allegato a ACN.AOO_ACN-US.REGISTRO UNICO.0043830.30-12-2024.I

PIANO STRATEGICO 2024-2026

Indice

Lettera del Direttore Generale, Prefetto Bruno Frattasi 4

1. Scenario di riferimento 6

2. La visione strategica 9

3. Gli obiettivi strategici e i piani di azione 11

OBIETTIVO STRATEGICO N. 1 12

OBIETTIVO STRATEGICO N. 2 14

OBIETTIVO STRATEGICO N. 3 15

OBIETTIVO STRATEGICO N. 4 16

OBIETTIVO STRATEGICO N. 5 17

Lettera del Direttore Generale, Prefetto Bruno Frattasi

Tra le lesson learned della mia lunga esperienza professionale rimane significativa e illuminante quella con cui - in occasione di un lontano corso di formazione presso la Scuola Superiore dell'Amministrazione dell'Interno - appresi che il compito primario e prioritario di un dirigente pubblico sta nell'interrogarsi circa il futuro del proprio ufficio, ossia della destinazione verso la quale impostare il percorso di crescita della struttura di cui si è responsabili, e nel farsene carico.

Uscire, infatti, dall'angusta ed effimera logica del "day-by-day" era e rimane un'essenziale necessità per indirizzare l'attività istituzionale al raggiungimento di traguardi realmente funzionali al miglior perseguimento del fine pubblico.

Questa di cui parlo - che è un'esigenza vitale per ogni struttura della Pubblica Amministrazione - lo è in maniera particolarmente perentoria per l'Agenzia per la cybersicurezza nazionale, che ha non solo il dovere di garantire la protezione del nostro sistema digitale per il presente ma anche di assicurarla per il futuro, cioè di progettarla e realizzarla in correlazione ai progressi della tecno-scienza. Perché non c'è nulla di più mutevole ed evolutivo della minaccia informatica, la cui incessante crescita esige una costante tensione verso gli scenari a venire e, dunque, una propensione naturale e indispensabile verso la ricerca e lo sviluppo tecnologico, in quanto entrambi potranno arricchire di nuovi strumenti, adeguati al grado e alla qualità offensiva degli attacchi, la difesa cibernetica dell'Italia.

La Strategia Nazionale per la Cybersicurezza 2022-2026, con il Piano di implementazione che ne rappresenta il versante attuativo, formano congiuntamente i documenti programmatici che hanno indicato gli obiettivi generali da raggiungere nel medio periodo e le misure #, cioè le diverse azioni pratiche, con cui poterli concretamente attingerli in modo che la navigazione del Paese verso una migliore postura di cybersicurezza possa avvenire seguendo una precisa mappa in cui è fissato il punto di arrivo e, insieme, il percorso da seguire, ispirato, a sua volta, da principi di gradualità e sostenibilità.

Come più volte ho affermato, se affrontassimo la minaccia limitandoci ad intervenire sulla superficie digitale aggredita ci comporteremmo alla stregua di quei carpentieri che, operando all'interno di una nave, si prodigano per ripararne le paratie colpite, e tuttavia ignorano verso quale porto quell'imbarcazione dovrà dirigersi; sicché la loro affannosa opera, per quanto meritoria, sarà sempre inevitabilmente segnata da un che di provvisorio o, per meglio dire, dalla provvisorietà del rimedio che conosce solo l'oggi ma non riesce a impadronirsi della bussola con cui orientare il domani.

La pianificazione strategica di ACN si iscrive in questo processo di maturazione nel definire il percorso da fare. Essa segue, dunque, la logica di ogni documento che ha siffatto proposito, per cui muove da ciascun macro-obiettivo per poi delineare e indicare gli obiettivi discendenti e più particolareggiati di carattere operativo.

Nel Piano Strategico ACN 2024-2026 è racchiuso, in sintesi, un articolato programma di lavoro che chiama l'intera Agenzia - il Vertice come la sua struttura di comando - a un responsabile impegno nei riguardi della comunità nazionale.

Aver varato questo documento, ed è la prima volta che accade dalla istituzione dell'Agenzia, è anche il segno che il funzionamento e l'efficacia delle nostre attività si confronteranno d'ora in poi con parametri rigorosi quanto trasparenti e verificabili, anche nel rispetto, tra gli altri, del principio di accountability.

