MISSIONE 1 – COMPONENTE 1 – La Strategia Nazionale di Cybersicurezza 2022-2026

PNRR

Dossier

La rilettura della versione operativa della **Strategia Nazionale di Cybersicurezza 2022-2026** ha come scopo quello di consentire una maggiore semplicità di lettura del documento, mantenendo l'altezza dell' analisi documentale necessaria per approfondire, per ogni misura, le metriche e gli indicatori di misurazione individuati, l'anno di prevalente implementazione delle stesse, oltre alle relative linee guida. Una verifica attenta dei progressi registrati nelle attività di attuazione delle misure richiede, infatti, la definizione di specifici indicatori, sintetizzati nelle 81 misure del **Piano di implementazione delle misure della strategia nazionale di cybersicurezza 2022-2026.** In seguito all'adozione da parte del Presidente del Consiglio dei Ministri, della Strategia Nazionale di Cybersicurezza 2022-2026 e dell'annesso Piano di implementazione, sono state poste in essere una serie di attività prodromiche all'attuazione delle misure. In particolare, è stato definito un modello ed un piano di lavoro per l'elaborazione degli indicatori di misurazione che consentiranno di elaborare, a partire dal secondo anno di implementazione, dei KPI che permetteranno di registrare i progressi effettivi rispetto agli obiettivi della Strategia e di identificare i trend delle prestazioni. Tali dati saranno visualizzabili grazie ad un apposito "cruscotto" che consentirà di automatizzarne l'elaborazione per le successive attività di reporting dei risultati conseguiti previste dal DL 82/2021. Sul punto si evidenzia che gli indicatori elaborati mirano a misurare l'effettivo grado di implementazione delle diverse misure e non l'efficacia delle attività poste in essere in attuazione delle stesse. Con riguardo a quest'ultimo aspetto, infatti, è buona prassi assicurarne l'efficacia e rilevare la stessa con le più opportune modalità a seconda del tipo di iniziativa posta in essere. Inoltre è importante verificare le misure di prioritaria attuazione, anche in considerazione delle propedeuticità tra le stesse, individuando l'anno di prevalente implementazione, riportato a fianco di ogni misura. L'anno indicato è utile ai fini della pianificazione delle attività e non si riferisce all'anno di rilevazione degli indicatori della misura, in quanto vi sono indicatori misurabili fin dall'avvio delle attività e altri che sono quantificabili solo in un momento successivo. In una prospettiva di pressa al documento è possibile considerare che la velocità di connessione, la numerosità di interazioni tra utenti e l'accessibilità di dati e informazioni online non sono parametri sufficienti a definire lo sviluppo digitale che caratterizza l'età contemporanea, né riescono a descrivere, nella sua interezza, quell'articolata dimensione che chiamiamo spazio cibernetico. In tale ambito trovano posto servizi concepiti per il soddisfacimento delle quotidiane esigenze delle nostre comunità e per lo svolgimento delle relative attività economiche: infrastrutture energetiche, mercati finanziari, forniture di acqua potabile, trasporti di massa, e, non ultime, le funzioni essenziali dello Stato, incluse la sua difesa e integrità. In uno sguardo ampio, proprio di ogni premessa documentale, è possibile altresì illustrare che la complessità e l'interdipendenza dei sistemi è

cresciuta fino a sfumare la dualità tra la dimensione digitale e il mondo reale, rendendo spesso problematica l'identificazione di confini e rispettive caratteristiche. Gli osservatori più attenti, infatti, mettono in luce che se, da una parte, si verifica l'incessante evoluzione delle moderne tecnologie tese a rendere più conveniente la migrazione verso il digitale, dall'altra, appare nella letteratura l'impostazione tesa a valorizzare l'idea che solo la resilienza e la sicurezza delle reti e dei sistemi su cui tali servizi si basano possono garantire la sicurezza per la nostra comunità e, in prospettiva, lo sviluppo economico e il benessere dello Stato. In tale prospettiva di analisi la ricerca scientifica e lo sviluppo industriale determinano, dal canto loro, la diffusione e il progressivo impiego delle cd. *Emerging and Disruptive Technologies* nel cui novero rientrano reti e protocolli di comunicazione di ultima generazione quali il 5G e il 6G, il *blockchain*, l'intelligenza artificiale, il *quantum computing*, l'high performance computing, l'internet of things, la robotica, gli strumenti crittografici evoluti e altre innovazioni di portata tale da parlare di nuova antropologia tecnologica.

Osservare tale complessità pone in risalto anche i rischi presenti in tale nuovo paradigma di pensiero e di azione e le ricadute negli ambiti economico, sociale e politico. In tale ambito si colloca la riflessione interdisciplinare sulla dipendenza tecnologica e potenziale perdita di autonomia strategica dello Stato, con particolare riguardo alle minacce di tipo antropico, in cui si pone il tema del *postumanesimo* e dell'*algoretica*. In tale nuova prospettiva antropologica gli osservatori più illuminati collocano anche le riflessioni sull'illeceità dei profitti strutturando una specifica area della letteratura penalistica afferente al *cyber-crime*. In tale sentiero di politica criminale si riflette anche sull'adozione di misure di prevenzione e mitigazione del rischio volte a innalzare la resilienza delle infrastrutture digitali. Queste ultime concernono sia l'aspetto umano che l'aspetto infrastrutturale infatti non includono soltanto reti, sistemi e dati, ma anche, e soprattutto attori istituzionali, imprese private o cittadini, descrivendo la via della cultura ascrivibile alla cybersicurezza. Se ad oggi, infatti, esiste una diffusa percezione dei rischi correlati alla sicurezza fisica, per cui ogni individuo pone in essere, nella propria quotidianità, azioni volte a tutelare sé stesso e i propri beni, lo stesso non può dirsi per la dimensione digitale, dei cui rischi non si ha ancora piena consapevolezza. Tale aspetto, unito alla sempre più ampia disponibilità – a costi relativamente bassi – di strumenti offensivi, all'accresciuto livello di complessità degli attacchi, alla difficoltà tecnica di attribuire gli stessi a un autore certo, nonché alla possibilità che esistano vulnerabilità di sicurezza gravanti su prodotti e soluzioni informatiche, fa registrare un numero complessivo di azioni ostili in costante aumento. Specificamente, i recenti trend di attacco forniscono potenziali danni economici per imprese con il possibile blocco dell'operatività di infrastrutture energetiche, sia con malfunzionamenti di sistemi informativi impiegati da aziende ospedaliere

e sanitarie sia con la diffusione di dati personali che mirano a screditare figure pubbliche, giornalisti e attivisti politici, fino a metterne in pericolo, talvolta, l'incolumità. Nella lettura di contesto è possibile collare la logica presente nel piano di implementazione della Strategia Nazionale di Cybersicurezza 2022-2026. Schematicamente è possibile articolare una valutazione poliedrica fondata sul tre pilatri:

1) la **definizione di adeguate strategie di cybersicurezza** volte a pianificare, coordinare e attuare misure tese a rendere il Paese sicuro e resiliente anche nel dominio digitale, assicurando, al contempo, la fiducia dei cittadini nella possibilità di sfruttarne i relativi vantaggi competitivi, nella piena tutela dei diritti e delle libertà fondamentali;

2) lo **sviluppo delle misure della cybersicurezza**[1], che sono divenute una questione di importanza strategica, fondamento del processo di digitalizzazione del Paese, quale elemento imprescindibile della trasformazione digitale, anche nell'ottica di conseguire l'autonomia nazionale strategica nel settore;

3) Il **progresso culturale** inter e transdisciplare, intergenerazionale e interclassista, verso un approccio "security-oriented", tassello indispensabile per tutelare il nostro sistema istituzionale e amministrativo.

Effettuando una lettura storica del dato giuridico, osservando quindi lo sviluppo delle normative sul tema di riferimento, è possibile notare che si sono adottati una serie di provvedimenti sostanzialmente diretti sia ad acquisire, sviluppare e rafforzare le necessarie capacità cyber nazionali, sia a garantire l'unicità istituzionale di indirizzo e di azione rispetto ad un'area di intervento ampia e trasversale, terreno di confronto alimentato dalla valutazione sistemica della cybersicurezza. Specificamente, la concretizzazione tesa alla modifica dell'architettura amministrativa si è manifestata attraverso l'adozione del decreto-legge 14 giugno 2021, n. 82. Il decreto ha istituito l'Agenzia per la Cybersicurezza Nazionale (ACN), con l'obiettivo di razionalizzare e semplificare il frammentato sistema di competenze, esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico. Nel dettaglio, con la creazione dell'ACN si è voluto mettere a sistema l'esperienza accumulata nel contesto del DPCM 17 febbraio 2017 [2]Direttiva recante indirizzi per la protezione cibernetica e la sicurezza

[1] la stessa deve poi essere percepita non come un costo, ma come un investimento e un fattore abilitante per lo sviluppo dell'economia e dell'industria nazionale, al fine di accrescere la competitività del Sistema-Paese a livello globale

