DISTRETTO TECNOLOGICO DI CYBER SECURITY

Che cosa è

Il **Distretto Tecnologico Cyber Security** rientra nelle iniziative di sviluppo e potenziamento del Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) relative a "Distretti ad Alta Tecnologia, Laboratori pubblico/privati nonché azioni finalizzate alla creazione di nuovi Distretti e/o nuove Aggregazioni Pubblico/Private" nell'ambito del Programma Operativo Nazionale "Ricerca e Competitività" 2007-2013 (PON R&C) per le Regioni della Convergenza (Calabria, Campania, Puglia, Sicilia). La **Regione di Convergenza** del Distretto è la **Calabria.**

Lo Studio di Fattibilità del Distretto Cyber Security è stato presentato a marzo 2011 ed è stato valutato idoneo dal MIUR con il punteggio di 67, che è risultato essere il punteggio più elevato nella graduatoria di tutte le proposte afferenti alla Regione Calabria e tra i più alti nella graduatoria complessiva. Successivamente, a seguito di una negoziazione con il MIUR e la Regione Calabria, a Dicembre 2012 il piano di sviluppo del Distretto Cyber Security è stato inserito all'interno del piano strategico di interventi coordinati per la costituzione di nuovi Distretti e nuove Aggregazioni Pubblico/Private nel settore ICT del Cluster ICT Horizon@Calabria2020.

Il Cluster *ICT Horizon@Calabria2020* costituisce una infrastruttura organizzativa leggera, localizzata nell'area di **Cosenza,** per il coordinamento di iniziative innovative in alcuni ambiti di frontiera del settore ICT, con particolare attenzione al supporto per lo sviluppo di nuove tecnologie e applicazioni basate su un approccio multi-disciplinare e con un'ampia prospettiva di crescita di mercato. Il Piano di Sviluppo del Cluster ICT Horizon@Calabria2020 prevede la costituzione di quattro aggregazioni, tra cui il Distretto Cyber Security, che si configura come un centro specializzato di competenza nel settore della sicurezza informatica, che costituisca a regime uno dei nodi specializzati nell'ambito della rete globale attiva per la protezione dalla minaccia che opera nel Cyber-spazio. Nella sua fase di avvio, il Distretto si concentrerà su tre ambiti della sicurezza informatica, individuati come rilevanti nell'analisi del contesto:

1. Protezione da alterazioni nel rilascio di servizi internet alle persone e strumenti per la rilevazione (***sicurezza delle interazioni degli end-user***);
2. Protezione da alterazioni dei processi di scambio sul sistema economico e strumenti per la rilevazione (***sicurezza dei sistemi di pagamento***);
3. Protezione da alterazioni dei processi di cooperazione nei flussi documentali e soluzioni avanzate per la riservatezza delle informazioni (***dematerializzazione sicura***).

Il Comitato Tecnico dell'Accordo di Programma tra MIUR e Regione Calabria ha inserito le linee strategiche del Custer nella relazione tecnica di accompagnamento dell'Accordo di Programma. Con Decreto Direttoriale n. 6408 del 27/03/2013, il MIUR ha approvato la Relazione Tecnica del Comitato Tecnico dell'Accordo di Programma e ha richiesto la presentazione dei progetti esecutivi relativi alle nuove iniziative afferenti al Cluster *ICT Horizon@Calabria2020*. A fronte di tale richiesta, il Distretto Cyber Security ha presentato tre progetti esecutivi, uno per ciascuno degli ambiti sopra elencati.

Obiettivi e Contenuti del Distretto

L'obiettivo del Distretto Tecnologico è quello di creare una piattaforma territoriale localizzata in Calabria, nell'Area di Cosenza, e specializzata nell'ambito specifico della **Cyber Security**, con un'ampia prospettiva di crescita tecnologica e di mercato, attraverso la creazione di una rete di attori pubblici e privati con competenze, esperienze, know how e capacità di intervenire attivamente nei mercati di sbocco finali, contribuendo così allo sviluppo e all'aumento della competitività delle imprese del Distretto e, più in generale, del sistema economico calabrese.

Il Distretto Cyber Security prevede due fasi distinte di sviluppo. La prima, triennale, di avvio del Distretto la cui governance è affidata ad una Associazione Temporanea di Scopo (ATS) degli attuali proponenti, che è dotata di una solida governance, coordinata dal soggetto mandatario, identificato in **Poste Italiane**. Successivamente, nella seconda fase di 5 anni, si procederà alla costituzione di una struttura di aggregazione più strutturata aperta ad ulteriori soggetti.