Il monitoraggio, cioè l'osservazione dei risultati ottenuti e la valutazione in corso d'opera della loro adesione o, al contrario, del loro discostamento rispetto al dato previsionale, è poi un'altra conseguenza virtuosa di una buona pianificazione, perché, rendendo possibile una costante sorveglianza dell'azione svolta, consente l'affinamento e il miglioramento progressivo dei mezzi messi a disposizione del fine.

Il "dover render conto", che è il cuore della trasparenza e dello stesso principio di accountability, con lo strumento della pianificazione strategica è innanzitutto un "render conto a sé stessi"; ed è per questo che tale strumento presenta una preziosa utilità, eventualmente anche interna, di cui non faremo a meno di avvalerci.

1. Scenario di riferimento

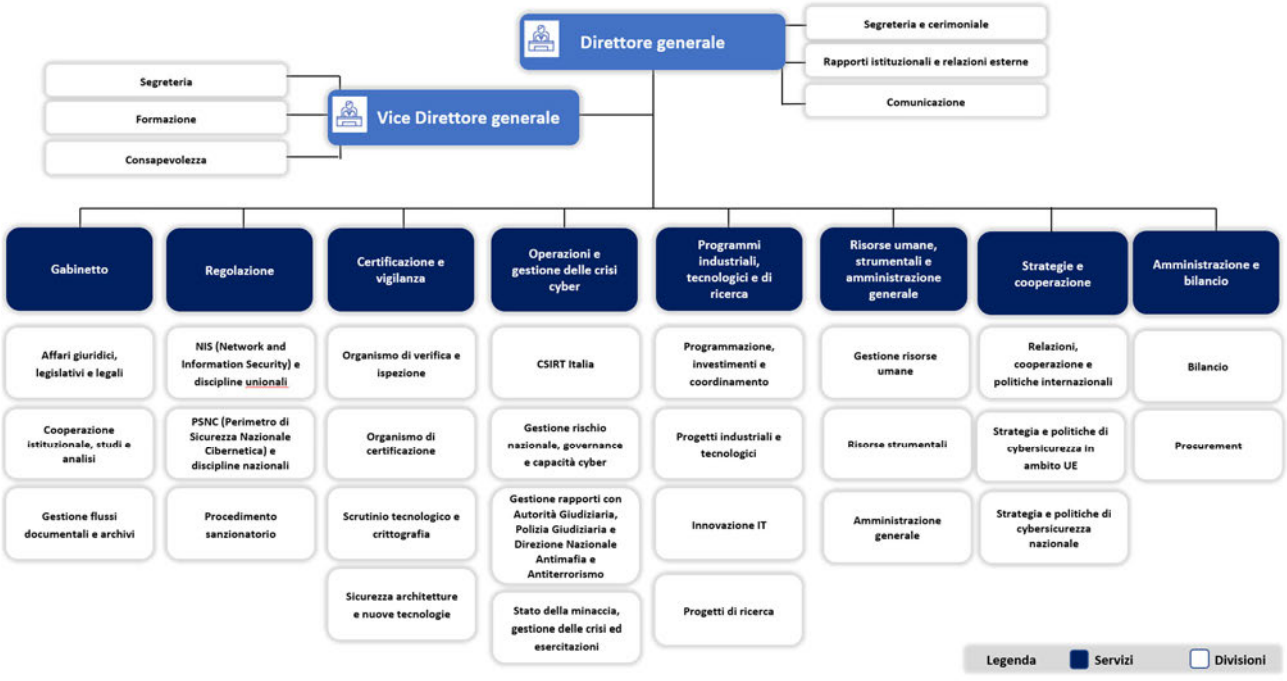
[KEYWORDS: #protezione, #risposta, #sviluppo, #sicurezza nazionale, #resilienza, #coordinamento, #minaccia, #scenario internazionale, #normativa, #vulnerabilità, #supply chain security #PNRR, #sviluppo tecnologico, #tecnologie emergenti, #IA, #quantum computing, #cloud, #crisi *cyber*, #formazione, #consapevolezza]

L'Agenzia per la cybersicurezza nazionale (ACN) è responsabile per l'attuazione della Strategia nazionale di cybersicurezza 2022-2026 e coordina la complessa azione dei soggetti pubblici chiamati a rafforzare la cybersicurezza, assicurando migliori capacità di protezione, risposta e sviluppo a tutela della sicurezza nazionale e degli interessi nazionali nello spazio cibernetico.

Elevare il livello di resilienza del Paese attraverso la sicurezza sistemi informativi e di rete nonché di prodotti, servizi e processi informatici è una funzione strategica.

