Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

CALL FOR IDEAS

FROM CONCEPT TO IMPACT:
IDEAS EMPOWERING THE FUTURE

Sommario

CALL FOR IDEAS

FROM CONCEPT TO IMPACT: IDEAS EMPOWERING THE FUTURE

1 Contesto e obiettivi

1.1 Contesto

Difendere il cyberspazio dalle minacce e dagli attacchi che, attraverso azioni informatiche dolose, perpetrano frodi, sottraggono dati aziendali sensibili e strategici e compromettono la stabilità finanziaria, l'ordine pubblico e la vita democratica dei Paesi è ormai di cruciale importanza per i governi di tutto il mondo. Gli attacchi informatici mettono in allarme la popolazione, danneggiano l'economia e mettono in pericolo la sicurezza stessa dei cittadini quando colpiscono le reti di distribuzione di servizi essenziali come la sanità, l'energia, i trasporti, cioè le infrastrutture critiche della società moderna.

In Italia, interi settori di eccellenza, come la meccanica, la cantieristica, il Made-in-Italy, il turismo, i beni culturali, l'agroalimentare, i trasporti, potrebbero subire pesanti riduzioni del loro fatturato, a causa di attacchi perpetrati nel cyberspazio da concorrenti commerciali, dalla criminalità organizzata, ma anche da Stati sovrani. Le fake news sono l'evoluzione degli attacchi basati sull'ingegneria sociale: confezionate, personalizzate e diffuse in modo mirato attraverso il cyberspazio, le false informazioni tendono a confondere e destabilizzare i cittadini.

1.2 Il Partenariato Esteso SERICS

Il Partenariato Esteso SERICS sta conducendo un ambizioso programma di ricerca sulla cybersecurity articolato in dieci aree tematiche strategiche (si veda successivo par.4 Aree tematiche di interesse) con il contributo di oltre 500 ricercatori e oltre 25 enti accademici e imprese di rilievo internazionale.

SERICS intende mettere a disposizione il patrimonio di conoscenze sviluppato all'interno della propria Comunità di Ricerca per promuovere la creazione, lo sviluppo e la commercializzazione di soluzioni di

cybersecurity all'avanguardia. A tal fine diviene essenziale canalizzare i risultati della ricerca nella cyber security nel quadro di solidi processi di trasferimento tecnologico verso il mercato che diano valore alle innovazioni.

Sulla base di questi presupposti, la Fondazione SERICS, soggetto attuatore del Partenariato esteso "SERICS – Security and Rights in CyberSpace" finanziato nell'ambito del PNRR, M4C2 - Investimento 1.3 ha avviato un importante Programma di trasferimento tecnologico e valorizzazione dei risultati della ricerca.

Le azioni previste riguardano la realizzazione di percorsi di accompagnamento per la gestione della proprietà intellettuale, lo sviluppo di startup innovative, lo scouting di risorse e l'avvio di partenariati industriali coerenti con il livello di maturità di risultati della ricerca/idee e i fabbisogni dei diversi team.

2 La Call for Ideas

Nell'ambito delle attività di valorizzazione della ricerca, la Fondazione SERICS lancia la presente Call for Ideas, finalizzata a selezionare idee attive ad alto contenuto tecnologico e supportarle in un percorso di accelerazione, a titolo gratuito, dedicato alla crescita e al consolidamento di queste idee nel settore della Cybersecurity e della trasformazione digitale. Gli obiettivi della Call for Ideas sono:

- Favorire il trasferimento tecnologico dai centri di ricerca al mercato, trasformando risultati scientifici in soluzioni imprenditoriali concrete;
- Supportare la crescita di startup e spin-off della ricerca attraverso un percorso strutturato che comprenda mentoring, formazione, networking con investitori e accesso a risorse strategiche;
- Creare una rete collaborativa tra accademia, industria e investitori per massimizzare le opportunità di sviluppo e finanziamento delle startup;
- Potenziare le competenze imprenditoriali dei partecipanti, fornendo strumenti pratici per la validazione del modello di business e la scalabilità dell'idea;
- Sostenere l'innovazione nel settore della cybersecurity, promuovendo tecnologie avanzate per la sicurezza informatica e la protezione dei dati;

- Promuovere un ambiente di validazione competitiva di idee di business in ambito Cybersecurity garantendo la cross fertilizzazione tra la comunità della ricerca SERICS e potenziali imprenditori.

