della resilienza cyber per la PA, quali nello specifico:

- M1C1-19 (target finale UE) "Supporto all'aggiornamento delle misure di sicurezza - 50 strutture di sicurezza adeguate entro dicembre 2024.

L'Avviso n. 3, pubblicato il 29 luglio 2022, aveva inizialmente stanziato una somma di euro 45.000.000,00 a valere sul Piano Nazionale di Ripresa e Resilienza - Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity"; somma diretta alla

realizzazione delle proposte progettuali ammesse a finanziamento a valere sull'Avviso in parola.

A seguito di rinuncia da parte del Comune di Firenze al finanziamento concesso per il progetto presentato e ammesso parzialmente per un importo pari a euro 12.620,00, si è ritenuto opportuno disimpegnare la medesima somma e impiegarla nello scorrimento della graduatoria dei progetti idonei ma non finanziabili per esaurimento delle risorse. Inoltre, considerato che nell'Avviso n. 03 è contemplata la facoltà per l'Agenzia di incrementare la dotazione finanziaria inizialmente stabilita e, parimenti, di procedere allo scorrimento della graduatoria dei progetti idonei ma non finanziabili per esaurimento delle risorse, in caso di rifinanziamento dell'Avviso, rinunce o revoche, con determina del 21 aprile 2023 è stato disposto di stanziare ulteriori 18.687.253,86 per il rifinanziamento dell'Avviso in esame. Di conseguenza, è stato disposto l'aggiornamento della graduatoria definitiva a valere sull'Avviso 3/2022, adottata con determina n. 7591 del 23 febbraio 2023, e conseguentemente i relativi allegati che costituiscono parte integrante del presente provvedimento:

- Allegato A - Graduatoria definitiva delle proposte progettuali ammesse e totalmente finanziabili;
- Allegato B - Graduatoria definitiva delle proposte progettuali ammesse e parzialmente finanziabili;
- Allegato C - Graduatoria definitiva delle proposte progettuali idonee ma non finanziabili;
- Allegato D - Elenco delle proposte progettuali non ammesse.

In tal modo, lo stanziamento iniziale così incrementato ha consentito di ammettere a finanziamento tutti i 75 progetti finanziabili, presentati dalle amministrazioni che hanno partecipato all'Avviso.

Nella nota istruttoria trasmessa dagli Enti interessati, si apprende che si è proceduto alla firma degli Atti d'Obbligo dei progetti ammessi con rifinanziamento che ha previsto l'incremento della dotazione finanziaria.

4 c) Evoluzione del Bando relativo a "60 assunzioni di diplomati per l'information and communication technology (ict)"

Il 28 ottobre del 2022 è stato pubblicato sulla Gazzetta Ufficiale - IV serie speciale

Concorsi ed esami – n. 86, il bando di assunzione presso l’Agenzia di 60 diplomati nell’ambito dell’Information and Communication Technology (ICT). Il bando presenta diversi profili relativi a 7 funzioni: Cyber Security Triage Operator e Digital Forensic and Incident Response Specialist, Security and Threat Analyst, Red Team Operator, Data Collection and Analysis, Tecnico di laboratorio software, Tecnico di laboratorio hardware, IT project coordinator and developer.

Secondo quanto disposto dal bando in esame i vincitori del concorso dovranno contribuire alla preparazione, prevenzione, gestione e risposta a eventi cibernetici, per valutare i prodotti e servizi informatici, nonché per soddisfare le esigenze di sicurezza informatica della rete, dei sistemi, dei dispositivi e dei servizi informatici dell’Agenzia.

Le domande pervenute all’Agenzia in ordine al concorso in essere ammontano a 800 e le prove scritte si sono svolte in data 20 giugno 2023, secondo le modalità indicate nel bando stesso.

Dalla consultazione del sito istituzionale dell’Agenzia per la cybersicurezza nazionale emerge che tra settembre e ottobre 2023 sono state approvate le graduatorie finali dei vari profili.

4 d) Erogazione di contributi dell’Avviso pubblico n. 5/2022, per l’attivazione di LAP a supporto delle attività di scrutinio tecnologico del CVCN per l’area di accreditamento Software e Network

Per quanto concerne l’Avviso n. 5 del 2022, nella deliberazione del 9 febbraio 2023, n. 5, adottata da questa Sezione, è stato evidenziato che, in merito alla procedura espletata ai fini dell’attribuzione della dotazione finanziaria stabilita per un ammontare complessivo di € 5.000.000,00, risultava in corso la fase dell’istruttoria amministrativa concernente la selezione dei progetti.

Giova evidenziare che questo Avviso contribuisce al raggiungimento dei seguenti traguardi e obiettivi dell’Investimento 1.5:

- M1C1-7 (milestone UE): “Avvio della rete dei laboratori di screening e certificazione della cybersecurity” entro dicembre 2022;
- M1C1-21 (milestone UE) “Completamento della rete dei laboratori e dei CVCN” entro dicembre 2024”.

Con il finanziamento di cui all’Avviso n. 5 l’Agenzia intende contribuire al

percorso di realizzazione della rete nazionale di scrutinio tecnologico del Centro di Valutazione e Certificazione Nazionale (CVCN) per l'area di accreditamento Software e Network, nonché irrobustire le competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza del Paese.

In tale ambito l'Agenzia ha curato la selezione di progetti volti all'attivazione di Laboratori di Prova (LAP) a supporto delle attività di scrutinio tecnologico per l'area di accreditamento "Software e Network" definita dal CVCN. L'Avviso, espletato mediante procedura a sportello, è destinato a finanziare progetti volti all'acquisizione e al consolidamento di capacità tecniche di valutazione e scrutinio tecnologico continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte dei Soggetti rientranti nel Perimetro di sicurezza nazionale cibernetica (PNSC).

A conclusione delle attività di valutazione dei 34 progetti presentati da Pubbliche Amministrazioni e Soggetti Privati, a fronte di una dotazione finanziaria complessiva pari ad euro 5 milioni, è stata adottata, con determinazione del Direttore generale dell'Agenzia del 23 maggio 2023, la graduatoria finale delle 27 progettualità ammesse a finanziamento.

Con successiva determinazione del 26 ottobre 2023, invece, è stato disposto l'aggiornamento della graduatoria di ammissione a finanziamento di cui alla precedente determina dell'Agenzia, n. 15093 del 23 maggio 2023, relativa agli aiuti concedibili a valere sull'Avviso 5/2022, a seguito delle risultanze dei controlli ex ante previsti dalla legge e delle verifiche RNA con l'indicazione dei RNA - COR acquisiti ai sensi dell'articolo 9 del decreto ministeriale 31 maggio 2017, n. 117.

In tale ambito, pertanto, è stato deciso di destinare l'importo complessivo pari a euro 4.234.150,05, a valere sul Piano Nazionale di Ripresa e resilienza (PNRR) M1C1 - I. 1.5 "Cybersecurity", per la realizzazione delle proposte progettuali ammesse totalmente o parzialmente al finanziamento nell'ambito dell'Avviso di che trattasi.

4 e) Avviso n. 6/2023 “a sportello per la presentazione di proposte di interventi volti all’attivazione e al potenziamento di CSIRT”. Determina di concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse

L’Agenzia per la Cybersicurezza Nazionale, in data 11 agosto 2023, ha pubblicato l’Avviso n. 6, con il quale intende contribuire, in qualità di Soggetto attuatore dell’Investimento 1.5 del PNRR, all’attuazione di investimenti finalizzati al rafforzamento delle capacità tecniche nazionali in materia di prevenzione e risoluzione di incidenti cyber, mediante l’attivazione di squadre di pronto intervento informatico deputate alla gestione degli incidenti e degli attacchi informatici sui propri sistemi informativi.

L’Avviso in parola, espletato mediante procedura a sportello, è volto a finanziare – secondo l’ordine cronologico di presentazione delle Istanze di partecipazione e fino alla concorrenza delle risorse disponibili – progettualità cd. a regia, tese all’attivazione o al potenziamento di Computer Security Incident Response Team (CSIRT) da costituirsi o già costituiti presso le Regioni e le Province autonome, coerentemente con i requisiti minimi individuati dalle “Linee Guida per la realizzazione di uno CSIRT”.

Una volta espletata la procedura di cui all’Avviso n. 6, i Soggetti ammessi a finanziamento potranno essere chiamati, una volta istituiti gli CSIRT Regionali, a stipulare specifici Accordi di Collaborazione con l’Agenzia stessa, al fine di collaborare nell’ambito di attività finalizzate a consentire la condivisione e lo scambio di informazioni, procedure e linee guida, nonché di beneficiare dell’accesso a servizi e strumenti offerti dalla stessa Agenzia in tema di prevenzione e risposta agli incidenti informatici.

I soggetti ammessi a partecipare al presente Avviso, ai fini del riconoscimento ed erogazione del contributo per la realizzazione di progetti volti alla realizzazione o al potenziamento di CSIRT da costituirsi o già costituiti, sono le Regioni e le Province autonome di Trento e Bolzano. Ciascun Soggetto partecipante potrà presentare una progettualità volta alla creazione o al potenziamento di uno CSIRT Regionale che operi

sui sistemi informativi del Soggetto stesso.

La determina del Direttore generale dell'Agenzia per la Cybersicurezza dell'8 agosto 2023 ha stanziato, per il finanziamento degli interventi volti all'attivazione e al potenziamento di CSIRT Regionali, per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici, la somma pari a 28.000.000,00 euro.

Il relativo termine per la presentazione delle istanze di partecipazione all'Avviso di cui trattasi è scaduto il giorno 25 settembre 2023, a seguito del quale sono pervenute n. 19 istanze di partecipazione.

Dalle risultanze dell'istruttoria sono state approvate proposte progettuali ammissibili e parzialmente finanziabili per esaurimento delle risorse, di cui all'Allegato B della determina del Direttore generale dell'Agenzia del 30 novembre 2023. L'Avviso, però, ai sensi del paragrafo 7.1, ha previsto la possibilità per l'Agenzia di procedere allo scorrimento dell'elenco delle proposte progettuali parzialmente finanziabili e idonee ma non finanziabili, in caso di rifinanziamento dell'Avviso, rinunce o revoche. Di talché si è stabilito di rifinanziare, con la medesima determina del 30 novembre 2023, con ulteriori euro 490.306,51 la dotazione finanziaria iniziale complessiva stabilita nell'Avviso 06/2023, al fine dello scorrimento della graduatoria dei progetti ammissibili ma parzialmente finanziabili per esaurimento delle risorse disponibili.

4 f) Avviso n. 7/2023 “Avviso Pubblico a sportello per l'erogazione di interventi di potenziamento e miglioramento delle capacità cyber degli Organi costituzionali e di rilevanza costituzionale, dei Ministeri, delle Agenzie Fiscali, degli Enti di regolazione dell'attività economica, delle Autorità amministrative indipendenti e degli Enti a struttura associativa”.

In data 11 ottobre 2023 è stato pubblicato sul sito istituzionale dell'Agenzia per la Cybersicurezza anche l'Avviso n. 7, relativo al potenziamento e al miglioramento delle capacità cyber delle Pubbliche Amministrazioni Centrali, mediante l'erogazione di servizi volti a supportare i Soggetti destinatari individuati nella realizzazione di un percorso virtuoso di gestione del rischio cyber.

L'Avviso, espletato mediante procedura a sportello, si propone di finanziare – secondo l'ordine cronologico di presentazione delle Istanze di partecipazione e fino a concorrenza delle risorse disponibili – progettualità cd. a titolarità volte alla realizzazione di:

- un censimento dei livelli di maturità della postura di sicurezza dei servizi e delle infrastrutture digitali delle PA;
- interventi di potenziamento dell'organizzazione, dei processi e procedure della gestione del rischio cyber nella PA;
- un piano programmatico di potenziamento delle capacità cyber a favore del personale in modo da rafforzare il percorso di trasformazione digitale sicura della PA.

I soggetti ammessi alla partecipazione di cui all'Avviso di che trattasi riguardano gli Organi costituzionali e a rilevanza costituzionale, i Ministeri, le Agenzie fiscali, gli Enti di regolazione dell'attività economica, le Autorità amministrative indipendenti e gli Enti a struttura associativa, come individuate da ISTAT nel settore delle Amministrazioni Pubbliche Centrali (Settore S.13).

La somma stanziata per il finanziamento di interventi volti al potenziamento e al miglioramento delle capacità cyber della Pubblica Amministrazione ammonta a euro 15.000.000,00.

In considerazione del fatto che l'art. 6 dell'Avviso in oggetto ha previsto la facoltà per l'Agenzia di riaprire lo sportello per la presentazione delle istanze, nel caso di risorse residue o rifinanziamento dell'Avviso, con determina del Direttore generale dell'Agenzia, del 13 novembre 2023, è stata disposta la proroga dei termini al fine di favorire la più ampia partecipazione all'Avviso tra le Pubbliche Amministrazioni Centrali così come individuate dal par. 3 dell'Avviso in oggetto e consentire la presentazione di ulteriori istanze di partecipazione, fermo restando le risorse finanziarie individuate nella sopracitata determina n. 22565 del 10 ottobre 2023. I relativi termini per la presentazione delle istanze, pertanto, sono stati prorogati al giorno 05 dicembre 2023.

5. Novità intervenute in materia

5 a) Linee guida per i soggetti attuatori individuati tramite avvisi pubblici Manuale Operativo

Si deve evidenziare che sul sito istituzionale dell'Agenzia per la Cybersicurezza il 6 giugno del 2023 è stato pubblicato il Manuale operativo in ordine alle Linee guida per i soggetti attuatori individuati tramite avvisi pubblici, giunta alla sua versione 3.0, mentre la prima versione risale al 10 novembre del 2022.

Nell'ambito del suddetto Piano Operativo per l'attuazione dell'investimento 1.5 e ai fini del raggiungimento di milestone e target assegnati, l'Agenzia prevede la selezione di progetti a titolarità di altri soggetti, sub-attuatori – ossia i Soggetti Attuatori degli interventi – i quali, in qualità di “soggetti pubblici o privati che provvedono alla realizzazione degli interventi previsti dal PNRR”, secondo quanto stabilito dall'art. 1, comma 4, lett. o) del citato decreto-legge n. 77 del 2021, sono responsabili dell'avvio, dell'attuazione e della funzionalità dei singoli interventi di competenza, della regolarità delle procedure e delle spese rendicontate a valere sulle risorse del PNRR, nonché del monitoraggio circa il conseguimento dei valori definiti per gli indicatori associati ai propri progetti.

Tale documento, pertanto, redatto in conformità con le Linee guida e il Sistema di Gestione e Controllo (SI.GE.CO.) dell'Amministrazione centrale titolare e della sua Unità di Missione del PNRR, fermo restando quanto previsto dalla normativa europea e nazionale che sovrintende l'attuazione del PNRR, si pone come obiettivo quello di fornire una guida operativa per l'avvio, attuazione e rendicontazione dei progetti che saranno intrapresi dai Soggetti Attuatori individuati nell'ambito delle procedure di selezione tramite Avvisi Pubblici attivate dall'ACN a valere sul PNRR.

5 b) Linee guida per i soggetti attuatori individuati tramite accordi ai sensi dell'art. 5, comma 6, del d.lgs. n. 50/2016 (Accordi Cyber Defence)

L'Agenzia per la cybersicurezza in data 7 aprile del 2023 ha pubblicato sul suo sito istituzionale un altro manuale operativo, relativo alle Linee guida per i soggetti attuatori individuati tramite accordi ai sensi dell'art. 5, comma 6, del d.lgs. n. 50/2016,

nella sua versione 2.0.

L'Agenzia per la Cybersicurezza Nazionale, dunque, in qualità di Soggetto attuatore dell'Investimento 1.5, Missione 1, Componente 1 del Piano Nazionale di Ripresa e Resilienza (PNRR), può anche coinvolgere altre Pubbliche amministrazioni e/o enti pubblici per il raggiungimento dei M&T associati alla misura di riferimento, attraverso la stipula di accordi con soggetti Sub-attuatori.