[2] Il presente decreto definisce, in un contesto unitario e integrato, l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, indicando a tal fine i compiti affidati a ciascuna componente ed i meccanismi e le procedure da seguire ai fini della riduzione delle vulnerabilita',

informatica nazionali, nonché di quella maturata da altri Paesi, riconoscendo autonoma dignità alla sicurezza e alla resilienza cibernetica ponendole sotto la responsabilità del Presidente del Consiglio dei ministri a fondamento del processo di digitalizzazione del Paese, attraverso un più ampio ruolo di sinergia e coordinamento con tutte le Amministrazioni competenti in materia. Scendendo nel sentiero applicativo, per assicurare la *cyber-resilience*, l'ACN tende a porsi come una fucina di competenze, interne nell'ambito di altre Pubbliche Amministrazioni al fine di innalzare l'approccio integrale in ambito cyber nazionale, sia da far crescere a livello esterno gli effetti più fecondi. Nel dettaglio, per svolgere i suoi molteplici compiti istituzionali l'ACN necessita di numerose ed elevate professionalità. Tale prospettiva è contemplata nel Piano con la specifica previsione di reclutamento di esperti, che raggiungeranno il target delle 800 unità nel 2027. Ciò consentirà anche di arginare la fuga delle competenze verso l'estero, il c.d. *brain drain*[3]. In altro versante, per quel che concerne le attività di prevenzione e contrasto ai crimini informatici, il Piano prevede che la Polizia di Stato attraverso il Servizio di Polizia Postale e delle Comunicazioni, operi con il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), quale unità specializzata nella protezione delle infrastrutture critiche informatizzate dai reati informatici e punto di contatto nazionale per le emergenze in materia di criminalità informatica transnazionale. Il Piano prevede altresì che nell'ambito del Dipartimento di Pubblica Sicurezza sia creata la Direzione Centrale per la polizia scientifica e la sicurezza cibernetica, nella quale confluiscono le attribuzioni di organo centrale del Ministero dell'Interno per la sicurezza e la regolarità delle comunicazioni e quelle di contrasto ai reati di sfruttamento sessuale per via informatica e di prevenzione del terrorismo, in precedenza assicurate dal Servizio polizia postale e delle comunicazioni. Infatti, presso la Direzione Centrale per la Sicurezza Cibernetica opererà il *Computer Emergency Response Team* (CERT) del Ministero dell'Interno, istituito per garantire la sicurezza delle reti e dei sistemi informativi del Dicastero, attraverso la prevenzione e la gestione degli eventi critici. In tale ambito tematico, per quanto riguarda l'Arma dei Carabinieri, il Reparto Indagini Telematiche del Raggruppamento Operativo Speciale (ROS) costituisce l'articolazione specializzata dell'Arma nel contrasto alla criminalità informatica, nello studio e sperimentazione delle tecnologie per l'esplorazione del web e l'intercettazione dei flussi telematici, mentre per la Guardia di Finanza è il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche (NSTPFT) quale Reparto Speciale deputato al contrasto

della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalita' dei sistemi in caso di crisi.

[3] È il fenomeno che produce come conseguenza la cosiddetta fuga dei cervelli, consistente nel trasferimento di studiosi e intellettuali da uno stato a un altro, nel quale trovano migliori opportunità di lavoro e retribuzioni più elevate

delle frodi telematiche ed informatiche, nonché alla tutela della privacy. All'interno della macro area della sicurezza informatica, con particolare riguardo alla difesa e sicurezza dello Stato, il Ministero della Difesa definisce e coordina la politica militare, la governance e le capacità militari nell'ambiente cibernetico, nonché lo sviluppo di capacità cibernetiche e la protezione delle proprie reti e sistemi sia sul territorio nazionale sia nei teatri operativi all'estero. La Difesa, attraverso le articolazioni specialistiche dedicate, conduce infatti operazioni militari cibernetiche offensive e difensive nei casi previsti. Il Ministero della Difesa, pertanto, assicura, anche in situazioni di crisi di natura cibernetica (sia nazionale sia internazionale), tutti i servizi e le attività necessari, da un lato, a garantire la protezione, la resilienza e l'efficienza delle reti e infrastrutture militari e, dall'altro, a sviluppare le proprie peculiari capacità necessarie all'implementazione di attività di supporto, difesa, reazione e stabilizzazione. La ricerca ed elaborazione informativa, finalizzata alla tutela degli interessi politici, militari, economici, scientifici e industriali dell'Italia, è affidata al Comparto intelligence, che a tali fini provvede anche alle attività volte alla rilevazione e alla sistematica azione di monitoraggio, prevenzione e contrasto delle minacce cibernetiche più insidiose, perpetrate nel o attraverso l'ambiente digitale, anche attraverso la conduzione di operazioni cyber. Un ruolo rilevante è inoltre costituito dalla **cyber diplomacy**, intesa come il ricorso a strumenti e iniziative diplomatiche per conseguire gli interessi nazionali del Paese nello spazio cibernetico e come parte delle più ampie attività di politica estera, tenuto conto dell'impatto della tecnologia sulle relazioni internazionali. Specificamente **tale attività fa capo all'Unità per le politiche e la sicurezza dello spazio cibernetico del Ministero per gli Affari Esteri e la Cooperazione Internazionale (MAECI).** Al di là degli attori istituzionali con competenze in materia cyber la presente strategia è ispirata ad un approccio "whole-of-society[4]", che vede coinvolti anche gli operatori privati, il **mondo accademico e della ricerca**, nonché la società civile nel suo complesso e la stessa cittadinanza. L'idea dell'interconnessione propria di un sistema antropologico di ecologia integrale consente di focalizzare che l'obiettivo della sicurezza cibernetica nazionale può essere raggiunto solo attraverso il contributo di tutte le componenti del tessuto sociale, nessuno escluso. La riflessione posta in tale direzione di sguardo deve tener conto della rapida evoluzione tecnologica che ormai caratterizza il mondo contemporaneo. Appare quindi necessario partire dalla valutazione dei rischi:

[4] La strategia dell'Unione della sicurezza si basa su un approccio dell'intera società, che riunisce tutte le istituzioni, le organizzazioni e le autorità con un ruolo nella protezione dei nostri cittadini. Oltre al sostegno e alle competenze che forniscono agli Stati membri, le agenzie dell'UE svolgono un ruolo cruciale nel promuovere la cooperazione e lo scambio di informazioni tra le autorità nazionali degli Stati membri a livello operativo.

1) rischi sistemici connessi ad attacchi cyber dovuti a cybercriminali, attivisti o a campagne statuali coordinate, che sfruttano errori software, errate configurazioni, debolezze nei protocolli e/o umane, per sottrarre dati o arrecare danni ai sistemi;

2) rischi connessi con le tecnologie impiegate, le quali sono sviluppate e prodotte da grandi realtà aziendali, talvolta controllate o, comunque, influenzate nel loro operato dai Governi in cui hanno sede, con conseguenti possibili ingerenze nella catena degli approvvigionamenti, sia in termini di disponibilità sul mercato delle relative componenti, sia di affidabilità delle stesse;

3) rischi legati alla diffusione, attraverso lo spazio cibernetico, di fake news, deepfake e campagne di disinformazione che tendono a confondere e destabilizzare i cittadini di un Paese immergendoli in uno spazio informativo estremamente dinamico e orizzontale, caratterizzato da un insieme pressoché infinito di sorgenti di notizie che polarizzano le opinioni cambiando il modo in cui percepiamo la realtà.

In considerazione dei citati rischi, la strategia Nazionale di Cybersicurezza 2022-2026 mira ad affrontare le sfide inerenti il rafforzamento della resilienza nella transizione digitale del sistema Paese, promuovendo un uso sicuro delle tecnologie, indispensabili per la nostra prosperità economica, presente e futura, tesa al conseguimento dell'autonomia strategica nella dimensione cibernetica, l'anticipazione dell'evoluzione della minaccia cyber, la gestione di crisi cibernetiche in scenari geopolitici complessi, nonché il contrasto della disinformazione online, nel rispetto dei diritti umani, dei nostri valori e principi costituzionali. Tale prospettiva appare cruciale poter assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione e in particolare nel suo tessuto produttivo. In questa direzione non ci può essere transizione digitale senza un'adeguata resilienza agli attacchi e agli incidenti cyber. Infatti, la cybersicurezza degli assetti e dei servizi digitali è l'elemento imprescindibile della loro fruibilità da parte del cittadino, il quale sarà non solo incentivato all'utilizzo degli stessi, ma ne farà ricorso in totale fiducia e con la consapevolezza che i suoi dati sono adeguatamente protetti. Conseguentemente, **la resilienza non deve essere intesa solo nell'accezione tecnica, ma anche sotto il profilo della cultura della sicurezza informatica e della disponibilità di un'adeguata forza lavoro qualificata**. In tale ambito, è fondamentale la professionalizzazione delle amministrazioni coinvolte nel processo della strategia nazionale, nelle discipline STEM (Scienze, Tecnologia, Ingegneria e Matematica) . Inoltre è opportuno considerare l'autonomia strategica nazionale ed europea nel settore del digitale. In tale ambito la reportistica istituzionale indica che a livello UE, l'eccessiva frammentazione e competizione tra gli Stati Membri ha costituito, fino ad oggi, un grosso ostacolo allo sviluppo di tecnologia