Terminata la fase di prima operatività, nel corso del 2024 l'Agenzia si è dotata di una nuova struttura organizzativa per assicurare elevati livelli di prontezza nell'assolvimento dei compiti istituzionali ed ha completato il trasferimento nella nuova sede di Roma, Corso d'Italia n. 41-43 e via Tevere n. 50.

Il processo di riordino ha coniugato interventi di soppressione, accorpamento e riorganizzazione dei Servizi e delle Divisioni nonché delle Articolazioni a supporto del Direttore generale e del Vice Direttore generale secondo il seguente organigramma, in vigore dal 1° luglio 2024.



Sul piano nazionale e su quello europeo, sono diversi i provvedimenti che ampliano il novero delle attribuzioni dell'ACN oltre a quanto già previsto dal decreto-legge istituivo (14 giugno 2021, n. 82): il rafforzamento della cybersicurezza nazionale, la resilienza della Pubblica Amministrazione e l'utilizzo della crittografia (**L. 28 giugno 2024, n. 90**); l'applicazione e l'attuazione della normativa nazionale ed europea in materia di intelligenza artificiale-IA, specie riguardo alla vigilanza dei sistemi di IA, incluse le attività ispettive e sanzionatorie, e alla promozione e allo sviluppo di tale tecnologia relativamente ai profili di cybersicurezza (secondo quanto stabilito dalla **normativa nazionale in materia di intelligenza artificiale** attualmente all'esame del Parlamento); l'innalzamento del livello comune di cybersicurezza nell'Unione e, in particolare, la gestione degli incidenti e delle crisi di cybersicurezza su larga scala anche europee (**Direttiva UE 2022/2555, cd. NIS2**).

Lo sviluppo normativo appare fisiologico rispetto al contesto delle minacce cibernetiche – ove si registra il **costante aumento di eventi ed incidenti** con elevati livelli di sofisticazione e impatti significativi su *asset* strategici – e alla spirale di **tensione sul piano internazionale**. L'insorgere di nuovi focolai di crisi suscettibili di influenzare il quadro di sicurezza europeo e l'improvviso riacutizzarsi di dispute mai risolte sono le scosse più evidenti e drammatiche di conflittualità che condizionano i rapporti internazionali, spingono la ricerca di nuovi equilibri e imprimono un nuovo carattere alla cooperazione internazionale. In tale contesto, l'ACN non è rimasta passiva e ha assunto le proprie responsabilità di Agenzia di sicurezza.

Lo scenario attuale è anche condizionato da un **notevole incremento di attacchi *cyber***, agevolato dalla "condizione di anonimato" e dalla "deterritorializzazione" della dimensione cibernetica ad opera di attori statuali e non, in grado di produrre impatti sull'erogazione, integrità e sicurezza di reti, sistemi e servizi essenziali dello Stato. A ciò si aggiunge il ricorso sempre più frequente a **campagne disinformative condotte nel dominio *cyber*** al fine di influenzare il dibattito pubblico, le campagne elettorali e il regolare svolgimento dei processi democratici.

In tale contesto, l'ACN continuerà a promuovere il **coordinamento tra i soggetti pubblici** coinvolti in materia di cybersicurezza nonché ogni utile iniziativa per il **rafforzamento della sicurezza e della resilienza cibernetiche**. L'attività di definizione di adeguati strumenti normativi e di aggiornamento del quadro regolamentare è quindi fondamentale per supportare il rafforzamento della postura di cybersicurezza nazionale in coerenza con l'evoluzione della minaccia e il progressivo incremento delle capacità degli attori coinvolti.

Parimenti irrinunciabile sarà l'azione volta ad assicurare al Paese un solido **posizionamento internazionale** nei principali consessi multilaterali deputati alla formulazione delle *policy* in materia di cybersicurezza, nonché la partecipazione a **programmi di cooperazione e assistenza** internazionale a beneficio di Paesi terzi (cd. *cyber capacity-building*).

Obiettivo questo che l'ACN intende perseguire assieme al MAECI tramite un'adeguata proiezione internazionale, la collaborazione con il settore privato, la partecipazione ai tavoli negoziali, nonché il presidio dei tavoli tecnici settoriali.

È persistente, inoltre, il cd. **rischio tecnologico**, alimentato dall'endemica presenza di vulnerabilità di sicurezza gravanti su prodotti e soluzioni tecnologiche e dalla frammentazione del rischio cibernetico lungo le catene di approvvigionamento (*supply chains*).

Al tempo stesso, il Paese è chiamato a rispondere alla sfida posta dalla ***governance* delle nuove tecnologie emergenti** tramite un approccio flessibile, in grado di non porre freni al mercato e, al contempo, prevenirne usi distorti o contrari al quadro normativo vigente.