Si precisa, inoltre, che il presente Manuale Operativo, redatto in conformità con le Linee guida e il Sistema di gestione e controllo degli interventi previsti nell'ambito del PNRR dell'Amministrazione centrale titolare e Unità di Missione, si prefigge l'obiettivo di fornire ai Soggetti Attuatori individuati dall'Agenzia tramite sottoscrizione di Accordi ai sensi dell'art. 5, comma 6, del decreto legislativo n. 50 del 2016 e art. 15 della legge n. 241 del 1990, indirizzi e strumenti operativi finalizzati a svolgere i necessari adempimenti di gestione, monitoraggio e controllo. Ciò al fine di agevolare il processo attuativo degli interventi fino alla rendicontazione delle spese e al raggiungimento degli obiettivi intermedi e finali, salvaguardando i principi di efficienza, efficacia ed economicità ed in generale il rispetto della sana gestione finanziaria delle risorse finanziarie.

È previsto, altresì, che tale documento possa essere oggetto di revisioni e modifiche sulla base delle decisioni e degli orientamenti provenienti dagli Organi dell'Unione Europea, ovvero, dal Ministero dell'Economia e delle Finanze, ovvero dall'Unità di Missione del PNRR del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri (DTD) in qualità di Amministrazione titolare. Il Manuale operativo può anche essere interessato da innovazioni e/o cambiamenti e dover tener conto di nuove normative. Trattasi, dunque, di uno strumento suscettibile di aggiornamenti in rispondenza a mutamenti del contesto di riferimento, ovvero sulla base di esigenze organizzative ed operative che dovessero manifestarsi nel corso dell'implementazione della procedura.

5 c) Firmato l'Accordo Quadro tra l'Agenzia per la Cybersicurezza Nazionale e la Scuola Nazionale dell'Amministrazione

In materia di attività di formazione svolta dall'Agenzia per la cybersicurezza un cenno deve essere rivolto all'accordo quadro firmato in data 17 ottobre 2023 dal

Presidente dell'Agenzia stessa e il Presidente della Scuola Nazionale dell'Amministrazione, volto a promuovere la diffusione della cultura della Cybersicurezza attraverso diverse iniziative riguardanti attività didattiche e formative, l'organizzazione di conferenze, dibattiti, seminari ed ogni altra iniziativa di comune interesse utile a sostenere e promuovere la diffusione della cultura della cybersicurezza.

Il Direttore dell'Agenzia ha dichiarato che attraverso la stipulazione di tale Accordo, di durata triennale, ci si propone "di rafforzare la capacità operativa delle PA secondo un piano di generale potenziamento della resilienza".

5 d) Protocollo d'Intesa finalizzato alla gestione di procedure di appalto congiunte per l'acquisizione di beni, servizi e lavori, secondo la disciplina di cui al d.lgs. 31 marzo 2023, n. 36.

Degno di interesse anche il Protocollo d'Intesa fra la Banca d'Italia, l'Autorità Garante della Concorrenza e del Mercato (AGCM), la Commissione Nazionale per le Società e la Borsa (CONSOB), l'Autorità Nazionale Anticorruzione (ANAC), l'Istituto per la Vigilanza sulle assicurazioni (IVASS) e l'Agenzia per la cybersicurezza nazionale (ACN), stipulato in data 20 novembre 2023.

Il Protocollo d'Intesa è finalizzato alla gestione di procedure di appalto congiunte per l'acquisizione di beni, servizi e lavori, secondo la disciplina di cui al d.lgs. 31 marzo 2023, n. 36 ed è stato sottoscritto ai sensi dell'art. 15 della legge 241/1990 per una durata quinquennale e con possibilità di rinnovo.

Tale Protocollo, altresì, si propone di definire le modalità di coordinamento tra gli Enti aderenti, nonché di individuare strategie congiunte di public procurement, per soddisfare esigenze di approvvigionamento comuni.

Le attività sottese al Protocollo d'Intesa si svolgeranno in continuità con la proficua collaborazione già sperimentata tra le Autorità in materia di spesa e risultano in linea con la disciplina del nuovo Codice dei contratti pubblici. A tal proposito, occorre evidenziare che tale normativa è incentrata sulla qualificazione delle stazioni appaltanti e sulla collaborazione tra le amministrazioni, con l'obiettivo di realizzare strategie di acquisto condivise sempre più efficienti, anche nell'ottica dello sviluppo

comune di progetti complessi e innovativi.

5 e) Linee guida internazionali sulla sicurezza dell'Intelligenza Artificiale (pubblicate il 27 novembre 2023)

Altro documento da porre in evidenza è costituito dalle “Linee guida per uno sviluppo sicuro dell'Intelligenza Artificiale” a cui l'Agenzia per la cybersicurezza nazionale ha aderito. Trattasi di un documento promosso dal National Cyber Security Centre del Regno Unito e sottoscritto da 23 Agenzie di 18 Paesi. Le linee-guida, inoltre, rappresentano il primo documento congiunto internazionale per un uso sicuro dell'Intelligenza Artificiale (IA), il cui contenuto è volto a sostenere gli sviluppatori nella creazione di un'IA responsabile, etica e sicura.

Il presupposto di tale documento si rinviene nella prima conferenza internazionale sull'Intelligenza Artificiale, c.d. “AI Safety Summit”, tenutasi nel Regno Unito tra l'1-2 novembre, a cui hanno partecipato esperti governativi e del settore privato, provenienti da 18 Paesi, i quali hanno elaborato una linea di indirizzo comune per supportare gli sviluppatori di qualsiasi sistema basato sull'IA.

Tra i Paesi che hanno contribuito alle linee guida si devono annoverare: Australia, Canada, Cile, Corea del Sud, Estonia, Francia, Germania, Giappone, Israele, Italia, Nigeria, Norvegia, Nuova Zelanda, Polonia, Regno Unito, Repubblica Ceca, Singapore e Stati Uniti.

L'obiettivo principale sotteso a tale documento è diretto a innalzare i livelli di cybersecurity dell'Intelligenza Artificiale per assicurare che sia progettata, sviluppata e impiegata in maniera sicura. Si deve specificare, infatti, che la cybersicurezza costituisce una preconditione essenziale dell'Intelligenza Artificiale, con la quale è possibile garantire resilienza, privacy, correttezza ed affidabilità, ovvero un cyberspazio più sicuro.

Ciò è avvalorato anche dalle parole dello stesso Direttore dell'Agenzia, estrapolate dal sito istituzionale dell'Istituto stesso, secondo il quale "L'Intelligenza Artificiale è una sfida a cui l'Agenzia non vuole e non può sottrarsi. Per questo abbiamo aderito con convinzione a questa iniziativa. È una sfida che può essere vinta solo tutti assieme:

dobbiamo mettere a disposizione le migliori energie, intellettuali e strumentali del nostro Paese e di tutti gli altri Paesi che si apprestano ad affrontare, a partire dal prossimo G7 a guida italiana, questa impresa così altamente impegnativa per l'intera umanità".

In ordine al contenuto delle linee-guida di cui trattasi si riportano brevemente i punti principali cui tendono le relative attività:

- sono volte ai fornitori di sistemi che utilizzano l'intelligenza artificiale (AI), indipendentemente dal fatto che tali sistemi siano stati creati da zero o costruiti su strumenti e servizi forniti da altri;
- è documento rivolto principalmente ai fornitori di sistemi di intelligenza artificiale che utilizzano modelli ospitati da un'organizzazione o utilizzano interfacce di programmazione di applicazioni esterne (API);
- offre un valido aiuto affinché l'Intelligenza Artificiale venga adeguatamente sviluppata, impiegata e gestita in modo sicuro e responsabile, in modo tale da apportare molti vantaggi alla società;
- visto che i sistemi di intelligenza artificiale sono soggetti a nuove vulnerabilità di sicurezza che devono essere considerate insieme alle minacce standard alla sicurezza informatica, le linee guida sono state suddivise in quattro aree chiave all'interno del ciclo di vita dello sviluppo del sistema IA: progettazione sicura, sviluppo sicuro, implementazione sicura e funzionamento e manutenzione sicuri;
- le linee guida seguono un approccio "secure by default" e sono strettamente allineate alle pratiche definite nelle linee guida per lo sviluppo e l'implementazione sicure dell'NCSC, nel Secure Software Development Framework del NIST e nei principi "secure by design" pubblicati da CISA, NCSC e agenzie informatiche internazionali.

5 f) Registro.it (pubblicato il 27 novembre 2027)

Altro dato interessante circa le attività espletate dall'Agenzia concerne il meeting annuale che si è svolto, in data 24 novembre 2023, presso l'Auditorium della Area della

ricerca di Pisa del Consiglio nazionale delle ricerche (CNR) in materia di Registro.it.

In tale occasione è stato posto in evidenza che i domini Made in Italy, quelli con suffisso nazionale ".it", ad ottobre 2023, hanno superato i 3 milioni e mezzo e che l'attività svolta dal Registro.it, ossia l'anagrafe dei domini internet italiana, è volta a far conseguire vantaggi alla comunità nazionale.

In tale ambito, quindi, l'Agenzia svolge un ruolo importante mettendo le sue competenze e la sua collaborazione a disposizione e fornendo, dunque, quelle misure di sicurezza necessarie per la protezione delle infrastrutture tecnologiche utilizzate da Registro.it. Ciò al fine di innalzare sempre di più "il livello di sicurezza e resilienza nel dominio cibernetico, nell'interesse del nostro Paese".

In occasione dell'incontro, infine, è stato evidenziato come i dati raccolti, quelli relativi al genere, non restituiscono variazioni di rilievo rispetto al 2022: i registranti maschi si attestano sul 75,16% mentre le femmine stazionano al 24,84%. Per quanto concerne l'età: ambedue i sessi registrano di più tra 42-49 anni (femmine 22,60%, maschi 21,63%).

6. Quadro finanziario

Come già rappresentato nelle deliberazioni della Corte 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.

L'investimento in esame è inserito, nell'ambito del medesimo Piano, nella Missione 1: Digitalizzazione, innovazione, competitività e cultura, per la quale si ritiene opportuno riportare il relativo budget finanziario, distinto per esercizio finanziario, frutto di stime elaborate dall'Agenzia per la Cybersicurezza in ordine a future liquidazioni subordinate all'avanzamento degli interventi a titolarità e a regia. In particolare, nel caso degli interventi a regia tale stima è vincolata all'avanzamento e alla rendicontazione delle attività da parte dei soggetti destinatari degli interventi.

Missione M1 Digitalizzazione, innovazione, competitività e cultura					
Anno	2022	2023	2024	2025	2026
Budget	6.041.194,49 M	45.755.424,92 M	circa 200 M	circa 245 M	circa 125 M

Occorre ricordare che le attività progettuali di cui si compone l'investimento 1.5 sulla "Cybersecurity" sono 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 la 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. 3828, del 28 novembre del 2023, ha chiesto alle Amministrazioni competenti di fornire il relativo aggiornamento per l'anno 2023.

A tal proposito, il Dipartimento per la trasformazione digitale congiuntamente con l'Agenzia per la cybersicurezza hanno inviato in data 13 dicembre 2023 una nota contenente le informazioni richieste, unitamente ai relativi allegati.

Nella tabella seguente, pertanto, si riporta il quadro economico finanziario dell'Investimento 1.5 Cybersecurity con separata indicazione, per ciascun gruppo di attività (WP), della dotazione finanziaria complessiva fino al 2026, per un totale pari a euro 623.000.000, e della previsione degli impegni per l'anno in corso, intendendo per quest'ultima, l'importo relativo alle risorse finanziarie pianificate in base allo svolgimento delle attività progettuali programmate per il 2023.

È stato poi evidenziato nella tabella di riferimento che per quanto attiene la dotazione finanziaria attribuita per le attività progettuali afferenti i WP dal n. 9 al n. 12 è in fase di valutazione una rimodulazione di circa 70.000.000,00 di euro.

Come si evince dalla tabella che si riporta qui di seguito, oltre agli importi totali degli impegni per l'anno 2023, sono stati indicati separatamente sia gli importi

impegnati a titolarità che quelli impegnati a regia nel 2023. Tali dati, da quanto indicato nella relativa tabella prodotta dalle Amministrazioni interessate, si devono intendere aggiornati al 12 dicembre 2023:

Investimento 1.5 Cybersecurity: Quadro economico finanziario				
WP	Dotazione finanziaria complessiva fino al 2026	Importi impegnati a titolarità nel 2023	Importi impegnati a regia nel 2023	Impegni 2023
WP 1 - Project Management	8.000.000,00	3.526.721,10 €	N/A	3.526.721,10 €
WP 2 - Agenzia per la Cybersicurezza Nazionale	53.000.000,00	422.931,73 €	N/A	422.931,73 €
WP 3 - Hyper SOC	18.000.000,00	499.362,74 €	N/A	499.362,74 €
WP 4 - Servizi PSNC an NIS	12.600.000,00		N/A	
WP 5 - HPC & AI/ML	30.000.000,00	21.900.000,00 €	N/A	21.900.000,00 €
WP 6 - ISAC	12.300.000,00		N/A	
WP 7 - CERT	32.000.000,00		28.490.306,51 €	28.490.306,51 €
WP 8 - Ispezioni PSNC/NIS	8.000.000,00	66.124,00 €	N/A	66.124,00 €
WP 9 - Interventi di potenziamento delle capacità cyber della PA	151.750.000,00		64.189.114,29 €	64.189.114,29 €
WP 10 - Interventi di potenziamento di capacità cyber - defence	150.000.000,00	N/A		
WP 11 - CVCN & Interno e Difesa	35.350.000,00	44.286,00 €		44.286,00 €
WP 12 - Rete di laboratori	112.000.000,00		4.234.150,05 €	4.234.150,05 €
Totale	623.000.000,00	26.459.425,57 €	96.913.570,85 €	123.372.996,42 €

Nella tabella fornita dalle Amministrazioni competenti è riportata, altresì, una distinta colonna afferente gli importi di ulteriori previsioni per impegni per il 2023, specificando che è in fase di attivazione un contratto tramite AQ Consip – ID 2296 – Lotto 1 – servizi da remoto, di compliance e controllo per le Pubbliche Amministrazioni. A tal riguardo, si indicano nella tabella sottostante gli importi divisi per ciascun gruppo di attività (WP), con il relativo totale di quanto impegnato nell’anno 2023.

	WP 1	WP 2	WP 3	WP 4	WP 5	WP 6	WP 7	WP 8	WP 9	WP 10	WP 11	WP 12
Previsioni ulteriori impegni per il 2023		€ 1.011.998,94	€ 603.850,98	€ 3.559.320,72		€ 3.559.320,72					€ 522.488,23	
Totale	9.256.979,59 €											

Nella nota istruttoria trasmessa congiuntamente dalle Amministrazioni interessate nel mese di dicembre 2023 sono contenute, in ordine all’investimento 1.5, anche le informazioni circa i movimenti dei fondi concernenti il versamento degli stessi al Dipartimento per la transizione digitale effettuati nell’anno 2023.

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 12 dicembre 2023, sono state trasferite risorse per un totale di euro 67.335174,65. Di tale somma 62,300.000 euro sono stati erogati a titolo di anticipazione in data 25 marzo 2022. Trattasi - così come è stato riscontrato dall’applicativo SICR e già riportato nella deliberazione precedente di questa sezione n. 5 del 2023 – 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

Nazionale che, dell’investimento, come detto, è il soggetto attuatore.