"made in EU" e alla creazione di grandi aziende di erogazione di servizi digitali. L'UE e, in particolare, l'Italia, si trova in una posizione di dipendenza tecnologica da altri Paesi, leader nella produzione di software e delle cosiddette *Emerging and Disruptive Technologies* quali, ad esempio, l'Intelligenza Artificiale e il quantum computing. Inoltre, a seguito dell'esperienza maturata dal nostro Paese nell'implementazione del "Quadro strategico nazionale per la protezione dello spazio cibernetico[5]" e dell'annesso "Piano nazionale per la protezione cibernetica e la sicurezza informatica[6]", quali primi documenti strategici nazionali in materia di cybersecurity, è apparso chiaro come sia necessario puntare su tattiche di difesa volte ad aumentare i costi di eventuali attività cyber offensive, così da renderle economicamente svantaggiose. Ciò presuppone, tuttavia, un cambio radicale di paradigma. Se è vero, infatti, che rincorrere la minaccia non è una strategia vincente, è anche vero che stare al passo con essa non è più sufficiente. Occorre, per quanto possibile, anticiparla, ossia prevederla, prevenirla e mitigarne il più possibile gli impatti. Analizzando il problema delle crisi cibernetiche emerge **l'importanza primaria di un meccanismo efficiente di gestione delle criticità**, che consenta, con l'apporto di tutti i soggetti interessati, di scalare l'intensità delle attività sulla base della pericolosità della minaccia cyber, dall'allerta preventiva in vista di possibili eventi cyber sistemici su larga scala, fino al loro verificarsi effettivo, che fa scattare l'immediata applicazione di strumenti, procedure e norme di linguaggio comuni. La rapidità con cui eventi cyber possono verificarsi e susseguirsi, specie in scenari geopolitici complessi, richiede, infatti, un coordinamento continuativo tra tutti i soggetti pubblici e privati interessati, nonché prontezza nel dispiegamento di un set predefinito di risposte concrete. Il carattere per definizione transnazionale della minaccia cibernetica e la sua pervasività richiedono un approccio internazionale alla tematica, posto che i singoli Stati devono necessariamente agire sinergicamente per far fronte alla stessa. Ciò presuppone, necessariamente, un comune livello di preparazione e di interoperabilità. In tale prospettiva si conferma strategico il **rafforzamento della cooperazione bilaterale e multilaterale**. Parimenti è determinate contrastare la disinformazione online nel più ampio contesto della cd. minaccia ibrida. Infatti, il ricorso sempre più massivo alla disinformazione online richiede, specie quando essa assume connotazioni strutturate, azioni preventive e di contrasto sinergiche e coordinate a livello sia nazionale che internazionale per ostacolare i tentativi di mettere a repentaglio il sistema di valori su cui si base il nostro Paese. In tale sguardo di sineriga, per implementare la Strategia Nazionale di Cybersicurezza 2022-2026 e affrontare le richiamate sfide, è previsto un adeguato programma di investimenti e leve finanziarie. Al di là degli strumenti finanziari già assegnati

[5] https://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf
[6] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

alle Amministrazioni con competenza in materia cyber, potranno anche essere messi a disposizione appositi fondi previsti di anno in anno dalle leggi finanziarie, per supportare specifici progetti di interesse. A tale fine sarà riservata una quota percentuale degli investimenti nazionali lordi su base annuale. Tali leve finanziarie potranno anche consistere in sgravi fiscali per le aziende o nell'introduzione di aree nazionali a tassazione agevolata per la costituzione, ad esempio, di un "**parco nazionale della cybersicurezza**[7]" e dei relativi "**hub**" delocalizzati sull'intero territorio nazionale. Vi saranno, inoltre, anche i finanziamenti che l'Agenzia sarà chiamata a gestire in quanto, sempre ai sensi del citato decreto, è designata quale Centro Nazionale di Coordinamento (NCC) sulla base dell'articolo 6 del regolamento 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021[8]. Nel dettaglio, tale atto normativo istituisce il **Centro europeo di competenza per la cybersicurezza** nell'ambito industriale, tecnologico e della ricerca, unitamente alla rete dei centri nazionali di coordinamento, il quale convoglierà in particolare i finanziamenti provenienti dai programmi

[7] Misura 49 – Attori responsabili ACN, MIDT, MEF, MISE, Realizzare un "parco nazionale della cybersicurezza" che ospiti le infrastrutture necessarie allo svolgimento di attività di ricerca e sviluppo nell'ambito della cybersecurity e delle tecnologie digitali, dotato di una struttura "diffusa", con ramificazioni distribuite sull'intero territorio nazionale.

[8] Uno Stato membro può, in qualsiasi momento, chiedere alla Commissione un parere in merito al possesso della necessaria capacità dell'ente che ha designato o intende designare quale proprio centro nazionale di coordinamento per la gestione dei fondi al fine di assolvere la missione e conseguire gli obiettivi di cui al presente regolamento. La Commissione emette il suo parere a tale Stato membro entro tre mesi dalla richiesta. Sulla base della notifica da parte di uno Stato membro di un ente, il consiglio di direzione provvede, entro tre mesi dalla notifica, a inserire nell'elenco tale ente in quanto centro nazionale di coordinamento. Il Centro di competenza pubblica l'elenco dei centri nazionali di coordinamento designati. Gli Stati membri possono designare in qualsiasi momento un nuovo ente come centro nazionale di coordinamento ai fini del presente regolamento. Il centro nazionale di coordinamento designato è un ente del settore pubblico o un ente a partecipazione pubblica maggioritaria che esercita funzioni amministrative pubbliche ai sensi del diritto nazionale, anche per delega, ed è in grado di sostenere il Centro di competenza e la rete nell'assolvimento della loro missione. Esso dispone di competenze in materia di cybersicurezza nell'ambito della ricerca e della tecnologia o vi ha accesso. Esso è in grado di interagire e di coordinarsi efficacemente con l'industria, il settore pubblico, la comunità accademica e della ricerca e i cittadini, nonché con le autorità designate a norma della direttiva (UE) 2016/1148. In qualsiasi momento, i centri nazionali di coordinamento possono chiedere di ottenere il riconoscimento della loro necessaria capacità di gestire i fondi in per assolvere la missione e conseguire gli obiettivi di cui al presente regolamento, conformemente ai regolamenti (UE) 2021/695 e (UE) 2021/694. Entro tre mesi da tale richiesta, la Commissione valuta tale capacità del centro nazionale di coordinamento in questione di gestire i fondi e adotta una decisione.

Orizzonte Europa[9] ed **Europa Digitale**[10]. Certamente uno strumento strategico per affrontare tali sfide strategiche è il Piano Nazionale di Ripresa e Resilienza. Analizzando il PNRR, nell'ambito della Missione 1 "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo", sono incluse le attività di transizione digitale della Pubblica Amministrazione, quali il progetto del Cloud Nazionale e la digitalizzazione dei processi e servizi per i cittadini, la cui realizzazione porterà al potenziamento delle capacità di resilienza delle infrastrutture e dei servizi digitali del Paese. Inoltre, lo specifico Investimento 1.5 "Cybersecurity", pari a 623 milioni di euro, rimesso all'Agenzia per la Cybersicurezza Nazionale quale soggetto attuatore, prevede la realizzazione di specifiche progettualità per la creazione e lo sviluppo di servizi all'avanguardia per la gestione del rischio cyber, con strette connessioni, a livello nazionale e internazionale, con tutti i principali partner della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia. Ciò, al fine di conseguire un'autonomia tecnologica nazionale ponendo la cybersicurezza e la resilienza a fondamento della trasformazione digitale della Pubblica Amministrazione. In particolare su tale linea di approfondimento il piano di attuazione, d'intesa con il Dipartimento per la Trasformazione Digitale (DTD) nella sua veste di Amministrazione Titolare dell'investimento, è organizzato in tre principali aree d'intervento e, in accordo alle regole tecnico-organizzative del PNRR, coinvolgerà tutti i principali attori nazionali, pubblici e privati, del mondo della cybersecurity[11]. Nello scorrere della Strategia

[9] Orizzonte Europa Bilancio totale 2021-2027: 95,51 miliardi di Euro Principale programma di finanziamento dell'UE per facilitare la collaborazione e rafforzare l'impatto della ricerca e dell'innovazione nello sviluppo, nel sostegno e nell'attuazione delle politiche dell'UE, affrontando, nel contempo, le sfide globali. Esso sostiene la creazione e una migliore diffusione di conoscenze e tecnologie di eccellenza. Inoltre, crea posti di lavoro, impegna pienamente il bacino di talenti dell'UE, stimola la crescita economica, promuove la competitività industriale e ottimizza l'impatto degli investimenti all'interno di uno Spazio europeo della ricerca rafforzato

[10] Primo piano europeo di finanziamento per espandere le competenze digitali dei cittadini e delle imprese e per velocizzare la ripresa economica e sociale. Il programma, che mira a colmare il divario tra la ricerca sulle tecnologie digitali e la diffusione sul mercato, finanzia progetti in cinque settori cruciali: supercalcolo, intelligenza artificiale, cybersicurezza, competenze digitali avanzate,uso diffuso delle tecnologie digitali nell'economia e nella società. Gli investimenti sostengono il duplice obiettivo dell'Unione europea della transizione verde e della trasformazione digitale e rafforzano la resilienza e la sovranità digitale dell'Unione.