2.1 Struttura della call

La Call for Ideas è articolata in round periodici che selezioneranno ciascuno fino a 10 progetti. I vincitori accederanno a un percorso di accelerazione mirato che offrirà:

- Mentoring e coaching personalizzato;
- Webinar e workshop su sviluppo tecnologico, business modeling e strategie di investimento;
- Connessione con esperti, investitori e partner industriali;
- Connessione con la comunità della Ricerca del Partenariato Esteso SERICS per mentoring tecnico, sperimentazione, validazione tecnologica;
- Supporto alla strutturazione del pitch e preparazione alla presentazione per investitori e stakeholder di settore.

Attraverso questa iniziativa, SERICS mira a stimolare la creazione di nuove imprese tecnologiche nel settore della cybersecurity, favorendo la crescita di un ecosistema innovativo e competitivo.

3 Destinatari e requisiti di partecipazione

3.1 Chi può partecipare

La Call for Ideas è aperta a:

- **Ricercatori singoli o in team** che intendano trasformare i risultati della loro ricerca in un'iniziativa imprenditoriale;

- **Startup e spin-off della ricerca** con tecnologie e soluzioni innovative in ambito cybersecurity e trasformazione digitale;
- **Team di innovatori** con competenze multidisciplinari interessati a sviluppare un'idea imprenditoriale basata su ricerca scientifica.

3.2 Requisiti di ammissibilità

Per partecipare, i candidati devono:

- Presentare un'idea innovativa coerente con gli ambiti tematici della Call (cfr. par. 4);
- Dimostrare competenze tecniche, scientifiche e/o imprenditoriali adeguate allo sviluppo del progetto;
- Essere maggiorenni e, in caso di team, designare un rappresentante;

Le startup e spin-off devono essere formalmente costituite e in fase di sviluppo.

Le candidature saranno valutate in base alla coerenza con gli obiettivi del programma e il potenziale di crescita dell'idea imprenditoriale.

4 Aree tematiche di interesse

Ogni proponente può candidare una sola idea ad alto contenuto tecnologico in linea con gli ambiti tematici (Spoke della Fondazione SERICS) di seguito riportati:

- **Aspetti umani, sociali e legali:** Analisi dell'impatto della cybersecurity sulla società, la regolamentazione e i diritti digitali **(Spoke 1).**
- **Disinformazione e falsificazioni:** Sviluppo di strumenti per il rilevamento e la mitigazione della disinformazione online **(Spoke 2).**
- **Attacchi e difese informatiche**: Tecniche avanzate per identificare, prevenire e mitigare cyber attacchi **(Spoke 3).**

- **Sicurezza dei sistemi operativi e della virtualizzazione**: Metodologie per proteggere OS e ambienti virtualizzati da vulnerabilità e minacce **(Spoke 4).**
- **Crittografia e sicurezza dei sistemi distribuiti**: Soluzioni avanzate per la protezione della comunicazione e dei dati sensibili **(Spoke 5).**
- **Sicurezza del software e delle piattaforme**: Tecniche di sviluppo sicuro e prevenzione delle vulnerabilità nelle applicazioni digitali **(Spoke 6).**
- **Sicurezza delle infrastrutture**: Protezione delle infrastrutture critiche, reti e sistemi di IT (Information Technology) e OT (Operational Technology) **(Spoke 7).**
- **Gestione del rischio e governance**: Approcci per valutare, mitigare e gestire il rischio in ambito cybersecurity **(Spoke 8).**
- **Garantire la trasformazione digitale**: Sicurezza delle nuove tecnologie emergenti e della digitalizzazione **(Spoke 9).**
- **Governance e protezione dei dati**: Normative, strategie e strumenti per la protezione della privacy e dei dati aziendali **(Spoke 10).**

In allegato 1 è riportato il dettaglio delle aree tematiche.

5 Struttura del Percorso di Accelerazione

5.1 Supporto offerto

Il percorso di accelerazione prevede:

- **Advisory**: sessioni di consulenza personalizzata in grado di offrire un supporto di tipo strategico e operativo di un progetto.
- **Webinar e moduli formativi**: formazione su temi chiave per lo sviluppo di un progetto (proprietà intellettuale, business plan, project management, ecc.).
- **Mentorship**: affiancamento con mentor esperti nei settori di riferimento di SERICS, che offriranno supporto e guida personalizzata.