Risultano, invece, erogati, in data 29 novembre 2023, euro 5.035.174,65 a titolo di rimborso del rendiconto di progetto n. 3000001478, presentato dallo stesso Soggetto Attuatore. In merito a quanto esposto, si riporta qui di seguito la tabella riepilogativa dei movimenti di entrata e in uscita della Contabilità Speciale del Dipartimento per la trasformazione digitale:

Movimentazione fondi Investimento 1.5									
Importi liquidati nel corso del 2023									
Movimentazioni in entrata sulla CS 6288dalconto 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 (€)
2022060003	21/03/2022	Anticipo per Accordo DTD-ACN del 14.12.2021	PCM/DTD*	CS-348-06288	80188230587	2022000003	22/03/2022	2022000003	62.300.000,00
2023060397	29/11/2023	Rimborso per R n. 4000000136 del 24/11/2023	PCM/DTD*	CS-348-06288	80188230587	2023000384	04/12/2023	2023000026	5.035.174,65 €

- Presidenza del Consiglio dei ministri/Dipartimento per la trasformazione digitale

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 (€)
2022420004	25/03/2022	Anticipo per Acc DTD-ACN del 14.12.2021	ACN*	TU-348-320645	96501130585	2022000003	30/03/2022	67320006732	62.300.000,00
2023420218	05.12.2023	Rimborso Rendiconto di progetto n. 3000001478	ACN*	TU-348-320645	96501130585	2023011212	07/12/2023	63122046312204	5.035.174,65 €

* Agenzia per la cybersicurezza nazionale

Dalla consultazione del cruscotto Monitoraggio Rendiconti di Misura è stato possibile verificare che l’unico progetto a rendiconto nell’anno 2023 riguarda il 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 indica qui di seguito la relativa tabella riepilogativa.

ID Rendiconto di progetto (misura)	Titolo Progetto	CUP	CLP	Soggetto Attuatore	Importo totale rendiconto	Importo Totale approvato
3000001478	Servizi a supporto dell'Agenzia per la Cybersicurezza Nazionale - Attività di costituzione operativa di ACN e successivo espletamento delle proprie funzioni	F84E21007910007	F84E21007910007	Agenzia per la Cybersicurezza nazionale	5.035.174,65	5.035.174,65
Totale €					5.035.174,65 €	5.035.174,65 €

La somma erogata a titolo di rimborso del rendiconto di progetto n. 3000001478 è stata verificata anche attraverso l’interrogazione del sistema SICR, al 31 dicembre 2023, in cui dal conto sulla contabilità speciale del Dipartimento per la trasformazione digitale risulta registrato l’importo di euro 5.035.174,65 di cui sopra.

Dal sistema applicativo REGIS, componente Rendicontazione di Progetto – Soggetto Attuatore, sezione Lista Pagamenti, è stato possibile estrapolare una tabella contenente i dati dettagliati degli importi di pagamento e dei rendiconti afferenti il progetto n. 3000001478 di cui sopra, effettuati tra il 2022 e il 2023 e corrispondenti ai diversi WP, il cui totale ammonta a euro 5.035.174,65. L’ultima colonna a destra della pagina concernente la “lista pagamenti” è dedicata alla voce degli “allegati”, in cui è possibile visionare i documenti relativi alle quietanze di pagamento – che per esigenze di sinteticità in questo Report non sono state inserite - riportanti sia la data in cui è stato effettuato il pagamento, sia la causale con l’indicazione specifica dei diversi WP collegati al progetto. Si indica qui di seguito la relativa tabella con i singoli pagamenti effettuati e rendicontati.

ID Rendiconto	Mandato	Codice Unico progetto	Codice Locale progetto	Importo del pagamento	Importo richiesto	Importo rendicontato	Importo approvato
3000001478	29/2023	F84E21007910007	F84E21007910007	35641,36	35641,36	35641,36	35641,36
3000001478	27/2023	F84E21007910007	F84E21007910007	30707,12	30707,12	30707,12	30707,12
3000001478	26/2023	F84E21007910007	F84E21007910007	49131,39	49131,39	49131,39	49131,39
3000001478	25/2023	F84E21007910007	F84E21007910007	93349,64	93349,64	93349,64	93349,64
3000001478	24/2023	F84E21007910007	F84E21007910007	31584,46	31584,46	31584,46	31584,46
3000001478	23/2023	F84E21007910007	F84E21007910007	12282,85	12282,85	12282,85	12282,85
3000001478	22/2023	F84E21007910007	F84E21007910007	103175,91	103175,91	103175,91	103175,91
3000001478	28/2023	F84E21007910007	F84E21007910007	37024,01	37024,01	37024,01	37024,01
3000001478	142	F84E21007910007	F84E21007910007	272679,21	272679,21	272679,21	272679,21
3000001478	150	F84E21007910007	F84E21007910007	24214,76	24214,76	24214,76	24214,76
3000001478	155	F84E21007910007	F84E21007910007	146341,35	146341,35	146341,35	146341,35
3000001478	154	F84E21007910007	F84E21007910007	139498,05	139498,05	139498,05	139498,05
3000001478	145	F84E21007910007	F84E21007910007	423711,80	423711,80	423711,80	423711,80
3000001478	146	F84E21007910007	F84E21007910007	72995,21	72995,21	72995,21	72995,21
3000001478	163	F84E21007910007	F84E21007910007	467268,80	467268,80	467268,80	467268,80
3000001478	153	F84E21007910007	F84E21007910007	92296,82	92296,82	92296,82	92296,82
3000001478	156	F84E21007910007	F84E21007910007	79487,56	79487,56	79487,56	79487,56
3000001478	152	F84E21007910007	F84E21007910007	145448,23	145448,23	145448,23	145448,23
3000001478	157	F84E21007910007	F84E21007910007	97034,49	97034,49	97034,49	97034,49
3000001478	147	F84E21007910007	F84E21007910007	78785,70	78785,70	78785,70	78785,70
3000001478	149	F84E21007910007	F84E21007910007	633093,04	633093,04	633093,04	633093,04
3000001478	151	F84E21007910007	F84E21007910007	97209,97	97209,97	97209,97	97209,97
3000001478	64	F84E21007910007	F84E21007910007	31584,46	31584,46	31584,46	31584,46
3000001478	63	F84E21007910007	F84E21007910007	43340,90	43340,90	43340,90	43340,90
3000001478	62	F84E21007910007	F84E21007910007	139673,52	139673,52	139673,52	139673,52
3000001478	61	F84E21007910007	F84E21007910007	58255,79	58255,79	58255,79	58255,79
3000001478	57	F84E21007910007	F84E21007910007	60712,36	60712,36	60712,36	60712,36
3000001478	56	F84E21007910007	F84E21007910007	232979,23	232979,23	232979,23	232979,23
3000001478	55	F84E21007910007	F84E21007910007	127390,67	127390,67	127390,67	127390,67
3000001478	54	F84E21007910007	F84E21007910007	303561,79	303561,79	303561,79	303561,79
3000001478	65	F84E21007910007	F84E21007910007	85278,05	85278,05	85278,05	85278,05
3000001478	66	F84E21007910007	F84E21007910007	133532,10	133532,10	133532,10	133532,10
3000001478	60	F84E21007910007	F84E21007910007	97209,97	97209,97	97209,97	97209,97
3000001478	59	F84E21007910007	F84E21007910007	70538,63	70538,63	70538,63	70538,63
3000001478	58	F84E21007910007	F84E21007910007	41761,69	41761,69	41761,69	41761,69
3000001478	69	F84E21007910007	F84E21007910007	45972,94	45972,94	45972,94	45972,94
3000001478	67	F84E21007910007	F84E21007910007	109141,87	109141,87	109141,87	109141,87
3000001478	68	F84E21007910007	F84E21007910007	24214,76	24214,76	24214,76	24214,76
3000001478	41	F84E21007910007	F84E21007910007	267064,19	267064,19	267064,19	267064,19
				TOTALE	TOTALE	TOTALE	TOTALE
				5035174,65	5035174,65	5035174,65	5035174,65

In risposta alle richieste istruttorie formulate da questa Sezione gli Enti competenti hanno trasmesso anche una tabella inclusiva del prospetto “Elenco spese Investimento 1.5”, riportante il dettaglio delle spese sostenute nell’anno 2022 e 2023, distinte per ciascun WP e rispetto alle modalità attuative adottate (“operazioni a regia” e “operazioni a titolarità”). Dalla tabella in esame si evince che il totale derivante dalla somma degli importi liquidati a titolarità nel 2023 e di quelli liquidati a regia nello stesso anno ammonta a 40.063.048,02 €.

Occorre evidenziare che nella nota collocata all’interno della colonna relativa agli Importi liquidati a regia nel 2023 e in corrispondenza del WP7 * (Rete di Computer Emergency Response Team – CERT) si deve tener conto di quanto disposto per l’Avviso a sportello (Avviso n. 6) “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”, il cui importo complessivo stanziato a seguito del rifinanziamento avvenuto con determina del 30 novembre 2023 – così come già esplicitato nel capitolo 3 – ammonta a euro 28.490.306,51. Anche in questo caso i dati forniti dalle Amministrazioni sono aggiornati alla data del 12 dicembre 2023.

Elenco spese Investimento 1.5					
Work Package	Dotazione Finanziaria	Importi liquidati titolarità nel 2022	Importi liquidati titolarità nel 2023	Importi liquidati regia nel 2023	Importi totali Liquidati
WP1 -Project Management	8.000.000,00 €	1.228.102,64 €	1.314.943,8 €	N/A	2.543.046,46 €
WP2 -Agenzia per la Cybersicurezza Nazionale	53.000.000,00 €	2.388.934,68 €	7.375.782,04 €	N/A	9.764.716,70 €
WP3 -HyperSOC	18.000.000,00 €	1.337.602,08 €	5.504.673,12 €	N/A	6.842.275,21 €
WP4 -Servizi PSNC e NIS	12.600.000,00 €	327.585,31 €	1.297.628,46 €	N/A	1.625.213,77 €
WP5 -High Performance Computing e Artificial Intelligence/Machine Learning	30.000.000,00 €	92.296,82 €	218.283,74 €	N/A	310.580,56 €
WP6 -Information Sharing and Analysis Center (ISAC)	12.300.000,00 €	389.541,72 €	1.489.334,74 €	N/A	1.878.876,46 €
WP7 -Rete di Computer Emergency Response Team (CERT)	32.000.000,00 €	97.034,49 €	175.820,18 €	*	272.854,67 €
WP8 -Ispezioni PSNC e NIS	8.000.000,00 €	-	218.565,44 €	N/A	218.565,44 €
WP9 -Interventi di potenziamento cyber per la PA	4151.750.000,00 €	119.899,45 €	3.159.838,59 €	1.977.337,43 €	5.257.075,46 €
WP10 -Interventi di potenziamento cyber-defence	150.000.000,00 €	N/A	N/A	14.400.000,00 €	14.400.000,00 €
WP11 -Centro di Valutazione e Certificazione Nazionale (CVCN) e i Centri di Valutazione (CV) di Interno e Difesa	35.350.000,00 €	-	291.278,48 €	1.850.000,00 €	2.141.278,48 €
WP12 -Rete di laboratori di scrutinio e certificazione tecnologica	4112.000.000,00 €	60.197,30 €	-	789.562,00 €	849.759,30 €
TOTALE euro	623.000.000,00	6.041.194,49 €	21.046.148,59 €	19.016.899,43	46.104.242,51

Dall'analisi della tabella in esame emerge che nel corso 2022 non sono state liquidate somme nell'ambito delle operazioni a regia, mentre per quanto concerne la dotazione finanziaria attribuita per le attività progettuali afferenti da WP n. 9 al WP n. 12, anche in questo caso, così come per la tabella concernente le risorse impegnate per il 2023, si deve tener conto che è in fase di valutazione una rimodulazione di circa 70.000.000,00 di euro.

In ultimo, nella citata nota istruttoria del 13 dicembre 2023, trasmessa congiuntamente dal Dipartimento per la trasformazione digitale e dall'Agenzia per la cybersicurezza si rappresenta che rispetto alla dotazione finanziaria complessiva dell'investimento, pari a 623.000.000 euro, allo stato in cui hanno elaborato i dati riportati si registrano impegni attivi per un totale di oltre 400 milioni. Di questi, circa 120 milioni riguardano attività a titolarità e circa 280 milioni riguardano attività a regia. Le spese già sostenute, infine, sono pari complessivamente a circa 46 milioni.

A seguito di successive interlocuzioni con l'Agenzia è stato possibile acquisire i dati aggregati delle spese sostenute per attività a titolarità e per attività a regia aggiornati al 31 dicembre 2023, visto che nel prospetto sopra riportato, come specificato in precedenza, i dati in esso indicati sono elaborati al 12 dicembre 2023.

Gli importi delle rispettive attività, pertanto, ammontano a euro 26.241.238,17 (per quelle a titolarità) e a euro 19.514.186,71 (per quelle a regia), il cui totale risulta pari a euro 45.755.424,88; importo, dunque, che non varia di molto rispetto a quello rappresentato nella tabella di cui sopra, intitolata " Elenco spese Investimento 1.5".

7. Stato di avanzamento dei milestone e target relativi all'Investimento in esame in relazione alla sua pianificazione per l'anno 2023

In ordine allo stato di avanzamento rispetto a target e milestone in prossima scadenza per l'Investimento 1.5, a seguito di diverse interlocuzioni scritte e orali intercorse con il Dipartimento per la trasformazione digitale e l'Agenzia per la cybersicurezza, è stato possibile acquisire una serie di informazioni utili che offrono un quadro di sintesi dell'argomento in esame, andando ad integrare, completandole, le informazioni già esposte da questa Sezione nei capitoli 3 e 5 del Rapporto di che trattasi. A tal proposito:

1. a) In merito al target M1C1-19, dalle risultanze prodotte dagli Enti di competenza

emerge che, nell'ambito del WP 9, il numero degli interventi connessi agli Avvisi presi in considerazione risultano essere complessivamente 160, rispettivamente:

- Avviso 1/2022: numero interventi = 13
- Avviso 2/2022: numero interventi = 21
- Avviso 3/2022: numero interventi = 75
- Avviso 7/2022: In tale ambito è stato fatto presente sia che la Determina di approvazione della graduatoria finale e di destinazione delle risorse dei 25 soggetti partecipanti all'Avviso è attualmente in fase di pubblicazione da parte dell'Agenzia, sia che in forza dell'Avviso medesimo verranno raggiunti 50 interventi, in considerazione del fatto che ogni Soggetto sarà interessato da almeno due interventi. Si ricorda, infatti, che il termine di presentazione delle domande per partecipare all'Avviso n. 7 scadeva il 5 dicembre 2023.

Dalle risultanze fornite dall'Agenzia emerge che il totale dei finanziamenti e rifinanziamenti legati alle somme stanziare in virtù dei primi 3 Avvisi (1, 2 e 3) ammonta a euro 87.039.114,29, suddiviso rispettivamente in: euro 15.501.860,43 per l'Avviso n.1, euro 7.850.000,00 per l'Avviso n. 2 ed euro 63.687.253,86 per l'Avviso n. 3.

Nel corso dell'istruttoria è stato fornito dagli Enti interessati un prospetto, che si riporta in calce a questo Report (Allegato 1), sugli "Approfondimento M1C1-19" nel quale viene riportato per ogni Avviso Pubblico afferente al M1C1-19, l'elenco degli interventi di interesse e il relativo stato progettuale (in corso, in conclusione, concluso), nonché il Soggetto Attuatore coinvolto.

1. b) Per quanto concerne la realizzazione degli interventi di potenziamento delle capacità di cyber-defense e alle attività di disegno e implementazione dei Centri di Valutazione (CV) del Ministero dell'Interno e Ministero della Difesa (WP 10 per risorse impegnate pari a 150 M), l'Agenzia evidenzia che, in ordine ai 6 Accordi di Collaborazione già stipulati nel 2022, sono in corso di esecuzione 6 interventi di potenziamento della capacità di cyber defence della PA. Nel succitato Allegato 1 vengono elencate anche le sei Amministrazioni coinvolte da tali Accordi, nonché gli interventi attivati e il relativo stato progettuale.