[11] 174 Milioni per servizi Cyber Nazionali - Contribuendo all'attivazione e piena operatività dell'Agenzia, le reti e i servizi che saranno realizzati potenzieranno le capacità nazionali di prevenzione, monitoraggio, risposta e mitigazione di minacce cyber. 301.7 Milioni per interventi di potenziamento della resilienza cyber per la PA - Le capacità cyber della PA sono un elemento fondante per una transizione digitale sicura del Paese, assicurando quindi adeguati livelli di sicurezza per i dati e i servizi dei cittadini. 147.3 Milioni per laboratori di scrutinio e certificazione tecnologica- Il raggiungimento di un'autonomia tecnologica nazionale passa necessariamente

Nazionale di Cybersicurezza viene descritta anche la visione strategica con gli obiettivi da perseguire. Nel merito, per fronteggiare al meglio le sfide per il sistema Paese sopra delineate, sono stati individuati tre obiettivi fondamentali – la protezione, la risposta e lo sviluppo – e relative misure, funzionali ad assicurare la concreta attuazione della strategia, raggruppate per aree tematiche e declinabili sia dal punto di vista organizzativo e di policy che prettamente operativo. Ciascuna misura è stata associata all'obiettivo maggiormente caratterizzante, per ognuna delle quali è indicato il novero degli attori responsabili dell'implementazione e tutti gli altri soggetti a vario titolo interessati, al netto di quelli direttamente beneficiari delle misure. In primo luogo appare opportuno soffermarsi sull'obiettivo protezione. La protezione degli asset strategici nazionali, attraverso un approccio sistemico orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli che possono abilitare una transizione digitale resiliente del Paese. Di particolare importanza è lo sviluppo di strategie e iniziative per la verifica e valutazione della sicurezza delle infrastrutture ICT, ivi inclusi gli aspetti di approvvigionamento e *supply-chain* a impatto nazionale. Per poter assicurare un livello di protezione efficace e duraturo è, infatti, indispensabile: il potenziamento delle capacità del Centro di Valutazione e Certificazione Nazionale dell'Agenzia per la Cybersicurezza Nazionale e, negli ambiti di competenza, dei Centri di Valutazione del Ministero dell'Interno e della Difesa, nonché l'integrazione con una rete di Laboratori Accreditati di Prova, permetterà di sviluppare capacità nazionali di valutazione delle vulnerabilità di tecnologie avanzate a servizio degli *asset* più critici del Paese. Inoltre, è necessaria la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente in materia di cybersicurezza, che tenga conto degli orientamenti e degli sviluppi in ambito europeo ed internazionale. Tale impianto non ricomprende solamente il livello normativo, ma anche l'insieme delle linee guida, gli schemi di certificazione e le policy settoriali rivolte ai soggetti pubblici e agli operatori privati. In tale contesto, assume rilevanza primaria:

- il supporto allo sviluppo di schemi di certificazione e standard europei e internazionali in materia di cybersicurezza;

anche dal potenziamento delle capacità nazionali di scrutinio e certificazione tecnologica, in stretta collaborazione con il mondo privato dell'industria e dell'accademia.

- la promozione dell'utilizzo di schemi di certificazione europea in materia di cybersicurezza, da parte delle imprese italiane specializzate, al fine di conseguire un vantaggio competitivo sul mercato;
- l'adozione di linee guida per le amministrazioni pubbliche, basate su di un approccio "zero trust" quale cambiamento di paradigma nella gestione del rischio cyber, affinché le relative reti, sistemi e servizi soddisfino elevati standard di cybersicurezza;
- la valorizzazione dell'inclusione di elementi di sicurezza cibernetica nelle attività di procurement ICT della Pubblica Amministrazione;
- la definizione di una politica nazionale sulla divulgazione coordinata di vulnerabilità, così da porre il Paese al passo con altre nazioni e con quanto richiesto dalla comunità internazionale;
- la conoscenza approfondita del quadro della minaccia cibernetica e il possesso di adeguati strumenti tecnici, competenze specialistiche e capacità operative, in capo agli attori a vario titolo coinvolti.

L'ulteriore rafforzamento della situational awareness[12] mediante il monitoraggio continuo degli eventi cibernetici e la tempestiva condivisione delle connesse risultanze, secondo gli specifici ambiti di competenza, costituisce, infatti, condizione necessaria ai fini dell'incremento delle capacità nazionali di difesa, resilienza, contrasto al crimine informatico e cyber intelligence. A tal fine, appare essenziale il costante scambio informativo tra pubblico e privato, anche mediante l'introduzione di canali di comunicazione protetti e di un sistema integrato di gestione del rischio cyber per identificare e analizzare vulnerabilità, minacce e rischi in chiave previsionale e programmatica. Inoltre è fondamentale un potenziamento del livello di maturità delle capacità cyber della Pubblica Amministrazione, assicurando una trasformazione digitale sicura e resiliente. A tal fine, la transizione verso il Cloud della Pubblica Amministrazione, sia verso tecnologie di Public Cloud che mediante il Polo Strategico Nazionale che rappresenta un elemento fondante per garantire adeguate garanzie di autonomia tecnologica del Paese. La migrazione a tecnologie Cloud, siano esse del PSN o del Public Cloud, sarà guidata e controllata da una metodologia di gestione del rischio il cui elemento principale è la classificazione dei dati e dei servizi della Pubblica Amministrazione. Al riguardo saranno altresì coordinati interventi di potenziamento delle capacità di identificazione, monitoraggio e controllo del rischio cyber

[12] E' il campo di studio che riguarda la comprensione dell'ambiente critico per i responsabili delle decisioni in aree complesse e dinamiche

nella Pubblica Amministrazione con lo sviluppo di capacità di protezione per le infrastrutture nazionali, realizzate anche mediante programmi con i privati, tra cui:

1) il monitoraggio delle configurazioni *Border Gateway Protocol* [13]mediante lo sviluppo di procedure, processi e strumenti in cooperazione con gli Internet Exchange Point nazionali, al fine di aumentare la resilienza delle infrastrutture nazionali;

2) un'infrastruttura di risoluzione *Domain Name System*[14] nazionale, con servizi di protezione della navigazione web a uso della PA, per un utilizzo più sicuro della rete Internet;

3) il monitoraggio di vulnerabilità e configurazioni erronee dei servizi digitali della PA, sia a livello applicativo che di configurazioni *Domain Name System*, al fine di ridurre in modo proattivo potenziali superfici di attacco;

4) il monitoraggio delle configurazioni dei domini di posta elettronica della PA, supportando e facilitando l'applicazione delle migliori configurazioni di sicurezza contro eventi di *phishing* [15]o abusi collegati;

5) la promozione dell'uso della crittografia come strumento di cybersicurezza, favorendo l'impiego di crittografia commerciale lungo l'intero ciclo di vita dei sistemi e servizi ICT, in conformità ai principi della sicurezza e della tutela della privacy, nel rispetto dei principi stabiliti dalla normativa nazionale ed europea.

6) l'implementazione di un'azione di coordinamento nazionale, coerente con le iniziative adottate a livello europeo, per prevenire e contrastare la disinformazione online, che sfruttando le caratteristiche del dominio cibernetico, mira a condizionare/influenzare processi politici, economici e sociali del Paese.

La Strategia Nazionale di Cybersicurezza 2022-2026 si sofferma anche sulle risposte alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso l'impiego di elevate capacità

[13] è un protocollo di routing di tipo EGP usato per connettere tra loro più router che appartengono a sistemi autonomi distinti e che vengono chiamati router gateway o router di bordo/confine. Specificamente è un protocollo di instradamento che agisce nel cuore della rete Internet. Il BGP funziona attraverso la gestione di una tabella di reti IP, o prefissi, che forniscono informazioni sulla raggiungibilità delle diverse reti tra più sistemi autonomi.

[14] indica un sistema utilizzato per assegnare nomi ai nodi della rete. Indica anche il protocollo che regola il funzionamento del servizio, i programmi che lo implementano, i server su cui questi vengono elaborati, l'insieme di questi server che cooperano per fornire il servizio più intelligente

[15] è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale

nazionali di monitoraggio, rilevamento, analisi e risposta e l'attivazione di processi che coinvolgano tutti gli attori facenti parte dell'ecosistema di cybersicurezza nazionale. Una risposta quanto più tempestiva e risolutiva deve, infatti, necessariamente basarsi su di un sistema di gestione crisi cibernetica nazionale e transnazionale , assicurato dal Nucleo per la Cybersicurezza (NCS) che sia fondato su procedure di collaborazione consolidate supportate da costanti flussi informativi ed elementi di conoscenza condivisi anche grazie a reti e infrastrutture nazionali e transnazionali, con il coinvolgimento delle Amministrazioni e degli operatori privati interessati[16]. Per poter realizzare fattivamente gli obiettivi descritti, è indispensabile fare riferimento a una serie di fattori abilitanti, in particolare la formazione e la promozione della cultura della sicurezza cibernetica e cooperazione, i quali, data la loro trasversalità, sono necessariamente correlati a tutti e tre gli obiettivi sopra delineati, quali elementi imprescindibili per la loro piena attuazione. In primo luogo, la **formazione in ambito cyber**, con particolare focus sulle nuove tecnologie. Lo sviluppo di nuove iniziative e il rafforzamento di quelle esistenti deve muovere, infatti, dall'esigenza sempre più concreta di stimolare la creazione di una solida forza lavoro nazionale, composta da esperti e giovani talenti in possesso delle capacità e delle competenze necessarie per poter essere applicate a beneficio delle imprese e delle amministrazioni italiane, con riferimento alle tecnologie informatiche in generale e a quelle relative alla sicurezza cibernetica in particolare. Questo deve realizzarsi attraverso meccanismi incentivanti che favoriscano la progressiva familiarizzazione degli studenti con le nuove tecnologie informatiche, **con approccio formativo e di respiro culturale, prima ancora che tecnico e pratico**. Inoltre a livello di istruzione di base è opportuno intervenire, prevedendo l'introduzione dell'informatica come disciplina, in tutti i livelli del sistema educativo, dalla scuola primaria all'università e, dalla secondaria di secondo grado in poi, in tutti i contesti, inclusi quelli generalisti e quelli orientati verso professioni non tecniche. Altro aspetto rilevante concerne i meccanismi incentivanti che promuovano l'inserimento in carriere tecnico-scientifiche con particolare riferimento agli aspetti ci cybersicurezza. Questo aspetto si può realizzare con interventi a vari livelli. In primis con i percorsi tecnici e professionali della scuola secondaria di secondo grado; secondariamente con gli Istituti Tecnici Superiori (ITS) e con i corsi di laurea ad orientamento professionale recentemente introdotti dalla normativa. In terzo luogo con i corsi di laurea e laurea magistrale tradizionali, i master e i dottorati di ricerca. Meritano specifica attenzione gli ITS e i corsi di laurea ad orientamento professionale che, realizzati in collaborazione con realtà produttive, possono favorire il rapido inserimento nel mondo del lavoro e la calibrazione dei