- **Servizi specialistici:** protezione e gestione della proprietà intellettuale, incontri con investitori, business angel, ricerca di partnership industriali e supporto per la partecipazione a bandi.

- **Networking e percorsi di coaching-supporto tecnico-scientifico** da parte di ricercatori e innovatori che operano all'interno della Comunità della Ricerca della Fondazione SERICS

5.2 Articolazione del percorso

Il percorso di accelerazione sarà svolto indicativamente nell'arco di 4 settimane ed avrà come oggetto le seguenti attività:

Settimana 1 - Assessment & Roadmap
Webinar su validazione del problema e analisi del mercato.
Sessioni one-to-one di Advisory per identificare i fabbisogni.
Settimana 2 e Settimana 3 - Business Model & Market Validation
Formazione su product-market fit e sui modelli di business.
Coaching personalizzato per definire la strategia di sviluppo.
Mentoring Tecnico Scientifico da parte di ricercatori e innovatori della Comunità di ricerca SERICS per la validazione tecnica delle soluzioni proposte
Settimana 4 - Pitch Readiness & Investor Approach
Webinar su pitch deck, storytelling e comunicazione.
Sessioni di refining del pitch con mentor ed esperti.
Pitch review finale con valutazione e feedback strategici nell'ambito di una giornata di presentazione.

6 Modalità di partecipazione

6.1 Procedura di candidatura

Le candidature devono essere presentate esclusivamente online tramite l'apposito modulo, cliccando QUI

I candidati dovranno fornire:

- Dati anagrafici del proponente o del team;
- Descrizione dell'idea progettuale, inclusi obiettivi, tecnologie utilizzate e applicazioni previste;
- Ambito tematico di riferimento tra quelli indicati nella Call;
- Livello di maturità tecnologica (TRL - Technology Readiness Level);
- Composizione e competenze del team (se presente);
- Eventuali collaborazioni con enti di ricerca o aziende;
- Dichiarazione di accettazione dei termini e delle condizioni della Call.

6.2 Tempistiche

La Call prevede 6 round di partecipazione al Percorso di accelerazione con il seguente calendario:

Call	Apertura Percorso di Accelerazione
Call 1	07.04.2025
Call 2	19.05.2025
Call 3	01.07.2025
Call 4	8.09.2025
Call 5	06.10.2025
Call 6	03.11.2025

I risultati dei candidati selezionati saranno comunicati via e-mail ai candidati 15 giorni prima dell'avvio del percorso di Accelerazione.

7 Criteri di selezione

7.1 Parametri di valutazione

Le candidature saranno valutate da una Commissione di Selezione con il coinvolgimento del Comitato Tecnico Scientifico della Fondazione SERICS sulla base dei seguenti criteri:

Criterio	Punteggio
Innovatività e originalità dell'idea. Livello di novità rispetto allo stato dell'arte e capacità di apportare valore nel settore della cybersecurity.	30
Coerenza con gli obiettivi di SERICS. Allineamento del progetto con gli ambiti tematici e gli obiettivi strategici dell'iniziativa.	30
Fattibilità tecnica ed economica. Solidità tecnologica e sostenibilità economica dell'idea proposta	15
Potenziale di mercato e scalabilità. Possibilità di espansione, attrattività per investitori e adattabilità a diversi contesti di mercato	15
Qualità del team e competenze imprenditoriali. Esperienze, competenze e capacità esecutive del team proponente	10
Totale	**100**

Il punteggio massimo ottenibile è **100 punti**. Saranno selezionati per il percorso di accelerazione i progetti che otterranno almeno **50 punti**. Le domande che otterranno un punteggio inferiore a 50 punti saranno automaticamente escluse dalla graduatoria.

8 Processo di selezione

Il processo di selezione prevede:

01. **Valutazione preliminare:** verifica della completezza della documentazione e della conformità ai requisiti di ammissibilità.
02. **Valutazione tecnica e strategica:** assegnazione del punteggio in base ai criteri sopra indicati.
03. **Eventuali richieste di integrazione:** il Comitato Tecnico potrà richiedere ulteriori chiarimenti o documenti integrativi.
04. **Pubblicazione dei risultati:** i candidati selezionati saranno notificati via email entro 15 giorni dalla chiusura del round.