Nella determina pubblicata sul sito istituzionale dell’Agenzia, del 29 settembre 2022, è indicato che per attività di disegno e implementazione dei Centri di Valutazione (CV) del Ministero dell’Interno e Ministero della Difesa sono stati stanziati ulteriori 18.500.000,00 euro, in aggiunta ai 150 milioni iniziali. Si riporta, pertanto, qui di seguito la tabella contenuta nella succitata determina, con il dettaglio delle risorse impegnate a valere sul PNRR – Investimento 1.5 per ogni singola Amministrazione attuatrice degli interventi: Ministero della Difesa, Ministero dell’Interno, Arma dei Carabinieri, Guardia di Finanza, Ministero della Giustizia e Consiglio di Stato.

Amministrazione Attuatrice	Totale Risorse impegnate a valere sul PNRR -Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity”	CUP
Ministero della Difesa	49.250.000,00€	D46G21002310006
Ministero dell’Interno	67.250.000,00€	F56G22000400006 F86G22002210006 F86G22002220006
Arma dei Carabinieri	39.000.000,00€	D56G22000410006 D86G22000440006 D86G22000450006 D56G22000420006 D86G22000460006 D86G22000470006 D56G22000430006 D86G22000480006 D86G22000490006
Guardia di Finanza	7.000.000,00€	G56G21009570006
Ministero della Giustizia	5.000.000,00€	J51B22001240006
Consiglio di Stato	1.000.000,00€	B56G21056820003
TOTALE	168.500.000,00	

1. c) Dalla documentazione prodotta dall’Agenzia si evince che in merito agli interventi di potenziamento della PA in linea con le misure di sicurezza PSNC e NIS, che interessano in particolare gli Avvisi 1 e 2, allo stato attuale ne risultano completati 20, mentre 4 sono in via di conclusione. Si precisa, infine, che in tale contesto per il raggiungimento della Milestone, entro il 2024, dovranno essere

completati almeno 50 interventi, così come indicato nella tabella (estrapolata dal sistema REGIS) riportata nelle pagine seguenti, afferente i target e milestone europei da raggiungere e comprensiva sia degli ulteriori step procedurali che delle date programmate ed effettive di inizio e di fine attività.

1. d) Dalla documentazione inviata congiuntamente dal Dipartimento per la trasformazione digitale e dall'Agenzia per la Cybersicurezza si apprende, altresì, che è in fase di pubblicazione il nuovo Avviso Pubblico - Avviso n. 08 - per il finanziamento della PA locale che consentirà di incrementare significativamente l'impegno dei fondi disponibili tramite interventi a regia dedicati alla resilienza della PA.
- 2) Per quanto concerne la scheda fornita nel corso dell'istruttoria contenente elementi utili in merito al raggiungimento della milestone M1C1 - 21 "Rete dei laboratori, del CVCN e dei CV di Interno e Difesa", in relazione ai WP 1,2, 11 e 12, si rammenta che entro dicembre 2024 dovrà essere portata a compimento l'attivazione del CVCN, a seguito dell'adozione di tutti gli atti normativi necessari alla sua attivazione, così come anche evidenziato nella tabella riportata in fondo al presente capitolo sullo stato di avanzamento dei milestone e target. Gli Avvisi interessati sono il n. 4 e 5.

Per quanto attiene l'Avviso n. 4 – Avviso pubblico a sportello per la presentazione di interventi di potenziamento delle capacità di analisi e scrutinio software della P.A. centrale – di cui si è profusamente discusso nella deliberazione di questa Sezione n. 5 del 2023, è stato evidenziato che a seguito della chiusura del presente Avviso è stato attivato il primo laboratorio di scrutinio tecnologico presso il MEF, unica PA partecipante all'Avviso, così come da determina del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 14 ottobre 2022. Inoltre, risultano in fase di completamento le attività amministrative di gestione della domanda di rimborsi.

L'Avviso n. 5, invece, come ampiamente descritto nel capitolo 4 di questo Rapporto, è volto ad erogare dei contributi per l'attivazione di LAP a supporto delle attività di scrutinio tecnologico del CVCN per l'area di accreditamento Software e Network, e come anche evidenziato dall'Agenzia a seguito

dell'espletamento della fase istruttoria è stata pubblicata la determina di approvazione della graduatoria finale e di destinazione delle risorse, che ha previsto l'ammissione di 27 soggetti con corrispondente numero di progetti per il finanziamento dei laboratori di scrutinio tecnologico anche in ambito privato. Gli adempimenti successivi riguarderanno l'avvio della fase di attuazione delle 27 progettualità ammesse a finanziamento a valere sull'Avviso 5 e il completamento dei lavori dei CV del Ministero dell'Interno e del Ministero della Difesa.

3. a) 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 approfondita nel capitolo 4 di questo Rapporto.

Nel corso dell'istruttoria è stata così evidenziata la determina di ammissione a finanziamento dell'ACN del 30 novembre 2023, pubblicata sul relativo sito istituzionale, per un importo pari a 28.490.306,51 euro a valere sull'Avviso stesso, che si rivolge alle Regioni. In tale contesto, è previsto il collegamento dei CSIRT regionali con l'Agenzia entro dicembre 2024. Nella documentazione fornita è stato, inoltre, evidenziato che oltre quanto già in essere per gli CSIRT Regionali, si prevede la possibilità di stipulare Accordi di Collaborazioni con le PA centrali per supportare l'attivazione di CSIRT dicasteriali.

3. b) Nella nota istruttoria prodotta dall'Agenzia è stato, altresì, rappresentato che in linea con la Strategia Nazionale di Cybersicurezza, che formalizza l'architettura dei servizi cyber nazionali in attuazione del Cyber Shield europeo, HyperSOC, rete dei CERT, ISAC Italia:
- sono stati attivati i servizi di HyperSOC: almeno 5 SOC collegati entro dicembre 2024;
 - è in fase di attivazione entro l'anno l'ISAC Italia.

A tal proposito appare utile ricordare che:

- 1) HyperSOC è un sistema di monitoraggio nazionale delle minacce cyber volto a operare su molteplici fonti dati e volto a essere integrato con i diversi SOC della constituency al fine di migliorare le attività di detection di minacce emergenti;
 - 2) Rete CERT è una rete federata di centri di risposta e mitigazione di incidenti di natura cyber che possa lavorare a stretto contratto con lo CSIRT Italia, istituito presso l'Agenzia, al fine di fornire una risposta coordinata ed integrata su tutto il territorio nazionale;
 - 3) ISAC è un sistema centrale a supporto del miglioramento continuo dei servizi di info-sharing, nonché delle analisi settoriali volte allo sviluppo di una conoscenza avanzata di minacce emergenti e potenziali fattori di rischio sistemici.
3. c) È stato, altresì, posto l'accento sul fatto che a supporto dei servizi cyber nazionali, saranno potenziati i sistemi di gestione del rischio cyber nazionali, anche in attuazione dei servizi necessari alla piena realizzazione del PSNC e della NIS.
3. d) È stato, infine, rilevato che recentemente l'Agenzia per la Cybersicurezza ha stipulato l'accordo con Cineca. Sul sito dell'Agenzia si evince che trattasi di un protocollo d'intesa tra ACN e il consorzio Cineca, firmato in data 11 settembre 2023, nell'ambito dell'evento inaugurativo dell'ampliamento della sede di CINECA a Napoli con la realizzazione di un data center ad alta efficienza energetica.

L'accordo prevede una procedura ad evidenza pubblica - di cui Cineca sarà stazione appaltante - per l'acquisizione del sistema High Performance Computing (HPC) dell'Agenzia da collocare presso il nuovo centro di Napoli. Il sistema sarà dedicato, come previsto dal PNRR, al monitoraggio della minaccia cyber centrale, l'HyperSOC, anche attraverso l'utilizzo di strumenti di intelligenza artificiale e machine learning.

La collaborazione tra l'ACN e il CINECA, inoltre, riguarda anche specifiche attività di sviluppo e ricerca nel settore del calcolo ad alte prestazioni e la gestione condivisa dell'HPC dell'Agenzia.

Sul sito dell'Agenzia è specificato anche che complessivamente, gli investimenti per la realizzazione del centro di calcolo, l'acquisizione dei sistemi HPC e i costi

operativi e di gestione saranno dell'ordine di circa 50 milioni di euro, di cui oltre 20 messi a disposizione dall'ACN. Dunque, sottolinea l'Agenzia trattasi di un grande investimento che sostiene e consolida il ruolo del Mezzogiorno nell'ambito dell'innovazione tecnologica. Con questo progetto l'infrastruttura di calcolo nazionale si arricchisce di un importante nodo HPC, integrato nel sistema europeo di supercalcolo. Il sistema di Napoli, infatti, farà parte di una rete di sistemi complementari del supercomputer Leonardo, e consentirà di supportare non solo le applicazioni consolidate della fisica, della chimica, delle scienze ambientali e dell'ingegneria, ma soprattutto le applicazioni di apprendimento automatico e di intelligenza artificiale sia classica che generativa.

4. Milestone M1C1 22 sulla "Piena operatività unità di audit per le misure di sicurezza PSNC/NIS", legata al gruppo di attività WP 1, 2 e 8: a tal proposito, nella deliberazione n. 5 del 2023 della Sezione è stato posto in evidenza che si è già 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 protocollo n. 13214 del 14 ottobre 2022.

In ordine al processo di assunzione del personale del Servizio Certificazione e Vigilanza era stato pubblicato il bando di concorso del 2 febbraio 2022, per l'assunzione di 50 unità, 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, per quanto riguarda il reclutamento di ispettori qualificati, oltre all'assegnazione di personale da altre amministrazioni, sono state pubblicate le graduatorie finali dei bandi di concorso e concluse le relative assunzioni.

Nella scheda trasmessa dall'Agenzia a dicembre 2023, pertanto, è stato rappresentato che a seguito dell'istituzione dell'unità centrale ispettiva presso

l'Agenzia, nonché delle procedure concorsuali per l'assunzione di personale tecnico, entro dicembre 2024 dovranno essere completate almeno 30 ispezioni sulle misure di sicurezza PSNC e NIS.

È stato, altresì, rilevato che in linea con il Manuale dell'Organismo di Verifica e Ispezione, predisposto ai sensi della UNI CEI EN ISO/IEC, si dovrà procedere entro dicembre 2024 alla piena attivazione dell'unità ispettiva completando, da un lato, le piattaforme digitali dell'Agenzia a supporto delle attività di gestione delle ispezioni, dall'altro, le attività di formazione del personale e delle procedure interne di istruttoria per l'avvio delle ispezioni stesse. Risultano, invece, ultimate le attività di acquisizione dei corsi di formazione rivolti agli ispettori e completati 4 corsi di formazione.

Nel documento, infine, si sottolinea che è in corso di definizione la piena attivazione della piattaforma SIRIO per la gestione dei conferimenti pervenuti da PSNC e della piattaforma di gestione delle ispezioni.

A titolo esemplificativo si fornisce, qui di seguito, anche una tabella contenenti i dati estrapolati dal sistema REGIS (aggiornati al 31 dicembre 2023) relativi alle Milestone e Target di rilevanza europea, dalla quale risultano completati 4 milestone e 1 un target:

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	IN CORSO
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	IN CORSO
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	IN CORSO
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	IN CORSO
Target	M1C1-9	Sostegno al potenziamento delle strutture di sicurezza T1	31.12.2022	M1C1I1.5	COMPLETATO

Per completezza espositiva, si riporta qui di seguito 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 2023, sul sistema REGIS, componente Report Indicatori M&T.

Attività	Tipologia attività	Iter procedurale	Monitor Esecuzione	Stato	ID indicatore	Data fine prevista	Data fine aggiornata	Data fine effettiva	Note di dettaglio	Output atteso	Appunti
"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	Fase Completata	Completato	M1C1-8	31/12/2022	31/12/2022	31/12/2022	Definizione del nucleo ispettivo	Relazioni fornite a dimostrazione dell'avvio dell'unità centrale di audit	Pubblicazione del Bando di concorso per l'assunzione di 50 unità di personale a tempo indeterminato nei segmenti di Esperto
"Avvio della rete dei laboratori di screening e certificazione della cybersecurity M1C1-7"	Milestone UE	Inizio fornitura	Fase Completata	Completato	M1C1-7	31/12/2022	31/12/2022	31/12/2022		Documentazione fornita a dimostrazione dei processi e delle procedure individuati da condividere tra i laboratori e relazione fornita a dimostrazione dell'attivazione di almeno un laboratorio.	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/
"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	Nei Tempi	In corso	M1C1-21	31/12/2024	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.	Relazioni fornite che dimostrino la piena attivazione di almeno 10 laboratori, dei due centri di valutazione (CV) e l'attivazione del laboratorio di certificazione UE	Sono state avviate le attività volte all'attivazione dei Centri di Valutazione di Difesa e Interno

"Dispiego iniziale dei servizi nazionali di cybersecurity M1C1-6"	Milestone UE	Realizzazione delle forniture/acquisizione di beni	Fase Completata	Completato	M1C1-6	31/12/2022	31/12/2022	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)	Relazione che illustra l'architettura completa dei servizi nazionali di cybersecurity	Atti di organizzazione dell'Agenzia
---	--------------	--	-----------------	------------	--------	------------	------------	------------	--	---	-------------------------------------

"Dispiego integrale dei servizi nazionali di cybersecurity M1C1-20"	Milestone UE	Realizzazione delle forniture/acquisizione di beni	Nei Tempi	In corso	M1C1-20	31/12/2024	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.	Relazione che illustra la completa attivazione dei servizi nazionali di cybersecurity	Sono state avviate le attività relative agli ulteriori interventi di potenziamento delle strutture di sicurezza.
"Sostegno al potenziamento delle strutture di sicurezza T1 M1C1-9"	Target UE	Verifica raggiungimento Target	Fase Completata	Completato	M1C1-9	31/12/2022	31/12/2022	31/12/2022		Relazioni fornite a dimostrazione che siano avviati almeno cinque interventi di potenziamento delle capacità cyber della PA	Pubblicazione Avvisi di selezione per le amministrazioni oggetto di intervento

"Sostegno al potenziamento delle strutture di sicurezza T2 M1C1-19"	Target UE	Verifica raggiungimento Target	Nei Tempi	In corso	M1C1-19	31/12/2024	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).	Relazioni fornite a dimostrazione che siano avviati almeno cinquanta interventi di potenziamento delle capacità cyber della PA	Nuovi bandi per Fase 2 potenziamento PA
Adozione atti di organizzazione dell'Agenzia	Step procedurale	Approvazione Regolamento	Fase Completata	Completato		09/12/2021	09/12/2021	09/12/2021	Adottati atti di organizzazione dell'Agenzia	Atti normativi	Atti di organizzazione dell'Agenzia

Attivazione del CVCN	Step procedurale	Attivazione servizi	Fase Completata	Completato		30/06/2022	30/06/2022	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/	DPCM transito di funzioni dal MISE e atti interni	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/
Avanzamento attivazione dei Centri di Valutazione di Difesa e Interno	Step procedurale	Monitoraggio stato avanzamento target	Nei Tempi	In corso		31/12/2023	31/12/2023		In vista di M1C1-21	Atti dei Ministeri Competenti	Sono state avviate le attività volte all'attivazione dei Centri di Valutazione di Difesa e Interno
Avanzamento del sostegno al potenziamento delle strutture di sicurezza T2	Step procedurale	Monitoraggio stato avanzamento target	Nei Tempi	In corso		31/12/2023	31/12/2023		in vista di M1C1-19	Convenzioni	Sono state avviate le attività relative agli ulteriori interventi di potenziamento delle strutture di sicurezza.
Avanzamento nello stato di attivazione dei servizi nazionali di cybersecurity	Step procedurale	Monitoraggio stato avanzamento target	Nei Tempi	In corso		31/12/2023	31/12/2023		in vista di M1C1-20	Relazioni fornite a dimostrazione dell'attivazione	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	Nei Tempi	In corso		31/12/2023	31/12/2023		In vista del conseguimento della Milestone M1C1-21	Avvisi pubblici	Sono state avviate le attività volte all'attivazione della rete dei laboratori e dei centri di valutazione per la valutazione e certificazione della cybersecurity
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	Nei Tempi	In corso		31/12/2023	31/12/2023		In vista di M1C1-22	Atti interni	Sono state avviate le attività volte all'avanzamento verso la piena operatività dell'unità di audit per le misure di sicurezza PSNC e NIS con il completamento di almeno 15 ispezioni
Istituzione della nuova Agenzia per la cybersicurezza nazionale M1C1-5	Milestone UE	Istituzione Agenzia	Fase Completata	Completato	M1C1-5	31/12/2022	31/12/2022	31/12/2022		Atto amministrativo di istituzione	Atti di organizzazione dell'Agenzia
Nuove procedure di selezione delle amministrazioni oggetto di intervento	Step procedurale	Pubblicazione Avvisi/Bandi	Nei Tempi	In corso		31/12/2023	31/12/2023		Nuovi bandi per Fase 2 potenziamento PA	Avvisi pubblici	Nuovi bandi per Fase 2 potenziamento PA
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	Nei Tempi	In corso	M1C1-22	31/12/2024	31/12/2024			Relazioni fornite, relazioni di ispezione	Sono state avviate le attività volte all'avanzamento verso la piena operatività dell'unità di audit per le misure di sicurezza PSNC e NIS con il completamento di almeno 15 ispezioni

Procedure di selezione delle amministrazioni oggetto di intervento	Step procedurale	Pubblicazione Avvisi/Bandi	Fase Completata	Completato		01/07/2022	01/07/2022	01/07/2022		Avvisi pubblici	Pubblicazione Avvisi di selezione per le amministrazioni oggetto di intervento
Selezione profili professionali	Step procedurale	Pubblicazione Avvisi/Bandi	Fase Completata	Completato		22/02/2022	22/02/2022	22/02/2022	Bando di concorso per l'assunzione di 50 unità di personale a tempo indeterminato nei segmenti di Esperto	Documentazione interna	Pubblicazione del Bando di concorso per l'assunzione di 50 unità di personale a tempo indeterminato nei segmenti di Esperto

8. Stato di avanzamento dei progetti.

Per quanto concerne lo stato di avanzamento dei progetti coinvolti nell'investimento 1.5, si è proceduto 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 afferenti 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 112, all'interno dei quali 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.