[16] In tale ambito dovranno altresì essere assicurati: lo sviluppo di un sistema di coordinamento continuativo di tutte le Amministrazioni che compongono il NCS, che garantisca una tempestiva e sinergica gestione dei vari possibili scenari di crisi cibernetica, nonché una immediata implementazione delle misure di risposta.

profili e quindi dei percorsi formativi. Sempre strategico appare il continuo aggiornamento della didattica e della preparazione del corpo docente, a tutti i livelli di istruzione scolastica e universitaria, affinché l'offerta educativa sia al passo con lo sviluppo delle conoscenze e delle tecnologie e con le esigenze dettate dal mercato del lavoro, secondo un approccio fondato sul binomio, ormai inscindibile, sviluppo e sicurezza. Inoltre, attraverso i fondi per la formazione specialistica e l'aggiornamento professionale nei settori pubblico e privato, da realizzarsi in modo continuo e multilivello è possibile favorire la crescita e la qualificazione delle risorse umane operanti nel campo della cybersicurezza per conseguire **una sovranità nazionale digitale delle competenze**. Parimenti, è necessario realizzare un sistema nazionale di certificazione di tali professionalità, sia in ambito accademico che lavorativo, mediante l'attivazione di percorsi di formazione ad hoc approvati dall'ACN e percorsi di formazione specifici per i non specialisti della materia, rivolti ai dipendenti di Pubbliche Amministrazioni e soggetti privati, incluse le PMI, ad iniziare dai top manager, così da sensibilizzare gli stessi in merito all'importanza di concepire la cybersicurezza più come un investimento che come un costo. L'attività formativa dovrà contemplare il potenziamento delle capacità di **cyber diplomacy**, attraverso percorsi mirati per il personale diplomatico da dispiegare nei principali consessi internazionali sulla tematica[17]. Altro fattore abilitante, che si muove in parallelo con le esigenze di formazione, è la promozione della **cultura della sicurezza cibernetica**, al fine di aumentare la consapevolezza del settore pubblico e privato e della società civile sui rischi e le minacce cyber, le quali includono non solo gli attacchi cibernetici propriamente intesi, ma anche la diffusione di contenuti *fake* e il fenomeno del cyberbullismo. In tal proposito è quindi importante che i soggetti pubblici, gli operatori privati e la società civile nel suo complesso, percepiscano il proprio ruolo quale parte attiva e responsabile all'interno del sistema-Paese, attuando comportamenti sicuri e virtuosi nello spazio cibernetico. Concretamente ciò può essere realizzato attraverso la previsione di un programma capillare di educazione digitale a beneficio della collettività e diretto all'adozione di buone prassi e all'acquisizione di capacità di verificare i contenuti e le informazioni reperite online avendo contezza di quegli indicatori che consentono di identificare le c.d. *fake news*. Specificamente all'interno delle organizzazioni pubbliche e private, è possibile escogitare

[17] La cyber diplomacy implica una forte volontà del governo italiano di portare la tematica cyber al centro dell'agenda diplomatica rendendolo un argomento centrale di discussione sui tavoli internazionali. Tale riferimento afferma il riconoscimento che in un dominio come quello cibernetico, connesso per definizione e dove non esiste il concetto di confine statale, è necessario un dialogo e un coordinamento internazionale al fine di prevenire i conflitti, ridurre le minacce e rafforzare le relazioni internazionali. Tale consapevolezza, cristallizzata nella strategia, è per di più in linea con le Conclusioni del Consiglio dell'Unione europea sullo sviluppo della sua posizione in materia di deterrenza informatica del 23 maggio 2022 che hanno sottolineato, per l'appunto, l'importanza della cyber diplomacy per la cyber posture europea.

soluzioni tese a fornire una forte sensibilizzazione delle risorse, ad iniziare dai livelli apicali, non soltanto per promuovere una *cyber hygiene* interna[18], quanto per accrescere la percezione delle esigenze di sicurezza dell'organizzazione e delle minacce a cui questa è esposta, nonché per mettere in campo le azioni di prevenzione più efficaci. A livello nazionale, ciascuna componente *dell'ecosistema cyber* è non solo responsabile, per gli ambiti di competenza, della sicurezza nel dominio digitale, ma è portatrice di esperienze e informazioni cruciali per incrementare le capacità di prevenzione e contrasto alle minacce, promuovere il trasferimento di know-how, tecnologie e risorse umane, nonché per consentire alle imprese innovative di espandersi con maggiore facilità sul mercato. **A livello internazionale, l'Italia collabora nella promozione del rispetto dei diritti umani, delle libertà fondamentali e dei valori democratici nel dominio cyber, per far sì che questo rimanga uno spazio globale, aperto, stabile e sicuro, in cui il diritto internazionale ed i principi condivisi siano rispettati**. A tal fine, il nostro Paese partecipa alle principali iniziative di cooperazione, di ***cyber diplomacy*** e di ***capacity building*** nei confronti di Paesi partner che stanno sperimentando un rapido sviluppo digitale[19]. Inoltre, l'Italia condivide le metodologie e gli strumenti di deterrenza e risposta ad attacchi cibernetici definiti a livello UE e NATO. In tale contesto, la partecipazione alle iniziative internazionali e la prosecuzione dei dialoghi e delle relazioni con i Paesi di interesse, sono elementi indispensabili per rafforzare ulteriormente il posizionamento dell'Italia, per favorire lo scambio di conoscenze e per promuovere l'internazionalizzazione delle imprese nazionali attive nel settore. Trasversale ai citati obiettivi di protezione, risposta e sviluppo, nonché ai richiamati fattori abilitanti della formazione, della promozione della cultura della cybersicurezza e della cooperazione, è la **Partnership Pubblico-Privato (PPP)**, la quale permea interamente la presente strategia, improntata come già detto ad un approccio *whole-of-society*[20], che vede il settore pubblico agire sinergicamente con quello privato, il mondo accademico e della ricerca, i media, le famiglie e gli individui per rafforzare la resilienza cibernetica della nazione e della società nel suo insieme. Infine, la strategia non può ritenersi completa senza un insieme di metriche e di Key Performance Indicator (KPI), quali strumenti che consentano di misurare non solo l'effettiva attuazione della stessa, ma anche tutte quelle azioni, da essa contemplate, la cui

[18] La Cyber Hygiene consiste in una serie di principi e regole da seguire quotidianamente per minimizzare i rischi cyber derivanti dall'uso di sistemi informatici che espongono ad cyber attacchi.

[19] Ciò, anche attraverso l'implementazione di confidence building measure (CBM) dell'OSCE, al fine di evitare l'emergere di tensioni a livello politico-militare derivanti dall'impiego delle tecnologie ICT

[20] La strategia dell'Unione della sicurezza si basa su un approccio dell'intera società, che riunisce tutte le istituzioni, le organizzazioni e le autorità con un ruolo nella protezione dei nostri cittadini. Oltre al sostegno e alle competenze che forniscono agli Stati membri, le agenzie dell'UE svolgono un ruolo cruciale nel promuovere la cooperazione e lo scambio di informazioni tra le autorità nazionali degli Stati membri a livello operativo. Fonte https://knowledge4policy.ec.europa.eu/glossary-item/whole-society-approach%C2%A0_en

effettiva efficacia e impatto resterebbero altrimenti inesplorati. In particolare, è stato definito un modello ed un piano di lavoro per l'elaborazione degli indicatori di misurazione che consentiranno di elaborare, a partire dal secondo anno di implementazione, dei KPI che permetteranno di registrare i progressi effettivi rispetto agli obiettivi della Strategia e di identificare i trend delle prestazioni. Tali dati saranno visualizzabili grazie ad un apposito "cruscotto" che consentirà di automatizzarne l'elaborazione per le successive attività di reporting dei risultati conseguiti previste dal DL 82/2021.

Il Piano di implementazione delle misure della strategia nazionale di cybersicurezza 2022-2026

Il piano di implementazione presenta 22 aree tematiche e 81 misure specifiche. Esso riporta per ciascuno degli obiettivi della Strategia Nazionale di Cybersicurezza – protezione, risposta e sviluppo – le misure da porre in essere per il loro conseguimento.