Per le proposte che raggiungeranno almeno 50 punti, verrà stilata una graduatoria in ordine decrescente di punteggio. Le **prime 10 proposte** in graduatoria saranno ammesse al programma di formazione, affiancamento e validazione. In caso di mancata selezione, il progetto sarà eleggibile per un round successivo.

Le candidature pervenute oltre il **24 ottobre 2025** o con modalità differenti da quelle indicate non saranno prese in considerazione.

9 Pubblicazione degli esiti e accesso al programma

9.1 Modalità di comunicazione degli esiti

Gli esiti della selezione saranno comunicati ai candidati via email almeno 15 giorni prima della data di apertura del percorso di accelerazione. Inoltre, l'elenco dei progetti selezionati sarà pubblicato sul sito ufficiale della Fondazione SERICS www.Serics.eu

9.2 Accettazione della partecipazione

I candidati selezionati dovranno confermare la loro partecipazione entro il termine indicato nella comunicazione ufficiale. In caso di rinuncia, il Comitato Tecnico si riserva la facoltà di selezionare altri progetti idonei tra quelli in graduatoria.

9.3 Impegni dei partecipanti

I partecipanti selezionati si impegnano a:

- Prendere parte attivamente a tutte le attività previste dal programma di accelerazione;
- Fornire aggiornamenti periodici sullo sviluppo del proprio progetto;
- Rispettare le clausole di riservatezza e le condizioni d'uso proposte da SERICS.

Il mancato rispetto di tali impegni potrà comportare l'esclusione dal programma.

10 Privacy e Trattamento dei Dati

10.1 Base giuridica del trattamento dei dati

I dati personali dei partecipanti saranno trattati nel rispetto del Regolamento Generale sulla Protezione dei Dati (GDPR - Regolamento UE 2016/679). Il trattamento avrà le seguenti finalità:

- Gestione della candidatura e del processo di selezione;
- Comunicazioni relative alla Call e al programma di accelerazione;
- Monitoraggio e valutazione dell'efficacia dell'iniziativa.

10.2 Tipologia di dati raccolti

I dati trattati includeranno:

- Dati anagrafici e di contatto (nome, cognome, email, telefono);
- Informazioni relative al progetto (descrizione dell'idea, stato di sviluppo, ambito tematico);
- Dati relativi ai membri del team (CV, esperienze, ruoli nel progetto).

10.3 Modalità di trattamento e conservazione

I dati saranno trattati con strumenti elettronici e cartacei, adottando misure di sicurezza adeguate per proteggerli da accessi non autorizzati, perdita o alterazione. I dati saranno conservati:

- Per l'intera durata della Call e del programma di accelerazione;
- Fino a un massimo di 5 anni dalla conclusione del programma, per finalità di rendicontazione e monitoraggio.

10.4 Diritti degli interessati

I partecipanti hanno il diritto di:

- Accedere ai propri dati personali;
- Richiederne la rettifica o la cancellazione;
- Limitare o opporsi al trattamento;
- Richiedere la portabilità dei dati;
- Presentare reclamo all'Autorità Garante per la protezione dei dati personali.

Per esercitare questi diritti, i partecipanti possono contattare l'organizzazione all'indirizzo email **trasferimento.tecnologico@serics.eu**.

11 Contatti e supporto

Per qualsiasi informazione relativa alla Call for Ideas, i candidati possono contattare il team della Fondazione SERICS all'indirizzo email: **trasferimento.tecnologico@serics.eu.**

12 Clausole di riservatezza e Proprietà Intellettuale

12.1 Riservatezza delle informazioni

Tutte le informazioni fornite dai candidati saranno trattate con la massima riservatezza e utilizzate esclusivamente per le finalità della Call for Ideas. Nessuna informazione sarà condivisa con terze parti senza il consenso esplicito dei partecipanti.

12.2 Diritti di proprietà intellettuale

I partecipanti mantengono tutti i diritti di proprietà intellettuale relativi alle idee e ai progetti presentati. La partecipazione al programma non implica alcuna cessione di diritti, né per SERICS né per eventuali partner dell'iniziativa. Tuttavia, eventuali sviluppi realizzati durante il percorso di accelerazione saranno oggetto di accordi specifici tra le parti coinvolte.

