Piano di lavoro del
Centro di Competenza in Cybersecurity Toscano

Il Centro di Competenza in Cybersecurity Toscano (C3T) lavorerà nel campo della sicurezza informatica con l'obiettivo di informare, sensibilizzare e rispondere alle esigenze delle piccole e medie imprese, dei professionisti, degli enti pubblici, delle università, delle scuole e delle altre istituzioni formative su come conoscere, comprendere e reagire alle minacce di sicurezza informatica e su come diffondere tali conoscenze.

In collaborazione con la Regione Toscana, C3T metterà a disposizione una serie di strumenti per analizzare la domanda e l'offerta di competenze in cyber security da parte delle aziende Toscane. C3T potrà anche fornire assistenza diretta alle PMI (selezionate dalla regione o dalle associazioni di categoria o distretti) per effettuare diagnosi dello stato di protezione delle aziende ed effettuare un gap analysis individuando in maniera neutrale e imparziale (proponendosi come entità terza e senza voler sostituire le aziende private che offrono servizi di cybersecurity) le azioni necessarie per la messa in sicurezza.

Inoltre, il C3T, sempre in collaborazione con Regione Toscana, metterà a disposizione delle singole università, del sistema scolastico e delle altre istituzioni formative operanti in regione, competenze e strumenti per integrare i percorsi formativi e i programmi didattici con l'offerta di conoscenze e lo sviluppo di competenze in ambito cyber security. A tal fine il C3T potrà esser promotore di progetti formativi, da realizzare in collaborazione con gli attori della filiera dell'istruzione dalla scuola dell'obbligo sino all'università.

L'azione del C3T nell'ambito del piano condiviso con la Regione Toscana si rivolgerà anche al settore della pubblica amministrazione con particolare riferimento al sistema regionale degli enti e delle agenzie ma anche come azione di sensibilizzazione e condivisione delle soluzioni con il sistema degli enti locali.

Per quanto riguarda gli enti e le agenzie regionali che hanno già manifestato o che manifesteranno l'interesse a condividere i temi della Protezione dei dati come aspetto della Cyber security il C3T fornirà il supporto diretto attraverso la partecipazione al tavolo di coordinamento in via di costituzione

L'azione del C3T si configura pertanto come un supporto tecnico scientifico e di ricerca ad una politica regionale sulla cybersecurity nella convinzione che tale tema debba essere affrontato in una forte logica di sistema.

Le varie attività potranno essere sviluppate in maniera incrementale in base alle risorse finanziare messe a disposizione dalla Regione, dalle aziende, dagli Enti Accademici e di Ricerca e dagli altri attori pubblici che condivideranno il percorso.

1. Osservatorio toscano sulla cybersecurity

Il primo strumento di intervento sarà la costituzione di un Osservatorio toscano sulla cybersecurity che punterà ad individuare sia i livelli di vulnerabilità dei sistemi sia le caratteristiche delle minacce. I risultati dell'osservatorio saranno distribuiti attraverso diversi canali di comunicazione (blog, media, social network, …) per sensibilizzare ed informare sulle minacce individuate.

In particolare, per individuare i livelli di vulnerabilità dei sistemi:

1. Saranno sviluppati strumenti ad hoc per conoscere e permettere alle aziende toscane e alla pubblica amministrazione auto valutazioni del livello di rischio informatico.
2. Saranno censite le necessità di sicurezza informatica a livello regionale con indagini contestualizzate alla tipologie di aziende o enti (settori merceologici, PA locali, Sanità, Musei, Biblioteche e Reti documentarie).
3. Sarà definito una struttura organizzativa che permetta confronto continuo e lavoro congiunto tra i membri del C3T e gli enti, le agenzie regionali e le aziende sanitarie per effettuare analisi settoriali, definire "best practices" ed individuare "benchmark".
4. Saranno attivati incontri con le aziende toscane che si occupano di cybersecurity e che sviluppano soluzioni e offrono servizi in tale campo, al fine di contribuire a creare un ecosistema innovativo per la sicurezza informatica e sarà fornito un quadro completo delle competenze di cybersecurity nei laboratori di ricerca della Regione.
5. Sarà realizzata una mappatura dell'offerta formativa analizzando i programmi di studio e i corsi che, nelle scuole dei diversi ordini e nelle università prevedono al loro interno moduli formativi e seminari in ambito cybersecurity.