Nella fase di avvio le attività fondamentali saranno legate allo sviluppo degli interventi di ricerca e di formazione all'interno del programma PON.
Sono previsti 3 progetti di ricerca con prevalenti attività di ricerca industriale (circa il 70%) e la restante parte di sviluppo sperimentale, ciascuno con durata di circa 2 anni (fino a dicembre 2015). I tre progetti di ricerca individuati sono:

Cyber Security End-User Protection (Codice Progetto: PON03PE_00032_1)

Il progetto intende fornire una risposta scientifica e tecnologica alle necessità di sicurezza dell'end-user nella fruizione di servizi in rete, preservando la riservatezza, l'integrità e la disponibilità delle informazioni trattate, in scenari operativi che non presentano alcuna soluzione di continuità tra esperienze d'uso private e lavorative. La strategia di gestione dei rischi di sicurezza che si intende mettere in campo si basa sulla capacità di sviluppare un processo di valutazione e trattamento di minacce, vulnerabilità e conseguenti impatti, ponendosi proprio dalla prospettiva dell'end-user. I principali risultati pevisti sono:

- Modelli di specifica delle politiche di sicurezza e dei processi di interazione degli utenti finali con i servizi internet
- Strumenti e procedure innovativi di controllo della sicurezza degli accessi degli utenti finali e dei dispositivi utilizzati.

Protezione dei Sistemi di Pagamento Elettronici (Codice Progetto: PON03PE_00032_2)

Il progetto si rivolge a un mercato in fortissima espansione, quello dei sistemi digitali di pagamento, nel quale transazioni finanziarie e pagamenti sono sempre più attuati utilizzando tecnologie, dispositivi e architetture di rete evolute, tra cui Cloud computing e dispositivi mobili. In tale contesto, la Cyber Security è ormai diventata un "fattore abilitante" per i sistemi di pagamento, in quanto il controllo degli scenari di rischio assume un ruolo particolarmente critico, specie se si fa riferimento alle caratteristiche che tale rischio ha acquisito negli ultimi anni e che possono essere sintetizzate in attacchi a scopo fraudolento o mirati a impedire l'erogazione dei servizi in rete, sfruttando l'aumento delle vulnerabilità legate ai nuovi dispositivi (come smartphone), alla crescita dei servizi Cloud ed alla virtualizzazione delle infrastrutture. I principali risultati pevisti sono:

- Modelli di riferimento e di specifica per l'utilizzo più sicuro dei sistemi di pagamento, riducendo la vulnerabilità e i rischi sia dal lato degli utenti che da quello dei sistemi Web utilizzati.
- Strumenti e meccanismi innovativi di sicurezza basati su approcci di frontiera nel contesto della ricerca scientifica, come labiometria, la gestione delle credenziali anonime, le tecniche di intelligenza artificiale per il contrasto delle frodi.

Dematerializzazione Sicura (Codice Progetto: PON03PE_00032_3)

Il patrimonio informativo delle organizzazioni sta migrando in maniera decisa dai formati cartacei a quelli digitali, quali email e loro allegati, documenti semi-strutturati e non, prodotti all'interno delle organizzazioni anche attraverso processi di dematerializzazione, contenuti strutturati quali basi di dati e data warehouse, registrazioni sotto forma di log di eventi all'interno di workflow. In tal contesto, assume fondamentale importanza la definizione di un approccio strutturato per la protezione delle informazioni, applicato a tutto il ciclo di vita delle informazioni stesse, dalle fasi di creazione di un documento a quelle di gestione operativa (conservazione, utilizzo, copia, condivisione, trasformazione) e di distruzione. Tale approccio consente, attraverso chiare assegnazioni di responsabilità dei flussi documentali, di limitare i rischi correlati alla sicurezza dei documenti. I principali risultati pevisti sono:

- Modelli di riferimento e di specifica di processi per il controllo della sicurezza nelle varie fasi di vita dei documenti digitali
- Piattaforma end-to-end di gestione sicura del ciclo di vita di un documento digitale, che includa strumenti adeguati per la copertura dei singoli controlli di sicurezza.

Accanto ai tre interventi di ricerca, è prevista anche un'**azione di formazione** con l'intento di **selezionare e formare** un totale di circa **60 giovani laureati** destinati ad attività di ricerca industriale e sviluppo sperimentale. L'azione di formazione sarà articolata in tre progetti di formazione, uno per ciascuno dei progetti di ricerca.

Il Piano di Sviluppo della seconda fase della iniziativa prevede non solo il raggiungimento di un livello di autofinanziamento dell'iniziativa, ma anche una marginalità sufficiente a recuperare, per i soggetti partecipanti, il cofinanziamento erogato nella prima fase.