Dalla componente in esame si evince, altresì, che il costo ammesso dei progetti in corso, comprensivo delle informazioni relative ai crediti di imposta, anche se ancora non presenti a sistema nella sezione dei progetti, ammonta a euro 444,56 milioni.

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:

- 1) Servizi a supporto dell'Agenzia per la cybersicurezza nazionale – Attività di costituzione operativa di ACN e successivo espletamento delle proprie funzioni: 192 milioni;
- 2) Nuove soluzioni basate su integrazioni di sistemi di monitoraggio cibernetico con sistemi C2, potenziamento SCADA e realizzazione centro di valutazione della difesa: 49 milioni;
- 3) Intervento creazione 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;
- 4) 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, UFO, centro di valutazione: 29 milioni di euro;
- 5) Beni e servizi per l'infrastruttura telematica dell'arma dei carabinieri: 20 milioni di euro.

Nella componente anagrafica dei progetti, tratta dal sistema Regis, sono registrati i dati relativi all'andamento di realizzazione di tutti i 112 progetti in corso:

PCM - DIPARTIM. TRASFORMAZIONE DIGITALE - Codice misura M1C1I1.5 Soggetto attuatore AGENZIA PER LA CYBERSICUREZZA NAZIONALE			
Codice Unico Progetto	Codice Locale Progetto	Descr. Titolo Progetto	Stato
F81B21008190007	F81B21008190007	Servizi a supporto dell'agenzia per la cybersicurezza - governance trasversale del programma	In Corso
F84E21007910007	F84E21007910007	Servizi a supporto dell'Agenzia per la Cybersicurezza Nazionale - Attività di costituzione operativa di ACN e successivo espletamento delle proprie funzioni	In Corso
F56G22000400006	F56G22000400006	PCM - DIPARTIM. TRASFORMAZIONE DIGITALE - Codice misura M1C1I1.5 +C2:H2Soggetto attuatore AGENZIA PER LA CYBERSICUREZZA NAZIONALE	In Corso
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	In Corso
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	In Corso
D46G21002310006	D46G21002310006	Nuove soluzioni basate su integrazione di sistemi di monitoraggio cibernetico con sistemi c2, potenziamento scada e realizzazione centro di valutazione della difesa	In Corso
G56G21009570006	G56G21009570006	Missione digitale	In Corso
B56G21056820003	B56G21056820003	Acquisto di soluzioni avanzate di cybersecurity	In Corso
J51B22001240006	J51B22001240006	Sicurezza dati ministero di giustizia	In Corso
D56G22000410006	D56G22000410006	Controllo remoto dei nodi	In Corso
D86G22000490006	D86G22000490006	SW HW DATACENTER ARMA	In Corso
E84I22000000006	07_WP9_RIST_AGDEM_1	Resilienza cyber Agenzia del Demanio	In Corso
G89B22000330006	05_WP9_RIST_AGDO_1	Postura di sicurezza awareness ADM	In Corso
G89B22000340006	06_WP9_RIST_AGDO_2	Governance e awareness personale ADM	In Corso
D86G21004980006	08_WP9_RIST_CAM_1	Sicurezza perimetro rete Camera	In Corso
H86G20000640006	10_WP9_RIST_CORTCOST_2	Licenze e servizi di supporto	In Corso
H86G21005760001	11_WP9_RIST_CORTCOST_3	Sala server della Corte Costituzionale	In Corso
H86G22000180005	09_WP9_RIST_CORTCOST_1	Incremento sicurezza CorteCostituzionale	In Corso
J84F22000800001	23_WP9_RIST_MAECEI_1	Adeguamento alle misure previste PSNC	In Corso
G86G22000230006	17_WP9_RIST_MEF_2	Security monitoring identity governance	In Corso
D86G21004990006	14_WP9_RIST_DIF_3	Nuclei Cyber Security proiettabili	In Corso
D51C22001320006	12_WP9_RIST_DIF_1	Incremento cultura cyber Security EI	In Corso
F89B22000130006	28_WP9_RIST_MITE_3	Cyber strategy & distributed visibility	In Corso
F89B22000140006	27_WP9_RIST_MITE_2	Posture Management & Attack Prevention	In Corso
F89B22000150006	26_WP9_RIST_MITE_1	Centralized Threat Monitoring	In Corso
J86G21007150006	03_WP9_RIST_PCM_3	User account Security Enforcement	In Corso
J86G21007160006	04_WP9_RIST_PCM_4	Client Security Enforcement	In Corso
J86G21007170006	02_WP9_RIST_PCM_2	Branch Office Security Enforcement	In Corso

I86G22000280006	22_WP9_RIST_SGPR_1	Potenziamento rilevamento eventi	In Corso
G84F22000630006	01_WP12_Rist_MEF_1	MEFLAB CYSEC	In Corso
D86G22000440006	D86G22000440006	INFRASTRUTTURA TELEMATICA CENTRALE DEL COMANDO GENERALE DELL'ARMA DEI CARABINIERI VIALE ROMANIA 45 SISTEMI DI INTRUSION DETECTION/PREVENTION	In Corso
D86G22000450006	D86G22000450006	Sistemi di discovery automatica di cose connesse alla rete dell'arma dei carabinieri	In Corso
D86G23000030006	D86G23000030006	Beni e servizi per l'infrastruttura telematica dell'arma dei carabinieri	In Corso
F89B22000160001	15_WP9_RIST_DVF_1	DIPARTIMENTO VIGILI DEL FUOCO UPGRADE PER IL POTENZIAMENTO DELLE capacità di monitoraggio del rischio cyber	In Corso
J14F22001120006	7_WP_9_RIST_REGIONE PIEMONTE	Transizione digitale e servizi sicuri	In Corso
B46G22015750004	45_WP_9_RIST_COMUNE DI MILANO	Cyber resilienza e potenziamento dei presidi	In Corso
B46G22015740004	44_WP_9_RIST_COMUNE DI MILANO	Analisi e miglioramento dei processi cyber	In Corso
H79B22000190001	37_WP_9_RIST_REGIONE VENETO	Assessment della postura Cyber	In Corso
J69B22000170006	19_WP_9_RIST_REGIONE CALABRIA	Strategia Cyber per la Regione Calabria	In Corso
E44F22005970006	64_WP_9_RIST_REGIONE EMILIA ROMAGNA	Realizzazione CSIRT EmiliaRomagna	In Corso
D66G21003160008	05_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	Potenziamento numero unico Emergenza Friuli	In Corso
D36G22000250006	70_WP_9_RIST_REGIONE MOLISE	Cybersecurity_r_molise	In Corso
E41B22004200006	67_WP_9_RIST_REGIONE EMILIA ROMAGNA	Potenziamento della resilienza EmiliaRomagna	In Corso
C61B22002620006	22_WP_9_RIST_PROVINCIA AUTONOMA DI TRENTO	Potenziamento della capacità cyber del trentino	In Corso
F84F22000850006	35_WP_9_RIST_REGIONE LAZIO	Security Enforcement Regione Lazio	In Corso
F81C22001910006	34_WP_9_RIST_REGIONE LAZIO	Rafforzamento cyber Defence Regione Lazio	In Corso
D76G22000390006	8_WP_9_RIST_COMUNE DI PALERMO	COCY Consapevolezza cyber	In Corso
B66G22017040006	56_WP_9_RIST_REGIONE CAMPANIA	Sinfonia	In Corso
G66G22000190008	63_WP_9_RIST_REGIONE SICILIA	SICUREZZA PERIMETRO INTERNO RTRS	In Corso
B59E22000100006	46_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	BozenAsset	In Corso
B31C22001720006	18_WP_9_RIST_REGIONE PUGLIA	CYBERSECURITY POSTURE ASSESSMENT Puglia	In Corso
B31C22001730006	17_WP_9_RIST_REGIONE PUGLIA	POTENZIAMENTO DNS SECURITY PER LA PUGLIA	In Corso
I67H22002880005	76_WP_9_RIST_REGIONE SICILIA	Cybervault per dati mission critical Bacino Orientale	In Corso
F49B22000100006	38_WP_9_RIST_COMUNE DI MESSINA	FORMAZIONE E PROCESSI PER LA CYBERSECURITY	In Corso

B59E22000110006	54_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	CERT territoriale dell'Alto Adige	In Corso
G36G22000250006	23_WP_9_RIST_REGIONE LIGURIA	Infrastruttura per bilanciamento workload	In Corso
F46G22000690006	42_WP_9_RIST_COMUNE DI MESSINA	POTENZIAMENTO SOC CYBERSECURITY Messina	In Corso
F31B22001080006	59_WP_9_RIST_COMUNE DI BOLOGNA	Linea progettuale 1 Bologna	In Corso
D66G22000350006	10_WP_9_RIST_COMUNE DI CATANIA	Analisi della postura di sicurezza Catania	In Corso
H11C22001670006	33_WP_9_RIST_COMUNE DI FIRENZE	CYBERSECURITY METROWIDE	In Corso
B69B22000330006	53_WP_9_RIST_COMUNE DI NAPOLI	Assessment ed evoluzione della postura Cyber	In Corso
F31B22001090006	60_WP_9_RIST_COMUNE DI BOLOGNA	Linea progettuale 2 Bologna	In Corso
J14F22001110006	6_WP_9_RIST_REGIONE PIEMONTE	Postazioni di lavoro a rete regionale Piemonte	In Corso
C17H22002830006	39_WP_9_RIST_COMUNE DI TORINO	Analisi e miglioramento cybersecurity della Torino	In Corso
B54F22007690006	72_WP_9_RIST_REGIONE VALLE D'AOSTA	Potenziamento resilienza cyber Valle d'Aosta	In Corso
H16G22000340006	2_WP_9_RIST_COMUNE DI FIRENZE	Cybersecurity Framework e tools	In Corso
J94F22001300006	27_WP_9_RIST_COMUNE DI BARI	Identity and Access Management CSIRT Puglia	In Corso
C17H22002840006	41_WP_9_RIST_COMUNE DI TORINO	incremento della consapevolezza del rischio cyber Torino	In Corso
J94F22001290006	40_WP_9_RIST_COMUNE DI BARI	definizione delle Cyber Strategy e formazione Cyber Security	In Corso
G29B21000000006	78_WP_9_RIST_COMUNE DI CAGLIARI	METROCAGLIARI ITSECURITY PROGETTO 1	In Corso
H79B22000180001	36_WP_9_RIST_REGIONE VENETO	sistemi propedeutici CERT Veneto	In Corso
E24E19000450002	69_WP_9_RIST_REGIONE SARDEGNA	GDPRSIBAR attività di sicurezza Sardegna	In Corso
J84F22000960006	16_WP_9_RIST_ROMA CAPITALE	Cyber Strategy di Roma Capitale	In Corso
D19B22000410006	32_WP_9_RIST_REGIONE TOSCANA	Gestione della qualità e miglioramento dei processi	In Corso
B37H22005440006	26_WP_9_RIST_COMUNE DI GENOVA	Analisi della Postura Cyber Genova	In Corso
H36G22000100006	62_WP_9_RIST_COMUNE DI REGGIO CALABRIA	ReggioCyber (RC)	In Corso
B39B22000840001	47_WP_9_RIST_REGIONE MARCHE	Rafforzamento dei processi cybersicurezza Marche	In Corso
G36G22000240006	4_WP_9_RIST_REGIONE BASILICATA	Centro per la cybersicurezza Regionale II Intervento	In Corso
J89B22000540001	14_WP_9_RIST_ROMA CAPITALE	Potenziamento cyber Roma Capitale	In Corso
C99B22000020006	12_WP_9_RIST_REGIONE ABRUZZO	cyber security cert sanità Regione Abruzzo	In Corso
F71B22001240006	58_WP_9_RIST_COMUNE DI VENEZIA	RESILIENZA CIBERNETICA COMUNE DI VENEZIA	In Corso

E87H22002580008	52_WP_9_RIST_REGIONE LOMBARDIA	Cyber Security Assessment Enti Sanitari Lombardia	In Corso
E87H22002560008	28_WP_9_RIST_REGIONE LOMBARDIA	Programma di sicurezza e protezione dei dati	In Corso
I64F22000070006	43_WP_9_RIST_REGIONE UMBRIA	Potenziamento cyber sanità umbra	In Corso
J83E23000060006	24_WP9_RIST_MAECI_2	MAECI HUMAN FIREWALL	In Corso
G36G22000230006	3_WP_9_RIST_REGIONE BASILICATA	Centro per la cybersicurezza regionale	In Corso
D76G22000400006	9_WP_9_RIST_COMUNE DI PALERMO	Resilienza cyber comune di palermo	In Corso
D66G22000340006	11_WP_9_RIST_COMUNE DI CATANIA	Potenziamento e sicurezza degli end-point	In Corso
C99B22000030006	13_WP_9_RIST_REGIONE ABRUZZO	Cert regionale dell'ambito della gestione delle acque	In Corso
J89B22000550001	15_WP_9_RIST_ROMA CAPITALE	Rafforzamento dei presidi di sicurezza Roma Capitale	In Corso
J69B22000160006	20_WP_9_RIST_REGIONE CALABRIA	Cybersicurezza servizi alle ASP e AO Regionali	In Corso
C64F22000320006	21_WP_9_RIST_PROVINCIA AUTONOMA DI TRENTO	Resilienza cyber per la provincia autonoma di trento	In Corso
G36G22000260006	24_WP_9_RIST_REGIONE LIGURIA	Adeguamento firewall e policy di sicurezza	In Corso
I64F22000060006	25_WP_9_RIST_REGIONE UMBRIA	Innalzamento livello di sicurezza regionale umbra	In Corso
D19B22000420006	31_WP_9_RIST_REGIONE TOSCANA	Disaster recovery e buisness continuity	In Corso
B69B22000310006	48_WP_9_RIST_COMUNE DI NAPOLI	Piattaforma soc/epp evoluto	In Corso
B39B22000850006	49_WP_9_RIST_REGIONE MARCHE	sicurezza servizi di assistenza sanitaria	In Corso
B69B22000320006	50_WP_9_RIST_COMUNE DI NAPOLI	Adozione framework zero trust access	In Corso
B59B22000690006	51_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	Ampliamento soc	In Corso
B66G22017050006	57_WP_9_RIST_REGIONE CAMPANIA	Cyber campania	In Corso
G66G22000200008	65_WP_9_RIST_REGIONE SICILIA	SICUREZZA ENDPOINT RTRS	In Corso
E41B22004190006	66_WP_9_RIST_REGIONE EMILIA ROMAGNA	Potenziamento cyber servizi sanitari regionali	In Corso
B53E22001890006	71_WP_9_RIST_REGIONE VALLE D'AOSTA	CYBER AWARENESS PA LOCALE DELLA VALLE D'AOSTA	In Corso
F71B22001250006	73_WP_9_RIST_COMUNE DI VENEZIA	PIANO DI CYBERSECURITY AWARENESS	In Corso
F76G22000380006	74_WP_9_RIST_COMUNE DI VENEZIA	TECNOLOGIE A MITIGAZIONE DEL RISCHIO CYBER	In Corso
E24I22000010005	75_WP_9_RIST_REGIONE SARDEGNA	potenziamento del sistema informativo regionale ambientale	In Corso
G29B22000280001	79_WP_9_RIST_COMUNE DI CAGLIARI	METROCAGLIARI IT-SECURITY PROGETTO 2	In Corso
F66G23000100006	2_WP12_A5_Innovation	INNONATION CYBER SECURITY LAB	In Corso
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	In Corso