Per quanto riguarda invece l'individuazione delle minacce:

1. Si svilupperanno strumenti per il monitoraggio dell'andamento delle discussioni inerenti le problematiche di sicurezza raccogliendo dati dai social-network e dal web (incluso il deep web), utilizzando strumenti di raccolta automatica dei contenuti prodotti dagli utenti.
2. Si useranno tecnologie per l'analisi di grandi quantità di dati provenienti da diverse sorgenti per individuare vulnerabilità e predisporre contromisure.
3. Saranno pubblicati report periodici per illustrare le più importanti minacce, mettendo in evidenza potenza di attacco e potenzialità di propagazione.

Per quanto riguarda il processo di attuazione del GDPR saranno fornite indicazioni atte a migliorare le condizioni di sicurezza alla luce dell'evoluzione tecnologica, dei rischi e delle minacce nel settore IT.

2. Supporto tecnico e scientifico a PMI e PA

Il C3T, partendo dall'analisi dei fabbisogni di cybersecurity rilevati attraverso le attività dell'Osservatorio, fornirà supporto alla PA e alle PMI toscane per l'identificazione di vulnerabilità ICT e possibili minacce, e la valutazione e il potenziamento delle capacità di difesa. I risultati dell'Osservatorio permetteranno anche di definire opportuni piani di formazione a supporto delle PMI e per la riqualificazione dei lavoratori. Analogamente i risultati dell'Osservatorio permetteranno di definire nuove proposte di corsi di formazione di livello terziario (cicli di seminari, moduli formativi e insegnamenti anche con il riconoscimento di CFU, master, dottorati, ecc.), nonché corsi e seminari, corredati di appositi contenuti multimediali orientati agli studenti e ai docenti delle scuole secondarie superiori. In particolare, il centro si farà promotore di azioni di divulgazione e promozione degli strumenti sviluppati dal Laboratorio Nazionale di Cybersecurity del CINI nel corso degli ultimi anni quali:

1. *Framework Nazionale per la Cybersecurity* (FNCS), pubblicato nel 2016 in collaborazione con diversi attori industriali e governativi, adatto ad aziende ed organizzazioni che abbiano già una qualche preparazione in termini di sicurezza;
2. *I Controlli Essenziali di Cybersecurity* (CECS), pubblicati nel 2017, i quali pongono l'attenzione su livelli di necessità o criticità, rispetto delle normative vigenti e gestione delle

responsabilità, uso di soluzioni tecniche adeguate per la protezione dei dati, formazione e gestione del personale addetto, gestione degli incidenti e relativo ripristino.

Tali strumenti saranno anche integrati con quanto indicato dalle circolari AGID relativamente alle misure minime di sicurezza informatica.

Relativamente a questi aspetti si prevedono due tipologie di attività di supporto ed informazione per le aziende e per i cittadini:

Contestualizzazioni FNCS - Il C3T si occuperà di adattare il FNCS ai diversi contesti eterogenei presenti nel panorama regionale tramite la creazione di apposite contestualizzazioni. Infatti a seconda di un insieme di fattori (quali settore merceologico, tipo di servizi o prodotti, dimensione, esposizione al rischio, etc.), le pratiche di sicurezza da mettere in atto e i processi necessari possono essere anche molto diversi tra loro. Oltre a innalzare il livello di sicurezza generale del tessuto imprenditoriale e della PA toscana, ciò consentirà una coerenza cross-settoriale nella gestione del rischio e un linguaggio cyber comune condiviso tra privato e pubblico, nonché tra privato e privato, che agevolerà la cooperazione e la condivisione dei requisiti.