In questo senso, meritano una menzione particolare, oltre alle già citate soluzioni di **intelligenza artificiale** (con potenziali effetti su proprietà intellettuale, *privacy* e sfera informativa), anche il ***quantum computing*** (la cui diffusione renderà inefficaci gli attuali *standard* crittografici a chiave pubblica e per cui sarà necessario definire una transizione ai nuovi algoritmi crittografici *quantum safe*) e le infrastrutture di ***cloud computing*** (verso le quali assicurare una migrazione sicura di dati e servizi), le **infrastrutture digitali sottomarine**, nonché i **sistemi satellitari** (in un dominio sempre più utilizzato per applicazioni d'uso quotidiano ed oggetto di ingenti investimenti).

Nel più ampio contesto della sicurezza delle catene di approvvigionamento, inoltre, va evidenziato il ruolo del *framework* europeo di certificazione della cybersicurezza, che vede la sua attuazione con l'entrata in vigore, dal febbraio 2025, del primo sistema di certificazione europeo EUCC. Il nuovo schema soppianta gli analoghi schemi preesistenti a livello nazionale e, in tal senso, l'Agenzia dovrà adeguare le sue strutture e i suoi processi in modo da svolgere le proprie funzioni di Autorità Nazionale per la Certificazione della Cybersicurezza (NCCA) nonché di Organismo di certificazione nazionale, in sinergia con la rete dei laboratori esterni che potranno condurre le attività tecniche di valutazione, sotto la supervisione di ACN.

Per far fronte a tali impegni e rispondere al meglio alle sfide attuali e future, assume importanza la **dotazione finanziaria dell'Agenzia** prevista dal decreto-legge 14 giugno 2021, n. 82, nonché il sostegno alla transizione digitale sicura e al rafforzamento della resilienza della Pubblica Amministrazione e alle capacità nazionali di scrutinio tecnologico e certificazione, tramite tre principali filoni di finanziamento: 1) il **Fondo per l'attuazione della Strategia nazionale di cybersicurezza** e il **Fondo per la gestione della cybersicurezza**, entrambi istituiti ai sensi della legge 29 dicembre 2022, n. 197, rispettivamente, per finanziare gli investimenti volti al conseguimento dell'autonomia tecnologica in ambito digitale e l'innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali, nonché per assicurare copertura economica alle attività di gestione operativa; 2) le risorse rese disponibili **dall'Investimento 1.5 *Cybersecurity*** della Missione 1, Componente 1, del Piano Nazionale di Ripresa e Resilienza – rispetto ai quali l'ACN è stata individuata come "Soggetto Attuatore" dal Dipartimento della Trasformazione Digitale della Presidenza del Consiglio dei Ministri; 3) i fondi assicurati dai programmi europei ***Horizon Europe*** e ***Digital Europe Programme***.

2. La visione strategica

Per rispondere in modo efficace, tempestivo e sostenibile alle richiamate sfide l'ordinamento ha riconosciuto all'Agenzia una **peculiare collocazione istituzionale** e un **marcato livello di autonomia** che le permettono di adottare paradigmi strategici, organizzativi e di gestione del personale che travalicano i tradizionali modelli della PA e, per tale via, le consentono di fronteggiare le sollecitazioni esterne adattando rapidamente **vision strategica**, **strutture** e **professionalità** per creare e/o proteggere "valore", attraverso un confronto continuo tra il mutevole contesto di riferimento, le aspettative del Paese e dei diversi stakeholder.

Il Piano Strategico è il "**documento unico**" di programmazione (anche operativa), governance e coordinamento dell'Agenzia, nel quale assumono rilievo trasversale gli **obiettivi strategici**.

In esso confluiscono, da una parte, le finalità istituzionali e la mission pubblica dell'ACN, dall'altro, l'organizzazione e gli obiettivi strategici da perseguire, in un'ottica di compatibilità con le risorse finanziarie disponibili e di semplificazione dell'azione amministrativa.

Il Piano è elaborato ogni tre anni, copre l'arco temporale di un triennio e può essere modificato o aggiornato anche su sollecitazione del Comitato di coordinamento e programmazione per esigenze di revisione della visione strategica.

Al contempo, essendo pubblicato sul sito istituzionale, è uno strumento di **trasparenza** sugli indirizzi dell'azione dell'Agenzia, sulle priorità strategiche verso cui allocare le risorse e sui miglioramenti organizzativi e gestionali da perseguire per una maggiore **efficienza e *performance***, anche attraverso un costante **monitoraggio** degli obiettivi programmati.