D21C22001380008	29_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	REGIONE FRIULI VENEZIA GIULIA Cyber Iniziative	In Corso
D21C22001400008	30_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	Cybersecurity FVG: Training&Awareness	In Corso
F83E22000060006	55_WP_9_RIST_REGIONE LAZIO	Piano di Security Awareness Regione Lazio	In Corso

In relazione ai 112 progetti, il costo ammesso dei progetti in corso, come già detto in precedenza, ammonta a euro 444,56 milioni. Nella tabella qui di seguito in evidenza, pertanto, è possibile visualizzare sia i titoli di ogni singolo progetto in corso, che i relativi costi. Nella penultima colonna, infine, sono riportate le date programmate per la conclusione di ogni singolo progetto in corso estrapolate al 31 dicembre 2023.

Titolo progetto	Codice CUP	Codice Locale di Progetto (CLP)	Data fine prevista progetto	Costo ammesso progetti
cyber security cert sanit regione abruzzo	C99B22000020006	12_WP_9_RIST_REGIONE ABRUZZO	30.11.2024	999.936,4
cyber strategy di roma capitale	J84F22000960006	16_WP_9_RIST_ROMA CAPITALE	30.11.2024	856.000
cybersicurezza servizi alle asp e ao regionali	J69B22000160006	20_WP_9_RIST_REGIONE CALABRIA	23.09.2024	897.397,23
governance e awareness personale adm	G89B22000340006	06_WP9_RIST_AGDO_2	07.05.2024	1.109.590
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	9.250.000
piano di cybersecurity awareness	F71B22001250006	73_WP_9_RIST_COMUNE DI VENEZIA	30.11.2024	428.000
potenziamento del sistema informativo regionale ambientale	E24I22000010005	75_WP_9_RIST_REGIONE SARDEGNA	30.11.2024	998.834,25
sicurezza servizi di assistenza sanitaria	B39B22000850006	49_WP_9_RIST_REGIONE MARCHE	30.11.2024	998.631

sistemi propedeutici cert veneto	H79B22000180001	36_WP_9_RIST_REGIONE VENETO	30.11.2024	1.000.000
tecnologie a mitigazione del rischio cyber	F76G22000380006	74_WP_9_RIST_COMUNE DI VENEZIA	30.11.2024	583.150
acquisto di soluzioni avanzate di cybersecurity	B56G21056820003	B56G21056820003	31.12.2023	1.000.000
adeguamento alle misure previste psnc	J84F22000800001	23_WP9_RIST_MAECL_1	30.09.2023	896.453,46
adeguamento firewall e policy di sicurezza	G36G22000260006	24_WP_9_RIST_REGIONE LIGURIA	30.11.2024	975.000
adozione framework zero trust access	B69B22000320006	50_WP_9_RIST_COMUNE DI NAPOLI	30.11.2024	605.740
ampliamento soc	B59B22000690006	51_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	30.11.2024	791.780
analisi della postura cyber genova	B37H22005440006	26_WP_9_RIST_COMUNE DI GENOVA	30.11.2024	648.649,6
analisi della postura di sicurezza catania	D66G22000350006	10_WP_9_RIST_COMUNE DI CATANIA	30.11.2024	1.000.000
analisi e miglioramento cybersecurity della torino	C17H22002830006	39_WP_9_RIST_COMUNE DI TORINO	30.11.2024	995.100
analisi e miglioramento dei processi cyber	B46G22015740004	44_WP_9_RIST_COMUNE DI MILANO	30.11.2024	999.380
assessment della postura cyber	H79B22000190001	37_WP_9_RIST_REGIONE VENETO	30.06.2024	1.000.000
assessment ed evoluzione della postura cyber	B69B22000330006	53_WP_9_RIST_COMUNE DI NAPOLI	31.10.2024	667.882
beni e servizi per l'infrastruttura telematica dell'arma dei carabinieri	D86G23000030006	D86G23000030006	31.12.2026	20.100.000
bozenasset	B59E22000100006	46_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	30.06.2023	456.890
branch office security enforcement	J86G21007170006	02_WP9_RIST_PCM_2	30.11.2024	363.006,55
centralized threat monitoring	F89B22000150006	26_WP9_RIST_MITE_1	31.12.2023	457.500
centro per la cybersicurezza regionale	G36G22000230006	3_WP_9_RIST_REGIONE BASILICATA	30.11.2024	999.180
centro per la cybersicurezza regionale ii intervento	G36G22000240006	4_WP_9_RIST_REGIONE BASILICATA	30.11.2024	1.000.000
cert regionale dell'ambito della gestione delle acque	C99B22000030006	13_WP_9_RIST_REGIONE ABRUZZO	30.11.2024	751.910

cert territoriale dell'alto adige	B59E22000110006	54_WP_9_RIST_PROVINCIA AUTONOMA DI BOLZANO	30.06.2023	749.299,6
client security enforcement	J86G21007160006	04_WP9_RIST_PCM_4	30.11.2024	586.647,64
cocy consapevolezza cyber	D76G22000390006	8_WP_9_RIST_COMUNE DI PALERMO	30.11.2024	992.104
controllo remoto dei nodi	D56G22000410006	D56G22000410006	30.06.2025	3.900.000
cyber awareness pa locale della valle d'aosta	B53E22001890006	71_WP_9_RIST_REGIONE VALLE D'AOSTA	20.11.2024	430.000
cyber campania	B66G22017050006	57_WP_9_RIST_REGIONE CAMPANIA	30.11.2024	976.000
cyber resilienza e potenziamento dei presidi	B46G22015750004	45_WP_9_RIST_COMUNE DI MILANO	30.11.2024	999.380
cyber security assessment enti sanitari lombardia	E87H22002580008	52_WP_9_RIST_REGIONE LOMBARDIA	31.12.2023	1.000.000
cyber strategy & distributed visibility	F89B22000130006	28_WP9_RIST_MITE_3	31.12.2023	519.720
cybersecurity framework e tools	H16G22000340006	2_WP_9_RIST_COMUNE DI FIRENZE	30.11.2024	988.200
cybersecurity fvg: training&awareness	D21C22001400008	30_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	30.11.2024	882.108
cybersecurity metrowide	H11C22001670006	33_WP_9_RIST_COMUNE DI FIRENZE	30.11.2024	999.180
cybersecurity posture assessment puglia	B31C22001720006	18_WP_9_RIST_REGIONE PUGLIA	30.11.2024	999.905,92
cybersecurity_r_molise	D36G22000250006	70_WP_9_RIST_REGIONE MOLISE	30.11.2024	1.000.000
cybervault per dati mission critical bacino orientale	I67H22002880005	76_WP_9_RIST_REGIONE SICILIA	30.11.2024	995.000
definizione delle cyber strategy e formazione cyber security	J94F22001290006	40_WP_9_RIST_COMUNE DI BARI	30.11.2024	818.550
dipartimento vigili del fuoco upgrade per il potenziamento delle capacit di monitoraggio del rischio cyber	F89B22000160001	15_WP9_RIST_DVF_1	30.11.2022	513.766
disaster recovery e buisness continuity	D19B22000420006	31_WP_9_RIST_REGIONE TOSCANA	30.11.2024	1.000.000
formazione e processi per la cybersecurity	F49B22000100006	38_WP_9_RIST_COMUNE DI MESSINA	30.11.2024	721.220,45
gdpr sbar attivit di sicurezza sardegna	E24E19000450002	69_WP_9_RIST_REGIONE SARDEGNA	30.11.2024	1.000.000

gestione della qualità e miglioramento dei processi	D19B22000410006	32_WP_9_RIST_REGIONE TOSCANA	31.12.2023	1.000.000
identity and access management csirt puglia	J94F22001300006	27_WP_9_RIST_COMUNE DI BARI	30.11.2024	995.100
incremento cultura cyber security ei	D51C22001320006	12_WP9_RIST_DIF_1	20.07.2022	123.571,2
incremento della consapevolezza del rischio cyber torino	C17H22002840006	41_WP_9_RIST_COMUNE DI TORINO	30.11.2024	995.100
incremento sicurezza cortecostituzionale	H86G22000180005	09_WP9_RIST_CORTCOST_1	30.11.2024	329.985,6
infrastruttura per bilanciamento workload	G36G22000250006	23_WP_9_RIST_REGIONE LIGURIA	30.11.2024	998.000
infrastruttura telematica centrale del comando generale dell'arma dei carabinieri viale romania 45 sistemi di intrusion detection/prevention	D86G22000440006	D86G22000440006	31.12.2025	2.000.000
innalzamento livello di sicurezza regionale umbra	I64F22000060006	25_WP_9_RIST_REGIONE UMBRIA	30.11.2024	1.000.000
innovation cyber security lab	F66G23000100006	2_WP12_A5_Innovation	30.09.2023	72.020
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	F56G22000400006	F56G22000400006	31.03.2026	29.000.000
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	29.000.000
licenze e servizi di supporto	H86G20000640006	10_WP9_RIST_CORTCOST_2	26.04.2024	386.004,28
linea progettuale 1 bologna	F31B22001080006	59_WP_9_RIST_COMUNE DI BOLOGNA	30.11.2024	1.000.000

linea progettuale 2 bologna	F31B22001090006	60_WP_9_RIST_COMUNE DI BOLOGNA	30.11.2024	998.692
maeci human firewall	J83E23000060006	24_WP9_RIST_MAECI_2	30.11.2024	446.062,5
meflab cysec	G84F22000630006	01_WP12_Rist_MEF_1	31.12.2022	1.160.000
metroagliari it-security progetto 2	G29B22000280001	79_WP_9_RIST_COMUNE DI CAGLIARI	30.11.2024	999.095,53
metroagliari itsecurity progetto 1	G29B21000000006	78_WP_9_RIST_COMUNE DI CAGLIARI	30.11.2024	999.893,85
missione digitale	G56G21009570006	G56G21009570006	29.11.2024	7.000.000
nuclei cyber security proiettabili	D86G21004990006	14_WP9_RIST_DIF_3	30.11.2022	1.334.640,13
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	49.250.000
piano di security awareness regione lazio	F83E22000060006	55_WP_9_RIST_REGIONE LAZIO	30.11.2024	770.186
piattaforma soc/epp evoluto	B69B22000310006	48_WP_9_RIST_COMUNE DI NAPOLI	30.11.2024	726.074
postazioni di lavoro a rete regionale piemonte	J14F22001110006	6_WP_9_RIST_REGIONE PIEMONTE	30.11.2024	984.400
postura di sicurezza awareness adm	G89B22000330006	05_WP9_RIST_AGDO_1	30.09.2024	789.767
posture management & attack prevention	F89B22000140006	27_WP9_RIST_MITE_2	31.12.2023	1.018.700
potenziamento cyber sanit umbra	I64F22000070006	43_WP_9_RIST_REGIONE UMBRIA	30.11.2024	1.000.000
potenziamento cyber servizi sanitari regionali	E41B22004190006	66_WP_9_RIST_REGIONE EMILIA ROMAGNA	30.11.2024	600.000
potenziamento cyber roma capitale	J89B22000540001	14_WP_9_RIST_ROMA CAPITALE	30.11.2024	995.100
potenziamento della capacit cyber del trentino	C61B22002620006	22_WP_9_RIST_PROVINCIA AUTONOMA DI TRENTO	30.11.2024	951.597,44
potenziamento della resilienza emiliaromagna	E41B22004200006	67_WP_9_RIST_REGIONE EMILIA ROMAGNA	30.11.2024	700.000
potenziamento dns security per la puglia	B31C22001730006	17_WP_9_RIST_REGIONE PUGLIA	30.11.2024	999.605,47

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	541.788,67
potenziamento e sicurezza degli end-point	D66G22000340006	11_WP_9_RIST_COMUNE DI CATANIA	30.11.2024	1.000.000
potenziamento numero unico emergenza friuli	D66G21003160008	05_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	30.11.2024	665.871,95
potenziamento resilienza cyber valle daosta	B54F22007690006	72_WP_9_RIST_REGIONE VALLE D'AOSTA	30.11.2024	920.000
potenziamento rilevamento eventi	I86G22000280006	22_WP9_RIST_SGPR_1	30.11.2022	1.026.430,16
potenziamento soc cybersecurity messina	F46G22000690006	42_WP_9_RIST_COMUNE DI MESSINA	30.11.2024	846.456,19
programma di sicurezza e protezione dei dati	E87H22002560008	28_WP_9_RIST_REGIONE LOMBARDIA	30.11.2024	1.000.000
rafforzamento cyber defence regione lazio	F81C22001910006	34_WP_9_RIST_REGIONE LAZIO	31.10.2024	717.970
rafforzamento dei presidi di sicurezza roma capitale	J89B22000550001	15_WP_9_RIST_ROMA CAPITALE	30.11.2024	148.730
rafforzamento dei processi cybersicurezza marche	B39B22000840001	47_WP_9_RIST_REGIONE MARCHE	30.11.2024	999.936,4
realizzazione csirt emiliaromagna	E44F22005970006	64_WP_9_RIST_REGIONE EMILIA ROMAGNA	30.11.2024	700.000
reggiocyber (rc)	H36G22000100006	62_WP_9_RIST_COMUNE DI REGGIO CALABRIA	30.11.2024	999.754
regione friuli venezia giulia cyber iniziative	D21C22001380008	29_WP_9_RIST_REGIONE FRIULI VENEZIA GIULIA	30.06.2023	334.128
resilienza cibernetica comune di venezia	F71B22001240006	58_WP_9_RIST_COMUNE DI VENEZIA	30.11.2024	240.750
resilienza cyber agenzia del demanio	E84I22000000006	07_WP9_RIST_AGDEM_1	30.11.2022	284.600
resilienza cyber comune di palermo	D76G22000400006	9_WP_9_RIST_COMUNE DI PALERMO	30.11.2024	999.422,64
resilienza cyber per la provincia autonoma di trento	C64F22000320006	21_WP_9_RIST_PROVINCIA AUTONOMA DI TRENTO	31.10.2024	757.132
sala server della corte costituzionale	H86G21005760001	11_WP9_RIST_CORTCOST_3	30.10.2022	325.714,82
security enforcement regione lazio	F84F22000850006	35_WP_9_RIST_REGIONE LAZIO	30.11.2024	511.716,8

security monitoring identity governance	G86G22000230006	17_WP9_RIST_MEF_2	30.11.2024	1.997.135,52
servizi a supporto dell'agenzia per la cybersicurezza - governance trasversale del programma	F81B21008190007	F81B21008190007	30.06.2026	3.789.015
servizi a supporto dell'agenzia per la cybersicurezza nazionale - attivit di costituzione operativa di acn e successivo espletamento delle proprie funzioni	F84E21007910007	F84E21007910007	30.06.2026	192.160.985
sicurezza perimetro rete camera	D86G21004980006	08_WP9_RIST_CAM_1	31.12.2023	1.100.000
sicurezza dati ministero di giustizia	J51B22001240006	J51B22001240006	30.09.2025	5.000.000
sicurezza endpoint rtrs	G66G22000200008	65_WP_9_RIST_REGIONE SICILIA	31.12.2023	5.298,19
sicurezza perimetro interno rtrs	G66G22000190008	63_WP_9_RIST_REGIONE SICILIA	31.12.2023	999.701,81
sinfonia	B66G22017040006	56_WP_9_RIST_REGIONE CAMPANIA	30.09.2024	966.188,31
sistemi di discovery automatica di cose connesse alla rete dell'arma dei carabinieri	D86G22000450006	D86G22000450006	31.12.2026	7.000.000
strategia cyber per la regione calabria	J69B22000170006	19_WP_9_RIST_REGIONE CALABRIA	30.12.2023	961.844,83
Sw HW Datacwnter Arma	D86G22000490006	D86G22000490006	31.12.2026	6.000.000
Transizione digitale e servizi sicuri	J14F22001120006	7_WP_9_RIST_REGIONE PIEMONTE	30.11.2024	995.100
User account Security Enforcement	J86G21007150006	03_WP9_RIST_PCM_3	30.11.2024	1.042.702,5
TOTALE				444.563.060

Nella tabella appena esposta si può notare come a fronte dei 112 progetti in corso, alcuni progetti riportano come data di conclusione il 30-31 dicembre 2023. A tal riguardo, a seguito di interlocuzione con i referenti dell'Agenzia per la cybersicurezza è stato fornito dalla stessa un prospetto riportante gli approfondimenti dei progetti che presentano un ritardo, in cui si indicano in modo dettagliato le motivazioni per ogni singolo progetto che presenta come "data di fine prevista" il 2023.