Soggetti Partecipanti

I nove soggetti che daranno vita al Distretto Cyber Security sono elencati di seguito in tre categorie:

- **Grandi Imprese**
  - POSTE ITALIANE SpA
  - POSTEL SpA
  - NTT DATA ITALIA SpA
  - ABRAMO PRINTING & LOGISTICS SpA
- **Piccole e Medie Imprese (PMI)**
  - Centro di Competenza ICT-SUD Scrl (che coinvolge varie PMI calabresi del settore ICT)
  - NOVA Systems Roma srl
- **Organismi di Ricerca**
  - Università della Calabria (Dipartimento di Informatica, Modellistica, Elettronica e Sistemistica - DIMES)
  - Università Mediterranea di Reggio Calabria (Dipartimento di Ingegneria dell'Informazione, delle Infrastrutture e dell'Energia Sostenibile - DIIIES)
  - CNR Dipartimento di Ingegneria, ICT e Tecnologie per l'Energia e Trasporti – DIITET (Istituto di Calcolo e Reti ad Alte Prestazioni – ICAR)

Partecipano all'iniziativa in qualità di soggetti terzi anche GCSEC, creata da Poste Italiane come Fondazione Internazionale su Cyber Security e il gruppo KPMG.

Complessivamente il partenariato è costituito da soggetti di natura pubblica e privata che intendono cooperare tra di loro per rafforzare le proprie competenze scientifiche e professionali nel settore della sicurezza informatica.

Benefici

Sono individuate quattro aree fondamentali di impatto rispetto alle quali, nel medio-lungo periodo, si prevedono rilevanti benefici per un'ampia gamma di attori, interni ed esterni al Distretto Cyber Security. Di seguito sono sintetizzati gli impatti più significativi, raggruppati in 4 aree.

1. IMPATTI SUL SISTEMA ECONOMICO DEL TERRITORIO

I benefici attesi per il territorio, connessi alla nascita del Distretto, possono essere sintetizzati in:

- Aumento della produzione locale;
- Crescita dell'occupazione;
- Incremento del livello di know-how nell'ambito ICT.

I benefici più rilevanti sono associati alla localizzazione nell'area di imprese esterne, partner dell'iniziativa, e alla loro integrazione con le aziende ICT locali, nonché alla nascita di aziende spin-off e start-up. Inoltre lo sviluppo, da parte del Distretto, di frame work applicativi, successivamente adattabili e implementabili in diversi contesti industriali e di settore, ha la potenzialità di rendere più competitivo il tessuto imprenditoriale regionale. Sono previsti benefici anche in termini di indotto generato tramite commesse e forniture a sostegno dell'ATS e dei singoli programmi di ricerca, nonché grazie alle necessità connesse al funzionamento delle strutture ed alle necessità delle risorse presenti sul territorio.

2. SVILUPPO COMPLESSIVO DEL KNOW HOW SUL TERRITORIO

La presenza del Distretto avrà ricadute anche indirette sul territorio grazie alla realizzazione di un sistema" di sapere condiviso; in particolare il sistema porterà benefici su quattro ambiti:

- Sostegno alla ricerca universitaria e all'alta formazione;
- Condivisione del know how;
- Accordi con altri distretti tecnologici;
- Internazionalizzazione.

3. IMPATTI SULLE IMPRESE PARTNER DELLE INIZIATIVE

Le Grandi Imprese potranno acquisire un vantaggio competitivo dovuto all'implementazione di una piattaforma e di un centro servizi localizzati territorialmente in Calabria, beneficiando del contesto favorevole alle nuove iniziative di sviluppo delle attività economiche e dell'occupazione, e saranno pertanto spinte a trasferire e mantenere, a livello regionale, una parte consistente delle proprie attività di ricerca.

Le PMI potranno focalizzare la propria offerta di servizi e risorse sul territorio con conseguente impatto sulle performance aziendali e possibilità di acquisire know-how specialistico sulla tematica, diventando provider di servizi e competenze, nonché potenziali fornitori di prodotti ad alto contenuto tecnologico.

4. BENEFICI SUL CLIENTE FINALE PUBBLICO E PRIVATO

Il Distretto avrà effetti molto positivi sui clienti finali sia pubblici sia privati: i benefici delle attività di ricerca e di sviluppo saranno, infatti, riadattabili e trasferibili sui servizi e prodotti diretti ai diversi segmenti e filiere di mercato e conseguentemente percepiti dai clienti finali. L'impatto di per sé presenta un vantaggio complessivo per le diverse filiere e segmenti di mercato che usufruiranno dell'innovazione connessa agli sviluppi industriali delle ricerche: è però indubbia la possibilità ed il vantaggio di avviare attività di sperimentazione, sia a livello di PA che di imprese private, nel contesto in cui è posizionato il Distretto Tecnologico, con immediato e evidente beneficio per il sistema regionale.