13 Modifiche e annullamento della call

La Fondazione SERICS si riserva il diritto di modificare i termini e le condizioni della Call for Ideas per necessità organizzative o per cause di forza maggiore. Eventuali aggiornamenti saranno comunicati tempestivamente ai candidati tramite il sito ufficiale e via email.

In casi straordinari, la Fondazione SERICS si riserva la possibilità di annullare la Call for Ideas o alcuni dei round previsti. In tal caso, i candidati saranno tempestivamente informati e non sarà dovuto alcun risarcimento per eventuali costi sostenuti dai partecipanti.

1. Allegato 1 – Dettaglio aree tematiche di riferimento

1. Area tematica 1: Aspetti umani, sociali e legali

L'obiettivo principale dell'AT 1 è riferito alla creazione di un Cyberspazio convincente e sicuro combinando sistemi tecnologici solidi con una forte e robusta regolamentazione del comportamento umano. Vale a dire strutturare un ecosistema innovativo in cui esperti di tecnologia, legge, etica, sociologia ed educazione insieme creano processi che anticipano e testano nuove politiche di cybersecurity. In particolare, l'AT 1 produce nuove conoscenze sugli aspetti normativi, legali ed etici del CyberSpace. Le finalità specifiche dell'AT 1 possono essere classificati in cinque macro-categorie. La prima categoria riguarda i diritti, le regole, le definizioni, le tassonomie e le autorità volte a creare nuove forme di coregolamentazione per il cyberspazio. La seconda categoria analizza le questioni legali ed etiche della cybersicurezza, come i diritti fondamentali legati a questo nuovo ecosistema. La terza categoria comprende l'apprendimento permanente e i modelli educativi sulle questioni legali della cybersicurezza. La quarta categoria comprende la criminalità informatica e la diplomazia informatica come elementi importanti e cruciali di una nuova strategia nazionale, sviluppando la conoscenza di questo tema presso il pubblico accademico e generale. La quinta categoria comprende la sovranità digitale, anche per i calcoli e le tecnologie basate sull'intelligenza artificiale, il cloud, il fog e l'edge computing, e le loro applicazioni in settori specifici, come quelli dell'energia e dei trasporti.

2. Area tematica 2: disinformazione e falsificazioni

L'AT2 mira a progettare e sviluppare soluzioni innovative per identificare e gestire le minacce al disordine informativo che si manifestano attraverso le fake news e la diffusione di notizie false. Queste azioni malevole, sfruttando i bias cognitivi delle persone, generano la disapprovazione dei cittadini e la sfiducia dei media e delle istituzioni. Occorre un approccio multidisciplinare sfruttando l'automazione open source ottenuta attraverso l'Intelligence Analysis, i recenti progressi dell'Intelligenza Artificiale e le conoscenze delle scienze politiche e geopolitiche. In primo luogo, la finalità è implementare metodologie di analisi dei contenuti testuali e multimediali per rilevare modelli significativi da utilizzare per individuare i tentativi di disinformazione e dare evidenza, mediante l'analisi delle comunità dei social media, delle vulnerabilità cognitive dei partecipanti e delle minacce legate alla diffusione di fake news. L'obiettivo è quello di progettare un sistema di allerta precoce per smascherare le informazioni false, sfruttando l'integrità sintattica dei contenuti e i modelli legati ai flussi di

disinformazione. Il framework risultante mira a sensibilizzare le persone sui comportamenti rischiosi associati alla condivisione di contenuti discutibili e a supportare gli esperti e i responsabili della sicurezza nel processo decisionale, adottando un approccio human-in-the-loop.

3. Area tematica 3: Attacchi e difese

L'AT 3 si propone di analizzare le metodologie di attacco emergenti e di sviluppare metodi avanzati per la rilevazione degli attacchi e l'individuazione di linee guida per la progettazione di sistemi informatici che garantiscano una ridotta vulnerabilità alle nuove categorie di attacco. Gli obiettivi di dettaglio possono essere suddivisi in quattro macro categorie: (i) Sviluppo di strumenti avanzati per l'analisi del malware e del software finalizzati all'identificazione delle vulnerabilità che potrebbero essere sfruttate dal malware; (ii) Sviluppo di strumenti per l'analisi del traffico di rete in grado di identificare le comunicazioni relative agli attacchi in corso; (iii) Sviluppo di sistemi di machine learning robusti agli attacchi e attraverso i quali è possibile estrarre conoscenze finalizzate alla creazione di strumenti più avanzati per l'analisi tempestiva degli attacchi e la loro individuazione precoce; (iv) Analisi dei "fattori umani" coinvolti in un attacco con lo sviluppo di strumenti per l'analisi e la correlazione di informazioni provenienti da OSINT (open sources intelligence) e la difesa e prevenzione di attacchi basati su tecniche di social engineering.