Protezione

Scrutinio tecnologico

- Misura 1 – Attore responsabile ACN Rafforzare il sistema di scrutinio tecnologico nazionale a supporto della sicurezza della supply chain delle particolari categorie di asset rientranti nel Perimetro e per l'adozione di schemi di certificazione europea di cybersecurity, anche mediante l'accreditamento di laboratori di valutazione pubblico/privati.
- Misura 2 -Attore responsabile Ministero Interni e Ministero Difesa Sviluppare le capacità dei Centri di Valutazione del Ministero dell'Interno e del Ministero della Difesa accreditati dall'ACN, quali organismi di valutazione della conformità, per i sistemi di rispettiva competenza.
- Misura 3 – Attore responsabile ACN Attivazione di un nucleo ispettivo centrale presso l'Agenzia a supporto delle attività ispettive in relazione agli obblighi derivanti dalle normative cyber vigenti.

- Misura 4 – Attore responsabile Ministero Interni e Ministero Difesa Attivazione di omologhe unità ispettive presso i Ministeri dell'Interno e della Difesa, a supporto delle attività ispettive in relazione agli obblighi derivanti dalle normative cyber vigenti.

Definizione e mantenimento di un quadro giuridico nazionale aggiornato e coerente

- Misura 5 – Attore responsabile ACN, MITD Supportare lo sviluppo, valutandone l'adeguatezza in termini di sicurezza nazionale, degli schemi di certificazione in materia di cybersicurezza e, in collaborazione con il settore privato, promuoverne l'adozione e l'utilizzo da parte dei fornitori di servizi e delle imprese italiane, favorendo lo sviluppo del tessuto imprenditoriale nazionale specializzato al fine di conseguire un vantaggio competitivo sul mercato.
- Misura 6 – Attore responsabile MITD, ACN Introdurre norme giuridiche che valorizzino l'inclusione di elementi di sicurezza cibernetica nelle attività di procurement ICT della Pubblica Amministrazione, fornendo indicazioni sia a quest'ultima che agli operatori di mercato per garantire che i beni e i servizi informatici, acquistati dai soggetti pubblici nell'ambito di gare d'appalto o di specifici accordi quadro, rispondano ad adeguati livelli di cybersicurezza. Ciò, compatibilmente con la celere definizione delle relative procedure di aggiudicazione.
- Misura 7 – Attori responsabile MITD, MEF, ACN Promuovere la realizzazione, a livello nazionale ed europeo, di un sistema di gare pubbliche impostato su criteri che garantiscano soluzioni di qualità sotto il profilo della cybersicurezza.
- Misura 8 – Attori responsabile PCM, ACN Introdurre norme giuridiche volte a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale
- Misura 9 – Attori responsabili ACN, Ministero Interno e Ministero Giustizia Definire una politica nazionale sulla divulgazione coordinata di vulnerabilità (coordinated vulnerability disclosure).
- Misura 10 – Attore responsabile ACN Pubblicare linee guida sulla cybersecurity per le Amministrazioni Pubbliche, con differenti gradi di cogenza (con riguardo, ad es., a MFA, registrazione e conservazione dei log, ecc.), anche in riferimento alla transizione

al cloud e favorendo una gestione continuativa e automatizzata del rischio cyber, secondo un approccio “zero trust”.

- Misura 11 – Attore responsabile ACN Porre in essere iniziative di sensibilizzazione per favorire l’applicazione del “Framework Nazionale per la Cybersecurity e la Data Protection” e dei “Controlli essenziali di cybersecurity”, opportunamente aggiornati in linea con il quadro della minaccia, da parte della PA, delle imprese e delle PMI.

Conoscenza approfondita del quadro della minaccia cibernetica

- Misura 12 - Attori responsabili ACN, Ministero Interno, Ministero Difesa, DIS, AISI, AISE Continuare ad accrescere le capacità nazionali di difesa, resilienza, contrasto al crimine e cyber intelligence, rafforzando ulteriormente la situational awareness mediante il monitoraggio continuo e l’analisi di minacce, vulnerabilità e attacchi, secondo gli specifici ambiti di competenza.
- Misura 13 – Attori responsabili ACN Realizzare un servizio di monitoraggio del rischio cyber nazionale a favore delle organizzazioni e del pubblico in generale, al fine di comunicare l’effettivo livello della minaccia, nonché di informare adeguatamente i processi decisionali.

Potenziamento capacità cyber della Pubblica Amministrazione

- Misura 14 - Attori responsabili ACN, Coordinare interventi di potenziamento delle capacità di identificazione, monitoraggio e controllo del rischio cyber nella Pubblica Amministrazione per la messa in sicurezza dei dati e dei servizi dei cittadini.
- Misura 15 – Attori responsabili ACN, Provvedere alla qualificazione dei servizi cloud per la Pubblica Amministrazione, in attuazione della Strategia Cloud Italia, al fine di assicurare adeguati livelli di sicurezza per i servizi e i dati della PA.
- Misura 16 – Attori responsabili MIDT, ACN Facilitare la migrazione sicura dei servizi e dei dati della Pubblica Amministrazione sul cloud, ovvero PSN o Public Cloud, in linea con le attività di classificazione dei dati e dei servizi come da Strategia Cloud Italia.

Sviluppo di capacità di protezione per le infrastrutture nazionali

- Misura 17 - Attori responsabili ACN, Promuovere lo sviluppo di procedure, processi e sistemi di monitoraggio e controllo delle configurazioni BGP nazionali in cooperazione con gli operatori IXP nazionali.
- Misura 18 - Attori responsabili ACN, Promuovere l'implementazione di una infrastruttura di risoluzione DNS nazionale al servizio degli operatori pubblici e privati, sostenendo l'applicazione di controlli di sicurezza sulla navigazione e protezione contro attività malevole condotte anche tramite il DNS.
- Misura 19 – Attori responsabili ACN Implementare servizi di monitoraggio di vulnerabilità e configurazioni erronee dei servizi digitali esposti su Internet di interesse della Pubblica Amministrazione, attuando politiche di early warning
- Misura 20 – Attori responsabili ACN, Ministero Interno, Promuovere l'utilizzo delle migliori pratiche di gestione dei domini di posta elettronica della Pubblica Amministrazione, implementando un servizio di monitoraggio e protezione contro campagne di phishing o abusi.
- Misura 21 - Attori responsabili ACN, Promuovere lo sviluppo e l'implementazione di un servizio nazionale di gestione delle copie dei backup "a freddo", al fine di offrire, alle Pubbliche Amministrazioni e operatori privati, un'infrastruttura con alti livelli di resilienza a supporto di una pronta riattivazione di sistemi e servizi a seguito di guasti o incidenti.

Promozione dell'uso della crittografia

- Misura 22 - Attori responsabili ACN, Promuovere l'uso della crittografia in ambito non classificato, quale impostazione predefinita e comunque fin dalla fase di progettazione di reti, applicazioni e servizi, in conformità ai principi della sicurezza e della tutela della vita privata, nel rispetto dei principi stabiliti dalla normativa nazionale ed europea.
- Misura 23 – Attori responsabili ACN Sviluppo di tecnologie/sistemi di cifratura nazionale in ambito non classificato. A sostegno di tale iniziativa è prevista la creazione di un ecosistema nazionale per il suo mantenimento ed evoluzione.

Definizione e implementazione di un piano di contrasto alla disinformazione online

- Misura 24 – Attori responsabili PCM, DIS Implementare un'azione di coordinamento nazionale, coerente con le iniziative adottate a livello europeo e in sinergia con i Paesi like-minded, per prevenire e contrastare – anche attraverso campagne informative – la disinformazione online che, sfruttando le caratteristiche del dominio cibernetico, mira a condizionare/influenzare processi politici, economici e sociali del Paese.

Risposta

Sistema di gestione crisi nazionale e transnazionale

- Misura 25 – Attori responsabili ACN, NCS Sviluppare un sistema di coordinamento continuativo di tutte le Amministrazioni che compongono il NCS, che garantisca una tempestiva e sinergica gestione dei vari possibili scenari di crisi cibernetica, nonché una immediata implementazione delle misure di risposta.
- Misura 26 - Attori responsabili ACN, NCS, Contribuire alla fattiva ed efficace attivazione dei meccanismi europei di risposta coordinata agli incidenti e alle crisi cibernetiche transnazionali su larga scala.
- Misura 27 – Attore responsabile ACN, Assicurare e facilitare modalità di notifica unitaria degli incidenti di sicurezza cibernetica allo CSIRT per rendere più efficace la capacità di risposta e allarme tempestivo.
- Misura 28 – Attori responsabili PCM, ACN, NCS, Sviluppare ulteriormente le capacità per assicurare una pronta attività di comunicazione istituzionale in caso di incidenti cyber rilevanti o di crisi cibernetica, nonché ogni qual volta si renda necessario svolgere azioni di sensibilizzazione nei confronti della popolazione civile.
- Misura 29 – Attori responsabili ACN NCS, Assicurare il periodico aggiornamento delle procedure operative relative alle misure di risposta connesse ai vari scenari della minaccia cyber per le determinazioni del Presidente del Consiglio, ai sensi della vigente normativa nazionale, e per la conseguente corretta implementazione da parte dei soggetti interessati.