Ne discende che, in una logica di coerenza tra pianificazione strategica, strutture organizzative e sviluppo delle persone, l'assegnazione della responsabilità in ordine al raggiungimento dei risultati strategici rappresenta il **parametro** sul quale misurare il livello di conseguimento degli obiettivi assegnati ai Responsabili nonché lo strumento per realizzare il pieno allineamento tra gli obiettivi dell'Istituzione e i comportamenti individuali delle persone che vi lavorano.

L'art. 3, comma 2, lett. f) del Regolamento di organizzazione dell'Agenzia (d.P.C.m. 9 dicembre 2021, n. 223) evidenzia, tra l'altro, tra i principi fondamentali, la **flessibilità** e l'**innovazione tecnologica a supporto dei processi gestionali**, al fine di garantire nella misura massima l'efficacia e l'efficienza necessarie per la **realizzazione degli obiettivi strategici dell'Agenzia**.

Per il triennio 2024-2026, le linee strategiche dell'azione dell'ACN prevedono di **creare valore pubblico** accompagnando il processo di ammodernamento delle infrastrutture potenziando la resilienza cibernetica del Paese, riducendone il grado di vulnerabilità e, al contempo, incrementandone l'autonomia e l'indipendenza tecnologica.

Funzionale alla realizzazione di questi obiettivi sarà l'attività di **coordinamento tra i soggetti pubblici** coinvolti nella materia della cybersicurezza, nonché lo sviluppo del quadro legislativo e regolamentare, anche al fine di garantire nei consessi internazionali una postura nazionale unitaria e coerente, la promozione di **azioni comuni con gli stakeholder** per il conseguimento dell'autonomia, nazionale ed europea, e dell'indipendenza tecnologica riguardo a prodotti e processi informatici di rilevanza strategica per gli interessi nel settore, nonché, attraverso dedicati bandi di finanziamento, la **creazione di un network degli operatori** per progettare e implementare programmi congiunti di supporto e accelerazione dell'innovazione e della ricerca applicata in aree tecnologiche di interesse.

Di pari rilievo sarà l'azione volta ad assicurare il costante mantenimento di un **quadro giuridico aggiornato nel dominio della cybersicurezza** - e il collegato impianto di obblighi e di supporto per soggetti nazionali - che tenga conto degli sviluppi in ambito internazionale, anche attraverso l'espressione di pareri, obbligatori ma non vincolanti, sulle iniziative legislative o regolamentari in materia.

Anche la **collaborazione con il mondo universitario e scolastico, delle aziende e delle Istituzioni**, svilupperà virtuose sinergie nel campo della formazione e nella crescita della cultura tecnologica e informatica del Paese, con specifica attenzione a quella della **sicurezza cibernetica**, per aumentare la **consapevolezza** del settore pubblico e privato e della società civile sui rischi e le minacce cyber.

Trasversale alle predette linee strategiche sarà quella di garantire processi di **reclutamento, formazione e sviluppo del personale** finalizzati a realizzare in ACN un centro di eccellenza che possa esaltare il **valore identitario** mantenendo elevata ed accrescendone la percezione di qualità all'esterno.

3. Gli obiettivi strategici e i piani di azione

Per conseguire la nostra visione, in linea con **la Strategia Nazionale di Cybersicurezza 2022-2026** e il relativo **Piano di implementazione**, per il triennio 2024-2026, abbiamo definito **5 obiettivi strategici**, articolati in **38 Piani d'azione**.

All'interno dell'Agenzia, ciascun piano d'azione è declinato in **obiettivi operativi** assegnati ai Servizi e alle Articolazioni, con l'indicazione dei responsabili, dei tempi, delle risorse, nonché dei criteri e degli indicatori per la valutazione periodica dei risultati raggiunti, delle risorse impiegate e dei progressi compiuti.