4. Area tematica 4: Sicurezza dei sistemi operativi e della virtualizzazione

I sistemi operativi (OS) e le tecnologie di virtualizzazione (VT) sono fattori abilitanti fondamentali per i paradigmi di calcolo e comunicazione esistenti ed emergenti, ovvero cloud, fog, edge computing e 5G/6G. Sfruttando i meccanismi di sicurezza primitivi forniti dall'hardware, i sistemi operativi e le tecnologie di virtualizzazione offrono meccanismi e servizi di sicurezza fondamentali (ad esempio, la gestione dell'identità di base e il controllo degli accessi) su cui si basa la sicurezza delle applicazioni e, in seguito, dell'intero cyberspazio. L'AT 4 si occupa di sviluppare servizi di sicurezza automatizzati di alto livello e metodologie innovative di valutazione e garanzia della sicurezza per supportare lo sviluppo e la verifica secure-by-design di applicazioni cloud, edge e 5G. L'efficacia delle tecniche proposte è valutata mediante stress-test in scenari di attacco simulati, ma altamente realistici, eseguiti in sicurezza all'interno di una piattaforma di Cyber Ranges federati.

5. Area tematica 5: Crittografia e sicurezza dei sistemi distribuiti

L'AT 5 si occupa principalmente di attività di ricerca nei domini della crittografia e della sicurezza dei sistemi distribuiti. Data la vastità di questi domini e per individuare obiettivi concreti volti a ottenere risultati a lungo termine di alto livello tecnologico e di possibile impatto sul Paese, l'AT 5 vede la coesistenza di due anime il cui denominatore comune è rappresentato dalla nozione di identificazione e tracciamento digitale. Tra le sotto-tematiche (i) primitive e protocolli crittografici, (ii) crittografia fondazionale e crittoanalisi, (iii) crittografia post-quantistica, (iv) identità digitale, autenticazione e accountability, e (v) distributed ledgers e blockchain. Le linee di ricerca dell'AT 5 si muovono su binari diversi, stimolando continue interazioni tra loro e applicazioni verticali dei risultati su specifici domini applicativi.

6. Area tematica 6: Sicurezza del software e delle piattaforme

Il primo obiettivo scientifico dell'AT 6 è fornire un ecosistema in cui gli sviluppatori di software possano facilmente ragionare sulla sicurezza del software. Ciò si basa su astrazioni di programmazione innovative e consapevoli della sicurezza e su nuovi modelli semantici che permettono di formalizzare, verificare e certificare le proprietà di sicurezza secondo una metodologia secure-by-design. La finalità è sviluppare nuove tecniche formali basate sulla compilazione sicura e sulla composizione sicura, per ridurre il divario tra i modelli formali, essenziali per fornire piene garanzie di correttezza, e le reali implementazioni. Il secondo obiettivo scientifico è fornire soluzioni innovative per proteggere la catena di fornitura del software, compresi i processi di gestione e sviluppo del software. L'obiettivo è sviluppare nuove tecniche per eseguire test di sicurezza attraverso un'analisi dinamica continua e per proteggere il software, rilevando attività dannose e prevenendone o limitandone l'impatto, secondo un paradigma di autodifesa. Verranno utilizzati scenari di test per validare e valutare sperimentalmente le tecniche proposte.