Divulgazione CECS - Il C3T promuoverà l'adozione dei CECS per PA e PMI e la divulgazione di circolari AGID sulle misure di sicurezza informatica. Essi sono fondamentali per una diffusione capillare della cultura della cybersecurity nella realtà imprenditoriale regionale e per produrre una generale diminuzione dell'esposizione al rischio di attacchi cyber. I CECS rappresentano infatti uno strumento attraverso cui definire un livello minimo di protezione da attacchi cibernetici e la loro adozione può rappresentare per le PMI un importante banco di prova, propedeutico ad una successiva fase di certificazione.

3. Supporto tecnico e scientifico per GDPR

Il *General Data Protection Regulation* (GDPR), Regolamento Ue 2016/679 relativo al trattamento e alla libera circolazione dei dati personali, da una parte garantisce protezione ai cittadini dall'altra pone sfide non banali alle aziende ed alle pubbliche amministrazioni. Spesso, l'interezza e la complessità delle regole disposte dal GDPR non sono di facile comprensione per persone operanti in contesti diversi dall'ICT. È pertanto necessario fornire alle PMI e alle PA informazioni e strumenti utili per adeguare il loro business al GDPR, per renderli autonomi nelle decisioni e salvaguardarli da sanzioni economiche che possono arrivare al 4% del fatturato annuo aziendale. Analogamente necessario prevedere che, specie a livello universitario, le discipline e gli insegnamenti che nei propri ambiti applicativi prevedono la raccolta, l'utilizzo e l'analisi di dati personali, siano integrati da specifici moduli formativi come anche le discipline.

La conformità al GDPR interessa varie entità, da quelle direttamente coinvolte nelle attività di trattamento dei dati (proprietario, responsabile del trattamento e incaricato al trattamento) a quelle il cui interesse principale riguarda l'attuazione del regolamento (organismi di certificazione, enti di controllo o gruppi di imprese). Il C3T contribuirà allo sviluppo di strumenti per verificare la conformità delle aziende al GDPR e fornirà il supporto informativo e informatico necessario ad assicurare la corretta interpretazione e implementazione del GDPR, che sia adattabile ai vari contesti in modo da garantire una efficiente e sicura gestione e trasferimento dei dati. In particolare si forniranno metodologie e strumenti (semi) automatici per il controllo della conformità al GDPR adattabili ed estendibili alle varie realtà delle PMI e PA e di pratiche per garantire la tutela della privacy. Il C3T contribuirà inoltre alla realizzazione di seminari e azioni di diffusione sulla nuova normativa introdotta dal DPGR nonché alla progettazione di corsi di alta formazione sul tema

specifico da affiancare all'attuale offerta formativa universitaria. Obiettivo del progetto sarà anche quello di accrescere la fiducia, nel contesto sia pubblico sia privato, nel diritto alla privacy e, per estensione, di promuovere nuove opportunità di mercato. In particolare il progetto punterà a:

1. Creare un modello di business specifico per la tipologia di PMI o PA in esame, focalizzato sugli aspetti relativi a gestione, tracciamento e trasferimento dei dati.
2. Valutare i rischi derivanti dalla manipolazione e trasmissione dei dati, sia all'interno dell'entità presa in esame, sia tra differenti organizzazioni distribuite sul territorio (filiere di distribuzione).
3. Sviluppare e/o utilizzare strumenti (semi) automatici per la verifica e validazione di criticità presenti nell'infrastruttura di rete ed applicativa che possano compromettere sia la sicurezza sia l'integrità dei dati.
4. Facilitare la creazione e la gestione di modulistica e documentazione necessarie per il soddisfacimento degli aspetti burocratici relativi al GDPR
5. Partecipare al coordinamento regionale in materia di GDPR fornendo specifiche azioni di supporto.