OBIETTIVO STRATEGICO N. 1

PROTEZIONE DEGLI ASSET STRATEGICI NAZIONALI, attraverso un approccio orientato alla gestione e mitigazione del rischio, caratterizzato da norme, misure, strumenti e controlli volti ad abilitare una transizione digitale resiliente del Paese con i seguenti **Piani d'azione**:

1.1 il potenziamento delle capacità del Centro di Valutazione e Certificazione Nazionale (CVCN) dell'ACN *(Capo Servizio Certificazione e vigilanza)*;

1.2 la conoscenza approfondita del quadro della minaccia cibernetica e il possesso di competenze specialistiche e capacità operative nonché il monitoraggio degli obblighi normativi *(Capo Servizio Operazioni e gestione delle crisi cyber per la preparazione, prevenzione e monitoraggio delle minacce e dei rischi cyber; Capo Servizio Regolazione per aggiornare la disciplina degli obblighi ed emanare direttive e linee guida per il loro adempimento)*;

1.3 la promozione dell'uso della crittografia come strumento di cybersicurezza *(Capo Servizio Certificazione e vigilanza)*;

1.4 il supporto allo sviluppo e mantenimento di un quadro giuridico aggiornato in materia di cybersicurezza che realizzi, al contempo, un affinamento degli istituti giuridici e un migliore coordinamento delle diverse componenti cyber del Paese (*Capo Servizio Gabinetto per la cura e promozione dell'attività legislativa al fine di garantire il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza; Capo Servizio Regolazione per il monitoraggio e l'adeguamento della regolazione in materia)*;

1.5 lo sviluppo degli atti di carattere normativo in materia cyber, anche di derivazione europea *(Capo Servizio Gabinetto)*;

1.6 lo sviluppo della disciplina cyber nazionale, anche di derivazione europea, supportando l'attività legislativa nonché adeguando e assicurando la coerenza del quadro regolamentare in materia, anche in termini di obblighi in capo ai soggetti *(Capo Servizio Regolazione)*;

1.7 il supporto ai soggetti nazionali per promuovere l'efficace attuazione della disciplina cyber e il relativo recepimento *(Capo Servizio Regolazione)*;

1.8 il supporto al processo di digitalizzazione sicuro della Pubblica Amministrazione, anche tramite migrazione a servizi cloud qualificati *(Capo Servizio Certificazione e vigilanza)*;

1.9 il supporto al processo di evoluzione dei sistemi di gestione dell'identità digitale, tramite la definizione, in sinergia con l'Agenzia per l'Italia Digitale e il Dipartimento per la Trasformazione Digitale, dei requisiti di cybersicurezza e di certificazione delle piattaforme nazionali, coerentemente con le iniziative europee *(Capo Servizio Certificazione e vigilanza per la definizione dello schema di certificazione, nonché il rilascio delle certificazioni delle soluzioni di identity wallet nazionali; Capo Servizio Regolazione per la definizione degli obblighi di cybersicurezza dell'identità digitale)*;

1.10 il potenziamento delle capacità di valutazione, certificazione e vigilanza dell'ACN *(Capo Servizio Certificazione e vigilanza)*;

1.11 la promozione dell'uso di procedure, pratiche, tassonomie, standardizzate e comuni, per la gestione degli incidenti, delle vulnerabilità e per il monitoraggio e controllo delle minacce e dei rischi cyber *(Capo Servizio Operazioni e gestione delle crisi cyber per la definizione e promozione di procedure, pratiche e tassonomie comuni per il monitoraggio e la gestione degli eventi ed incidenti cyber; Capo Servizio Gabinetto per gli aspetti giuridici ed il coordinamento in materia cyber)*.

OBIETTIVO STRATEGICO N. 2

RISPOSTA ALLE MINACCE, AGLI INCIDENTI E ALLE CRISI CYBER NAZIONALI E TRANSNAZIONALI, mediante sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale, tenuto anche conto delle sinergie e delle attività sviluppate nell'ambito della collaborazione internazionale, con i seguenti **Piani d'azione**:

2.1 lo sviluppo di un sistema di gestione degli incidenti e delle crisi informatiche su larga scala che sia fondato su procedure di collaborazione consolidate, sia a livello nazionale che europeo e internazionale (*Capo Servizio Gabinetto per gli aspetti giuridici ed il coordinamento in materia cyber; Capo Servizio Operazioni e gestione delle crisi cyber per la gestione e risposta agli incidenti ed alle crisi informatiche)*;

2.2 l'erogazione di servizi operativi di raccolta, correlazione e analisi di eventi cyber nonché di condivisione di informazioni su minacce e rischi cyber, anche connessi agli attuali servizi cyber nazionali (HyperSOC e ISAC) *(Capo Servizio Operazioni e gestione delle crisi cyber e Capo Servizio di Gabinetto)*;

2.3 l'organizzazione di periodiche esercitazioni di sicurezza cibernetica e resilienza, anche nell'ambito del Perimetro di Sicurezza Nazionale Cibernetica (PSNC), nonché la promozione e il coordinamento della partecipazione del Paese a quelle europee e internazionali *(Capo Servizio Operazioni e gestione delle crisi cyber)*;

2.4 il monitoraggio dello stato di adozione degli obblighi in capo ai soggetti nazionali e la loro coerenza in relazione al rischio a cui sono esposti i rispettivi sistemi di rete e informativi *(Capo Servizio Regolazione)*.