Approfondimento sui progetti in ritardo

Data di fine progetto in ReGiS confermata allo stato attuale

Data di fine progetto in ReGiS posticipata

Tipologia Avviso	Soggetto attuatore	CUP	CLP	Data di fine prevista	Riscontro
Avviso n. 01/2022	Ministero dell'Ambiente e della Sicurezza Energetica	F89B22000150006	26_WP9_Rist_MITE_1	31.12.2023	In base alle informazioni fornite in fase di monitoraggio progettuale, i progetti dovrebbero essere terminati. Si rimane in attesa della relativa domanda di rimborso da parte del Soggetto Attuatore.
		F89B22000140006	27_WP9_Rist_MITE_2	31.12.2023	
		F89B22000130006	28_WP9_Rist_MITE_3	31.12.2023	
	Camera dei deputati	D86G21004980006	08_WP9_Rist_CAM_1	31.12.2023	Progetto terminato il 30 settembre 2023, per il quale è stata presentata la domanda di rimborso. ACN ha analizzato la documentazione e richiesto ulteriori integrazioni.
	Ministero degli affari esteri e della cooperazione internazionale	J84F22000800001	23_WP9_Rist_MAECL_1	30.09.2023	
Avviso n. 03/2022	Regione Calabria	J69B22000170006	19_WP_9_rist_Regione Calabria	30.12.2023	In base alle informazioni fornite durante l'ultimo monitoraggio progettuale effettuato (sett-ott 2023), il SA dichiara un avanzamento in linea con la data di conclusione. Si rimane pertanto in attesa della relativa domanda di rimborso.
	Regione Toscana	D19B22000410006	32_WP_9_rist_Regione Toscana	31.12.2023	Pervenuta una richiesta di modifica al cronoprogramma progettuale, valutata positivamente dall'ACN, che posticipa la fine del progetto al 30.11.2024. E' stato di conseguenza aggiornato il sistema ReGiS.
	Provincia Autonoma di Bolzano	B59E22000100006	46_WP_9_rist_Provinsi a autonoma di Bolzano	30.06.2023	Pervenuta una richiesta di modifica al cronoprogramma progettuale, valutata positivamente dall'ACN, che posticipa la fine del progetto al 30.11.2024. E' stato di conseguenza aggiornato il sistema ReGiS.
		B59E22000110006	54_WP_9_rist_Provinsi a autonoma di Bolzano	30.06.2023	Pervenuta una richiesta di modifica al cronoprogramma progettuale, valutata positivamente dall'ACN, che posticipa la fine del progetto al 30.11.2024. E' stato di conseguenza aggiornato il sistema ReGiS.
	Regione Lombardia	E87H22002580008	52_WP_9_rist_Regione Lombardia	31.12.2023	In base alle ultime interlocuzioni fornite dal Soggetto Attuatore in fase di monitoraggio progettuale, il progetto dovrebbe essere concluso. Si rimane in attesa della relativa domanda di rimborso da parte del Soggetto Attuatore.
	Regione Sicilia	G66G22000190008	63_WP_9_rist_Regione Sicilia	31.12.2023	Pervenuta una richiesta di modifica al cronoprogramma progettuale, valutata positivamente dall'ACN, che posticipa la fine del progetto al 30.06.2024. E' stato di conseguenza aggiornato il sistema ReGiS.
		G66G22000200008	65_WP_9_rist_Regione Sicilia	31.12.2023	Pervenuta una richiesta di modifica al cronoprogramma progettuale, valutata positivamente dall'ACN, che posticipa la fine del progetto al 30.09.2024. E' stato di conseguenza aggiornato il sistema ReGiS.
	Regione Friuli Venezia Giulia	D21C22001380008	29_WP_9_rist_Regione Friuli Venezia Giulia	30.06.2023	In base alle ultime interlocuzioni fornite dal Soggetto Attuatore in fase di monitoraggio progettuale, il progetto dovrebbe essere concluso. Si rimane in attesa della relativa domanda di rimborso da parte del Soggetto Attuatore.



Finanziato dall'Unione europea NextGenerationEU



DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE



2

A seguito della disamina svolta in materia l'Agenzia per la cybersicurezza ha osservato in conclusione che tutti i progetti non riportano comunque criticità rispetto al raggiungimento delle Milestone & Target dell'Investimento 1.5.

9. Conclusioni.

L'attività svolta dall'Agenzia nel corso del 2023 offre una panoramica generale sulle attività, dati e progettualità, mostrando il processo di maturazione della stessa che ha portato tale Istituto 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.

Il lavoro svolto dall'Agenzia a tutela degli interessi nazionali nel campo della cybersicurezza, ha comportato un dialogo costante con le Amministrazioni che compongono l'architettura nazionale, incoraggiando, parimenti, 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 lavoro è stato compiuto lavorando 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.

Tale positivo approccio risulta concretato in un numero complessivo di 112 progetti in corso di ammontare pari a euro 444,56 milioni (oltre il 70% del valore complessivo dell'investimento), all'interno dei quali è possibile distinguere 3 tipologie progettuali relative all'acquisto di beni, all'acquisto o realizzazione di servizi e infine a concessioni di incentivi ad unità produttive, nell'ambito delle quali è constatabile la massima concentrazione nell'acquisto o realizzazione di servizi (77,68%), seguito dall'acquisto di beni (21,43%), mentre poco è stato destinato alla concessione di incentivi (0,89%).

Va notato peraltro che i progetti in esame spaziano sull'intero arco di vigenza del Piano (e quindi con scadenze anche nel 2024/2026) e che quindi non tutte le risorse disponibili risultano tuttora impiegate nell'ambito delle finalità proprie dell'Agenzia la cui recente creazione, si rammenta, ha richiesto uno sforzo organizzativo in partenza certamente non scevro di difficoltà e complessità anche in ordine alle tipologie di interventi da realizzare.

Peraltro, come evidenziato nella relazione, l'ultimazione di taluni progetti, pur se in misura minoritaria, la cui scadenza era stata programmata nel corso od alla fine del 2023, è stata posticipata ad altra data del 2024. Si tratta di progetti di cui l'Agenzia non è soggetto attuatore e per i quali – soprattutto quelli affidati per la realizzazione ad Amministrazioni centrali – in realtà si attende solo la richiesta di rimborso.

In ogni caso, non emergono difficoltà sostanziali e criticità nel raggiungimento

degli obiettivi da parte dell'Agenzia. Una valutazione di merito sulla efficacia complessiva dell'attività in corso potrà essere effettuata solo una volta ricomposto il quadro dei numerosi progetti previsti ed in fase di realizzazione, motivo per cui proseguirà il costante monitoraggio dell'intero complesso degli interventi e delle interazioni da essi determinate.

ALLEGATO 1
“Approfondimento M1C1-19”

Avviso/Accordo	ID Progetto	Soggetto Attuatore	Interventi	Stato
02/2022	N.A.	MIMIT	Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber, Analisi delle capacità dei sistemi e strumenti di sicurezza in essere	Concluso
02/2022	N.A.	MIMIT	Analisi di valutazione del rischio eseguita sui principali asset dell'organizzazione, Revisione e potenziamento dei processi e metodologie di sviluppo sicuro, Revisione e potenziamento dei processi a supporto della continuità operativa	Concluso
02/2022	N.A.	MAECI	Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber, Revisione e potenziamento della metodologia di Cyber Risk Management	Concluso
02/2022	N.A.	MAECI	Analisi di valutazione del rischio eseguita sui principali asset dell'organizzazione, Revisione e potenziamento del processo e delle relative procedure di risposta ad attacchi ransomware, o incidenti di natura cyber, Revisione e potenziamento dei processi di rilevazione e gestione delle	Concluso
02/2022	N.A.	PCM	Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber, Analisi dei processi e strumenti di gestione delle identità digitali	Concluso
02/2022	N.A.	PCM	Revisione e potenziamento del processo e delle relative procedure di risposta ad attacchi ransomware, o incidenti di natura cyber, Revisione e potenziamento della metodologia di Cyber Risk Management, Potenziamento framework documentale (Revisione e potenziamento dei processi a supporto	Concluso
02/2022	N.A.	MEF	Analisi dei processi e strumenti di gestione delle identità digitali, (Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber)	In conclusione
02/2022	N.A.	MEF	Revisione e potenziamento del processo e delle relative procedure di risposta ad attacchi ransomware, o incidenti di natura cyber, Revisione e potenziamento dei processi di rilevazione e gestione delle vulnerabilità (processo di revisione del codice, processo di vulnerability assessment,	In conclusione
02/2022	N.A.	MEF	Revisione e potenziamento dei processi e metodologie di security-by-design, Revisione e potenziamento del processo di gestione delle identità digitali e degli accessi ai sistemi informativi	In conclusione
02/2022	N.A.	MDS	Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber, Analisi delle capacità dei sistemi e strumenti di sicurezza in essere	Concluso
02/2022	N.A.	MDS	Revisione e potenziamento dei processi e metodologie di security-by-design, Revisione e potenziamento della metodologia di Cyber Risk Management, Servizi di Cyber Security Awareness (ad es. contrasto mail di phishing)	Concluso
02/2022	N.A.	MIT	Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber, Analisi delle capacità dei sistemi e strumenti di sicurezza in essere	Concluso
02/2022	N.A.	MIT	Analisi dei processi e strumenti di gestione delle identità digitali, Analisi di valutazione del rischio eseguita sui principali asset dell'organizzazione, Revisione e potenziamento del processo e delle relative procedure di risposta ad attacchi ransomware, o incidenti di natura cyber	Concluso
02/2022	N.A.	AgDem	Intervento complessivo	Concluso
02/2022	N.A.	Senato	Intervento complessivo	Concluso
02/2022	N.A.	DVF	Revisione e potenziamento del processo e delle relative procedure di risposta ad attacchi ransomware, o incidenti di natura cyber, Supporto in ambito Network Security analisi della rete e piano di reingegnerizzazione	Concluso
02/2022	N.A.	DVF	Revisione e potenziamento dei processi e metodologie di sviluppo sicuro, Servizi di Cyber Security Awareness (ad es. contrasto mail di phishing), Revisione e potenziamento del processo di gestione delle identità digitali e degli accessi ai sistemi informativi	Concluso
02/2022	N.A.	Camera	Revisione e potenziamento del processo e delle relative procedure di risposta ad attacchi ransomware, o incidenti di natura cyber, Servizi di Cyber Security Awareness (ad es. contrasto mail di phishing)	Concluso
02/2022	N.A.	DPC	Revisione e potenziamento dei processi a supporto della continuità operativa, Servizi di Cyber Security Awareness (ad es. contrasto mail di phishing)	In conclusione
02/2022	N.A.	DPC	Revisione e potenziamento dei processi di rilevazione e gestione delle vulnerabilità (processo di revisione del codice, processo di vulnerability assessment, processodi penetration test, processo di gestione dei piani di rimedio), Revisione e potenziamento del processo di gestione delle identità	Concluso
02/2022	N.A.	MD	Intervento complessivo	Concluso
01/2022	05_WP9_Rist_AgDO_1	Agenzia delle Dogane e dei Monopoli	Intervento 1- Resilienza cibernetica ADM: postura di sicurezza e potenziamento dell'awareness	In corso
01/2022	06_WP9_Rist_AgDO_2	Agenzia delle Dogane e dei Monopoli	Intervento 2 - Resilienza cibernetica ADM: modello di governance e awareness del personale	In corso
01/2022	08_WP9_Rist_CAM_1	Camera	Ammodernamento e messa in sicurezza del perimetro interno ed esterno della rete Camera	In corso

01/2022	11_WP9_Rist_CORTCOST_3	Corte Costituzionale	Adeguamento hw e sw sala server della corte costituzionale	Concluso
01/2022	10_WP9_Rist_CORTCOST_2	Corte Costituzionale	Acquisizione di nuovi servizi e strumenti (licenze e servizi di supporto)	In corso
01/2022	15_WP9_Rist_DVF_1	DVF	Upgrade dei tool per il potenziamento delle capacità di monitoraggio del rischio cyber	In corso
01/2022	23_WP9_Rist_MAECl_1	MAECI	Adeguamento alle misure previste dal PSNC	Concluso
01/2022	14_WP9_Rist_DIF_3	MD	Ammodernamento equipaggiamento per nuclei Cyber Security proiettabili (SIEM Tattici EI)	In corso
01/2022	12_WP9_Rist_DIF_1	MD	Sviluppo applicazione per incrementare cultura cyber security per EI	In corso
01/2022	28_WP9_Rist_MITE_3	MITE	Cyber Strategy & Distributed	In corso
01/2022	27_WP9_Rist_MITE_2	MITE	Posture Management & Attack	In corso
01/2022	26_WP9_Rist_MITE_1	MITE	Centralized Threat Monitoring	In corso
01/2022	22_WP9_Rist_SGPR_1	Segretariato Generale della Presidenza della Repubblica	Potenziamento capacità di analisi e rilevamento eventi	Concluso
03/2022	2_WP_9_rist_Comune di Firenze	Comune di Firenze	Cybersecurity - Framework e tools	In corso
03/2022	3_WP_9_rist_Regionale Basilicata	Regione Basilicata	Centro per la cybersicurezza Regionale	In corso
03/2022	4_WP_9_rist_Regionale Basilicata	Regione Basilicata	Centro per la cybersicurezza Regionale II Intervento	In corso
03/2022	5_WP_9_rist_Regionale Friuli Venezia Giulia	Regione Friuli Venezia Giulia	Potenziamento della resilienza cyber del numero unico emergenza (NUE 112) della centrale unica di risposta (CUR) del Friuli Venezia Giulia	In corso
03/2022	6_WP_9_rist_Regionale Piemonte	Regione Piemonte	Postazioni di lavoro a rete regionale: l'evoluzione in sicurezza	In corso
03/2022	7_WP_9_rist_Regionale Piemonte	Regione Piemonte	Transizione digitale e servizi sicuri	In corso
03/2022	8_WP_9_rist_Comune di Palermo	Comune di Palermo	COCY - Consapevolezza cyber	In corso
03/2022	9_WP_9_rist_Comune di Palermo	Comune di Palermo	RECYPA -Resilienza cyber delle infrastrutture del Comune di Palermo	In corso
03/2022	10_WP_9_rist_Comune di Catania	Comune di Catania	Analisi della postura di sicurezza, progettazione e implementazione del potenziamento del livello di protezione	In corso
03/2022	11_WP_9_rist_Comune di Catania	Comune di Catania	Potenziamento e messa in sicurezza degli end-point	In corso
03/2022	12_WP_9_rist_Regionale Abruzzo	Regione Abruzzo	Infrastruttura a supporto della cyber security per il cert Regionale nell'ambito della sanità- Regione Abruzzo Infrastrutture di sicurezza	In corso
03/2022	13_WP_9_rist_Regionale Abruzzo	Regione Abruzzo	Infrastruttura a supporto della cyber security per il cert Regionale dell'ambito della gestione delle acque - Regione Abruzzo - Infrastrutture di sicurezza	In corso
03/2022	14_WP_9_rist_Roma Capitale	Roma Capitale	Potenziamento capacità di Roma Capitale per la rilevazione e la risposta agli incidenti cyber	In corso
03/2022	15_WP_9_rist_Roma Capitale	Roma Capitale	Rafforzamento dei presidi di sicurezza Roma Capitale	In corso