4. Servizi di certificazione e monitoraggio

La certificazione del software è uno dei meccanismi fondamentali per la costruzione di una infrastruttura digitale affidabile. Il C3T interverrà su questo problema in due fasi, in una prima fase fornirà informazioni sulla tipologia di certificazioni di cybersecurity disponibili ed in una seconda lavorerà a strumenti di monitoraggio dei servizi esposti in rete e alla messa a punto di strumenti automatici o semi-automatici di supporto alla certificazione. Potranno essere messi a fattor comune l'esperienza, e le infrastrutture di cui Regione Toscana si è dotata per i processi di Continuous Integration e controllo di qualità del codice sorgente. Nel breve-medio periodo si punterà a sviluppare le seguenti iniziative.

Portale informativo di servizi di certificazione - Per garantire correttezza ed efficacia, i processi di certificazione sono in costante revisione. Pertanto un portale informativo sui servizi di certificazione attualmente disponibili che offra una informazione chiara e accessibile sulle tipologie di certificazioni può rappresentare un importante contributo alle aziende. Va inoltre precisato che la certificazione deve adattarsi al contesto applicativo differenziando tra processi di certificazione per il mercato consumer e il mercato legato alla sicurezza nazionale. Un altro fattore per aumentare la chiarezza dei processi di certificazione riguarda la coesistenza di più enti e normative. In particolare, le normative europee e nazionali possono generare conflitti e ambiguità che il portale informativo potrebbe aiutare a superare.

Monitoraggio continuo dei servizi esposti in rete - I portali e le applicazioni web della PA e delle aziende sono sottoposti ad aggiornamenti continui che possono invalidare le certificazioni in essere. Un processo di monitoraggio potrebbe superare questo limite estendendo nel tempo la validità delle certificazioni anche utilizzando strumenti automatici o semi-automatici. Tali strumenti potranno evidenziare difetti e vulnerabilità che richiedono iniziative di correzione. In alcuni casi, essi possono addirittura certificare l'assenza di alcune tipologie di minacce. Una delle tecniche più comuni per la ricerca di difetti nella sicurezza sono le metodologie di Vulnerability Assessment and Penetration Testing che si basano su batterie di controlli definite da enti indipendenti ed eseguite da personale esperto. L'automazione di questi controlli può evitare errori umani e velocizzare i processi di verifica e correzione. Anche in questo caso potranno essere messe a fattor comune l'esperienza e le infrastrutture di Regione Toscana utili all'esecuzione di processi VAI (Vulnerability Assessment Infrastrutturali) e VAA (Vulnerability Assessment Applicativi). Per gli aspetti di certificazione e

monitoraggio, nell'ambito del coordinamento regionale saranno identificate specifiche azioni atte a fornire adeguato supporto ai soggetti pubblici che ne fanno parte definendo uno specifico piano di lavoro condiviso anche con l'obiettivo della valutazione e progettazione di soluzioni tecnologiche e organizzative come presidio stabile attraverso Security Operation Center (SOC) per affrontare le problematiche di cybersecurity del sistema regionale.

5. Progetti di ricerca e trasferimento tecnologico

L'attività relativa ai progetti di ricerca e trasferimento per bandi regionali, nazionali e della Commissione europea sarà un'attività chiave del C3T che si articolerà in due punti, che riguarderanno il supporto alla Regione Toscana nella definizione dei programmi di finanziamento per i bandi regionali e la predisposizione di progetti di ricerca e trasferimento tecnologico.

Supporto alla RT nella definizione dei programmi di finanziamento - Il C3T, partendo dall'analisi dei fabbisogni di cybersecurity delle Pubbliche Amministrazioni e delle PMI Toscane (rilevati attraverso le attività dell'Osservatorio), e tenendo conto del Piano Nazionale della Ricerca e della programmazione europea, fornirà (se richiesto) supporto alla Regione Toscana nella identificazione delle tematiche di cybersecurity da inserire nei bandi regionali. Questo potrà riguardare sia la definizione di bandi regionali focalizzati sulla cybersecurity per innalzare il livello di resilienza delle PMI e della Pubblica Amministrazione agli attacchi cyber, sia l'inserimento delle tematiche di cybersecurity all'interno di bandi regionali relativi alle varie aree di *smart specialization* della Regione Toscana, per garantire che la cybersecurity sia uno dei vincoli nella progettazione e sviluppo di tutti i sistemi che presentano una dimensione cyber. Il C3T potrà inoltre supportare la Regione Toscana nella definizione di bandi regionali per corsi di alta formazione, per percorsi di alternanza fra ricerca e lavoro, e per attività di formazione tramite la ricerca, focalizzati sulle tematiche della cybersecurity.