7. Area tematica 7: Sicurezza delle infrastrutture

L'AT 7 ha come obiettivo generale il progresso delle tecnologie di sicurezza delle infrastrutture. Questo obiettivo generale si traduce in quattro obiettivi specifici: (i) Progettare e sviluppare un'architettura informatica sicura aperta e disponibile a livello nazionale, che sarà il punto di partenza per la costruzione di infrastrutture sicure che non soffrano dei potenziali rischi derivanti dall'uso di tecnologie proprietarie; (ii) Migliorare la sicurezza dell'infrastruttura automobilistica che, con la massiccia interconnessione ed elettrificazione delle

auto, diventerà uno degli asset più vulnerabili del Paese; (iii) Migliorare la sicurezza, la protezione e la resilienza delle Smart power grid, che sono una componente fondamentale per ottimizzare l'uso dell'energia e per raggiungere il Green deal; (iv) Contribuire al miglioramento della postura di sicurezza degli asset ITC (es.e., reti, sistemi e servizi IT/OT) inclusi nel "Perimetro di Sicurezza Nazionale Cibernetica", fornendo ontologie, metodologie, linee guida, best practice e strumenti.

8. Area tematica 8: Gestione del rischio e governance

L'AT 8 intende contribuire alla resilienza informatica dei futuri sistemi e servizi caratterizzati da componenti digitali sempre più interconnessi e intrinsecamente vulnerabili, come richiesto dall'UE attraverso NIS e NIS2, e dall'Agenzia Nazionale Italiana per la Cybersecurity (ACN). A tal fine, propone un approccio olistico alla cybersecurity basato sul rischio che deve includere anche la resilienza, la privacy, la sicurezza delle organizzazioni, delle industrie, delle infrastrutture critiche e delle relative filiere. Questa AT include competenze interdisciplinari adatte ad affrontare sia le sfide scientifico-tecnologiche che quelle legali e politiche attraverso nuovi modelli per la valutazione continua delle minacce e delle vulnerabilità, ma anche attraverso la progettazione di componenti di rete autodifensivi. L'AT 8 mira anche a promuovere la visione secondo cui un'Europa digitale sviluppata richiede la protezione dei diritti e delle libertà fondamentali, la promozione della consapevolezza sociale e una formazione informatica diffusa, nonché il raggiungimento di un equilibrio di genere nella sicurezza informatica.

9. Area tematica 9: Garantire la trasformazione digitale

L'AT 9 ha l'obiettivo principale di studiare nuovi approcci, metodologie, soluzioni e strumenti in grado di fornire adeguate garanzie di sicurezza per i nuovi scenari applicativi che stanno emergendo oggi come conseguenza della forte accelerazione verso la trasformazione digitale pervasiva. In particolare, sono quattro gli scenari di riferimento: (i) lo sviluppo di soluzioni di finanza decentralizzata basate su tecnologie distribuite sicure come le DLT e gli smart contract; (ii) il rafforzamento delle proprietà di sicurezza dei dati e della privacy nei servizi forniti dalla pubblica amministrazione nell'ambito di programmi di e-government; (iii) soluzioni di sanità remota basate su dispositivi personali, essenziali per una gestione più efficiente dei pazienti malati cronici o che necessitano di un monitoraggio continuo; (iv) tecnologie di distribuzione di chiavi quantistiche per applicazioni critiche.

10. Area tematica 10: Governance e protezione dei dati

La moderna società digitale si basa sulla raccolta, la condivisione e l'analisi di grandi collezioni di dati, con evidenti vantaggi, dall'ambito personale a quello aziendale, della ricerca e sociale. La piena realizzazione di una società digitale basata sui dati può avvenire solo se c'è fiducia nella sicurezza e nella privacy di tali dati, e quindi se sono disponibili soluzioni che garantiscano la corretta protezione e l'uso dei dati. Le leggi e i regolamenti sulla protezione dei dati impongono restrizioni che ne limitano l'uso e i singoli, così come le aziende, chiedono il rispetto dei requisiti di protezione e la garanzia di un'efficace protezione dei loro dati. L'AT 10 risponde a questa esigenza dando ai vari attori coinvolti nella condivisione dei dati e nell'utilizzo degli scenari il controllo sui propri dati, supportando la condivisione dei dati in modo selettivo e sicuro, garantendo al contempo funzionalità, efficienza e scalabilità. Le soluzioni per la protezione dei dati sviluppate nell'ambito dell'AT 10 consentono nuovi scenari applicativi e introducono nuove opportunità di condivisione dei dati, in modo controllato, nel rispetto della privacy e delle restrizioni di accesso, garantendo l'integrità dei dati e dei risultati delle analisi. L'AT 10 contribuisce quindi a una vera e piena realizzazione della sovranità digitale.