03/2022	16_WP_9_rist_Roma Capitale	Roma Capitale	Cyber security Posture Assessment, definizione delle Cyber Strategy di Roma Capitale e Vulnerability Assessment e Penetration	In corso
03/2022	17_WP_9_rist_Regione Puglia	Regione Puglia	POTENZIAMENTO DELLA INFRASTRUTTURA DI DNS SECURITY PER LA REGIONE PUGLIA, LE AZIENDE SANITARIE LOCALI, LE AGENZIE REGIONALI E LE SOCIETA' IN HOUSE PUGLIESI	In corso
03/2022	18_WP_9_rist_Regione Puglia	Regione Puglia	CYBERSECURITY POSTURE ASSESSMENT E SECURITY AWARENESS TRAINING	In corso
03/2022	19_WP_9_rist_Regione Calabria	Regione Calabria	Strategia Cyber per la Regione Calabria	In corso
03/2022	20_WP_9_rist_Regione Calabria	Regione Calabria	Rafforzamento della cybersicurezza e della data protection dei sistemi e dei processi connessi all'erogazione dei servizi della Regione Calabria alle ASP e AO Regionali	In corso
03/2022	21_WP_9_rist_Provincia autonoma di Trento	Provincia autonoma di Trento	Resilienza cyber per la provincia autonoma di Trento: Analisi della postura e interventi di potenziamento	In corso
03/2022	22_WP_9_rist_Provincia autonoma di Trento	Provincia autonoma di Trento	Potenziamento della capacità cyber del trentino a supporto della trasformazione digitale sicura della PA	In corso
03/2022	23_WP_9_rist_Regione Liguria	Regione Liguria	Infrastruttura per bilanciamento workload e protezione applicativa (application Delivery control - WAF/IPS)	In corso
03/2022	24_WP_9_rist_Regione Liguria	Regione Liguria	Adeguamento dell'infrastruttura firewall e verifica policy di sicurezza con firewall Orchestrator	In corso
03/2022	25_WP_9_rist_Regione Umbria	Regione Umbria	Innalzamento livello di Sicurezza dell'infrastruttura tecnologica regionale Umbra	In corso
03/2022	26_WP_9_rist_Comune di Genova	Comune di Genova	Analisi della Postura Cyber, mitigazione del rischio e Awareness	In corso
03/2022	27_WP_9_rist_Comune di Bari	Comune di Bari	Identity and Access Management e modello di integrazione al servizio di CSIRT offerto dalla Regione Puglia	In corso
03/2022	28_WP_9_rist_Regione Lombardia	Regione Lombardia	Programma di sicurezza e protezione dei dati	In corso
03/2022	29_WP_9_rist_Regione Friuli Venezia Giulia	Regione Friuli Venezia Giulia	Cyber Iniziative	In corso
03/2022	30_WP_9_rist_Regione Friuli Venezia Giulia	Regione Friuli Venezia Giulia	Cybersecurity FVG: Training&Awareness	In corso
03/2022	31_WP_9_rist_Regione Toscana	Regione Toscana	Assessment, catalogo degli asset per Disaster Recovery e Buisness Continuity, sensibilizzazione e formazione utenti	In corso
03/2022	32_WP_9_rist_Regione Toscana	Regione Toscana	Gestione della qualità e miglioramento dei processi, consapevolezza cyber e data protection	In corso
03/2022	33_WP_9_rist_Comune di Firenze	Comune di Firenze	CYBERSECURITY METROWIDE	In corso
03/2022	34_WP_9_rist_Regione Lazio	Regione Lazio	Rafforzamento cyber Defence Regione Lazio	In corso
03/2022	35_WP_9_rist_Regione Lazio	Regione Lazio	Security Enforcement Regione Lazio	In corso
03/2022	36_WP_9_rist_Regione Veneto	Regione Veneto	Realizzazione sistemi propedeutici per la costituzione del CERT della Regione Veneto	In corso
03/2022	37_WP_9_rist_Regione Veneto	Regione Veneto	Assessment della postura Cyber	In corso
03/2022	38_WP_9_rist_Comune di Messina	Comune di Messina	FORMAZIONE E PROCESSI PER LA CYBERSECURITY	In corso
03/2022	39_WP_9_rist_Comune di Torino	Comune di Torino	Analisi della postura di sicurezza e miglioramento nella gestione dei processi legati alla cybersecurity della Città di Torino	In corso

03/2022	40_WP_9_rist_Comune di Bari	Comune di Bari	Cyber Security Posture Assessment, definizione delle Cyber Strategy e formazione in materia di Cyber Security	In corso
03/2022	41_WP_9_rist_Comune di Torino	Comune di Torino	Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio	In corso
03/2022	42_WP_9_rist_Comune di Messina	Comune di Messina	POTENZIAMENTO SOC E NUOVI SERVIZI/FORNITURE CYBERSECURITY	In corso
03/2022	43_WP_9_rist_Region Umbria	Regione Umbria	Potenziamento della resilienza cyber della sanità umbra	In corso
03/2022	44_WP_9_rist_Comune di Milano	Comune di Milano	Analisi e miglioramento dei processi cyber	In corso
03/2022	45_WP_9_rist_Comune di Milano	Comune di Milano	Cyber resilienza e potenziamento dei presidi	In corso
03/2022	46_WP_9_rist_Provincia autonoma di Bolzano	Provincia autonoma di Bolzano	BozenAsset	In corso
03/2022	47_WP_9_rist_Region Marche	Regione Marche	Rafforzamento dei processi e delle procedure relative alla cybersicurezza erogati tramite infrastruttura Cloud regionale	In corso
03/2022	48_WP_9_rist_Comune di Napoli	Comune di Napoli	Piattaforma SOC/EPP evoluto	In corso
03/2022	49_WP_9_rist_Region Marche	Regione Marche	Miglioramento della sicurezza con coinvolgimento dei servizi di assistenza sanitaria	In corso
03/2022	50_WP_9_rist_Comune di Napoli	Comune di Napoli	Adozione Framework Zero Trust Access	In corso
03/2022	51_WP_9_rist_Provincia autonoma di Bolzano	Provincia autonoma di Bolzano	Ampliamento SOC	In corso
03/2022	52_WP_9_rist_Region Lombardia	Regione Lombardia	Cyber Security Assessment & Remediation Enti Sanitari Regione Lombardia	In corso
03/2022	53_WP_9_rist_Comune di Napoli	Comune di Napoli	Assessment ed evoluzione della postura Cyber	In corso
03/2022	54_WP_9_rist_Provincia autonoma di Bolzano	Provincia autonoma di Bolzano	CERT territoriale dell'Alto Adige	In corso
03/2022	55_WP_9_rist_Region Lazio	Regione Lazio	Piano di Security Awareness Regione Lazio	In corso
03/2022	56_WP_9_rist_Region Campania	Regione Campania	Sinfonia	In corso
03/2022	57_WP_9_rist_Region Campania	Regione Campania	Cyber Campania	In corso
03/2022	58_WP_9_rist_Comune di Venezia	Comune di Venezia	RESILIENZA CIBERNETICA COMUNE DI VENEZIA – MATURITY ASSESSMENT E PIANO DI MIGLIORAMENTO	In corso
03/2022	59_WP_9_rist_Comune di Bologna	Comune di Bologna	Linea progettuale 1: potenziamento della sicurezza a livello metropolitano	In corso
03/2022	60_WP_9_rist_Comune di Bologna	Comune di Bologna	Linea progettuale 2: attivazione di un sistema di EDR a livello metropolitano	In corso
03/2022	62_WP_9_rist_Comune di Reggio Calabria	Comune di Reggio Calabria	ReggioCyber (RC)	In corso
03/2022	63_WP_9_rist_Region Sicilia	Regione Sicilia	SICUREZZA PERIMETRO INTERNO RTRS	In corso
03/2022	64_WP_9_rist_Region Emilia Romagna	Regione Emilia Romagna	Realizzazione CSIRT Regione Emilia Romagna (CSIRT-RER)	In corso

03/2022	65_WP_9_rist_Regione Sicilia	Regione Sicilia	SICUREZZA ENDPOINT RTRS	In corso
03/2022	66_WP_9_rist_Regione Emilia Romagna	Regione Emilia Romagna	Potenziamento della resilienza cyber delle infrastrutture dei servizi sanitari regionali	In corso
03/2022	67_WP_9_rist_Regione Emilia Romagna	Regione Emilia Romagna	Potenziamento della resilienza e della gestione del rischio cyber di Regione Emilia-Romagna	In corso
03/2022	69_WP_9_rist_Regione Sardegna	Regione Sardegna	GDPR-SIBAR - Realizzazione di attività di sicurezza applicativa ed infrastrutture nell'ambito del sistema informativo di base dell'amministrazione regionale (SIBAR) in attuazione del GDPR (regolamento generale di protezione dei dati) regolamento europeo 2016/679 e delle misure minime di sicurezza del	In corso
03/2022	70_WP_9_rist_Regione Molise	Regione Molise	Cybersecurity_r_molise	In corso
03/2022	71_WP_9_rist_Regione Valle d'Aosta	Regione Valle d'Aosta	CYBER AWARENESS E FORMAZIONE SPECIALISTICA PER LA PA LOCALE DELLA VALLE D'AOSTA	In corso
03/2022	72_WP_9_rist_Regione Valle d'Aosta	Regione Valle d'Aosta	POTENZIAMENTO RESILIENZA cyber per la PALocale della Valle d'Aosta	In corso
03/2022	73_WP_9_rist_Comune di Venezia	Comune di Venezia	RESILIENZA CIBERNETICA COMUNE DI VENEZIA – PIANO DI CYBERSECURITY AWARENESS	In corso
03/2022	74_WP_9_rist_Comune di Venezia	Comune di Venezia	RESILIENZA CIBERNETICA COMUNE DI VENEZIA – NUOVE TECNOLOGIE DI SICUREZZA A MITIGAZIONE DEL RISCHIO CYBER	In corso
03/2022	75_WP_9_rist_Regione Sardegna	Regione Sardegna	SIRA-Segùra – Intervento evolutivo di potenziamento del Sistema Informativo Regionale Ambientale SIRA Sardegna	In corso
03/2022	76_WP_9_rist_Regione Sicilia	Regione Sicilia	Cybervault per dati mission critical Bacino Orientale	In corso
03/2022	78_WP_9_rist_Comune di Cagliari	Comune di Cagliari	METROCAGLIARI IT-SECURITY PROGETTO 1	In corso
03/2022	79_WP_9_rist_Comune di Cagliari	Comune di Cagliari	METROCAGLIARI IT-SECURITY PROGETTO 2	In corso
07/2023	1_WP9_A7_ANSV	Agenzia nazionale per la sicurezza del volo		In corso
07/2023	3_WP9_A7_Ministero della giustizia	Ministero della giustizia		In corso
07/2023	4_WP9_A7_AIFA	Agenzia Italiana del Farmaco		In corso
07/2023	5_WP9_A7_MASE	Ministero dell'Ambiente e della Sicurezza Energetica		In corso
07/2023	6_WP9_A7_AGCOM	Autorità per le garanzie nelle comunicazioni		In corso
07/2023	7_WP9_A7_CSM	Consiglio Superiore della Magistratura		In corso
07/2023	8_WP9_A7_ANAC	Autorità Nazionale Anticorruzione		In corso
07/2023	9_WP9_A7_MIM	Ministero dell'Istruzione e del Merito		In corso
07/2023	10_WP9_A7_ANVUR	Agenzia Nazionale di Valutazione del sistema Universitario e della Ricerca		In corso
07/2023	11_WP9_A7_AGCM	Autorità Garante della Concorrenza e del Mercato		In corso
07/2023	13_WP9_A7_ANSFISA	Agenzia nazionale per la sicurezza delle ferrovie e delle infrastrutture stradali e autostradali		In corso

07/2023	14_WP9_A7_MUR	Ministero dell'Università e della Ricerca		In corso
07/2023	16_WP9_A7_Ente Nazionale Microcredito	Ente Nazionale per il Microcredito		In corso
07/2023	17_WP9_A7_ARERA	Autorità di regolazione per energia reti e ambiente		In corso
07/2023	18_WP9_A7_Ministero del turismo	Ministero del turismo		In corso
07/2023	19_WP9_A7_GSE	Gestore dei servizi energetici		In corso
07/2023	20_WP9_A7_Agenzia per la coesione territoriale	Agenzia per la coesione territoriale		In corso
07/2023	22_WP9_A7_CSEA	Cassa per i servizi energetici e ambientali		In corso
07/2023	23_WP9_A7_AGENAS	Agenzia nazionale per i servizi sanitari regionali		In corso
07/2023	24_WP9_A7_Ministero del lavoro	Ministero del lavoro		In corso
07/2023	25_WP9_A7_Ministero della cultura	Ministero della Cultura		In corso
07/2023	26_WP9_A7_GDPD	Garante per la protezione dei dati personali		In corso
07/2023	27_WP9_A7_ANPAL	Agenzia Nazionale per le Politiche Attive del Lavoro		In corso
07/2023	28_WP9_A7_ISIN	Ispettorato nazionale per la sicurezza nucleare e la radioprotezione		In corso
07/2023	29_WP9_A7_Ministero dell'Interno	Ministero dell'Interno		In corso
Accordo Cyber Defence	N.A.	Ministero dell'Interno	Progetto di Realizzazione SOC, C-LAB e UFO, Centro di Valutazione	In corso
Accordo Cyber Defence	N.A.	Ministero della Giustizia	Programma di interventi in ambito sicurezza dei dati e dei servizi applicativi del Ministero di Giustizia	In corso
Accordo Cyber Defence	N.A.	Ministero della Difesa	Nuove soluzioni basate su integrazione di sistemi di monitoraggio cibernetico con sistemi C2, potenziamento SCADA e realizzazione Centro di Valutazione della Difesa	In corso
Accordo Cyber Defence	N.A.	Comando Generale dell'Arma dei Carabinieri	1. Miglioramento della postura di sicurezza dell'Arma, 2. Attività nei confronti del personale dell'Arma, 3. Implementazioni hardware/software per i Datacenter Arma	In corso
Accordo Cyber Defence	N.A.	Comando Generale della Guardia di Finanza	Missione Digitale	In corso
Accordo Cyber Defence	N.A.	Consiglio di Stato	Acquisto di soluzioni avanzate di cybersecurity	In corso

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