Predisposizione di progetti di ricerca e trasferimento tecnologico - La predisposizione di progetti di ricerca e trasferimento tecnologico, in risposta ai bandi regionali, nazionali e della Commissione Europea, costituirà uno dei principali canali di autofinanziamento delle attività del centro C3T. Nella predisposizione dei progetti il centro cercherà di promuovere la partecipazione delle PMI e, se previsto dal bando, delle pubbliche amministrazioni toscane. Inoltre, il centro organizzerà dei workshop con le aziende toscane per la presentazione dei bandi regionali, nazionali e della Commissione Europea con l'obiettivo di favorire la costituzione di partenariati centrati sulle aziende, università e centri di ricerca toscani per presentare dei progetti di ricerca e/o di trasferimento tecnologico in risposta a tali bandi. Infine, il centro rappresenterà un punto di riferimento per le PMI toscane interessate a trovare interlocutori nel mondo della ricerca per presentare dei progetti di ricerca e trasferimento tecnologico che richiedano competenze nel settore della cybersecurity.

6. Percorsi di formazione ed educazione

Il C3T collaborerà con la Regione Toscana nella predisposizione di programmi di formazione ed educazione in materia di cybersecurity che potranno articolarsi sui seguenti punti.

Educazione di base - Realizzazione di presentazioni standard e definizione di un programma di incontri, con studenti e/o docenti, a partire almeno dalle scuole medie di secondo grado, indipendentemente dall'indirizzo specifico del percorso scolastico, con l'obiettivo di fornire i concetti fondamentali della cybersecurity e porre le basi per una migliore comprensione della tematica. Nell'ambito di queste iniziative, anche per garantire una maggiore capillarità della diffusione, saranno

realizzati corsi e materiali multimediali da mettere a disposizione di docenti e studenti. Queste attività potrebbero essere svolte anche in collaborazione con la Polizia Postale.

Formazione continua - Definizione e realizzazione di percorsi di formazione continua, anche ad hoc, per le professioni che sempre più dovranno confrontarsi con problematiche di cybersecurity e consolidare, migliorare e valutare le capacità operative nel contrasto e nella gestione degli incidenti informatici all'interno delle organizzazioni. Particolare attenzione sarà posta alla formazione dei dirigenti sia delle imprese sia della Pubblica Amministrazione. Per facilitare la partecipazione del personale dipendente, la modalità di erogazione potrà essere sia convenzionale sia remota. Inoltre, ciascun percorso formativo si articolerà su un numero limitato di moduli. La Regione pubblicizzerà le iniziative presso le PA del territorio e associazioni di categoria. Il C3T organizzerà eventi per divulgare e fornire conoscenza e soluzioni ai principali attori coinvolti nel mondo della cyber-security, anche focalizzandosi su tematiche specifiche.

Sensibilizzazione - Promozione di iniziative di sensibilizzazione dei cittadini ai molteplici rischi connessi alla rivoluzione digitale, dalle intrusioni nei computer alla dipendenza digitale, dal furto di dati ai riscatti, dal sabotaggio alle truffe, dalla circolazione di notizie e contenuti multimediali (immagini e video) falsi, all'incitamento all'odio on-line. L'obiettivo è colmare un settore, quello dei singoli cittadini, ancora privo di strumenti dal punto di vista della gestione del rischio cyber. Il centro effettuerà azioni di divulgazione finalizzate a fornire ai cittadini le nozioni elementari di cybersecurity e le regole di base della igiene-cyber.