OBIETTIVO STRATEGICO N. 3

SVILUPPO SICURO DELLE TECNOLOGIE DIGITALI, per rispondere alle esigenze del mercato, agevolando iniziative volte a supportare i centri di eccellenza, le attività di ricerca e le imprese, con i seguenti **Piani d'azione**:

3.1 il rafforzamento del ruolo del Centro Nazionale di Coordinamento (NCC) a supporto dello sviluppo e del potenziamento dell'autonomia strategico-tecnologica e digitale del Paese e dell'Unione europea mediante il continuo impulso all'innovazione tecnologica *(Capo Servizio Programmi industriali, tecnologici e di ricerca)*;

3.2 la realizzazione di un Piano per l'industria cyber nazionale e di un "parco nazionale della cybersicurezza" per lo svolgimento di attività di ricerca e sviluppo nell'ambito della cybersecurity e delle tecnologie digitali *(Capo Servizio Programmi industriali, tecnologici e di ricerca)*;

3.3 la promozione dell'internazionalizzazione delle imprese italiane che offrono prodotti e servizi di cybersecurity *(Capo Servizio Programmi industriali, tecnologici e di ricerca)*;

3.4 la realizzazione della digitalizzazione sicura della Pubblica Amministrazione e del tessuto produttivo del Paese, anche attraverso le risorse messe a disposizione dal PNRR *(Capo Servizio Programmi industriali, tecnologici e di ricerca)*;

3.5 l'accrescimento della capacità *cyber* del Paese promuovendo sia l'educazione digitale che lo sviluppo di competenze *(Capo Divisione Formazione)*;

3.6 la promozione di iniziative che sostengano l'attuazione della disciplina cyber, anche a livello nazionale, nel contesto pubblico e in quello privato *(Capo Divisione Consapevolezza)*;

3.7 la predisposizione e realizzazione delle infrastrutture IT dei servizi di protezione degli asset nazionali, dei sistemi HPC e, più in generale, delle piattaforme IT dell'Agenzia *(Capo Servizio Programmi industriali, tecnologici e di ricerca)*.

OBIETTIVO STRATEGICO N. 4

RAFFORZAMENTO DELLA COOPERAZIONE IN MATERIA DI CYBERSICUREZZA sia in ambito interno che internazionale, per rispondere alle esigenze connesse alla tutela della sicurezza nazionale nello spazio cibernetico, favorendo il dialogo con le Pubbliche Amministrazioni, il settore privato, le omologhe Agenzie estere e le Organizzazioni internazionali, con i seguenti **Piani d'azione**:

4.1 il sostegno agli interessi strategici nazionali in ambito europeo e a livello globale, tramite il rafforzamento delle sinergie con i Paesi *like-minded* e le Organizzazioni internazionali nell'ambito dei negoziati di atti normativi e di policy sovranazionali *(Capo Servizio Strategie e cooperazione)*;

4.2 lo sviluppo delle attività di cooperazione bilaterale e multilaterale, con particolare riguardo all'ambito UE e G7 *(Capo Servizio Strategie e cooperazione)*;

4.3 il dialogo e la cooperazione con il settore pubblico e quello privato nella più ampia cornice delineata dalla Strategia Nazionale di Cybersicurezza 2022-2026 *(Capo Servizio Strategie e cooperazione)*;

4.4 il rafforzamento dell'interazione informativa con il Parlamento e con l'organo parlamentare di controllo per la sicurezza della Repubblica, garantendo al contempo la migliore gestione dei consessi governativi e interistituzionali, attraverso i quali si provvede, da un lato, a determinare le prerogative e le decisioni di alta amministrazione che definiscono l'architettura di operatività dell'Agenzia e, dall'altro, a migliorare il coordinamento di livello strategico e tattico nel settore della cybersicurezza *(Capo Servizio Gabinetto)*;

4.5 lo sviluppo delle attività di cooperazione internazionale a supporto della definizione delle priorità di ricerca e sviluppo per conseguire un'autonomia tecnologica dell'UE (*Capo Servizio Strategie e Cooperazione per l'allineamento del quadro strategico e di cooperazione internazionale; Capo Servizio Programmi industriali, tecnologici e di ricerca per il quadro delle priorità di ricerca e sviluppo*).