Servizi cyber nazionali

- Misura 30 – Attori responsabili ACN, Realizzare un sistema di raccolta e analisi HyperSOC per aggregare, correlare ed analizzare eventi di sicurezza di interesse al fine di individuare precocemente eventuali "pattern" di attacco complessi, nonché abilitare una gestione del rischio cyber in chiave preventiva e integrata tra molteplici sorgenti dati, sfruttando anche infrastrutture di High Performance Computing e tecnologie di Intelligenza Artificiale e il machine learning.

- Misura 31 – Attori responsabili ACN, Stipulare apposite convenzioni con gli Internet Service Provider (ISP), al fine di condividere eventi di interesse, così da supportare sia il raggiungimento della misura 30, sia l'individuazione precoce di eventuali minacce emergenti e la mitigazione di attacchi al nostro Paese.

- Misura 32 – Attori responsabili ACN, Creare un'infrastruttura di High Performance Computing dedicata alla cybersecurity nazionale per il potenziamento dei servizi cyber nazionali dell'Agenzia, nonché lo sviluppo di strumenti di simulazione, basati sull'Intelligenza Artificiale e il machine learning, per supportare le fasi di prevenzione, scoperta, risposta e predizione degli impatti di attacchi cyber di natura sistemica.

- Misura 33 -Attori responsabili ACN, NCS, Accrescere le capacità di risposta e ripristino a seguito di crisi cibernetiche implementando una rete di CERT settoriali integrata con lo CSIRT Italia, nonché un piano nazionale di gestione crisi che definisca procedure, processi e strumenti da utilizzare in coordinamento con gli operatori pubblici e privati, con l'obiettivo di assicurare la continuità operativa delle reti, dei sistemi informativi e dei servizi informatici.

- Misura 34 – Attori responsabili ACN, Creare un ISAC presso l'ACN, con il compito di coordinare la collazione e l'analisi di informazioni operazionali e strategiche a maggior valor aggiunto prodotte dai vari servizi cyber nazionali. La struttura sarà collegata alla rete europea degli ISAC contribuendo alla realizzazione dello "European CyberShield", previsto dalla Strategia di cybersecurity dell'UE.

- Misura 35 – Attori responsabili ACN, Promuovere la creazione di ISAC settoriali integrati con l'ISAC dell'ACN, anche mediante iniziative pubblico-private, così da favorire il potenziamento dello scambio informativo e di best-practice a servizio delle Pubbliche Amministrazioni e dell'industria nazionale.

- Misura 36 – Attori responsabili ACN, Realizzare un programma di qualificazione in materia di incident response dei SOC/CERT/CSIRT di un gruppo di aziende selezionate, in grado di fornire supporto allo CSIRT Italia nel caso in cui dovesse verificarsi una moltitudine di incidenti cyber di natura sistemica.
- Misura 37 –Attori responsabili ACN, Promuovere la creazione di una gestione integrata e continuativa del rischio cyber nazionale, facilitata da attività di analisi della postura di sicurezza della Pubblica Amministrazione, nonché da strumenti di controllo e monitoraggio della supply chain.

Esercitazioni di cybersicurezza

- Misura 38 – Attori responsabili ACN, Prevedere l'organizzazione di periodiche esercitazioni interministeriali, anche in ambito Perimetro, che riguardano aspetti tecnici e operativi di gestione di eventi o crisi con profili di cybersicurezza.
- Misura 39 – Attori responsabili ACN, NCS, Promuovere e coordinare la partecipazione a esercitazioni europee e internazionali che riguardano la simulazione di eventi di natura cibernetica, al fine di innalzare la resilienza del Paese.

Definizione del posizionamento e della procedura nazionale in materia di attribuzione

- Misura 40 – Attori responsabili DIS, AISE, AISI, MAECI Rafforzare i meccanismi nazionali volti all'applicazione degli strumenti di deterrenza definiti a livello europeo e internazionale per la risposta ad attacchi cyber. In tale contesto, si pone l'esigenza di definire un documento sul posizionamento e sulla procedura nazionale in materia di attribuzione.

Contrasto al cybercrime

- Misura 41 – Attori responsabili Ministero Interno, Ministero Giustizia, MEF Potenziare ulteriormente le capacità di prevenzione e contrasto al crimine informatico da parte della Polizia Postale e delle comunicazioni e delle Forze di polizia, prevedendo anche specifiche attività di addestramento

- Misura 42 – Attori responsabili Ministero Interno, Ministero Giustizia, DIS Potenziare le competenze nel contrasto di attività volte a diffondere contenuti di odio, violenza e discriminazione online.
- Misura 43 – Attori responsabili MAECI, Ministero Interno e Ministero Giustizia, Rafforzare ulteriormente la cooperazione internazionale e lo scambio informativo in materia di contrasto al crimine informatico con gli analoghi organismi europei, internazionali e degli altri Stati.
- Misura 44 – Attori responsabili Ministero Interno e Ministero Giustizia Assicurare una puntuale rilevazione statistica dei dati relativi ai reati informatici e quelli favoriti dall'informatica, acquisiti dalle Forze di polizia e dall'Autorità giudiziaria, per agevolarne l'analisi, anche al fine di eventuali integrazioni normative.

Capacità di deterrenza in ambito cibernetico

- Misura 45 – Attori responsabili DIS, AISI, AISE, Ministero Difesa e MAECI Rafforzare le capacità di deterrenza in ambito cibernetico, in ragione degli scenari in atto.

Centro nazionale di coordinamento

- Misura 46 – Attori responsabili ACN, NCC Realizzare e promuovere la partecipazione a progetti volti a supportare lo sviluppo di capacità, tecnologie e infrastrutture di cybersicurezza, mediante l'accesso ai pertinenti programmi di finanziamento dell'UE, assicurando il coinvolgimento del mondo industriale, accademico, della ricerca e della società civile, nonché favorendo sinergie con analoghe progettualità attive a livello nazionale.
- Misura 47 – Attori responsabili MISE, MIDT, ACN Supportare l'operatività dei Digital Innovation Hub e favorirne le sinergie con il Centro nazionale di coordinamento, con i Centri di competenza ad alta specializzazione e con i Cluster tecnologici, per agevolare il trasferimento tecnologico verso le PMI.

Sviluppo di tecnologia nazionale ed europea

- Misura 48 – Attori responsabili ACN, Ministero della Difesa, Autorità delegata alle politiche dello spazio e dell'aerospazio Sviluppare tecnologia nazionale ed europea, specie nei segmenti più innovativi e sensibili (ad es. cloud ed edge computing, tecnologie basate su blockchain, spazio, ecc.), attraverso l'avvio di dedicate progettualità.

Realizzazione di un "parco nazionale della cybersicurezza"

- Misura 49 – Attori responsabili ACN, MIDT, MEF, MISE, Realizzare un "parco nazionale della cybersicurezza" che ospiti le infrastrutture necessarie allo svolgimento di attività di ricerca e sviluppo nell'ambito della cybersecurity e delle tecnologie digitali, dotato di una struttura "diffusa", con ramificazioni distribuite sull'intero territorio nazionale.

Sviluppo industriale, tecnologico e della ricerca

- Misura 50 – Attori responsabili MAECI, MISE, ACN Promuovere l'internazionalizzazione delle imprese italiane che offrono prodotti e servizi di cybersecurity mediante il supporto agli investimenti, all'innovazione e alle esportazioni.
- Misura 51 – Attori responsabili MISE, MIDT, MAECI, ACN Implementare un Piano per l'industria cyber nazionale volto a sostenere imprese e startup per la progettazione e la realizzazione di prodotti e servizi ad alta affidabilità (tra cui un'infrastruttura di comunicazione nazionale), che rispondano agli interessi strategici del Paese e che possano essere promossi presso Stati like-minded.
- Misura 52 – Attori responsabili ACN, MISE Incoraggiare la creazione di Product Security Incident Response Team (PSIRT) da parte degli operatori privati, per accrescere le loro capacità di gestire le vulnerabilità di prodotti ICT e per contribuire all'adozione di policy di divulgazione coordinata di vulnerabilità e alla relativa implementazione.

Impulso all'innovazione tecnologica e alla digitalizzazione

- Misura 53 – Attori responsabili ACN, MISE, MIDT, MUR, Ministero della Difesa, Promuovere ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, riguardo a prodotti e processi informatici di rilevanza strategica ed a tutela degli interessi nazionali nel settore, anche valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali.
- Misura 54 – Attori responsabili ACN, MIDT, MEF, MISE Favorire la ricerca e lo sviluppo, specialmente nelle nuove tecnologie, promuovendo l'inclusione dei principi di cybersicurezza e supportando, anche mediante finanziamenti, investimenti pubblici e privati e meccanismi di semplificazione, progetti di sicurezza cibernetica da parte del settore privato – con particolare riferimento alle startup e alle PMI innovative – e dei Centri di competenza e di ricerca attivi sul territorio nazionale.
- Misura 55 – Attori responsabili MIDT, ACN Promuovere la digitalizzazione e l'innovazione, nonché rafforzare la sicurezza nella Pubblica Amministrazione, anche mediante l'impiego delle risorse del PNRR.
- Misura 56 – Attori responsabili MIDT, MISE, ACN Promuovere la digitalizzazione e l'innovazione del sistema produttivo nazionale, anche mediante l'impiego delle risorse del PNRR.
- Misura 57 – Attori responsabili ACN Promuovere la sicurezza cibernetica degli Internet Exchange Point nazionali, anche al fine di assicurare una rete Internet libera, aperta e trasparente.
- Misura 58 – Attori responsabili MIDT Sviluppare servizi pubblici digitali per la Pubblica Amministrazione a livello centrale e locale.