Consapevolezza dei cittadini - Definizione e realizzazione di "pillole di cybersecurity" (ad esempio brevi filmati, brochure, messaggi audio) finalizzate a fornire ai cittadini le nozioni elementari di cybersecurity ed i concetti base di quella che viene ormai comunemente chiamata igiene-cyber, anche utilizzando spazi su TV, radio e quotidiani locali.

7. Alta Formazione

A livello mondiale è previsto uno skill shortage di tre milioni e mezzo di esperti di cyber security entro il 202. In Italia la carenza di professionisti nell'area della cybersecurity è esacerbata dalla fuga di giovani, formati nelle nostre università, ma attratti all'estero da stipendi più appetibili. Per compensare questa tendenza riteniamo siano necessari iniziative che coinvolgano Università, Ricerca, Pubblica Amministrazione e mondo produttivo incrementando il numero di corsi di laurea, master universitari e programmi di dottorato in cybersecurity nei vari atenei. A tal fine il C3T potrà supportare le singole università Toscane nella progettazione di corsi di alta formazione sui temi della cyber security (cicli di seminari, moduli formativi e insegnamenti, anche con il riconoscimento di CFU ecc.) da realizzare, anche con il contributo regionale, e da affiancare alla offerta formativa degli attuali percorsi di laurea.

Master - Si definiranno, insieme alla Regione ed alle organizzazioni industriali, nuovi curricula per master universitari di I e II livello in cybersecurity finalizzati a fornire gli strumenti tecnici e metodologici fondamentali della cybersecurity. Questi programmi saranno destinati a giovani laureati ma anche a professionisti, sia della Pubblica Amministrazione sia del mondo delle imprese. In considerazione dello "skill shortage" menzionato sopra è necessario attivare master in tutte le università toscane, ma al momento è attivo in Toscana solo un master di I livello tenuto presso l'Università di Pisa in collaborazione col CNR. La Regione parteciperà all'organizzazione e supporto dei Master attraverso la partecipazione programmate di personale proprio, delle agenzie ed enti regionali e delle aziende sanitarie ed eventualmente contribuendo ai costi di partecipazione degli allievi provenienti da aziende o da pubbliche amministrazioni locali e, eventualmente, mettendo a

disposizione appositi voucher per la copertura delle spese di iscrizione per gli studenti meritevoli e/o privi di mezzi.

Dottorato - Per limitare il problema derivante dallo skill shortage è fondamentale formare ricercatori e formatori. Riteniamo pertanto importante iniziare dalla cima della piramide e formare dottori di ricerca in cybersecurity. Una prima iniziativa sarà la messa a punto di un programma di formazione a livello dottorale realizzato in rete dalle singole università toscane e dal CNR. Tale programma formativo, definito anche a seguito di confronti con le imprese del territorio, potrà trovare supporto nelle misure annualmente attivate dalla Regione. Nello specifico, il programma potrà essere finanziato attraverso borse assegnate nell'ambito delle proposte di corsi di dottorato presentate, sui bandi FSE per il finanziamento delle Borse di dottorato Pegaso, su tematiche affini alla cyber security o su applicazioni della cyber security a specifici contesti produttivi e/o organizzativi. In tali proposte potranno essere inserite borse a tematica vincolata per le quali i dottorandi che svilupperanno tesi collegate ad ambiti applicativi della cyber security potranno seguire specifici corsi presso il C3T. Presso il centro C3T potranno anche essere organizzati corsi specialistici tenuti anche da "distinguished researchers" invitati con il supporto finanziario della Regione, e che permetteranno agli studenti iscritti ai corsi di dottorato, e più in generale, ai corsi di laurea e post laurea degli atenei toscani, di venire in contatto con eccellenze internazionali della cybersecurity.