OBIETTIVO STRATEGICO N. 5

ESSERE UN CENTRO DI ECCELLENZA CON UN'ORGANIZZAZIONE A GEOMETRIE VARIABILI, capace di modulare *vision*, persone e organizzazione per promuovere l'acquisizione di nuove competenze nel campo della cybersicurezza e l'adozione di strutture organizzative agili, in un contesto giuridico, normativo e comunicativo in continua evoluzione, con i seguenti **Piani d'azione**:

5.1 il reclutamento delle eccellenze nel campo della *cybersecurity*, attraendo i migliori talenti, anche dall'estero, per supportare l'attuazione della Strategia Nazionale di Cybersicurezza 2022-2026 e del relativo Piano di implementazione, anticipando i fabbisogni di personale legati all'evoluzione delle funzioni dell'Agenzia attraverso una pianificazione assunzionale con una proiezione temporale delle spese almeno decennale *(Capo Servizio Risorse umane, strumentali e amministrazione generale e Capo Servizio Amministrazione e bilancio)*;

5.2 lo sviluppo del capitale umano, mediante l'attenzione alla persona sin dall'ingresso in Agenzia e la costante formazione del personale, garantendo la massima efficienza delle risorse finanziarie destinate a tal fine e la sostenibilità finanziaria nel lungo periodo *(Capo Servizio Risorse umane, strumentali e amministrazione generale e Capo Servizio Amministrazione e bilancio)*;

5.3 la creazione di percorsi professionali per favorire la contaminazione dei saperi e la creazione di una solida forza lavoro nazionale, da mettere a disposizione del sistema Paese (*Capo Divisione formazione e Capo Divisione consapevolezza)*;

5.4 l'adozione di assetti organizzativi flessibili, per accrescere la tempestività delle risposte alle sollecitazioni esterne garantendo al contempo processi decisionali tracciabili per favorire la misurazione dei risultati attesi, in linea con gli obiettivi attuali e prospettici dell'Agenzia *(Capo Servizio Risorse umane, strumentali e amministrazione generale)*;

5.5 lo sviluppo e il mantenimento in condizioni evolutive di una piattaforma per la "*knowlegde base*" che permetta di organizzare e modellare il patrimonio informativo a disposizione dell'Agenzia anche derivante dall'applicazione delle varie normative cyber, basato sull'impiego di un'anagrafica unica dei soggetti coinvolti, al fine di fornire funzioni di consultazione ed analisi integrate tra i vari Servizi *(Capi Servizio interessati ratione materiae)*;

5.6 l'introduzione di principi, tecniche e metodologie lavorative nell'ottica di coniugare l'efficacia della gestione operativa con la correttezza dell'azione amministrativa e l'efficiente impiego delle risorse pubbliche *(Capo Servizio Risorse umane, strumentali e amministrazione generale)*;

5.7 la dotazione di un insieme di apparati strumentali, ivi compresi quelli logistici, che risultino sempre più in linea con l'evoluzione tecnologica e con gli obiettivi di continuo sviluppo digitale *(Capo Servizio Risorse umane, strumentali e amministrazione generale; Capo Servizio Programmi industriali, tecnologici e di ricerca; Capo Servizio Amministrazione e bilancio e Capo Servizio Gabinetto)*;

5.8 la gestione degli immobili secondo principi di efficienza, anche in situazioni di emergenza, garantendone il costante rispetto della normativa a tutela della salute e della sicurezza nei luoghi di lavoro *(Capo Servizio Risorse umane, strumentali e amministrazione generale)*;

5.9 l'evoluzione dei processi e delle procedure al fine di garantire la tutela dei dati personali per le finalità istituzionali dell'Agenzia in conformità alla normativa vigente, nonché la valorizzazione del patrimonio informativo nel rispetto del fattore sicurezza *(Capo Servizio Gabinetto)*;

5.10 il miglioramento delle attività di informazione e comunicazione relative alle iniziative di resilienza cibernetica realizzate dall'Agenzia attraverso tutte le sue articolazioni (*Capo Divisione Comunicazione e Capo Divisione consapevolezza*);

5.11 la produzione di sistemi di pianificazione, sostenibili finanziariamente, strumentali alla valorizzazione, all'efficientamento e all'innovazione dell'Agenzia nonché di sistemi di acquisizioni utili al raggiungimento delle finalità strategiche del presente Piano (*Capo Servizio Amministrazione e bilancio*).