Fattori abilitanti

Formazione

- Misura 59 – Attori responsabili Ministero Istruzione, MUR, Atenei, Ministero della Difesa Potenziare lo sviluppo di percorsi formativi dedicati con diversi livelli di specializzazione in cybersecurity (scuola primaria e secondaria, corsi post-diploma (ITS), corsi universitari di laurea e laurea magistrale, dottorati di ricerca e master,

Scuole di formazione delle Pubbliche Amministrazioni) – anche investendo nella formazione del personale docente – per allineare l'offerta educativa alla domanda del mercato del lavoro e creare, così, una forza lavoro rispondente alle relative esigenze.

- Misura 60 – Attori responsabili Ministero Istruzione, MUR, Atenei, ACN Attivare Istituti Tecnici Superiori (ITS) con percorsi di cybersecurity, contribuendo a sostenere le specializzazioni produttive della manifattura locale. I programmi e le attività prevederanno, come previsto, una significativa docenza aziendale (50%) e un tirocinio (almeno 30% del tempo).
- Misura 61 – Attori responsabili ACN, Atenei, Ministero Istruzione, MUR Sviluppare un sistema nazionale di certificazione dell'apprendimento e dell'acquisizione di specifiche professionalità, non solo tecniche, sia a livello di istruzione secondaria di secondo grado, sia a livello universitario e professionale. L'ACN mantiene una lista dei percorsi di formazione, approvati dalla stessa Agenzia, al termine dei quali il discente consegue, oltre al titolo di studio/professionale, la relativa certificazione.
- Misura 62 – Attori responsabili ACN Elaborare uno strumento di formazione e sensibilizzazione online, rivolto alla cittadinanza in generale, che consente, al termine del percorso, di auto-testare le competenze e le sensibilità acquisite e di ottenere un attestato. Lo scopo è quello di creare un primo modulo per avviare una e-Academy dell'Agenzia per la Cybersicurezza Nazionale.
- Misura 63 – Attori responsabili MIDT, MEF Dispiegare fondi da dedicare alla formazione professionale nei settori pubblico e privato, al fine di agevolare il passaggio dal mondo scolastico a quello del lavoro e conseguire, così, una sovranità nazionale digitale delle competenze.
- Misura 64 – Attori responsabili MEF, MISE, MIDT Prevedere incentivi per lo sviluppo di startup operanti nel settore della cybersecurity e partnership pubblico-privato con aziende di cybersecurity a conduzione femminile.
- Misura 65 – Attori responsabili PCM, MUR, Ministero Istruzione, Atenei, CINI, ACN Favorire l'organizzazione di iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica, che tengano in debita considerazione principi di bilanciamento di genere, mirate all'individuazione di giovani talenti anche al fine di propiziarne l'ulteriore formazione e l'inserimento nel mondo del lavoro. Ciò, anche al fine di promuovere iniziative volte a colmare il "confidence gap" delle studentesse nei confronti di carriere in ambiti scientifici e tecnologici.

- Misura 66 – Attori responsabili MISE, MUR, Ministero Istruzione, MIDT, MEF, Prevedere meccanismi per agevolare la transizione di studenti e neolaureati, con competenze in cybersecurity, verso il mondo del lavoro, mediante programmi di alternanza scuola-lavoro e di inserimento quali stage e apprendistato, nonché incentivi all'assunzione di personale "junior", favorendo altresì la riqualificazione e la ricollocazione professionale di coloro che si trovano al di fuori del mercato del lavoro.
- Misura 67 – Attori responsabili MUR, MIDT, MAECI, Ministero della Difesa, CINI, Prevedere programmi di scambio, a livello europeo e internazionale, per attività di istruzione universitaria e in ambito professionale, che promuovano anche una sempre maggiore inclusione della popolazione femminile.
- Misura 68 – Attori responsabili Ministero Interno e Ministero della Giustizia Favorire la formazione specialistica di tutte le figure impegnate nel contrasto alla criminalità informatica in ambito giudiziario e investigativo.
- Misura 69 – Attori responsabili ACN, MAECI Potenziare la formazione del personale diplomatico così da rafforzare le capacità di cyber diplomacy.
- Misura 70 – Attori responsabili MISE, MIDT, ACN Promuovere, per tutti i lavoratori pubblici e privati, inclusi quelli di livello apicale, il costante aggiornamento professionale, anche attraverso percorsi di formazione in materia di sicurezza cibernetica, pure nell'ottica di riqualificare la forza lavoro già in organico.

Promozione della cultura della sicurezza cibernetica

- Misura 71 – Attori responsabili ACN, Ministero Interni, MUR, MIDT Avviare iniziative e campagne di sensibilizzazione volte a promuovere le competenze degli utenti e i comportamenti responsabili nello spazio cibernetico, contrastando la disattenzione digitale e accrescendo la consapevolezza sui rischi derivanti dall'uso delle tecnologie informatiche e su come proteggere la propria privacy online, considerando anche le esigenze di particolari fasce della popolazione come le persone anziane e diversamente abili, oltre che di alcune categorie di pubblici dipendenti (come, ad esempio, i magistrati). Ciò, attraverso la diffusione di informazioni facilmente comprensibili dai non addetti ai lavori sulle vulnerabilità di sicurezza di prodotti e servizi ICT di largo impiego.

- Misura 72 – Attori responsabili Ministero Istruzione, MUR, Atenei, ACN Promuovere l'educazione digitale, comprensiva di aspetti di sicurezza cibernetica, per tutti i livelli di istruzione scolastica, affinché si diffondano conoscenze tecniche e operative sulla gestione sicura delle informazioni e delle tecnologie di comunicazione, prevedendo anche raccordi con il mondo accademico per massimizzare l'apprendimento degli studenti su tali tematiche.
- Misura 73 – Attori responsabili PCM, Ministero Interno Predisporre e implementare un'autonoma strategia nazionale, con relativo piano d'azione, dedicata alla protezione online dei minori dai crimini informatici, che contempli iniziative come la realizzazione di campagne di sensibilizzazione indirizzate non solo ai minori, ma anche a genitori, tutori ed educatori.

Cooperazione

- Misura 74 – Attori responsabili ACN Istituire tavoli operativi permanenti con i soggetti Perimetro, suddivisi per settore, che svolgano a livello operativo specifici compiti in materia di prevenzione, allertamento, risposta agli incidenti e ripristino.
- Misura 75 – Attori responsabili MAECI, ACN, Ministero Interno, Ministero Giustizia, Ministero Difesa, MISE Rafforzare il ruolo dell'Italia all'interno dei consessi multilaterali impegnati in ambito di sicurezza cibernetica (quali Unione europea, NATO, G7, OSCE e Consiglio d'Europa) e il posizionamento strategico nazionale in Europa e nel mondo, promuovendo sinergie con i Paesi "like-minded"
- Misura 76 – Attori responsabili MAECI, ACN Assicurare l'implementazione delle Confidence Building Measure (CBM) dell'OSCE in materia di sicurezza cibernetica.
- Misura 77 – Attori responsabili MAECI, ACN, Ministero Difesa Rafforzare la cooperazione con altri Paesi, per contribuire alla stabilità e alla sicurezza dello spazio cibernetico.
- Misura 78 – Attori responsabili ACN, MAECI, Realizzare un ecosistema nazionale volto a sviluppare capacità di capacity building a favore di Paesi terzi.
- Misura 79 – Attori responsabili MAECI, ACN, Ministero Interni Stipulare accordi bilaterali e multilaterali con i Paesi di interesse strategico, prevedendo anche lo sviluppo di attività di capacity building.

- Misura 80 – Attori responsabili MAECI, ACN Contribuire attivamente, in ambito di Unione europea, alla definizione di policy/regolamentazioni in materia di cybersicurezza.
- Misura 81 – Attori responsabili ACN, MIT, MISE Contribuire attivamente, in ambito di Unione europea, all'individuazione delle priorità di ricerca e sviluppo per traguardare l'obiettivo dell'autonomia tecnologica UE in ambito digitale.

Metriche e Key Performance Indicators

- Misura 81 – Attori responsabili ACN, Altri attori responsabili dell' implementazione della strategia Sviluppare, entro 12 mesi dall'adozione della presente strategia, apposite metriche e key performance indicator (KPI) per misurare: il livello di implementazione della presente strategia il livello di maturità nel settore della cybersecurity dei diversi OSE/FSD la partecipazione di particolari fasce della popolazione (ad es. donne, giovani e disoccupati o inoccupati) in attività di sensibilizzazione, istruzione e formazione nel campo della sicurezza informatica, e la loro efficacia la partecipazione di particolari fasce della popolazione (ad es. donne e giovani) nell'industria della sicurezza informatica iniziative e relativi investimenti, anche da parte dell'industria nazionale, in attività di ricerca e sviluppo nel campo della sicurezza informatica il totale degli investimenti in sicurezza informatica da parte di soggetti pubblici e privati il totale delle imprese nazionali coperte da polizza assicurativa contro gli incidenti informatici