8. Formazione (inter-) attiva

Altre iniziative concrete da attivare in collaborazione con la Regione Toscana nel breve termine sono l'organizzazione di gare di cosiddetto "Capture the Flag" e la creazione di una rete di "Cyber Range".

Capture the Flag - Per far conoscere le problematiche di cybersecurity e per incoraggiare, attraverso contesti ludico-formativi, i giovani toscani ad intraprendere studi universitari in un settore che offre sfide notevoli assieme a numerose possibilità di lavoro, si organizzeranno gare di cybersecurity in stile "capture the flag" mirate a scoprire e valorizzare il talento "cyber" dei giovani toscani. Si punterà anche a formare una rappresentativa Toscana per la partecipazione al progetto CyberChallenge.IT, organizzato dal Laboratorio Nazionale di Cybersecurity del CINI che già quest'anno vede coinvolte 8 università italiane, ma nessuna della nostra regione.

Cyber Range - Si progetterà e si attiverà una rete di cosiddetti "Cyber Range" (poligoni virtuali dedicati all'addestramento dei professionisti del settore, costituiti da ambienti e sistemi controllati). Tale rete, condivisa tra Università, Ricerca, Pubblica Amministrazione e mondo produttivo, permetterà all'accademia di potenziare i programmi formativi sulla cybersecurity con sessioni pratiche tramite le quali gli studenti potranno acquisire competenze spendibili nel mondo lavorativo; al mondo della ricerca di sperimentare e valutare l'efficacia di tecniche innovative in un ambiente controllato; alla PA di addestrare il personale preposto alla difesa cyber; alle aziende di valutare sperimentalmente l'efficacia degli strumenti di difesa che si prevede di acquisire. La Regione Toscana parteciperà alla definizione, alla costruzione ed all'utilizzo dei cyber range con proprio personale, con personale degli enti e agenzie regionali e con quelli delle aziende sanitarie.

9. Sito web informativo

C3T gestirà in collaborazione con la Regione Toscana un sito web dove saranno sistematicamente riportate informazioni aggiornate su attacchi, nuovi strumenti di difesa, aziende toscane che offrono servizi legati alla cybersecurity ed il know how dei componenti del C3T che potrà servire per

collaborazioni, per partecipazioni a bandi regionali, nazionali o europei, per consulenze individuali . L'indirizzo web è www.c3t.

10. Governance

Organi di governo del C3T sono l'organo di indirizzo e il comitato tecnico-scientifico.

L'organo di indirizzo è formato da un rappresentante per ogni Università/Ente di ricerca che ha aderito al centro ed elegge al proprio interno il Direttore con il compito di rappresentare il centro verso la Regione Toscana e verso i possibili committenti. L'organo ha il compito di:

- mantenere i rapporti con la Regione Toscana;
- definire le regole per la partecipazione ad iniziative e progetti;
- approvare i piano costi delle attività e dei progetti e stabilire quale soggetto gestisce i relativi budget.

Il comitato tecnico-scientifico è formato da un rappresentante per ogni dipartimento universitario, istituto di ricerca che ha aderito al centro all'iniziativa ed ha il compito di definire progetti con relativi costi e coordinare le attività assegnate al centro. Il Direttore del Centro partecipa al Comitato tecnico-scientifico, in rappresentanza del proprio dipartimento universitario/istituto di ricerca, e ne è il coordinatore.

Per ogni progetto proposto al Centro (osservatorio, formazione, divulgazione, sensibilizzazione, sviluppo, consulenza, ricerca, …), l'organo di indirizzo, sentito il comitato tecnico-scientifico, nomina un responsabile e un suo vice che hanno la responsabilità della realizzazione del progetto stesso.

In una fase iniziale il C3T non si costituirà come soggetto giuridico. In occasione di ciascun progetto specifico, da svolgere con o per la Regione Toscana verranno individuati i Dipartimenti Universitari, le Scuole o gli Istituti partecipanti, e verrà stipulata un accordo di collaborazione e/o una convenzione tra questi e le Direzioni Regionali interessate ed eventuali altre parti.